

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Gregory G. Raleigh Attorney Docket No.:39843-0184IP1
U.S. Patent No.: 11,096,055
Issue Date: August 17, 2021
Appl. Serial No.: 16/421,121
Filing Date: May 23, 2019
Title: AUTOMATED DEVICE PROVISIONING AND ACTIVATION

DECLARATION OF DR. PATRICK TRAYNOR

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

Date: 24 February 2025

By: 
Patrick Traynor, Ph.D.

Table of Contents

I.	QUALIFICATIONS AND BACKGROUND INFORMATION.....	4
II.	LEGAL PRINCIPLES.....	9
	A. Anticipation.....	9
	B. Obviousness	10
III.	OVERVIEW OF CONCLUSIONS FORMED	12
IV.	BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE '055 PATENT	13
V.	INTERPRETATIONS OF THE '055 PATENT CLAIMS AT ISSUE.....	14
VI.	THE '055 PATENT.....	14
	A. Overview of the '055 Patent	14
	B. Prosecution History of the '055 Patent.....	15
VII.	OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES ..	16
	A. Jheng	16
	B. Chiu	17
	C. Rao	18
	D. Collins.....	20
	E. Camilleri	21
	F. Bajko	22
	G. Liu	23
	H. Brown.....	24
VIII.	MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '055 CLAIMS UNPATENTABLE	25
IX.	GROUND 1A/2A: CLAIMS 1-2, 6-7, 9-10 AND 12 ARE OBVIOUS OVER JHENG IN VIEW OF CHIU (WITH OR WITHOUT RAO).....	26
	A. The combination of Jheng and Chiu.....	26
	B. The combination of Jheng, Chiu, and Rao	32
	C. Analysis.....	37
X.	GROUND 1B/2B: CLAIMS 3-4 ARE OBVIOUS OVER JHENG IN VIEW OF CHIU AND COLLINS (WITH OR WITHOUT RAO).....	83
	A. The combination of Jheng, Chiu, and Collins (with or without Rao)	83
	B. Analysis.....	87
XI.	GROUND 1C/2C: CLAIM 5 IS OBVIOUS OVER JHENG IN VIEW OF CHIU AND CAMILLERI (WITH OR WITHOUT RAO).....	92
	A. The combination of Jheng, Chiu, and Camilleri (with or without Rao).	92

B. Analysis.....	95
XII. GROUND 1D/2D: CLAIM 8 IS OBVIOUS JHENG IN VIEW OF CHIU AND BAJKO (WITH OR WITHOUT RAO).....	97
A. The combination of Jheng, Chiu, and Bajko (with or without Rao)	97
B. Analysis.....	100
XIII. GROUND 1E/2E: CLAIM 11 IS OBVIOUS OVER JHENG IN VIEW OF CHIU AND LIU (WITH OR WITHOUT RAO)	102
A. The combination of Jheng, Chiu, and Liu (with or without Rao)	102
B. Analysis.....	105
XIV. GROUND 1F/2F: CLAIM 13 IS OBVIOUS OVER JHENG IN VIEW OF CHIU AND BROWN (WITH OR WITHOUT RAO).....	107
A. The combination of Jheng, Chiu, and Brown (with or without Rao)...	107
B. Analysis.....	110
XV. CONCLUSION.....	111

DECLARATION OF DR. PATRICK TRAYNOR

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

I. QUALIFICATIONS AND BACKGROUND INFORMATION

1. My name is Patrick Gerard Traynor and I have been retained as an expert witness by Samsung in the matter of Samsung Electronics Co., Ltd. (“Samsung”) vs. Headwater Research, LLC. My qualifications for forming these conclusions are summarized below.

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

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

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

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

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

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

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

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

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

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

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

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

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

13. I am a named inventor on ten US patents. These patents detail methods for determining the origin and path taken by phone calls as they traverse various networks, cryptographically authenticating phone calls, providing a secure means of indoor localization using mobile/wireless devices, detecting credit card skimmers, identifying cloned credit cards, and blocking ransomware from encrypting data.

14. My curriculum vitae, included with this declaration as SAMSUNG-1003, includes a list of publications on which I am a named author. It contains further details regarding my experience, education, publications, and other qualifications to render an expert opinion in connection with this proceeding.

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

- U.S. Patent No. 11,096,055 (SAMSUNG-1001), and its accompanying prosecution history (SAMSUNG-1002)
- U.S. Patent Publication No. 2009/0239584 (“Jheng”) (SAMSUNG-1005)
- PCT Patent Publication No. WO2004/031488 (“Chiu”) (SAMSUNG-1006)
- U.S. Patent Publication No. 2006/0039354 (“Rao”) (SAMSUNG-1007)
- U.S. Patent Publication No. 2006/0206941 (“Collins”) (SAMSUNG-1008)
- U.S. Patent Publication No. 2009/0149220 (“Camilleri”) (SAMSUNG-1009)
- U.S. Patent Publication No. 2004/0196796 (“Bajko”) (SAMSUNG-1010)
- U.S. Patent Publication No. 2005/0107066 (“Erskine”) (SAMSUNG-1011)
- U.S. Patent Publication No. 2005/0164737 (“Brown”) (SAMSUNG-1012)
- European Patent Publication No. 1 484 871 A1 (“Kelz”) (SAMSUNG-1013)
- 3rd Generation Partnership Project; Technical Specification Group
Terminals; Characteristics of the USIM application (Release 7) (“3GPP TS
31.102”) (SAMSUNG-1014)
- Digital cellular telecommunications system (Phase 2+); Specification of the
Subscriber Identity Module-Mobile Equipment (SIM - ME) interface (“GSM
11.11”) (SAMSUNG-1015)
- U.S. Patent Publication No. 2008/0080458 (“Cole”) (SAMSUNG-1016)
- U.S. Patent Publication No. 2007/0184858 (“Landschaft”) (SAMSUNG-
1017)

- 3GPP2 S.R0048-A Version 4.0, 3G Mobile Equipment Identifier (MEID) Stage 1 (“3GPP2 S.R0048-A”) (SAMSUNG-1018)
- IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture (“IEEE 802-2001”) (SAMSUNG-1019)
- *Security Engineering*, Second Edition (“Anderson”) (SAMSUNG-1020)
- *Developing a new Protection Profile for (U)SIM UICC platforms*, (“Wary”) (SAMSUNG-1021)
- *Mobile Virtual Network Operators*, Teletronikk Volume 97 No. 4 – 2001 (“Thanh”) (SAMSUNG-1022)
- *The Symbian OS Architecture Sourcebook* (“Morris”) (SAMSUNG-1023)
- U.S. Patent Publication No. 2010/0273450 A1 (“Papineau”) (SAMSUNG-1024)
- U.S. Patent No. 7,929,993 B2 (“Nagarajan”) (SAMSUNG-1028)
- *Learning XML*, Erik. T Ray (“Ray”), published January 2001 (SAMSUNG-1029)
- U.S. Patent Publication No. 2008/0020755 (“Liu”) (SAMSUNG-1030)

II. LEGAL PRINCIPLES

A. Anticipation

16. I have been informed that a patent claim is invalid as anticipated under 35 U.S.C. § 102 if each and every element of a claim, as properly construed, is found

either explicitly or inherently in a single prior art reference. Under the principles of inherency, if the prior art necessarily functions in accordance with, or includes the claimed limitations, it anticipates.

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

B. Obviousness

18. I have been informed that a patent claim is invalid as "obvious" under 35 U.S.C. § 103 in light of one or more prior art references if it would have been obvious to a POSITA, taking into account (1) the scope and content of the prior art, (2) the differences between the prior art and the claims, (3) the level of ordinary skill in the art, and (4) any so called "secondary considerations" of non-obviousness, which include: (i) "long felt need" for the claimed invention, (ii) commercial success

attributable to the claimed invention, (iii) unexpected results of the claimed invention, and (iv) “copying” of the claimed invention by others. For purposes of my analysis, I have applied a date of January 28, 2009 as the date of invention in my obviousness analyses, although in many cases the same analysis would hold true even at an earlier time than January 28, 2009. I understand the priority date of the '918 Patent is in dispute.

19. I have been informed that a claim can be obvious in light of a single prior art reference or multiple prior art references. To be obvious in light of a single prior art reference or multiple prior art references, there must be a reason to modify the single prior art reference, or combine two or more references, in order to achieve the claimed invention. This reason may come from a teaching, suggestion, or motivation to combine, or may come from the reference or references themselves, the knowledge or “common sense” of one skilled in the art, or from the nature of the problem to be solved, and may be explicit or implicit from the prior art as a whole. I have been informed that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. I also understand it is improper to rely on hindsight in making the obviousness determination.

III. OVERVIEW OF CONCLUSIONS FORMED

20. This expert Declaration explains the conclusions that I have formed based on my analysis. To summarize those conclusions:

- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 1-2, 6-7, 9-10, and 12 of the '055 Patent are obvious over Jheng in view of Chiu (with or without Rao) (Grounds 1A/2A)
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 3-4 of the '055 Patent are obvious over Jheng in view of Chiu and Collins (with or without Rao) (Grounds 1B/2B).
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claim 5 of the '055 Patent is obvious over Jheng in view of Chiu and Camilleri (with or without Rao) (Grounds 1C/2C).
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claim 8 of the '055 Patent is obvious over Jheng in view of Chiu and Bajko (with or without Rao) (Grounds 1D/2D).

- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claim 11 of the '055 Patent is obvious over Jheng in view of Chiu and Liu (with or without Rao) (Grounds 1E/2E).
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claim 13 of the '055 Patent is obvious over Jheng in view of Chiu and Brown (with or without Rao) (Grounds 1F/2F).

IV. BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE '055 PATENT

21. A person of ordinary skill in the art (“POSITA”) relating to the subject matter of the '055 Patent as of January 28, 2009 would have had (1) at least a bachelor’s degree in computer science, computer engineering, electrical engineering, or a related field, and (2) at least two years of industry experience in wireless communication network applications and software. Additional graduate education could substitute for professional experience, and *vice versa*.

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

V. INTERPRETATIONS OF THE '055 PATENT CLAIMS AT ISSUE

23. I have been informed by Counsel and understand that the best indicator of claim meaning is its usage in the context of the patent specification as understood by one of ordinary skill. I further understand that the words of the claims should be given their plain meaning unless that meaning is inconsistent with the patent specification or the patent's history of examination before the Patent Office. Counsel has also informed me, and I understand that, the words of the claims should be interpreted as they would have been interpreted by one of ordinary skill at the time of the invention was made (not today). I have been informed by Counsel that I should use January 28, 2009 as the point in time for claim interpretation purposes.

VI. THE '055 PATENT

A. Overview of the '055 Patent

24. The '055 Patent is directed to “a services policy communication system and method.” SAMSUNG-1001, Abstract. The communication system includes (see FIG. 29 (reproduced below)): service profiles including “a set of one or more service policy settings for the device for a service on the network” (SAMSUNG-1001, 8:44-67); a connection manager (annotated in green below) that “provides a control and supervision function for one or more modem drivers or modems that connect to an access network” (SAMSUNG-1001, 82:54-59); and a policy control agent (annotated in red below) that “performs a policy control function to adapt instantaneous service policies to achieve a service usage objective.” SAMSUNG-

1001, 48:47-49:13. The policy control agent and connection manager are illustrated in FIG. 29 (reproduced below) of the '055 patent. SAMSUNG-1001, FIG. 29.

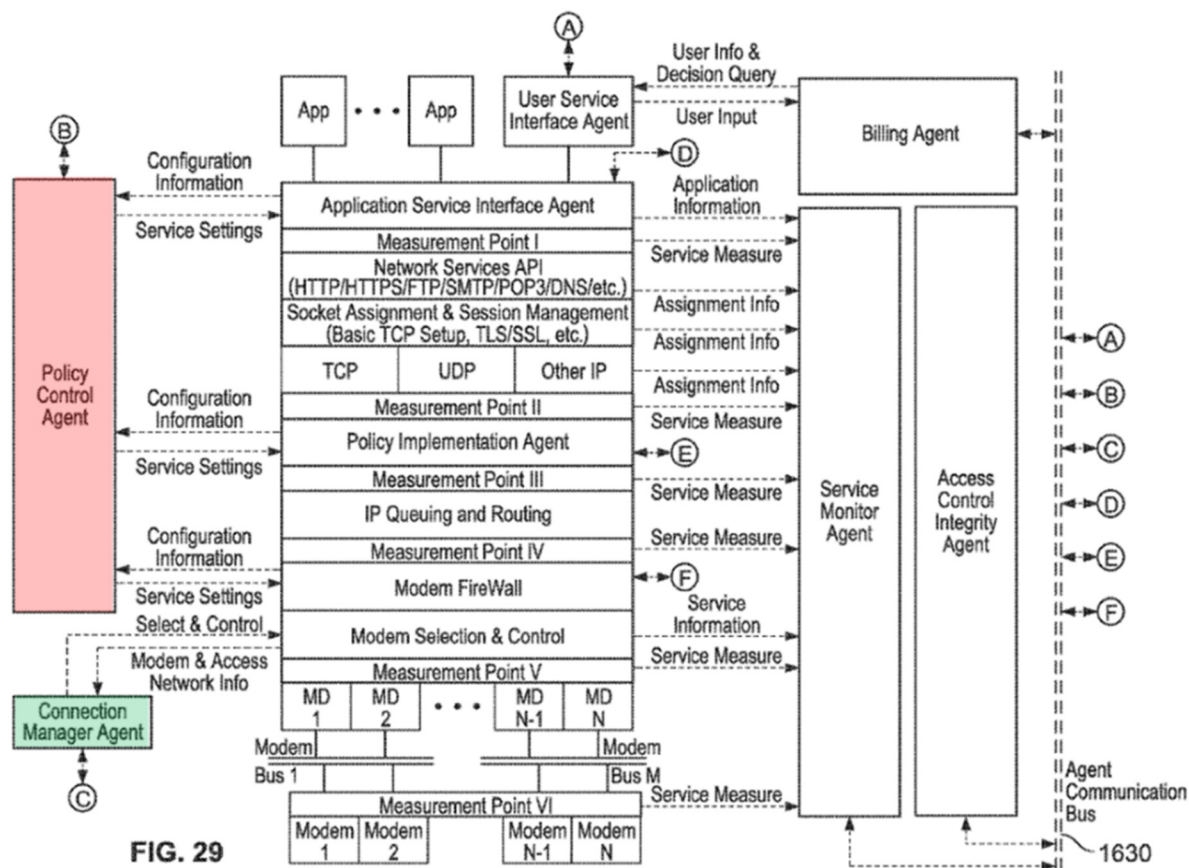


FIG. 29

SAMSUNG-1001, FIG. 29¹.

B. Prosecution History of the '055 Patent

25. The '055 Patent was allowed on its first action without any prior art rejections. SAMSUNG-1002, 18-21. In the notice of allowability, the Examiner did not indicate a particular limitation or feature as the reason for allowance.

¹ Annotations to figures are shown in color.

VII. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES

A. Jheng

26. Jheng discloses a “mobile station” (e.g., a “mobile phone”) that includes “dual Subscriber identity cards” (“SIM” or universal SIM (“USIM”) cards) that can “simultaneously access two core networks.” SAMSUNG-1005, ¶¶[0006], [0033]. Referring to Jheng’s FIGS. 1 and 2B, a user can “make a voice call with the subscriber identity card A to the called party 120 through the cell 140A” and also “make a voice call with the subscriber identity card B to the called party 120 through the cell 140B.” *Id.* This capability enables a user to reduce roaming charges, as a user can “issue an MO [(mobile-originated)] request to a cell that a Subscriber identity card camps on without roaming.” SAMSUNG-1005, ¶¶[0050]-[0052].

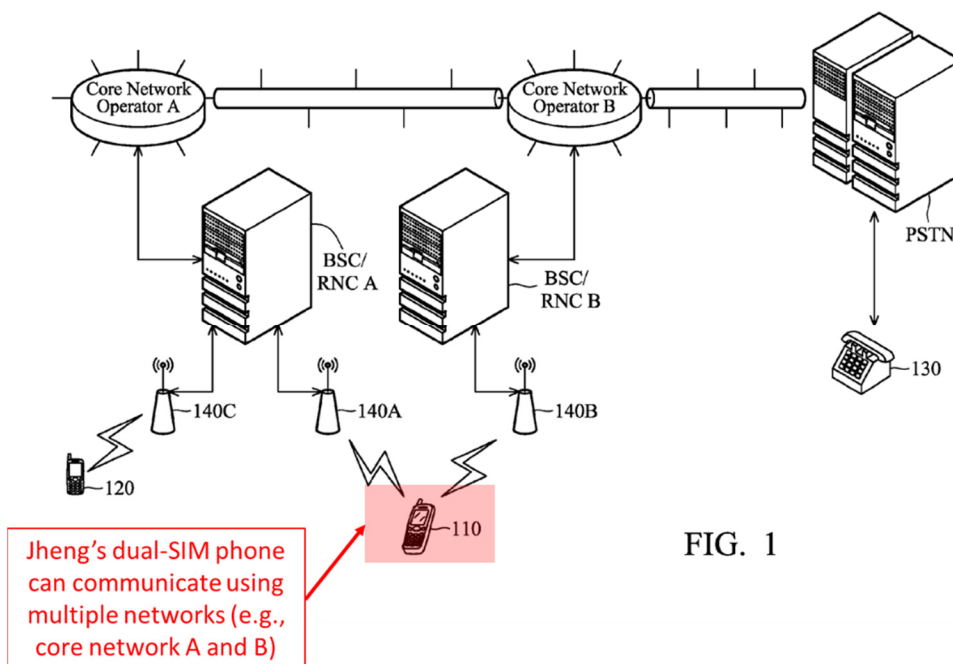


FIG. 1

SAMSUNG-1005, FIG. 1.

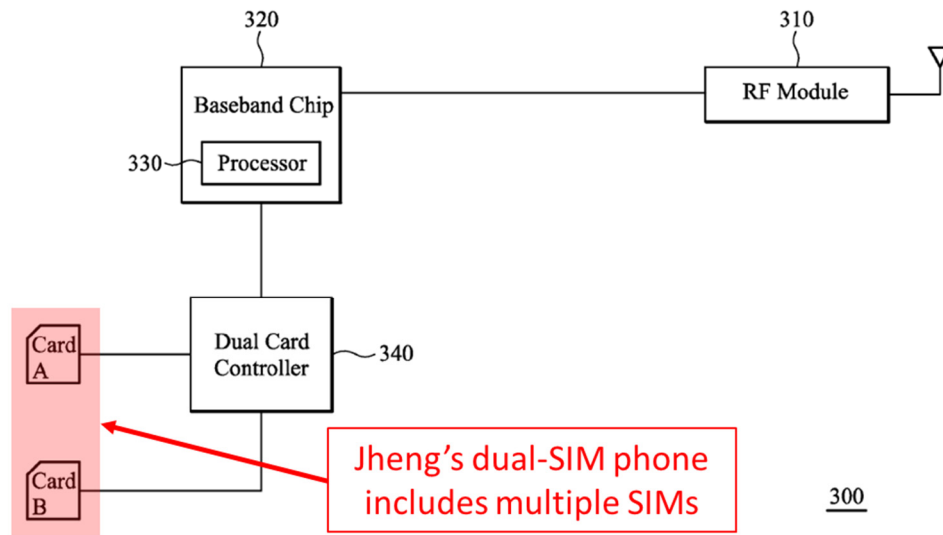
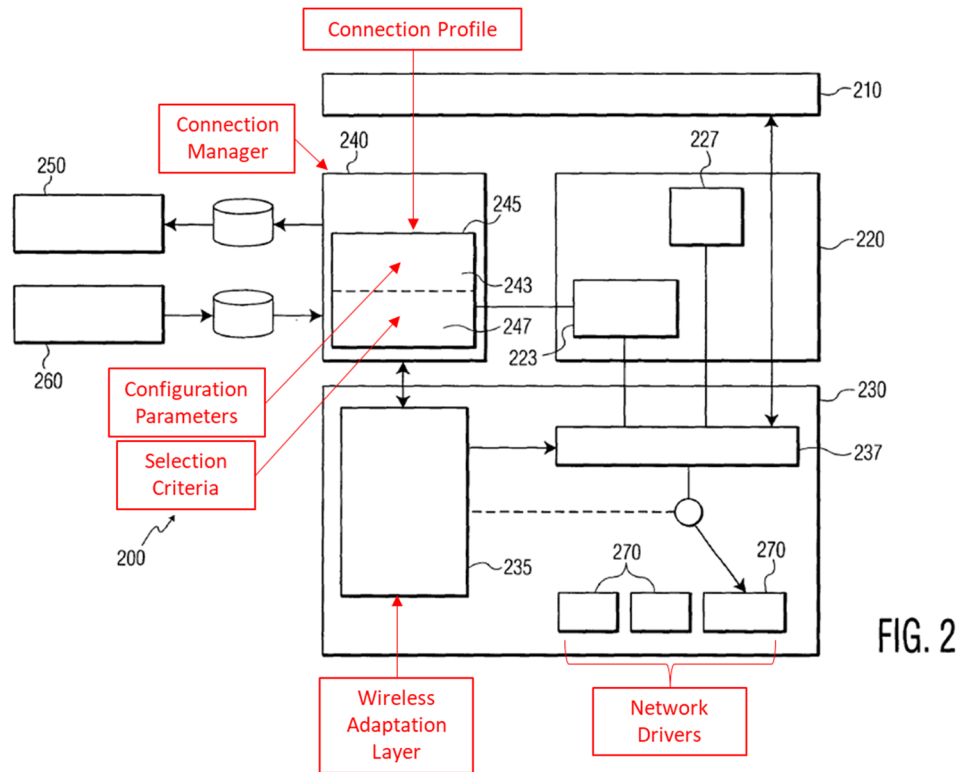


FIG. 2B

SAMSUNG-1005, FIG. 2B.

B. Chiu

27. Chiu discloses techniques for “smart connection management of portable devices” that use “profiles” with “configuration parameters” and “selection criteria” that determine which network connection should be active at any given time. SAMSUNG-1006, 7:17-10:11. Referring to Chiu’s FIG. 2 below, Chiu’s “connection manager” “activat[es] the best available connection based on configuration parameters 243 and selection criteria 247 stored with a connection profile 245.” SAMSUNG-1006, 10:12-11:3. Chiu’s connection manager effectuates its selection of networks using a “wireless adaptation layer 235” that changes the active “network driver 270.” SAMSUNG-1006, 13:4-14:18.



SAMSUNG-1006, FIG. 2

C. Rao

28. Rao discloses performing “intelligent and client centric prioritization of application network communications on a client based on the type and/or priority of an application.” SAMSUNG-1007, ¶[0179], FIG. 5A. Rao’s method can be used to prioritize “data communications” of some applications over others (e.g., “real-time data communications” over data communications from “non-real-time data communication applications”), and can be used to “compliment Quality of Service (QOS) networks where network traffic prioritization occurs in intermediary network devices, such as switches and routers.” SAMSUNG-1007, ¶[0184]. To effectuate

this prioritization, Rao describes using a “packet capture mechanism” that “inspects” the network packets of applications and a “frame monitor” that “identifies an application ... that generated the packet.” SAMSUNG-1007, ¶¶[0109], [0158]-[0159], [0176], [0180], [0185], [0191], FIG. 5A.

29. As shown in Rao’s FIG. 5A below, Rao’s remote access client 105 is connected to network 104 through one or more LAN or WAN links and/or wireless connections. SAMSUNG-1007, ¶[0179]. Rao uses a network interface, e.g., a modem, to communicate with a WWAN network. SAMSUNG-1007, ¶[0125]. “The client 105 may execute one or more applications 338a-338n, which access the network 104 via the agent 326 and filter 322 of the remote access client 120.” SAMSUNG-1007, ¶¶[0179], [0090].

30. Rao’s system implements “one or more policies 520 for specifying client-side prioritization of network communications related to applications 338a-338n.” SAMSUNG-1007, ¶[0182]. These policies “may be specified by any suitable means and/or mechanisms.” SAMSUNG-1007, ¶[0182]. For instance, these policies can “define prioritization” based on criteria such as: “the name of the application,” “the type of application,” “the type of one or more protocols used by the application[s],” “the size of the payload of the network packet,” “whether an application is running in the foreground or the background of the client,” and/or “the

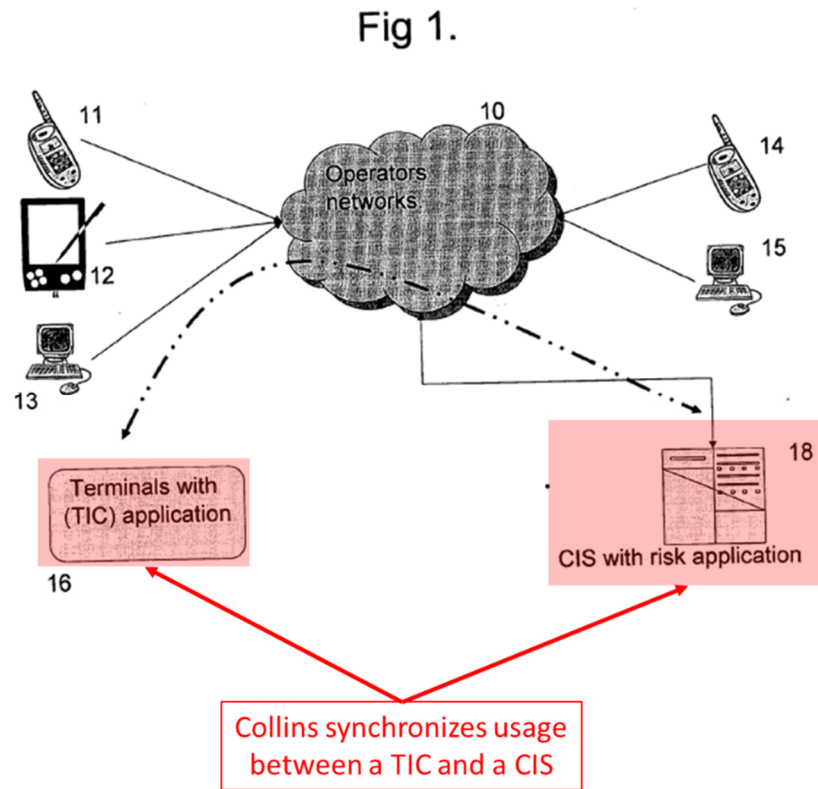
destination network address, such as host name or IP address, and/or destination port number.” SAMSUNG-1007, ¶[0182].

31. Rao deploys these policies by intercepting packets of network traffic associated with applications, determining the priority of the packets based on the application that is associated with each packet, and selectively communicating the packets to the network based on the determined priority. SAMSUNG-1007, ¶¶[0184]-[0190], FIG. 5B. As an example, Rao’s system can “use the policies 520 to determine which network packets to queue and/or discard.” SAMSUNG-1007, ¶[0207]. In particular, Rao’s system includes a packet capture mechanism 365 for “intercepting network traffic of any of the applications 338a-338n of the client 105.” SAMSUNG-1007, ¶¶[0080], [0184]-[0186], FIG. 5A.

D. Collins

32. Collins discloses a Terminal Information Collector (TIC) that collects usage information relating to “each activity or session that occurs through the network,” for example, “URLs of websites visited” and “addresses and sizes of received and sent SMS messages.” SAMSUNG-1008, ¶¶[0025], [0037], [0039], [0041], [0049]-[0050], FIGS. 1 (reproduced below), 3. A central information server (CIS) receives usage information from each device’s TIC for each network and operator where an associated device accrues usage. SAMSUNG-1008, ¶¶[0035]-[0045], FIG. 2. Data consumption for a consumer is “recorded in the network” and

“then compared to the information sent from the TIC to the CIS” (synchronizing the two different values of consumption—the consumption calculated by the network with the consumption reported by the TIC). SAMSUNG-1008, ¶[0084]. If the resulting two values differ by a threshold amount, the CIS “raise[s] an event alarm.” SAMSUNG-1008, ¶[0092].



SAMSUNG-1008, FIG. 1.

E. Camilleri

33. Camilleri discloses a ‘proprietary applications module’ (PAM) that “is connected to, or built into, a wireless device (WD). The PAM is capable of switching all incoming traffic by associating the WD to one specific subscriber identity sub-

module, referred to as ‘Local SIM’ (LS). SAMSUNG-1009, Abstract, SAMSUNG-1009, ¶¶[0044]-[0046]. It can also switch or re-route all outgoing traffic by associating the same WD with a different subscriber identity sub-module, typically a ‘Roaming SIM’ (RS).” *Id.* The RS allows a user of the WD to keep an original number associated with the LS while also benefitting from the advantageous call tariffs for the end-user when originating calls with such RS from the country in which the user resides compared to calls tariffs when originating calls with the user’s LS from the country in which the user resides. SAMSUNG-1009, ¶¶[0044]-[0046]. RS and LS are provided by a Mobile Virtual Network Operator (MVNO) configured by the PAM. SAMSUNG-1009, ¶[0047]. The MVNO can compete even in the country of its own LHWN for international call tariffs, and definitely abroad when its WD users are roaming. *Id.* This is an advantage that few or no other MVNOs have in the country of their own LHWN, allowing subscribers to this innovative MVNO to make use of any of the Wireless Networks, using the PAM and RS in their own devices; this will always ensure the best available wireless coverage. SAMSUNG-1009, ¶[0047].

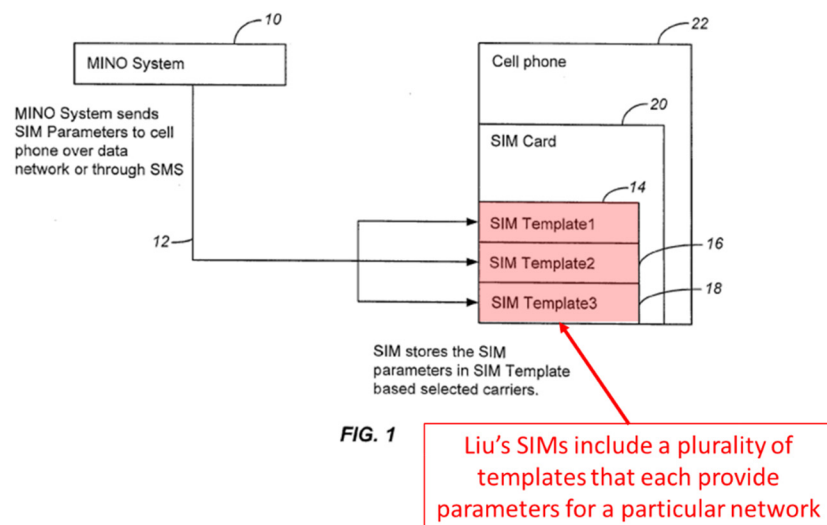
F. Bajko

34. Bajko discloses a common service profile that includes a “common feature that refers to common services” (“subscriptions”) associated with a plurality of IP Multimedia Private Identities (“IMPIs”) including service profiles stored on

separate SIM cards. SAMSUNG-1010, ¶¶[0014], [0039]-[0041], FIG. 4. Bajko's subscriptions are used by a home subscriber server (HSS) to provide services (e.g., calls, browsing, multimedia) in a 3GPP IP Multimedia Subsystem ("IMS"). SAMSUNG-1010, ¶¶[0035]-[0041], FIG. 2.

G. Liu

35. Liu discloses a SIM with a template manager system that includes SIM templates (e.g., phone books, call logs, messages) for a particular area (e.g., a country) where a user will travel. SAMSUNG-1030, ¶¶[0017]-[0022], FIGS. 1-2. Liu's template manager system applies SIM templates to the SIM and reboots the SIM when a new template is loaded. SAMSUNG-1030, ¶[0041], FIG. 3. Liu's FIG. 1 depicts a compartmentalized SIM with SIM templates, while FIG. 2 depicts the composition of an example SIM.



SAMSUNG-1030, FIG. 1.

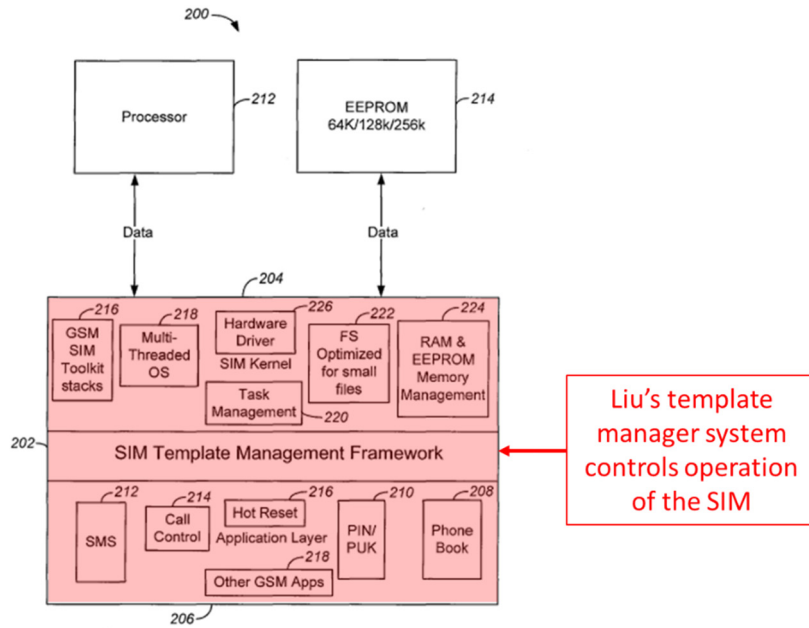


FIG. 2

SAMSUNG-1030, FIG. 2.

H. Brown

36. Brown discloses a SIM card with “a plurality of sets of subscription parameters, with each set of subscription parameters including identification and configuration information for a different type of operation.” SAMSUNG-1012, ¶¶[0019]-[0024], FIG. 1 (reproduced below). For example, the SIM can include subscription parameters for “different operating markets or regions.” *Id.* Brown’s subscription parameters can be activated and deactivated. SAMSUNG-1012, ¶¶[0018], [0020], [0024], [0032]-[0034].

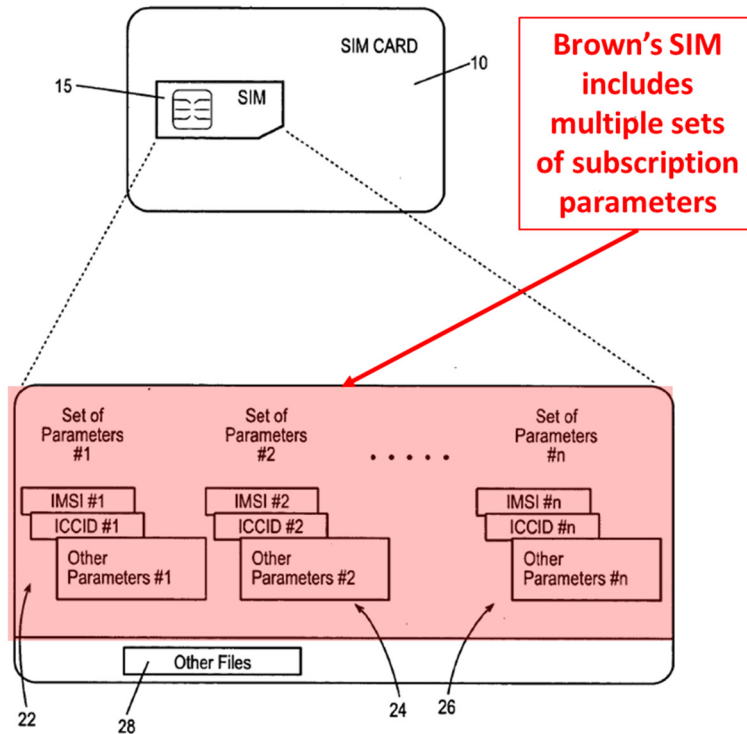


Fig. 1

SAMSUNG-1012, FIG. 1.

VIII. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '055 CLAIMS UNPATENTABLE

37. Below, I present a first set of grounds based on Jheng and Chiu and a second set of grounds based on Jheng, Chiu, and Rao. Under the first ground 1A, I analyze why the Jheng-Chiu combination renders obvious claims 1-2, 6-7, and 9-12. In the second ground 2A, the Jheng-Chiu combination is complemented with Rao's additional disclosure for select features of limitations 1.1, 1.5, and 1.6 ("*a Wireless Wide-Area Network (WWAN) modem,*" "*adaptive service policy control agent,*"

and “*an application service interface*,” respectively)². Although claim 1 is rendered obvious by Jheng and Chiu as explained below, I have presented the Jheng-Chiu-Rao combination for claim 1 to the extent it is argued that a POSITA would not have found features 1.1, 1.5, and 1.6 obvious based on the Jheng-Chiu combination.

IX. GROUNDS 1A/2A: CLAIMS 1-2, 6-7, 9-10 AND 12 ARE OBVIOUS OVER JHENG IN VIEW OF CHIU (WITH OR WITHOUT RAO)

A. The combination of Jheng and Chiu

38. It would have been obvious for a POSITA to combine the teachings of Jheng and Chiu such that (1) Chiu’s user configurable connection profiles would have been incorporated into and stored in Jheng’s system, e.g., on the USIMs of Jheng’s dual-SIM phone; (2) Chiu’s “smart connection management” (including, at least, Chiu’s connection manager, wireless adaptation layer, tunneling interface, and network drivers—an example of which is shown in Chiu’s FIG. 2) would have been used by the Jheng dual-SIM phone to manage network connections, in accordance with the stored connection profiles; and (3) implementation details of Chiu’s profile database interfaces would have been incorporated into Jheng’s man-machine interface (MMI). SAMSUNG-1005, ¶¶[0033]-[0035], [0050]-[0053]; SAMSUNG-

² All emphasis is added unless otherwise noted. Claim language is shown in bold italics.

1006, 4:19-6:29, 7:22-27, 8:26-10:20, 14:7-18, FIG. 2. A POSITA would have been motivated to combine Jheng and Chiu for the following reasons.

39. First, the ability of Chiu's connection profiles to retain a user's preferences for different networks would have been especially beneficial to Jheng's system, given that Jheng expressly describes traveling among different networks (e.g., "roaming"). SAMSUNG-1005, ¶¶[0050]-[0053]; SAMSUNG-1006, 4:19-6:29, 7:22-27, 8:26-10:20, 14:7-18, FIG. 2. Using Chiu's connection profiles and smart connection management would allow a user to avoid configuring Jheng's device every time the user encounters a different network when traveling, (e.g., a user would only have to configure the connection profile of the second Jheng USIM once to manage networks frequently encountered while traveling). *Id.* Indeed, Chiu discloses that setting up network connections "requires complex procedures to be performed by the end user," and removing the need to manually configure a user's preferences for each encountered network would have improved the user experience. SAMSUNG-1006, 3:16-2:5. Chiu recognizes that relying on a user to manually configure a device can be problematic because "the end user is often unable to take full advantage of the connections available to the portable device," and therefore, establishing user preferences in Chiu's connection profiles would have prevented the user from repeatedly performing complex operations. SAMSUNG-1005, ¶[0059], FIG. 13; SAMSUNG-1006, 3:16-2:5.

40. Second, incorporating Chiu's connection profiles onto Jheng USIMs would have provided a convenient way for Jheng service providers to implement network-wide policies, as Chiu discloses that such policies can be periodically "pushed" to the device. SAMSUNG-1006, 6:4-7, 9:2-10. Chiu explains that, prior to its techniques, providers "experience[d] problems enforcing consistent communication policies across a group of users" because the process of establishing network connections was "mostly manual and require[d] complex procedures to be performed by the end user." SAMSUNG-1006, 3:16-2:5. Although Jheng allows a user to manually configure a USIM, a POSITA would have recognized and found obvious that Chiu's techniques would have alleviated difficulties in establishing network-wide policies by reducing the need for user action. *Id.*

41. Third, Chiu's functionality of displaying available connection profiles stored in a profile database, would have allowed the user of Jheng's dual-SIM phone to easily view and "fine tune" connection profiles, as taught by Chiu, to better achieve the user's individual service needs. SAMSUNG-1005, ¶¶[0050]-[0060], FIGS. 6, 9, 11; SAMSUNG-1006, 8:26-9:10.

42. Jheng and Chiu are analogous art to the '055 patent, which is generally directed to "a services policy communication system and method" for controlling wireless network usage by a mobile device in a wireless network. SAMSUNG-1001, Abstract, 8:44-67, 48:47-49:13, 82:54-59. Indeed, Jheng generally describes

transmitting “mobile originated (MO) request[s] by a mobile station with a first subscriber identity card and a second subscriber identity card,” and Chiu generally describes “systems and methods for providing smart connection management of portable devices within a network communication system.” SAMSUNG-1005, ¶¶[0007]. Accordingly, the prior art references are all directed to the same field of wireless network communications. *Id.*

43. Additionally, as explained below in more detail, combining Jheng and Chiu would have been obvious at least because such a combination would have merely involved (1) combining prior art elements according to known methods to yield predictable results; and the (2) use of known techniques to improve similar devices in the same way.

44. Incorporating Chiu’s connection profiles into Jheng’s USIMs would have been predictable and foreseeable with a reasonable expectation of success because Jheng describes USIMs that store user account information and authentication information associated with a user, similar to Chiu’s stored connection profiles that describe users’ network preferences. SAMSUNG-1005, ¶¶[0029]-[0030]; SAMSUNG-1006, 4:19-6:29, 7:22-27, 8:26-10:20, 14:7-18, FIG. 2. Indeed, before the Benefit Date, USIMs included various elementary files (EF) that stored information associated with the user, their connection preferences, and the services provided by the USIM, for example, “MMS User Preferences” and

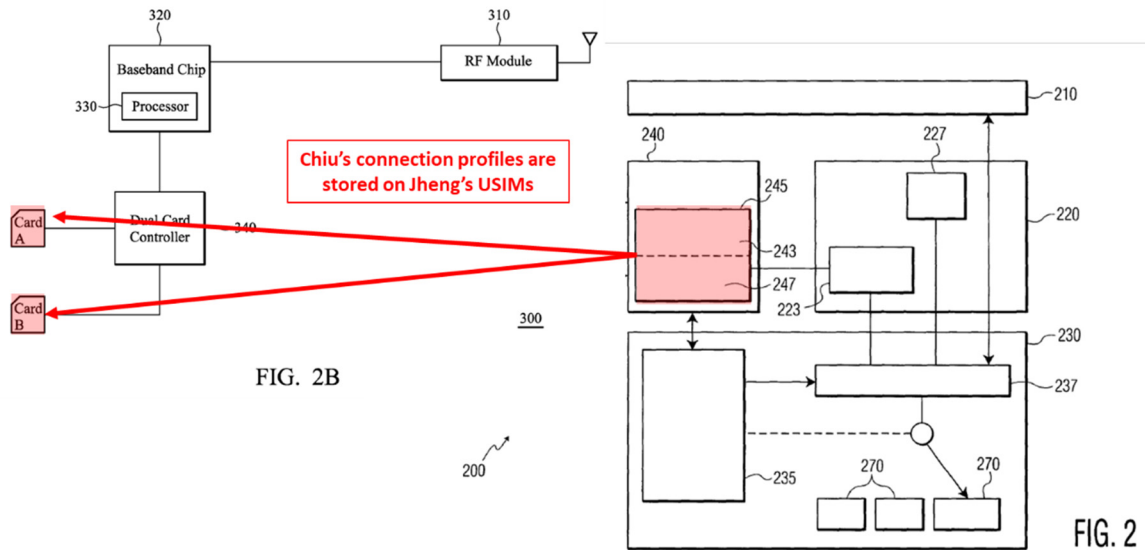
“MMS User Connectivity parameters” which are “used by the [mobile equipment] for MMS network connection.” SAMSUNG-1014, 69-70; SAMSUNG-1015, 50-83.

45. Additionally, incorporating Chiu’s smart connection management system into a mobile device, like Jheng’s mobile station, to manage wireless networks was well known as of the ’055 Benefit Date. SAMSUNG-1006, 6:8-22, 10:12-20, 13:4-14:18; SAMSUNG-1016, Cover, ¶¶[0036]-[0039], FIG. 2; SAMSUNG-1016. For example, Cole discloses a “connection manager” that manages multiple wireless networks to determine what network connections should be active at any given time. SAMSUNG-1016, Cover, ¶¶[0036]-[0039], FIG. 2. Cole’s connection manager—like Chiu’s—is implemented on a mobile device with a standard processor (like Jheng’s dual SIM phone, which also includes a processor). SAMSUNG-1016, ¶[0033]; SAMSUNG-1005, ¶¶[0007]-[0010], [0034]-[0035], [0052], [0055], [0058], [0060], FIGS. 2A-2B.

46. Further, the implementation of Chiu’s smart connection management system would have involved only routine coding ability that would have been well within a POSITA’s capability (e.g., coding the functions of Chiu’s smart connection management system as machine readable code to be executed by Jheng dual-SIM phone’s processors). For example, the smart connection management system would have been capable of being embodied as executable functions that provide an output

(e.g., the selection of a connection profile) in response to a detected input (e.g., a discovered network). It would have been well within the ability of POSITA to code such functions, as a POSITA would have been exposed to various suitable programming languages throughout their education (e.g., Java, C, or Objective-C). *See above*, §IV. Additionally, Chiu discloses that profiles can be coded in Extensible Markup Language (“XML”), a well-known language that would have been part of a POSITA’s general knowledge. SAMSUNG-1006, 7:25-27; *see, e.g.*, SAMSUNG-1029, 5.

47. One example of the combined Jheng-Chiu system is illustrated below in Jheng FIG. 2 and Chiu FIG. 2B. As shown, Chiu’s user configurable connection profiles would have been incorporated into and stored on the USIMs of Jheng’s dual-SIM phone, such that these profiles would govern the operation of the “smart connection system” of the Jheng-Chiu device. SAMSUNG-1005, ¶¶[0033]-[0035], [0050]-[0053]; SAMSUNG-1006, 4:19-6:29, 7:22-27, 8:26-10:20, 14:7-18, FIG. 2.



SAMSUNG-1005, FIG. 2B and SAMSUNG-1006, FIG. 2 (Cropped, annotated, and modified by Jheng/Chiu).

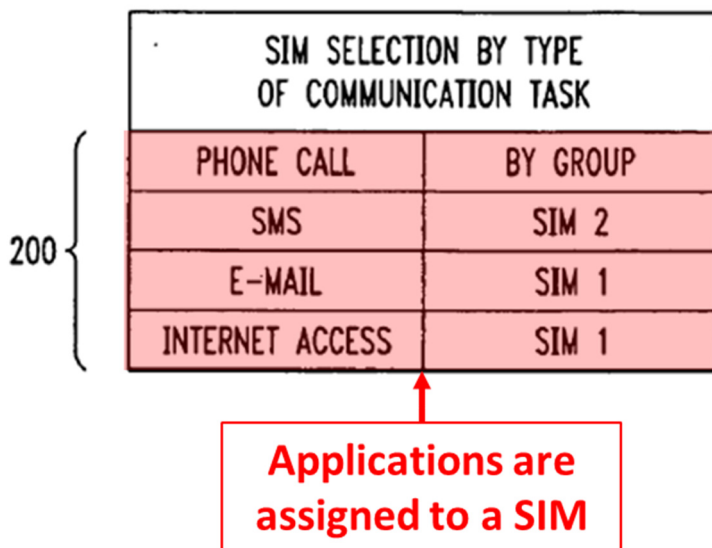
B. The combination of Jheng, Chiu, and Rao

48. It would have been obvious for a POSITA to modify the Jheng-Chiu mobile station to incorporate (1) Rao's remote access client and prioritization techniques, and (2) Rao's WWAN modem for at least the following reasons. SAMSUNG-1007, ¶¶[0099]-[0116], [0125].

49. First, incorporating the functionality of Rao's remote access client into the Jheng-Chiu mobile station would have beneficially provided the Jheng-Chiu system with the additional capability to identify individual application traffic, thus allowing a USIM's connection profiles to restrict specific application traffic to a specific network associated with that USIM. SAMSUNG-1007, ¶¶[0109], [0179]-[0184]. A POSITA would have recognized this benefit, as this was known in the art, as evidenced by other prior art references. SAMSUNG-1017, ¶¶[0043]-[0046], FIG.

2. For example, Landschaft similarly discloses a dual SIM phone where applications are assigned to a particular SIM (e.g., “SMS” to “SIM 2”). SAMSUNG-1017, ¶¶[0043]-[0046], FIG. 2.

FIG. 2



The diagram shows a table titled "SIM SELECTION BY TYPE OF COMMUNICATION TASK". To the left of the table is a bracket labeled "200". Below the table is a red box with the text "Applications are assigned to a SIM" and a red arrow pointing up to the bottom row of the table.

SIM SELECTION BY TYPE OF COMMUNICATION TASK	
PHONE CALL	BY GROUP
SMS	SIM 2
E-MAIL	SIM 1
INTERNET ACCESS	SIM 1

SAMSUNG-1017, FIG. 2.

50. Second, Rao’s prioritization techniques (e.g., “the size of the payload of the network packet”) would have enhanced the utility of the Jheng-Chiu mobile station, particularly for a user wanting to prioritize certain traffic while traveling (e.g., avoiding certain application traffic that may be more expensive on a foreign network). SAMSUNG-1007, ¶¶[0109], [0179]-[0184]. For example, Rao describes data intensive applications like streaming video and/or audio that would have been exceedingly expensive to operate while roaming based on their data consumption. SAMSUNG-1007, ¶[0088].

51. Jheng, Chiu, and Rao are analogous art to the '055 patent, which is generally directed to “a services policy communication system and method” for controlling wireless network usage by a mobile device in a wireless network. SAMSUNG-1001, Abstract, 8:44-67, 48:47-49:13, 82:54-59. Indeed, Jheng generally describes transmitting “mobile originated (MO) request[s] by a mobile station with a first subscriber identity card and a second subscriber identity card,” Chiu generally describes “systems and methods for providing smart connection management of portable devices within a network communication system,” and Rao generally describes “a remote access architecture for providing peer-to-peer communications and remote access connectivity.” SAMSUNG-1005, ¶[0007]; SAMSUNG-1006, 1:1-4; SAMSUNG-1007, Abstract, ¶[0004]. Accordingly, the prior art references are all directed to the same field of wireless network communications. *Id.*

52. Additionally, as explained below in more detail, combining Jheng-Chiu with the teachings of Rao would have involved (1) combining prior art elements according to known methods to yield predictable results; and (2) using known techniques to improve similar devices in the same way.

53. Incorporating Rao’s remote access client and prioritization techniques into the Jheng-Chiu device would have been predictable and foreseeable with a reasonable expectation of success because Rao describes that its techniques can be

implemented in end-user devices (mobile telephones), such as Jheng's mobile station. SAMSUNG-1007, ¶[0130]. The use of computer program modules to monitor application packet flows on mobile stations was known as of the '055 Benefit Date. SAMSUNG-1013, ¶[0036]. For example, Kelz (a European patent application) describes a "controller module" that includes a "QoS packet processor," which can "monitor the packet flow" of applications. SAMSUNG-1013, ¶[0036].

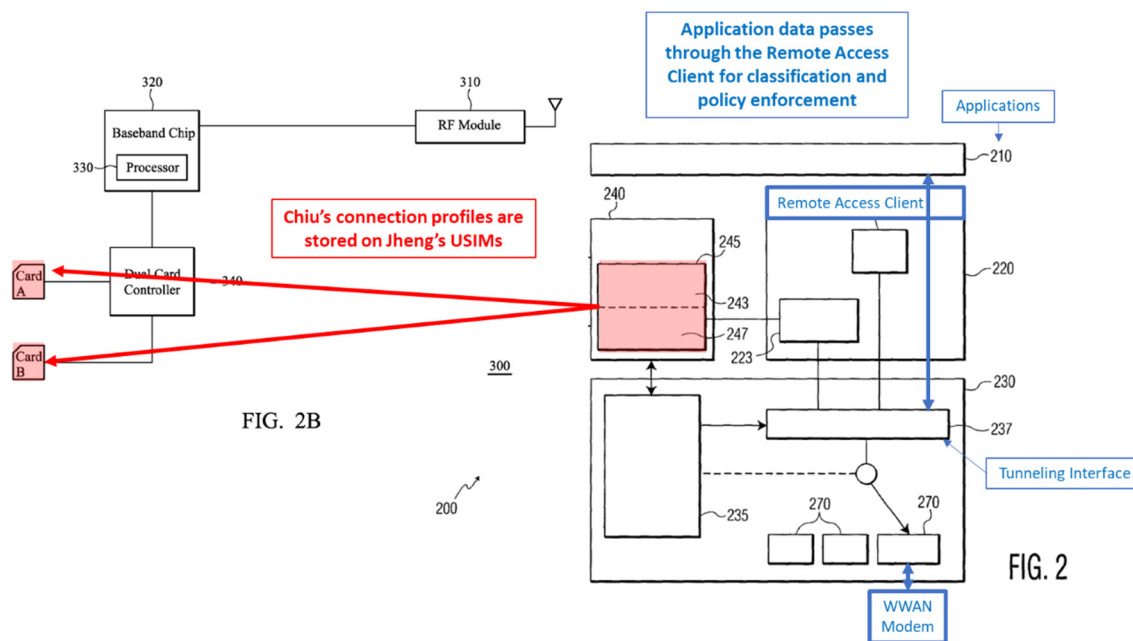
54. Additionally, the incorporation of Rao's prioritization techniques would have simply involved implementing software in a system already designed to execute similar program modules. SAMSUNG-1007, ¶[0092] (a "software set-up"). Indeed, implementing Rao's remote access client would have involved only routine coding ability that would have been well within a POSITA's capability (e.g., coding the functions of Rao's remote access client as machine readable code to be executed by Jheng's processors). For example, the remote access client would have been capable of being embodied as executable functions that provide an output (e.g., the application of a policy) in response to a detected input (e.g., a received data packet). It would have been well within the ability of POSITA to code such functions, as a POSITA would have been exposed to various suitable programming languages throughout their education. *See above*, §IV. Rao itself corroborates the ability of a POSITA to embody the remote access client as executable instructions. SAMSUNG-1007, ¶[0116].

55. Further, it was known before the Benefit Date of the '055 patent that drivers (e.g., Chiu's network drivers) controlled wireless modems in wireless devices (e.g., Rao's WWAN modem). SAMSUNG-1024, ¶¶[0035]-[0039], FIG. 4). Indeed, Papineau explains that modems "communicate with [a] processor 45 through a modem driver 43" and that "[d]ata and instructions intended for the modem are sent to the modem driver 43 which formats the data and instructions in a manner suitable for the modem 40." *Id.*

56. In an example of the combined system, illustrated below in Jheng's FIG. 2 and Chiu's FIG. 2B, Rao's remote access client would have been positioned between the applications and network drivers of the Jheng-Chiu mobile station, such that it would monitor, identify, and prioritize data packets transmitted from applications on the mobile station. SAMSUNG-1007, ¶¶[0109], [0158]-[0159], [0176], [0180], [0185], [0191], FIG. 5A.

57. Additionally, to the extent there is any question as to whether the Jheng-Chiu mobile station includes a modem, Rao's WWAN modem would have been used to establish network connections with the GSM, GPRS, and other WWAN networks disclosed by Jheng and Chiu. SAMSUNG-1005, ¶¶[0005], [0032]-[0033]; SAMSUNG-1006, 7:17-27, 11:4-12; SAMSUNG-1007, ¶[0125]. Rao describes that modems are suitable for interfacing mobile devices to a wireless network for

communication (e.g., a wireless “Wide Area Network,” or WWAN). SAMSUNG-1007, ¶[0125]; see also SAMSUNG-1024, ¶¶[0030]-[0032], FIG. 4.



SAMSUNG-1006, FIG. 2 (Cropped, annotated, and modified by Rao).

C. Analysis

[1.pre] A wireless end-user device comprising:

58. The Jheng-Chiu combination renders [1.pre] obvious. Jheng discloses a dual SIM media phone (“*a wireless end-user device*”) equipped with multiple SIM cards. SAMSUNG-1005, ¶¶[0006], [0037]. Jheng’s FIG. 1 (reproduced below) depicts one example of the media phone as a mobile station 110 and explains that it “may be called *user equipment* interchangeably.” SAMSUNG-1005, ¶[0033]. “A subscriber identity module (SIM) card typically contains user account information, [and] an international mobile subscriber identity (IMSI),” which can be used to obtain details of the mobile user. SAMSUNG-1005, ¶¶[0029], [0032].

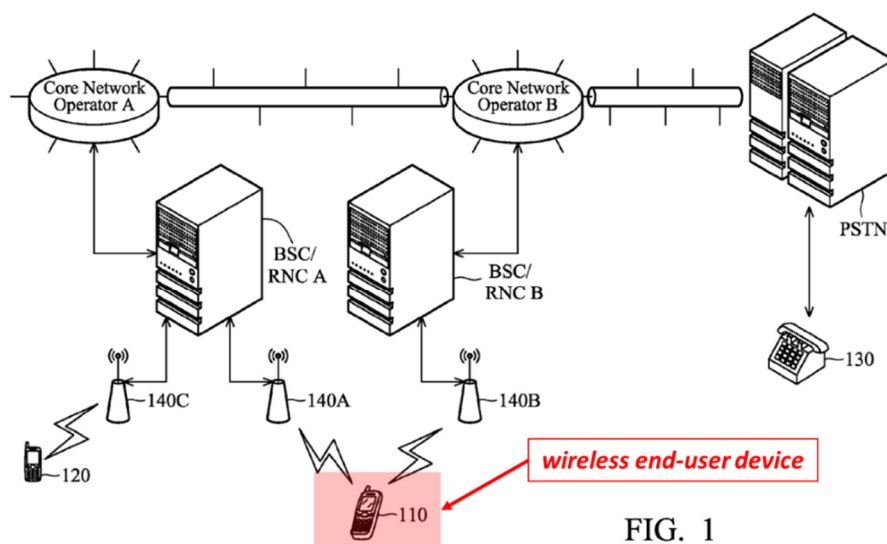


FIG. 1

SAMSUNG-1005, FIG. 1.

59. Jheng’s mobile station 110 can make a voice or data call and “may simultaneously access two core networks such as a Global System for Mobile Communications (GSM), Wideband Code Division Multiple Access (WCDMA), CDMA 2000 and Time Division-Synchronous Code Division Multiple Access (TD-SCDMA) network and the like after camping on two cells 140A and 140B (i.e. each may be a base station, a node-B or others).” SAMSUNG-1005, ¶[0033]. Because Jheng’s mobile station 110 is used by an end-user and communicates with wireless networks such as GSM and CDMA networks, Jheng discloses “*a wireless end-user device.*”

60. Moreover, such a mapping is consistent with the '055 patent, which describes “general purpose devices like smart phones and computers,” as examples of a wireless end-user device. SAMSUNG-1001, 5:41-56.

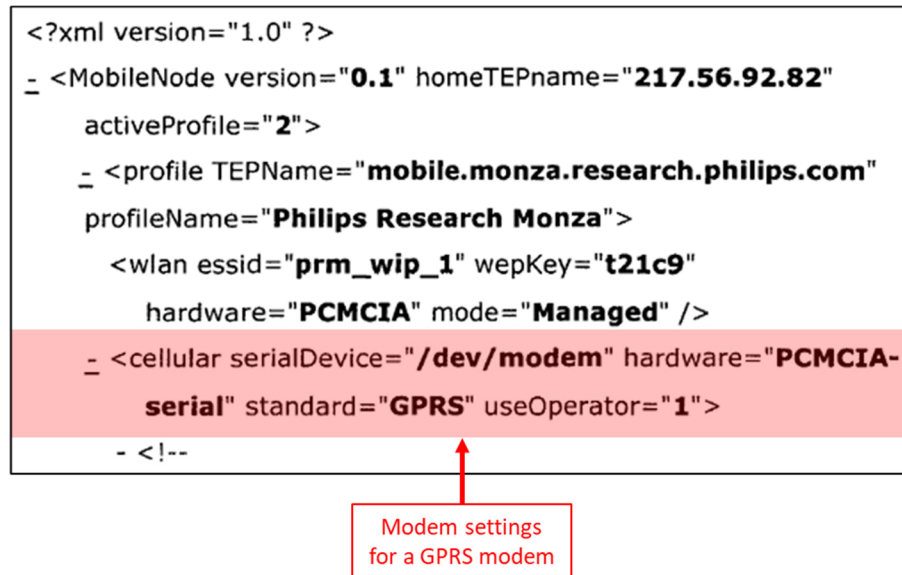
[1.1] a Wireless Wide-Area Network (WWAN) modem;

Ground 1A Mapping

61. Jheng’s mobile station communicates over several WWAN networks, e.g., GSM, GPRS, WCDMA, TDMA, TD-SCDMA, and other 3G networks. SAMSUNG-1005, ¶¶[0005], [0032]-[0033]. Thus, it would have been obvious to a POSITA that Jheng’s mobile station would have included a WWAN modem to wirelessly communicate with the above-noted WWAN networks because modems are used to implement modulation/demodulation schemes for the wireless communication over such WWAN networks. Wireless signals transmitted across wireless networks are modulated and demodulated using a modem so that the transmitted signal can be configured at a desired frequency and amplitude. When communicating across a WWAN network, a POSITA would have understood that Jheng’s mobile station would have included a WWAN modem.

62. To the extent Patent Owner disputes the disclosure of a WWAN network and WWAN modem in Jheng, Chiu discloses these features. For example, Chiu discloses that its portable device 110 “is configured to connect to services on the Internet 130 via a variety of network connection types, such as Ethernet,

WWAN" SAMSUNG-1006, 7:17-27. Chiu teaches that the portable device 110 can include a profile that "can be used to store configuration parameters 243 ... for different connection types." SAMSUNG-1006, 10:31-33, 7:22-33. Excerpts of an exemplary profile 245 are shown below. SAMSUNG-1006, 11:1-13:3.



SAMSUNG-1006, 11:4-12.

63. As shown above, Chiu's profile includes modem setting information. SAMSUNG-1006, 11:4-12. A POSITA would have understood that when configuring parameters for a WWAN connection, Chiu's profile would have also included settings for the WWAN modem. Indeed, a GPRS network is one example of a WWAN, and thus the disclosure above indicates that a setting for a type of WWAN modem is provided. Therefore, it would have been obvious to a POSITA that the Jheng-Chiu device includes settings for a WWAN modem because Jheng-Chiu's portable device includes a WWAN modem.

64. Additionally, a POSITA would have understood and found obvious that mobile devices at the time of the Benefit Date typically included *a Wireless Wide-Area Network (WWAN) modem*, and as such, using a WWAN modem to communicate with a wireless network would have simply been the use of a well-known communication component in devices where a POSITA would have expected such a component to be used. SAMSUNG-1016, ¶¶[0034]-[0035], FIG. 2; SAMSUNG-1013, ¶¶[0125], [0130]. Indeed, Cole discloses a “mobile device” that includes a plurality of “*wireless modem[s]*,” to include a “WWAN modem 230,” a “WLAN modem 235,” and a “voice band modem 250.” SAMSUNG-1016, ¶¶[0034]-[0035], FIG. 2.

Ground 2A Mapping

65. To the extent it is argued that Jheng and Chiu do not render [1.1] obvious, Rao explicitly discloses that wireless devices included a network interface 118, such as a modem, for connecting to Wide-Area Networks (“*a Wireless Wide-Area Network (WWAN) modem*”). SAMSUNG-1007, ¶[0125], FIG. 1D (reproduced below). In combination with Jheng and Chiu, discussed above, one or more of the network interfaces in the Jheng-Chiu mobile station would have included Rao’s WWAN modem to facilitate the mobile station’s connection to a WWAN (networks explicitly disclosed by Jheng and Chiu). SAMSUNG-1005, ¶¶[0005], [0032]-[0033]; SAMSUNG-1006, 7:17-27; SAMSUNG-1007, ¶[0125].

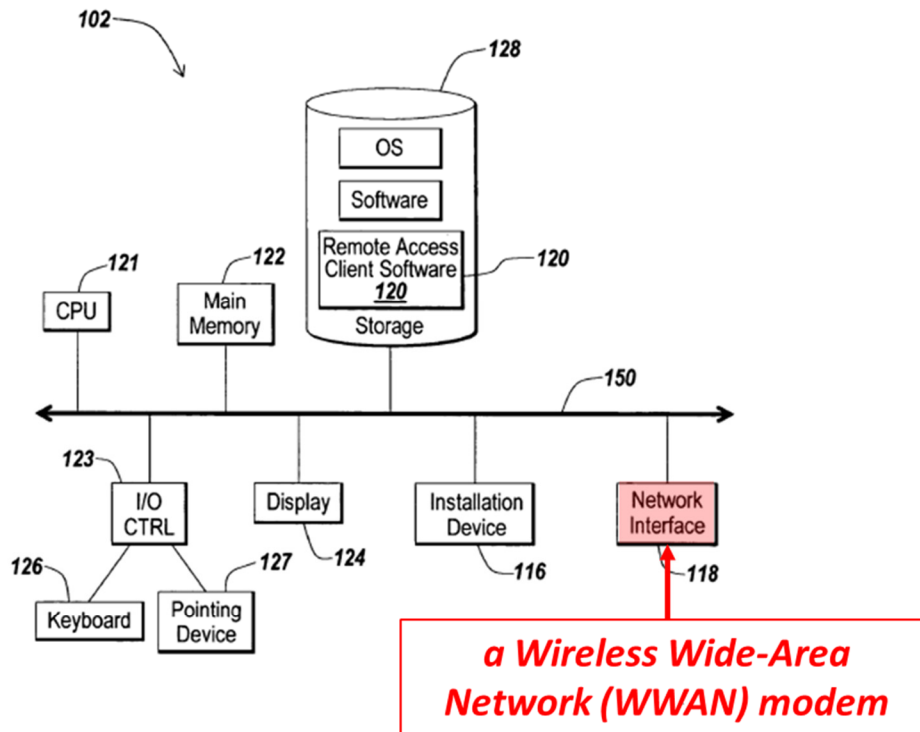


Fig. 1D

SAMSUNG-1007, FIG. 1D.

[1.2] a secure memory to store a first service profile associated with a first service plan and a first wireless network accessible through the WWAN modem, the first service profile comprising a first set of network service policies, and

a secure memory to store ...

66. Jheng discloses a “universal SIM” (USIM) that “stores user account information, an IMSI, authentication information and a set of USIM Application Toolkit (USAT) commands.” SAMSUNG-1005, ¶[0030]. The USIM stores “a long-term pre-shared secret key K, which is shared with the Authentication Center

(AuC) in the network.” *Id.* A POSITA would have understood and found obvious that the memory of the USIM includes a “*secure memory*,” at least because it was well known before the ’055 Benefit Date that (1) USIMs included measures to control access to their memory (even to the host device), and (2) USIMs included keys (which would need to be stored securely for protection) to authenticate their use (e.g., to a network). SAMSUNG-1008, ¶[0022] (describing USIMs as a “secure storage device”); SAMSUNG-1014, 140-141; SAMSUNG-1015, 27-28; SAMSUNG-1021, 6, 9.

67. A POSITA’s understanding of Jheng’s “pre-shared secret key K” and storage in a secure memory is corroborated by other prior art references that describe USIMs. SAMSUNG-1014, 141. For example, the 3rd Generation Partnership Project (3GPP) published a specification for USIMs prior to the ’055 Benefit Date (3GPP TS 31.102) that discloses that a USIM is authenticated to a network using “a secret key K” which is “available only to the USIM and the AuC” (thus achieving mutual authentication and controlling how the information in the USIM could be used). SAMSUNG-1014, 141. Further, 3GPP TS 31.102 discloses “file access conditions” that define different requirements to access certain information on the USIM. SAMSUNG-1014, 140-141. The Global System for Mobile Communications (GSM) Standard 11.11 (“GSM 11.11”), published before the ’055 Benefit Date, explains that file access conditions ensure that “[e]very file has its own

specific access condition for each command.” SAMSUNG-1015, 27-28. For example, a “NEVER” condition completely restricts access to the file to only the USIM itself (excluding even the host device). *Id.* This type of restriction is important because a service provider would have wanted to restrict a user’s ability to modify an issued USIM that includes service restrictions and authentication information—information a user generally should not have access to. SAMSUNG-1015, 27-28.

68. This is consistent with the ’055 patent, which similarly describes that functions are protected in secure memory “so that other undesired programs (and/or unauthorized users) have difficulty accessing the functions or software.” SAMSUNG-1001, 28:30-55. The Jheng-Chiu secure memory goes beyond the level of protection in the ’055 patent, which simply requires that the protection offers increased difficulty in accessing the information. SAMSUNG-1001, 28:30-55; SAMSUNG-1015, 27-28 (e.g., disclosing a “NEVER” condition). Other publications also describe USIMs as secure. SAMSUNG-1008, ¶[0022]; SAMSUNG-1021, 6, 9. For example, Collins (discussed below in §X), describes USIMs as a “secure storage device.” SAMSUNG-1008, ¶[0022]. Additionally, Wary—a presentation for the 9th International Common Criteria Conference (ICCC) in 2008—describes USIMs as a “secure platform.” SAMSUNG-1021, 6, 9.

69. Accordingly, a POSITA would have understood or found obvious that Jheng's subscriber cards, can be implemented as USIMs, include a "*secure memory*." SAMSUNG-1005, ¶¶[0030], [0035], FIG. 2B (reproduced below); SAMSUNG-1014, 140-141; SAMSUNG-1015, 27-28. Moreover, when USIMs ("card A" and "card B") are physically connected via a socket to the dual card controller 340, the controller 340 has access to the "*secure memory*" in both cards. SAMSUNG-1005, ¶[0035], FIG. 2B.

70. As discussed above in §IX.A, a POSITA would have found it obvious to implement Chiu's connection profiles into Jheng's USIMs because Jheng describes USIMs that store user account information and authentication information associated with a user, similar to Chiu's connection profile that describes a user's network preferences. SAMSUNG-1005, ¶¶[0029]-[0030]; SAMSUNG-1006, 4:19-5:2, 5:30-6:7, 6:23-29, 7:22-27, 8:26-9:10, 9:25-10:11, 10:16-20, 14:7-18, FIG. 2; *see above*, §IX.A. Indeed, USIMs included various elementary files (EF) that stored information associated with the user, their connection preferences, and the services provided by the USIM, for example, "MMS User Preferences" and "MMS User Connectivity parameters," which are "used by the [mobile equipment] for MMS network connection." SAMSUNG-1014, 69-70; SAMSUNG-1015, 50-83.

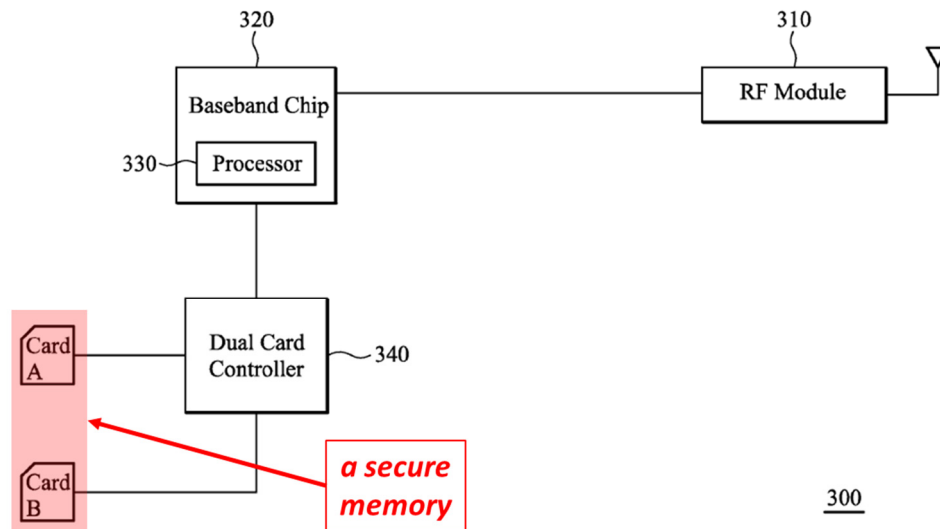
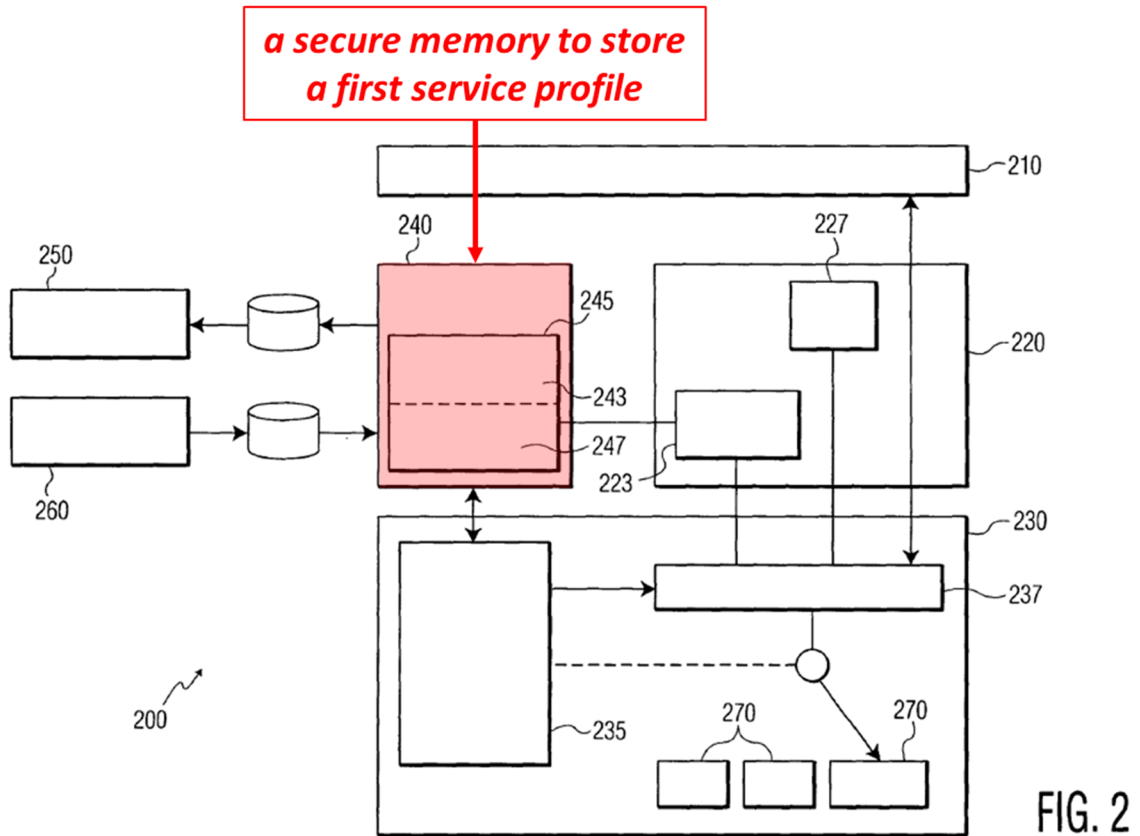


FIG. 2B

SAMSUNG-1005, FIG. 2B.

71. Jheng and Chiu also render a “*secure memory*” obvious in other ways. For example, Chiu’s connection manager stores connection profiles that can be downloaded from external sources. SAMSUNG-1006, 10:21-30, 13:27-31, FIG. 2. Thus, it would have been obvious to a POSITA that the connection manager would have downloaded the connection profiles from Jheng’s USIMs, for example, when Jheng’s USIMs are plugged into the socket of the controller 340.

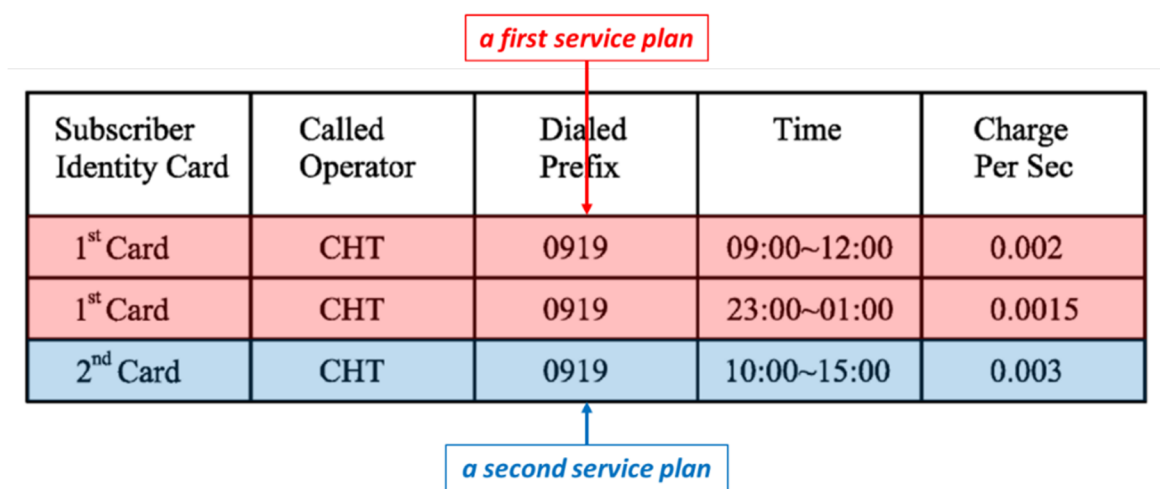


SAMSUNG-1006, FIG. 2.

... a first service plan

72. Jheng discloses that USIMs are associated with a fare plan (“*a first service plan*”) that specifies USIM and mobile station use charges (e.g., “a charge per second is 0.002 dollar when making an MO call to a called party with a prefix ‘0919’ of a phone number between a time duration of 9 to 12 o’clock via the first subscriber identity card”). SAMSUNG-1005, ¶¶[0056]-[0060], FIG. 10. Similarly, Chiu discloses that selection criteria can be based on billing information, and that service profiles can implement company-wide communication policies (additional examples of “*a first service plan*”). SAMSUNG-1006, 8:13-17. This is consistent

with the '055 patent, which similarly describes that a service plan includes “billing/costs information associated with that service profile.” SAMSUNG-1001, 9:5-16. Jheng discloses that each USIM can be associated with a fare plan (a “first” fare plan and a “second” fare plan), which as discussed below in [1.3], additionally renders obvious “*a second service plan.*” SAMSUNG-1005, ¶[0056], FIG. 10; *see below*, [1.3].



Subscriber Identity Card	Called Operator	Dialled Prefix	Time	Charge Per Sec
1 st Card	CHT	0919	09:00~12:00	0.002
1 st Card	CHT	0919	23:00~01:00	0.0015
2 nd Card	CHT	0919	10:00~15:00	0.003

FIG. 10

SAMSUNG-1005, FIG. 10.

73. Additionally, it was known before the Benefit Date to outline network usage for a USIM in a “*service plan*,” as evidenced by Jheng and other prior art references. SAMSUNG-1005, ¶¶[0056]-[0060], FIG. 10; SAMSUNG-1028; 1:10-40. For example, Nagarajan discloses that a user can change service plans “simply by changing the SIM card.” SAMSUNG-1028, 1:10-40.

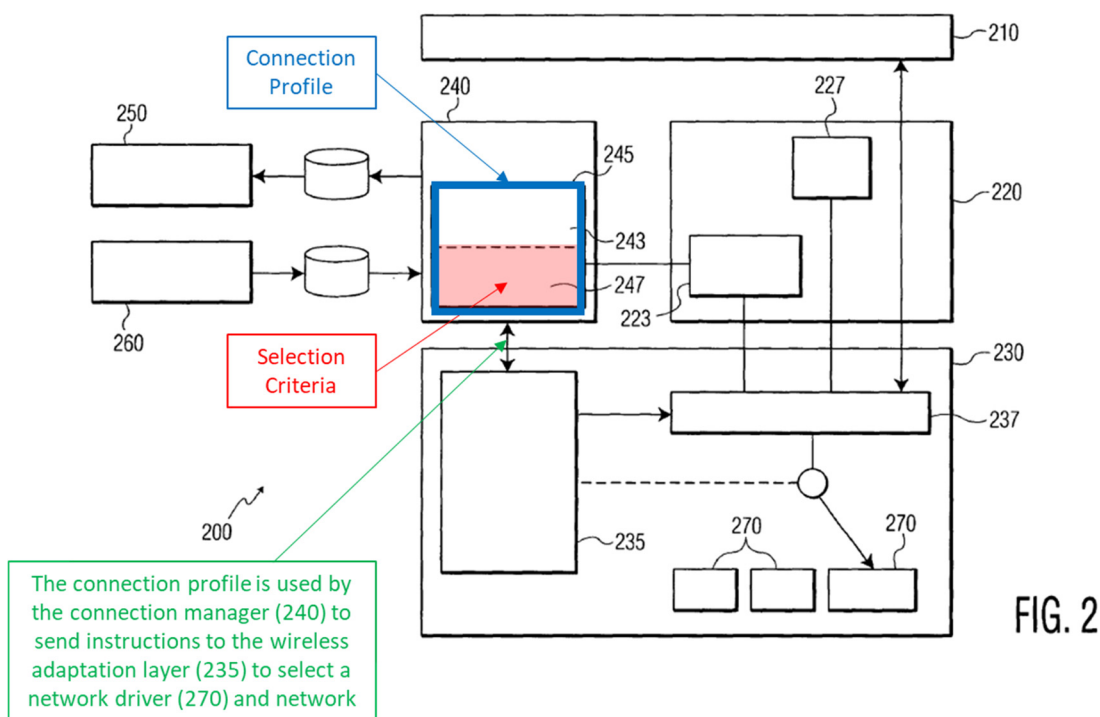
... a first service profile ... the first service profile comprising a first set of network service policies

Ground 1A Mapping

74. Chiu's portable device stores connection profiles including at least one connection profile ("***a first service profile***") that stores "selection criteria for selecting between the plurality of network connection types" ("***a first set of network service policies***"). SAMSUNG-1006, 4:19-5:2, 5:30-6:7, 6:23-29, 7:22-27, 8:26-9:10, 9:25-10:11, 10:16-20, 14:7-18, FIG. 2. Chiu's connection manager (discussed below in [1.4]) selects a particular network connection based on the selection criteria defined in the user's connection profile. *Id.* Additionally, Chiu discloses that a company (e.g., a service provider) can specify changes in a communication policy that would cause changes to a profile's configuration parameters or selection criteria, which further impacts the communication network service provided to a user's mobile device. SAMSUNG-1006, 6:4-7, 9:2-10.

75. The selection criteria includes "rules or parameters that define the user's preferences in selecting between connection types" ("***a first set of network service policies***") to include a selection based on a "location parameter," among other things. SAMSUNG-1006, 5:16-29, 6:8-22, 8:11-25, 9:11-24, 10:7-11. For instance, the selection criteria include "rules for selecting between a plurality of GPRS connection configurations" based on the identity of the carrier. SAMSUNG-1006, 8:11-25. A POSITA would have understood or recognized that rules specifying the type of

connection and network configurations provide a set of network service policies for using the wireless end-user device in Jheng-Chiu's system.



SAMSUNG-1006, FIG. 2.

76. In the combination with Jheng, as discussed above in §IX.A, Chiu's connection profiles would have been associated with and stored on a USIM (including a "*secure memory*"), including the selection criteria and priority policies associated with the connection profile. SAMSUNG-1005, ¶¶[0050]-[0053]; SAMSUNG-1006, 4:19-5:15; *see above*, §IX.A.

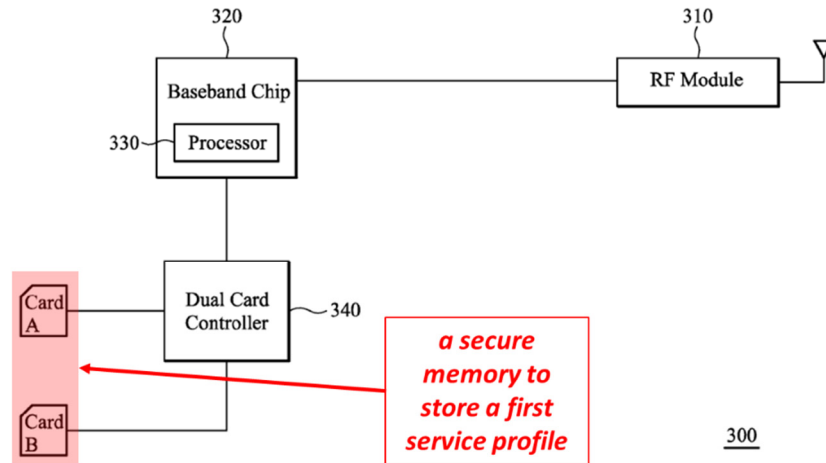


FIG. 2B

SAMSUNG-1005, FIG. 2B.

Ground 2A Mapping

77. Rao discloses a “remote access client” (discussed more below in [1.5] and [1.6]) that monitors the application data traffic transmitted by applications over a wireless network. SAMSUNG-1007, ¶¶[0099]-[0118], [0179], FIG. 1C; *see below*, [1.5]-[1.6]. Rao’s remote access client enforces “one or more policies 520 for specifying client-side prioritization of network communications related to applications 338 a-338 n” by intercepting, classifying, and filtering the application data traffic. SAMSUNG-1007, ¶[0182]. For instance, Rao’s policies can define “prioritization” based on criteria such as: “the name of the application,” “the type of application,” “the type of one or more protocols used by the application[s],” “the size of the payload of the network packet,” “whether an application is running in the foreground or the background of the client,” and/or “the destination network address,

such as host name or IP address, and/or destination port number.” SAMSUNG-1007, ¶[0182].

78. In the Jheng-Chiu-Rao combination, Rao’s priority policies are an additional example of “*network service policies*,” because these policies define actions to be taken for specific application traffic with respect to their network use. SAMSUNG-1007, ¶¶[0099]-[0118], [0179], FIG. 1C. Rao’s policies, along with Chiu’s selection criteria, would have been included in Chiu’s connection profiles that are stored on Jheng’s USIMs, thus enabling the network operator to define prioritization policies for specific applications by issuing a consumer a USIM pre-loaded with these policies (as recognized in the art before the ’055 Benefit Date, discussed above). SAMSUNG-1007, ¶¶[0109], [0179]-[0184]; SAMSUNG-1017, ¶¶[0043]-[0046], FIG. 2; *see above*, §IX.B.

a first service profile associated with ...a first wireless network accessible through the WWAN modem

79. As discussed above in [1.1], Jheng’s mobile station communicates over several types of WWAN networks (e.g., “Core Network Operator A”—“*a first wireless network*,” and “Core Network Operator B”—“*a second wireless network*”), and in combination with Rao, the device would have included a modem to access these networks (“*accessible through the WWAN modem*”). SAMSUNG-1005, ¶¶[0005], [0032]-[0033], FIG. 1; SAMSUNG-1007, ¶[0125]; *see above*, [1.1]. Further, Jheng discloses that each USIM can be “provided by a particular network

operator” (“*a first service profile associated with ... a first wireless network*”). SAMSUNG-1005, ¶¶[0033]-[0035], FIG. 1. For example, in the system of FIG. 1, USIM A can be provided by “Core Network Operator A” and USIM B can be provided by “Core Network Operator B.” *Id.*

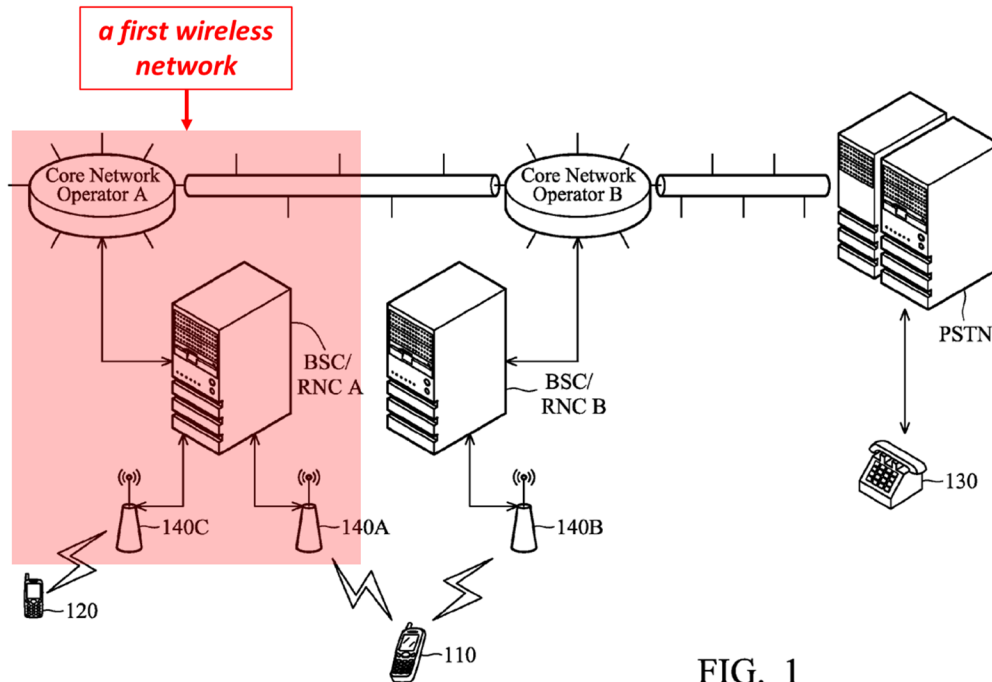


FIG. 1

SAMSUNG-1005, FIG. 1.

[1.3] [a secure memory to store] a second service profile associated with a second service plan and a second wireless network accessible through the WWAN modem, the second service profile comprising a second set of network service policies;

(i) Ground 1A Mapping

80. As discussed in the Overview of Jheng, [1.1], and [1.2] above, Jheng discloses a mobile station with dual USIMs (including “*secure memory to store*” a

“*first*” and “*second service profile*”) that can simultaneously access two core networks (a “*first*” and “*second wireless network accessible through the WWAN modem*”). SAMSUNG-1005, ¶¶[0006], [0033]; *see above*, §VII.A. For example, Jheng’s FIG. 1 shows two wireless networks each associated with a different core network operator. SAMSUNG-1005, ¶[0033], FIG. 1. Mobile station 110 makes calls using either cell 140A or 140B using its USIMs. *Id.*

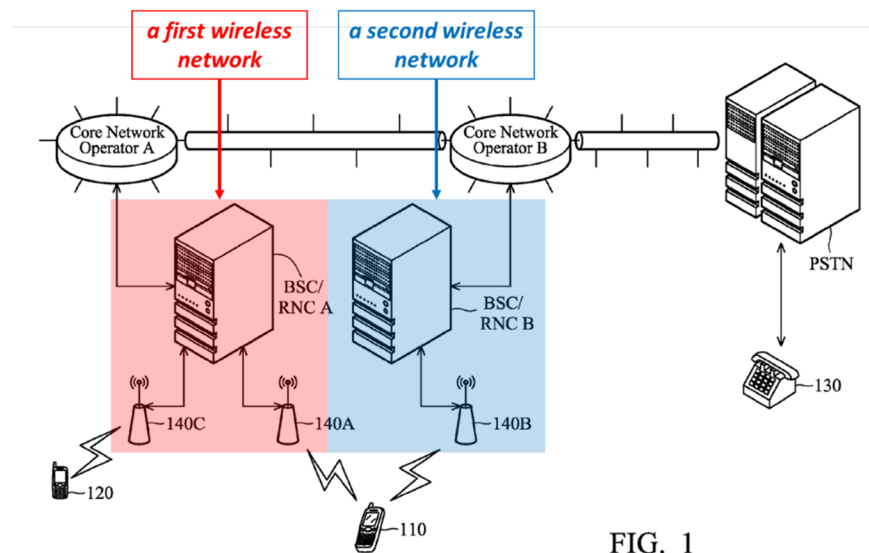


FIG. 1

SAMSUNG-1005, FIG. 1.

81. As discussed above in [1.2], Jheng’s USIMs are associated with a fare plan, to include a second fare plan for the second USIM (“*a second service plan*”). SAMSUNG-1005, ¶[0056]; *see above*, [1.2]. Additionally, as discussed above in [1.2], in the combination with Jheng, Chiu’s connection profiles would have been associated with and stored on a USIM including the selection criteria associated with the connection profile (“*the second service profile comprising a second set of*

network service policies”). SAMSUNG-1005, ¶¶[0050]-[0053]; SAMSUNG-1006, 4:19-5:15; *see above*, §IX.A, [1.2]. Also, as discussed above in [1.2], Jheng discloses that each USIM can be “provided by a particular network operator” (“*a second service profile associated with ... a second wireless network*”). SAMSUNG-1005, ¶¶[0033]-[0035], FIG. 1.

(ii) **Ground 1B Mapping**

82. As discussed above in [1.2], Rao’s priority policies are an additional example of “*network service policies*,” and in the combination, Rao’s policies, along with Chiu’s selection criteria, would have been included in Chiu’s connection profiles that are stored on Jheng’s USIMs, such that a second set of Rao’s policies stored on a second USIM are “*a second set of network service policies*.” SAMSUNG-1007, ¶¶[0099]-[0118], [0179], FIG. 1C; *see above*, [1.2].

83. Moreover, both sets of policies under the Ground 1A and 1B mappings perform substantially the same role and therefore the recitation of “first” and “second” does not produce an unexpected result.

[1.4] a connection manager to select an access network connection for the WWAN modem, based on a selected one of the first and second service profiles;

84. Jheng’s mobile station communicates over several types of WWAN networks, for example, GSM, GPRS, WCDMA, TDMA, TD-SCDMA, and other 3G networks. SAMSUNG-1005, ¶¶[0005], [0032]-[0033]; *see above*, [1.1]. his is

consistent with the '055 patent, which describes that “access networks” include “2G and/or 3G WWAN.” SAMSUNG-1001, 34:15-21.

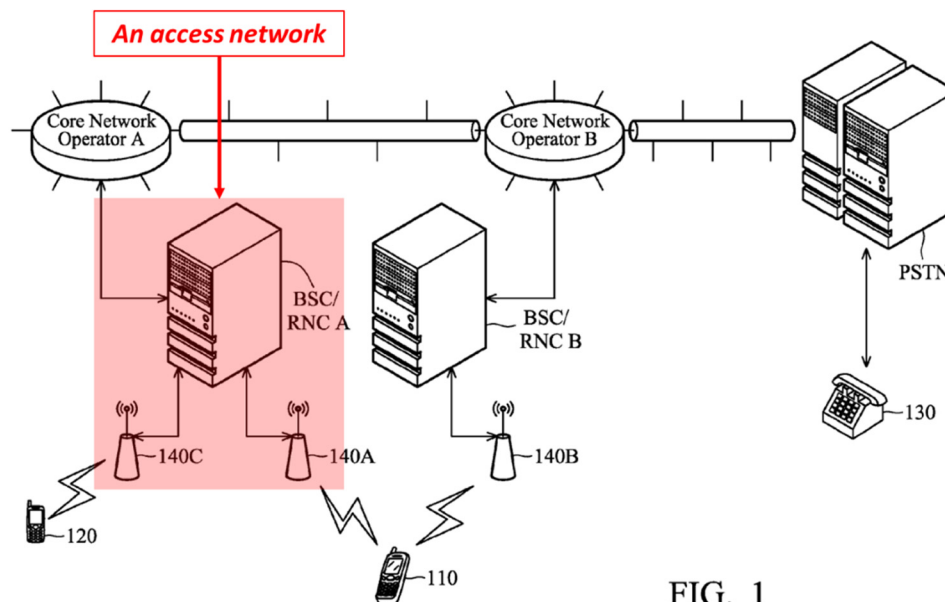


FIG. 1

SAMSUNG-1005, FIG. 1.

85. In the Jheng-Chiu system, Chiu’s connection manager would have first determined which USIM was not roaming (as taught by Jheng). SAMSUNG-1005, ¶¶[0050]-[0052]. Next, the non-roaming setting that only allows service (“MO voice or a data call, or transmitting an SMS message”) of a particular service profile in the USIM when the phone is not roaming would have been verified (“*a selected one of the first and second service profiles*”). SAMSUNG-1005, ¶¶[0050]-[0052], [0059]-[0060], FIGS. 4, 6, 9, 12-14; SAMSUNG-1006, 8:11-19.

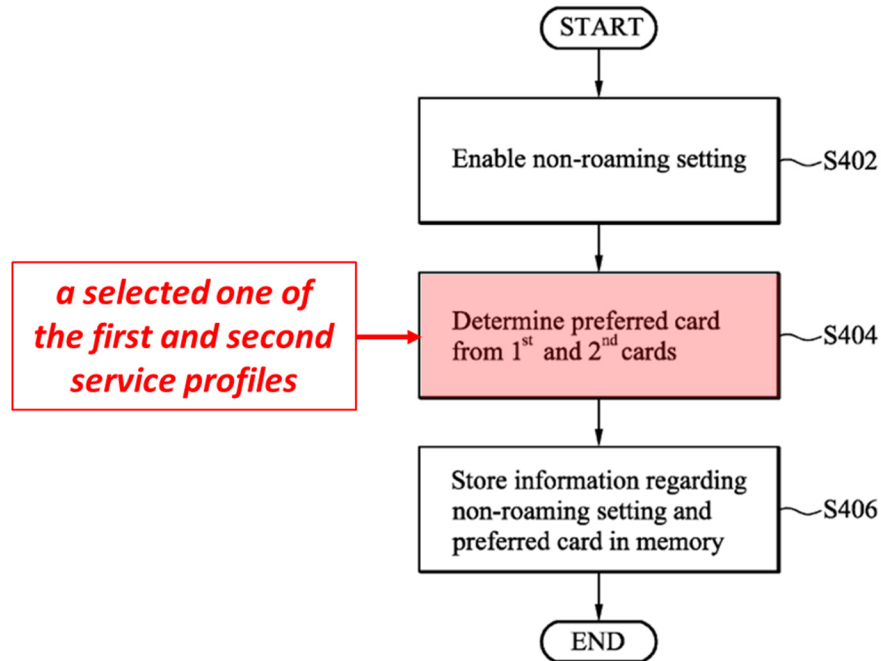
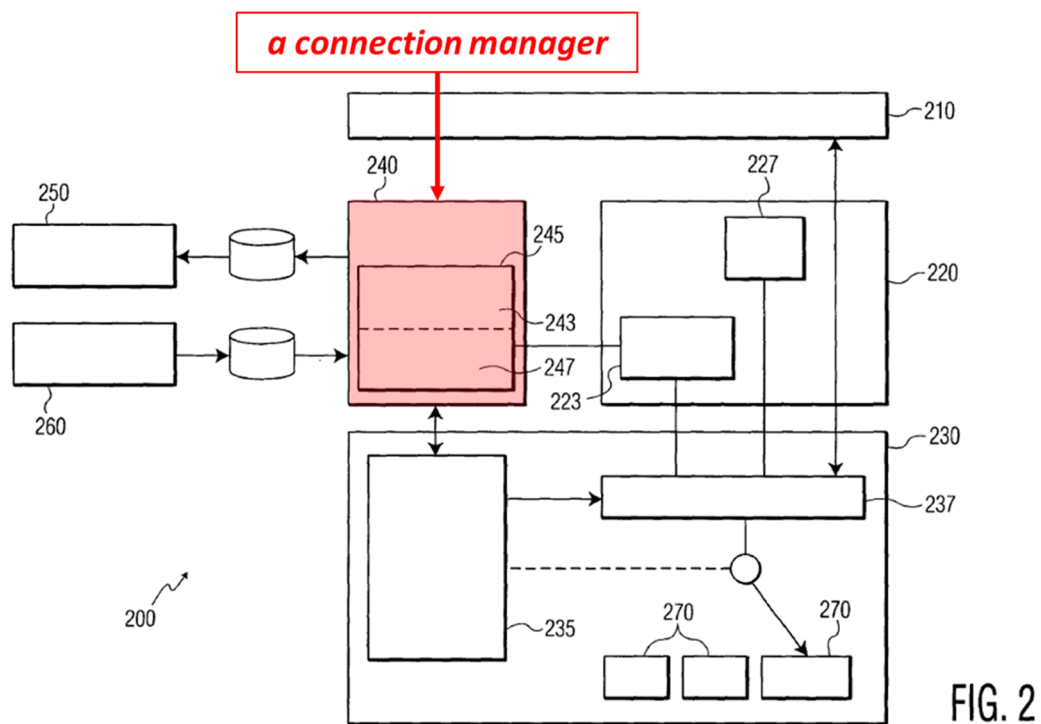


FIG. 4

SAMSUNG-1005, FIG. 4.

86. In addition to the non-roaming determination discussed above, Chiu’s connection manager monitors the status of available networks and selects the network connection that best satisfies the selection criteria of the connection profile (*“to select an access network connection based on a selected one of the first and second service profiles”*). SAMSUNG-1006, 4:29-5:2, 6:8-22, 10:16-20, 13:4-14:18, FIG. 2 (reproduced below). As discussed above in [1.2], connection profiles stored in USIMs (*“the first and second service profiles”*) include selection criteria (the “set of network service policies”) for connecting to a wireless network (*“an*

access network connection”) and would have been used by the connection manager to select an access a network connection (“*select an access network connection ... based on a selected one of the first and second service profiles*”). SAMSUNG-1006, 4:19-5:2, 5:30-6:7, 6:23-29, 7:22-27, 8:26-9:10, 9:25-10:11, 10:16-20, 14:7-18, FIG. 2; *above*, [1.2]. After selecting an access network connection, the connection manager provides instructions to the “wireless adaptation layer” to control the appropriate “network driver.” SAMSUNG-1006, 11:4-13, 11:31-12:18, FIG. 2.



SAMSUNG-1006, FIG. 2.

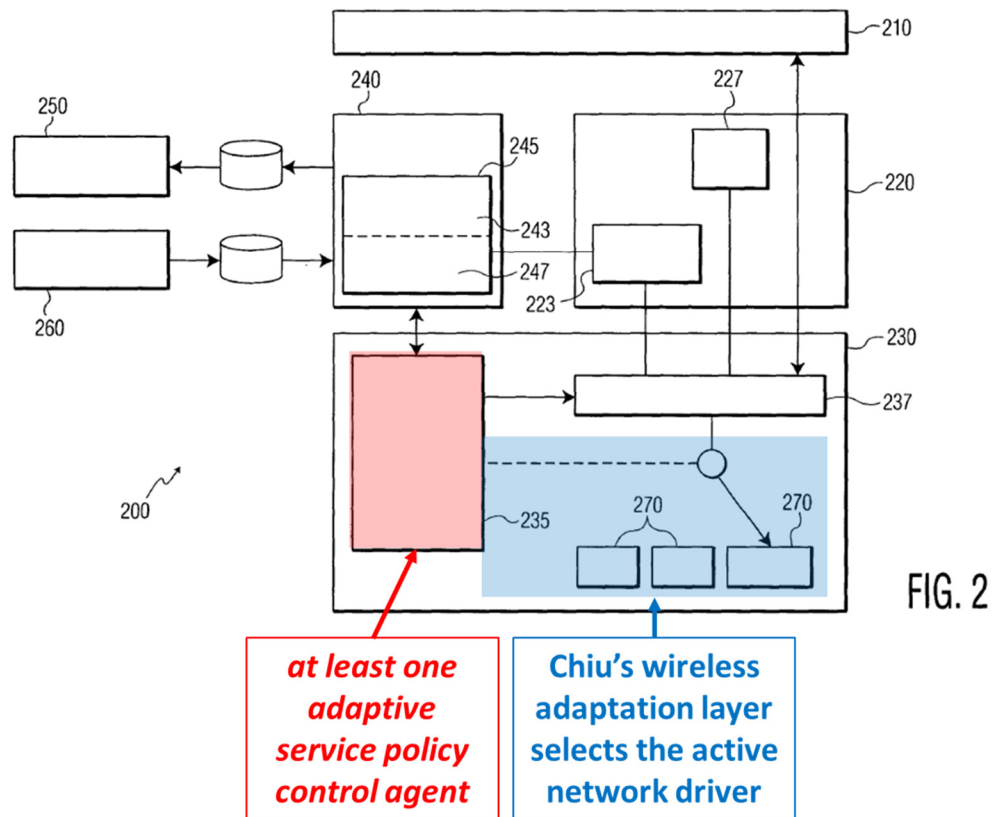
[1.5] at least one adaptive service policy control agent to enforce network service policies associated with the selected one of the first and second service profiles,

Ground 1A Mapping

87. Chiu discloses a “wireless adaptation layer” (“***at least one adaptive service policy control agent***”) that “switches data flow to the appropriate network driver” in response to instructions from the connection manager (“***to enforce network service policies associated with the selected one of the first and second service profiles***”). SAMSUNG-1006, 13:27-14:6. As discussed above in [1.4], the connection manager makes the selection of a network driver based on the selected connection profile and the associated selection criteria (“***the selected one of the first and second service profiles***”), and subsequently instructs the wireless adaptation layer to connect to the selected network using the appropriate network driver. SAMSUNG-1006, 4:29-5:2, 6:8-22, 10:16-20, 13:4-14:18; *see above*, [1.4]. Additionally, Chiu’s connection profiles include “configuration parameters” that are “network settings and user preferences for each network connection type” (“***network service policies associated with the selected one of the first and second service profiles***”). SAMSUNG-1006, 5:3-15. For example, configuration parameters can include “parameters for automatically controlling connection authentication” and “parameters for automatically performing IP tunneling negotiation” that are applied when connecting to a network (“***network service policies***”). *Id.* Chiu’s FIG. 2 below

illustrates the wireless adaptation layer's control of the network drivers.

SAMSUNG-1006, FIG. 2.



SAMSUNG-1006, FIG. 2.

Ground 2A Mapping

88. Rao provides an additional example of an “*adaptive service policy control agent*.” SAMSUNG-1007, ¶[0182]. Rao’s remote access client (“*at least one adaptive service policy control agent*”) enforces “one or more policies 520 for specifying client-side prioritization of network communications related to applications 338 a-338 n” (“*to enforce network service policies*”) by intercepting,

classifying, and filtering the application data traffic. SAMSUNG-1007, ¶[0182]. For instance, Rao’s policies can define “prioritization” based on criteria such as: “the name of the application,” “the type of application,” “the type of one or more protocols used by the application[s],” “the size of the payload of the network packet,” “whether an application is running in the foreground or the background of the client,” and/or “the destination network address, such as host name or IP address, and/or destination port number.” SAMSUNG-1007, ¶[0182]. In the combination, Rao’s policies would have been included in Chiu’s connection profiles (“*the selected one of the first and second service profiles*”) and stored on Jheng’s USIMs, thus enabling the network operator to define prioritization policies for specific applications by issuing a consumer a USIM pre-loaded with these policies (as recognized in the art before the ’055 Benefit Date, discussed above). SAMSUNG-1007, ¶¶[0109], [0179]-[0184]; SAMSUNG-1017, ¶¶[0043]-[0046], FIG. 2; *see above*, §IX.B. Rao’s remote access client would have then effectuated these policies on application data traffic between the application and the network stack. *Id.*

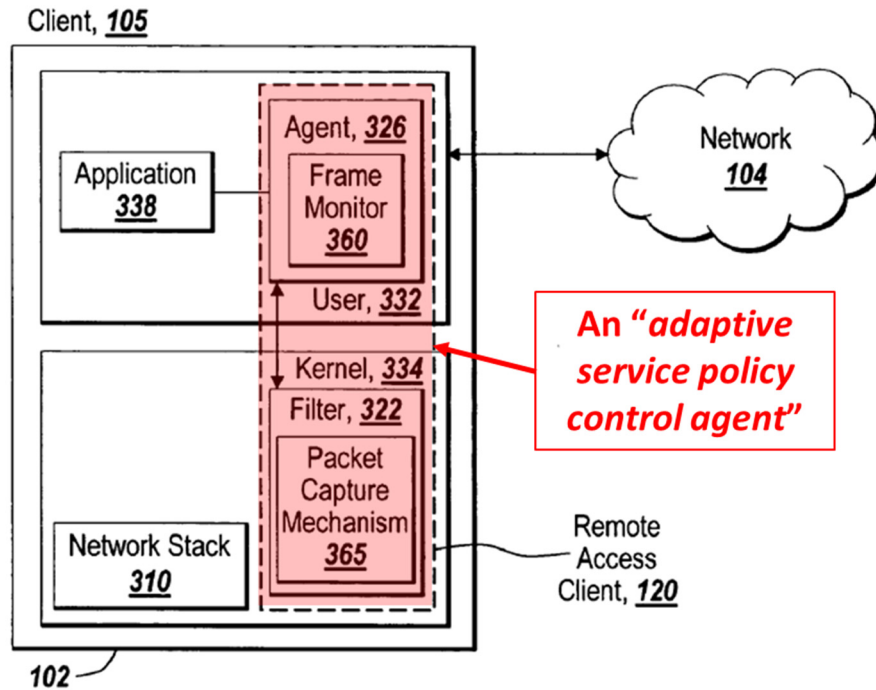


Fig. 1C

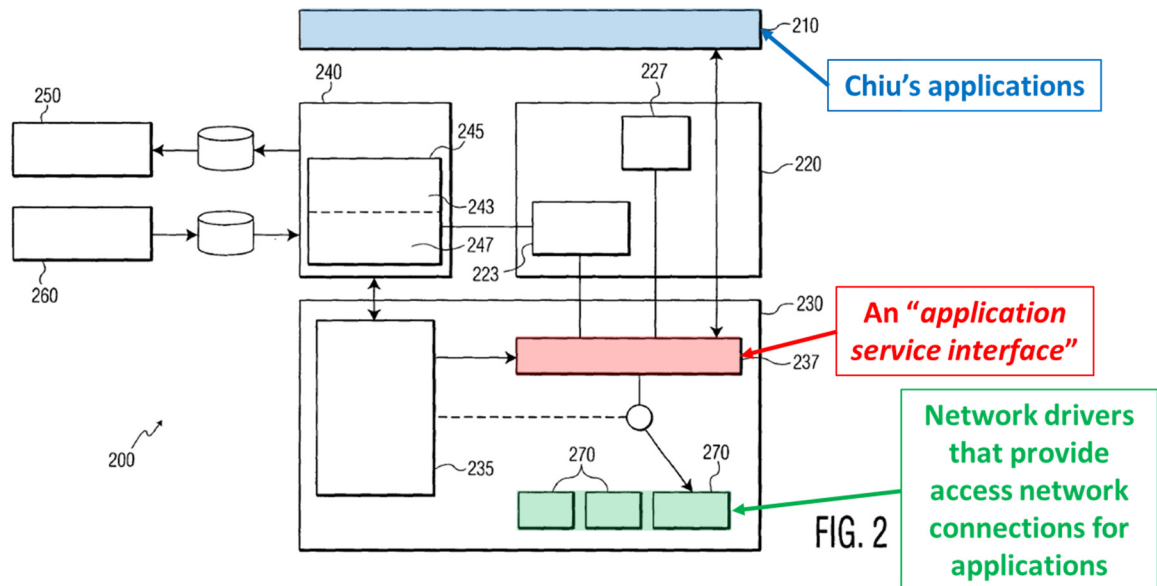
SAMSUNG-1007, FIG. 1C.

[1.6] the enforced network service policies including policies enforced at an application service interface on network data connections for selected applications resident on the device.

Ground 1A Mapping

89. Chiu's FIG. 2 (reproduced below) illustrates a wireless adaptation layer 325 controlling a tunneling interface 237 between applications 210 and network drivers 270. SAMSUNG-1006, FIG. 2. Chiu's tunneling interface ("an application service interface") is "exposed to the applications" on the device, "thereby enabling the network driver 270 to be dynamically changed without adversely affecting the application." SAMSUNG-1006, 13:9-13, 14:12-18, FIG. 2. The tunneling interface

provides “a seamless transition between network connections of a different connection type” when a connection profile requires a change of network based on its selection criteria. *Id.* Additionally, Chiu’s configuration parameters define network connection, which would have been applied at the tunneling interface (e.g., “parameters for automatically performing IP tunneling negotiation”) (“*policies enforced at an application service interface on network data connections*”). *Id.* Finally, because the applications access the selected access network through the tunneling interface, these connections are “*for selected applications resident on the device.*” *Id.* Chiu’s FIG. 2 illustrates the wireless adaptation layer controlling the tunneling interface between the applications and network drivers. SAMSUNG-1006, FIG. 2.



SAMSUNG-1006, FIG. 2.

Ground 2A Mapping

90. Rao provides an additional example of an “*application service interface*.” SAMSUNG-1007, ¶¶[0099]-[0118], FIG. 1C. Rao discloses a remote access client 120 (“*application service interface*”) with an agent 326 and filter 322 that intercept and classify data packets transmitted by applications in response to policies. SAMSUNG-1007, ¶¶[0099]-[0118], FIG. 1C. Rao’s remote access client 120 is positioned between the applications 338 and the network stack 310 and provides access to network connections (“*an application service interface on network data connections for selected applications resident on the device*”). *Id.*

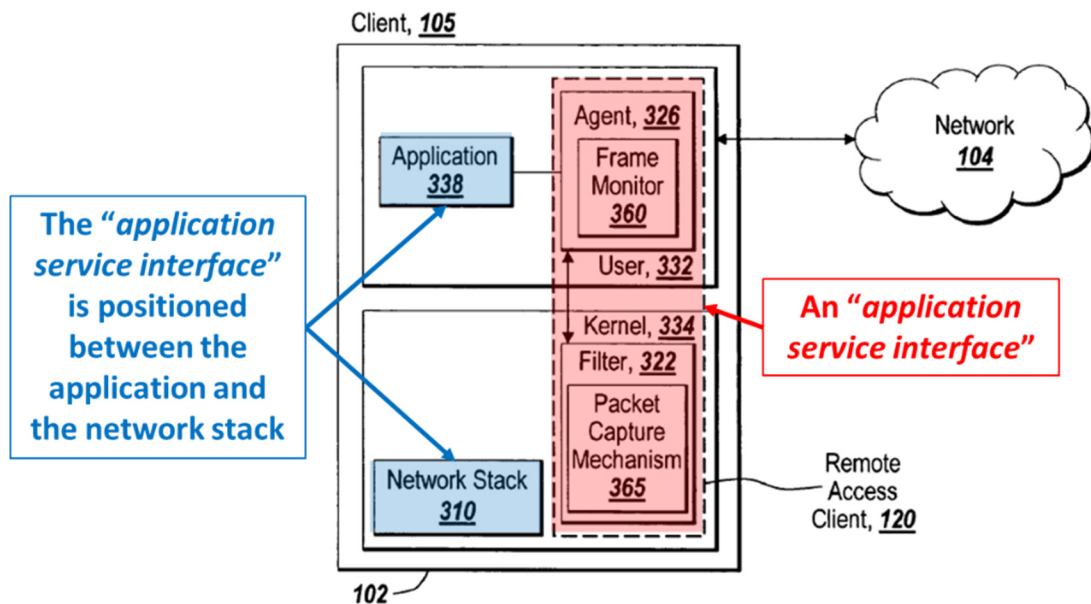


Fig. 1C

SAMSUNG-1001, FIG. 1C.

91. As discussed above in [1.2] and [1.5], Rao’s remote access client enforces “one or more policies 520 for specifying client-side prioritization of network communications related to applications 338 a-338 n” (“*policies enforced ... for selected applications resident on the device*”) by intercepting, classifying, and filtering the application data traffic (“*policies enforced at an application service interface on network data connections*”). SAMSUNG-1007, ¶[0182]. For instance, Rao’s policies can define “prioritization” based on criteria such as: “the name of the application,” “the type of application,” “the type of one or more protocols used by the application[s],” “the size of the payload of the network packet,” “whether an application is running in the foreground or the background of the client,” and/or “the destination network address, such as host name or IP address, and/or destination port number.” SAMSUNG-1007, ¶[0182].

92. Rao’s policies would have been included in Chiu’s connection profiles and stored on Jheng’s USIMs, thus enabling the network operator to define prioritization policies for specific applications by issuing a consumer a USIM pre-loaded with these policies (as recognized in the art before the ’055 Benefit Date, discussed above). SAMSUNG-1007, ¶¶[0109], [0179]-[0184]; SAMSUNG-1017, ¶¶[0043]-[0046], FIG. 2; *see above*, §IX.B. Rao’s remote access client would have then effectuated these policies on application data traffic between the application and the network stack (at “*an application service interface*”). *Id.*

[2.1] The wireless end-user device of claim 1, the first service profile further comprising first device credentials and the second service profile further comprising second device credentials,

93. The Jheng-Chiu combination, alone or in combination with Rao, render [2.1] obvious for multiple reasons, particularly in light of how broadly “credentials” are described by the ’055 patent. ’055 patent describes that “[t]he decision of whether or not to admit a device onto the femto cell can be made through the service processor 115 connection to the service controller 122 and subsequent look up of the credentials for the device and the associated service plan and service profile.” SAMSUNG-1001, 25:24-30. In particular, the ’055 patent describes credentials as including a “phone number,” a “device identification number,” a “security signature or other security credentials,” a “security key,” and “secure authorization information.” SAMSUNG-1001, 123:8-45.

94. Consistent with the ’055 patent, Jheng’s USIM card stores “a long-term pre-shared secret key K (‘security credentials’ or ‘security key’), which is shared with the Authentication Center (AuC) in the network” (“***the first service profile further comprising first device credentials and the second service profile further comprising second device credentials***”). SAMSUNG-1005, ¶[0030]; SAMSUNG-1001, 123:8-45; *see above*, [1.2]-[1.3]. A POSITA would have recognized and found obvious that the secret key K is used to authenticate both the USIM and mobile device when providing the mobile device access to the network (“***device***

credentials”). SAMSUNG-1014, 141; SAMSUNG-1015, 26-27. For example, 3GPP TS 31.102 explains that the secret key K is used by the network to generate an authentication token (a “random number,” or “RAND”) which is shared with the USIM. SAMSUNG-1014, 141; SAMSUNG-1015, 26-27. Using the secret key K, common to both the USIM and network, the USIM decrypts the random number and sends the response to the network (“SRES”) (sending “*device credentials*” to the network). *Id.* If the USIM successfully decrypts the random number (determined by the network also calculating a SRES value to which the USIM’s response is compared), the USIM and mobile device are authenticated. *Id.*

95. Additionally, each of the first and second USIMs in the mobile station include a secret key K (“*first device credentials and ... second device credentials*”). SAMSUNG-1005, ¶[0006], [0030], [0033]; *see above*, [1.3]. A POSITA would have found obvious that, in most cases, the first and second USIM would contain different credentials as different service providers used different keys for authentication. *Id.* For example, competing service providers would have used different secret keys in order to prevent outside users from accessing their networks (thus preventing “revenue leakage” by servicing outside users). SAMSUNG-1008, ¶[0038].

96. Jheng also discloses that USIMs include a unique “international mobile subscriber identity (IMSI)” (“device identification number”—“*first device*

credentials and ... second device credentials”), which Jheng explains “is a unique number associated with a global system for mobile communication (GSM) or a universal mobile telecommunications system (UMTS) network user.” SAMSUNG-1005, ¶¶[0029]-[0030], [0032], [0038], [0042], [0051]; SAMSUNG-1001, 123:8-45. A POSITA would have recognized and found obvious that IMSIs are credentials in the context of GSM and GPRS networks, where this identification is primarily used. SAMSUNG-1005, ¶[0005].

97. Finally, Jheng discloses that each USIM is associated with a different “telephone number,” which the ’055 patent explicitly lists as a credential (“*first device credentials and ... second device credentials*”). SAMSUNG-1005, ¶¶[0006], [0056], SAMSUNG-1001, 123:8-45.

[2.2] the wireless end-user device further comprising a device master agent credential that is independent of the first and second device credentials.

98. The ’055 patent describes that a “device master agent programs a unique credential in [a] device that cannot be re-programmed or removed (or is difficult to re-program or remove) and that can be recognized and recorded by the network at the time of activation or at some other time,” and that examples of this unique credential include “MEID, hardware MAC address, and/or serial number.” SAMSUNG-1001, 120:23-40. Jheng and Chiu (with or without Rao) render [2.2] obvious for multiple reasons.

99. First, Chiu discloses that devices have a “MAC[]Address”—an explicit example of a “*device master agent credential*” described by the ’055 patent. SAMSUNG-1006, 11:14-30. A MAC address is “*independent of the first and second device credentials*,” at least because the MAC address of a device are independent of the device’s USIM secret key, IMSI, and telephone number. SAMSUNG-1019, 31-33 (describing the MAC address as a “48-bit universal address” of hexadecimal code).

100. Second, Mobile Equipment Identifiers (“MEIDs”) (a “*device master agent credential*”) were well known before the ’055 Benefit Date for identifying a mobile station on a Code Division Multiple Access (“CDMA”) network—networks that are disclosed by Jheng. SAMSUNG-1005, ¶¶[0005], [0030]-[0031], [0033]. Accordingly, a POSITA would have found obvious that mobile stations communicating in a CDMA network (like Jheng’s) would have included a MEID for the purposes of identifying the device to the network. *Id.* This is particularly obvious because the use of MEID is established in 3GPP standard S.R0048-A. SAMSUNG-1018, 1-15. The MEID is a hexadecimal code that is independent of a device’s USIM secret key, IMSI, and telephone number (“*independent of the first and second device credentials*”). SAMSUNG-1018, 9. A POSITA would have been generally familiar with 3GPP publications, as they typically promulgate standards for WWANs (e.g., Global System for Mobile communications (“GSM”))

and General Packet Radio Service (“GPRS”) – also known as 2G and 2.5G, respectively). See, e.g., SAMSUNG-1014, 13, 103-104.

[6] The wireless end-user device of claim 1, further comprising a user service interface to allow a user to make a user selection between the first and second service profiles, the connection manager to, responsive to the user selection, select an access network connection for the WWAN modem.

101. Jheng discloses a man-machine interface (MMI) (“***a user service interface***”) that allows a user to make a manual selection that enables the non-roaming setting which “force[s] an [mobile originated] request to be issued to a called party via a cell (i.e. BSS, node-B or others) that a subscriber identity card camps on without roaming” (“***allow a user to make a user selection between the first and second service profiles***”). SAMSUNG-1005, ¶¶[0050], [0052], [0054]-[0055], [0057]-[0060], FIGS. 6, 9, 11.

102. As discussed above in [1.4], the connection manager would have selected a USIM (e.g., the non-roaming USIM) to connect to an access network, using the WWAN modem, after input is received from the user via the MMI (as disclosed by Jheng) (“***the connection manager to, responsive to the user selection, select an access network connection for the WWAN modem***”). SAMSUNG-1006, 4:29-5:2, 6:8-22, 10:16-20, 13:4-14:18; see above, [1.4]. By selecting one of the USIMs, the user effectively selects a corresponding service profile stored on the selected USIM (e.g., a “preferred subscriber identity card” selected “by the user

through interactions with the MMI”) and access network connection associated with the selected USIM (“a cell ... that a subscriber identity card camps on without roaming”). SAMSUNG-1005, ¶¶[0050], [0052], [0054]-[0055], [0057]-[0060], FIGS. 6, 9. The selection of the access network is “*responsive to*” the user selecting the particular USIM. *Id.*

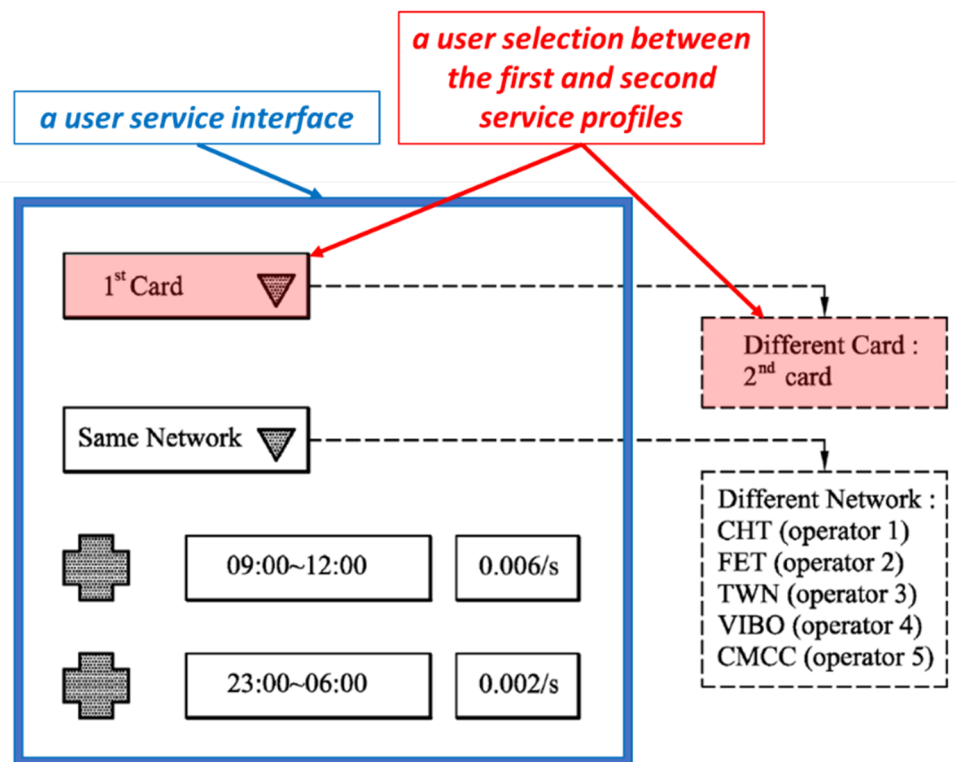


FIG. 11

SAMSUNG-1005, FIG. 11.

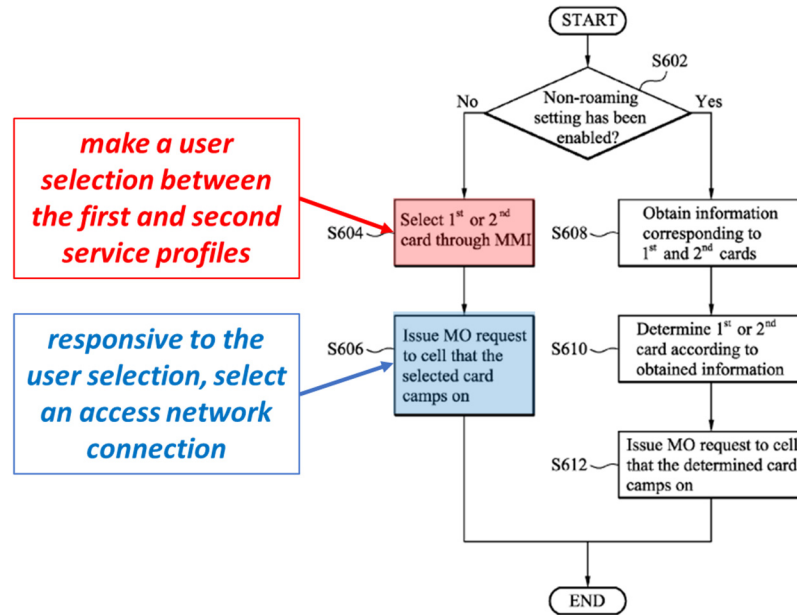


FIG. 6

SAMSUNG-1005, FIG. 6.

[7] The wireless end-user device of claim 1, further comprising a service notification and billing interface to display service usage options for each of the first and second service profiles.

103. Jheng's man-machine interface (MMI) ("***a service notification and billing interface***") is used by a user to enable the non-roaming setting which "force[s] an MO request to be issued to a called party via a cell (i.e. BSS, node-B or others) that a subscriber identity card camps on without roaming." SAMSUNG-1005, ¶¶[0050], [0052], [0054]-[0055], [0057]-[0060], FIGS. 6, 9, 11. "The MMI may comprise screen menus and icons, command language and online help displayed on a display of the mobile station with at least one input device." SAMSUNG-1005, ¶[0050]. Jheng's MMI displays available networks and billing information for those

networks, for each USIM, as illustrated below in FIG. 11 (“*display service usage options for each of the first and second service profiles*”). SAMSUNG-1005, ¶¶[0050], [0056]-[0057], FIG. 11.

104. Additionally, Chiu’s profile database allows a user to browse available connection profiles on their mobile station, and to allow the user to fine-tune a profile prior to downloading (thus displaying “*service usage options*” for these connection profiles). SAMSUNG-1006, 8:26-9:10. In the combination, Jheng’s MMI would have been modified to incorporate Chiu’s functionality of displaying available connection profiles stored in a profile database, and further would have allowed the user to modify these profiles, as taught by Chiu. SAMSUNG-1005, ¶¶[0050], [0052], [0054]-[0055], [0057]-[0060], FIGS. 6, 9, 11; SAMSUNG-1006, 8:26-9:10. Thus, Chiu’s teachings provide another example of “*a service notification and billing interface*.” SAMSUNG-1006, 8:26-9:10.

105. To the extent it is argued that the “*service notification and billing interface*” must display “*billing*” information (which is not required by [7]), Jheng’s MMI displays such information, as illustrated below in FIG. 10 (“0.006/s” for service between “0:900-12:00”). SAMSUNG-1005, ¶¶[0056]-[0057], FIG. 10. A POSITA would have understood that “*billing*” messages encompass *service notification and billing* information regarding a service bill including the rate at which service charges are applied (e.g., 0.006/s) (“the network operator may send

an Advice of Charge (AOC) message regarding call cost per unit time to the mobile station for the ongoing MO call”). Chiu similarly discloses that its selection criteria include “billing information.” SAMSUNG-1006, 8:11-17.

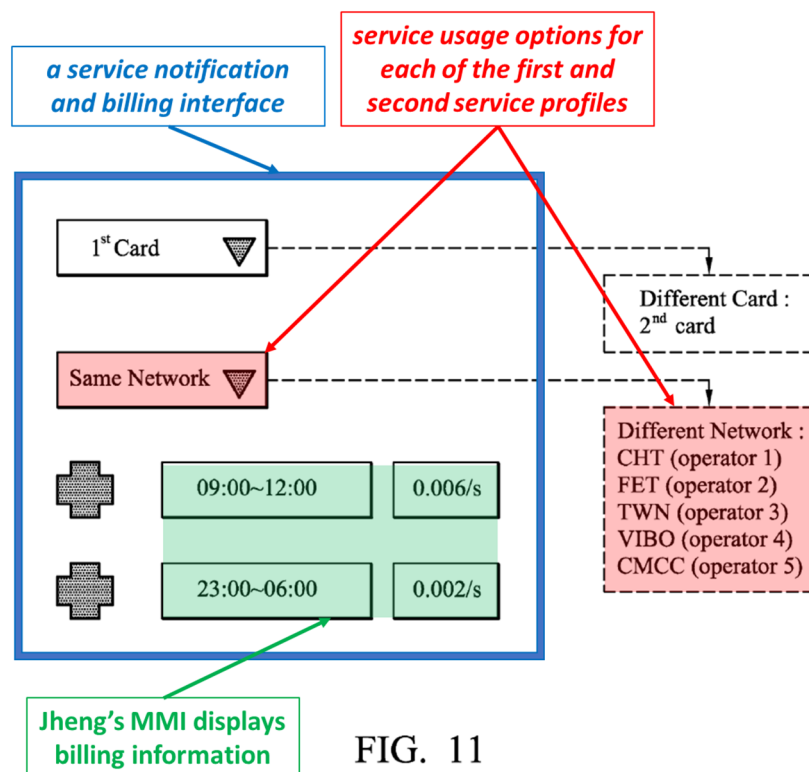


FIG. 11

SAMSUNG-1005, FIG. 11.

[9] The wireless end-user device of claim 1, wherein the at least one adaptive service policy control agent detects network connection changes from the first wireless network to the second wireless network, and in response enforces the second set of network service policies.

Ground 1A Mapping

106. Chiu’s connection manager can detect “[i]f the selected network connection ceases to satisfy the selection criteria,” (e.g., “a link quality of the selected network connection, cumulative access fees associated with the selected

network connection, an amount of time that the selected network connection has been activated, a location of the portable device, or a remaining battery capacity of the portable device”) and in response, “activate a new network connection” (*“changes from the first wireless network to the second wireless network”*). SAMSUNG-1006, 6:8-22. Chiu’s wireless adaptation layer (*“at least one adaptive service policy control agent”*) “switches data flow to the appropriate network driver 270” in response to instructions from the connection manager. SAMSUNG-1006, 13:27-14:6. As discussed above in [1.4], upon receiving an indication that the selected network no longer satisfies the selection criteria, the connection manager would have subsequently instructed the wireless adaptation layer to select a new network driver corresponding to the network service policies of the new network and associated USIM (e.g., the selection criteria and configuration parameters of the connection profile) (*“in response enforces the second set of network service policies”*). *Id.* For example, Chiu describes that the selection criteria of a connection profile can be based on the “location of the portable device,” “link quality,” and “billing information,” among other things. SAMSUNG-1006, 8:11-25. For a user that is traveling and encountering different networks, the location of the portable device would have determined the available networks to the device, and thus, determined which connection profile is appropriate for that network. *Id.* Similarly, a user that encounters a more expensive roaming network while traveling would

have triggered the selection of a roaming connection profile that would have provided service in the roaming network at local rates. *Id.*

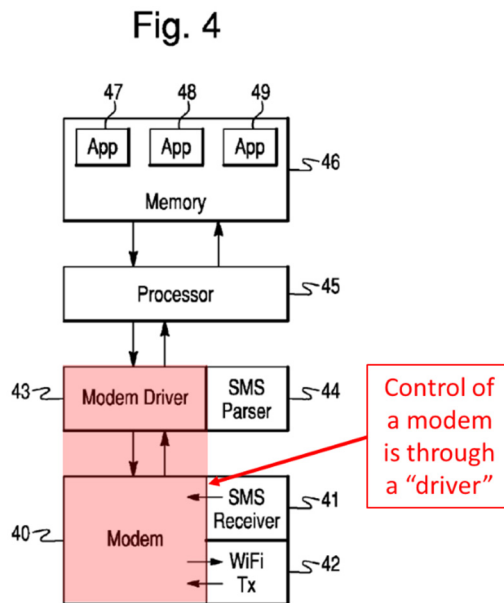
Ground 2A Mapping

107. As discussed above in [1.5], Rao’s remote access client (“***at least one adaptive service policy control agent***”) enforces “one or more policies 520 for specifying client-side prioritization of network communications related to applications 338 a-338 n.” SAMSUNG-1007, ¶[0182]. Rao’s remote access client detects a change in network when the client device “moves from a first wireless network to a second wireless network” (“***detects network connection changes from the first wireless network to the second wireless network***”). SAMSUNG-1007, ¶[0217]. A POSITA would have recognized and found obvious that the remote access client would have “***enforce[d] the second set of network service policies***” after switching to the second wireless network, because as discussed above in [1.3], Rao’s “***second set of network service policies***” would have been particular to the “***second wireless network.***” SAMSUNG-1007, ¶¶[0099]-[0118], [0179], FIG. 1C.

[10] The wireless end-user device of claim 1, wherein the connection manager further comprises a modem selection and control layer that routes certain types of data traffic to the first wireless network and other types of data traffic to the second wireless network.

108. It would have been obvious to a POSITA that Chiu’s drivers provided operational control of network interfaces (e.g., modems) because network drivers were used to control wireless modems in wireless devices. SAMSUNG-1024,

¶¶[0035]-[0039], FIG. 4. For example, the prior art reference, Papineau, explains that modems “communicate with [a] processor 45 through a modem driver 43” and that “[d]ata and instructions intended for the modem are sent to the modem driver 43 which formats the data and instructions in a manner suitable for the modem 40.”
Id.



SAMSUNG-1024, FIG. 4.

109. Chiu’s data link control layer 230 (“*a modem selection and control layer*”) includes the wireless adaptation layer that “switches data flow to the appropriate network driver 270” (“*modem selection*”) in response to instructions from the connection manager (“*routes ... data traffic to the first wireless network and ... the second wireless network*”). SAMSUNG-1006, 13:27-14:6, FIG.2 (reproduced below). As depicted in FIG. 2, the combination device included

multiple drivers 270, which would have each controlled a separate modem. *Id.* For example, Rao discloses that devices can include network interfaces for different network types, to include a “Local Area Network (LAN)” and a “Wide Area Network (WAN),” indicating that multiple modems would have been included in the combination device to allow for connection to these networks (e.g., a WWAN modem and a WLAN modem). SAMSUNG-1007, ¶[0125]. Similarly, Chiu also describes that its devices connect to a plurality of network types (e.g., “WWAN” and “WLAN”). SAMSUNG-1006, 7:17-22, 9:25-10:11.

110. Additionally, the data link control layer 230 includes the network drivers that a POSITA would have recognized and found obvious provided operational control of the WWAN modem (“*modem ... control*”). SAMSUNG-1024, ¶¶[0035]-[0039], FIG. 4; *see below*, [12].

111. It would have been an obvious design choice for a POSITA to place the “*modem selection and control layer*” within the “*connection manager*” as the connection manager controls the operation of the data link control layer 230 in selecting a suitable network driver for network connection. SAMSUNG-1006, 7:17-22, 9:25-10:11, 13:27-14:6. For example, this arrangement would have realized efficiencies within the combination device, allowing the connection manager to select a network connection by directly communicating with the appropriate interface (e.g., a modem). *Id.* The ability of a connection manager to directly

interface with modems on a wireless device was also known before the Benefit Date, corroborating that this design choice was used in the art. SAMSUNG-1016, ¶¶[0035]-[0036], FIG. 2 (disclosing a connection manager that manages “communication interfaces” that can be a “WWAN modem”).

112. Additionally, it would have been obvious to a POSITA that the “*modem selection and control layer*” can be placed in various suitable locations, e.g., outside or within the “*connection manager*” because the function of the “*modem selection and control layer*” would be the same regardless of whether it is placed inside of or connected to the connection manager. Indeed, placing the “*modem selection and control layer*” within the connection manager has no patentable weight as this would have been the mere rearrangement of known parts without any functional change in the operation of those parts (e.g., placing the known “*modem selection and control layer*” in a “*connection manager*” where the modem selection and control layer performs its same functions). SAMSUNG-1006, 13:4-13. Using a “*connection manager*” to control and select modems was known in the art before the Benefit Date, and would have been known to a POSITA. SAMSUNG-1016, ¶¶[0035]-[0036], FIG. 2.

113. Further, a POSITA would have understood and found obvious that the application of policies would have been based, at least in part, on the “*type of data*” being communicated (and thus, the routing of data by the wireless adaptation layer).

SAMSUNG-1017, ¶¶[0043]-[0046], FIG. 2. For example, Landschaft discloses a dual SIM phone where applications are assigned to a particular SIM (e.g., “SMS” to “SIM 2”). *Id.* The need to delegate certain “*type[s]*” of traffic to particular networks to avoid unacceptable resource consumption while roaming was also well known in the art (e.g., performing data-intensive activities on a non-roaming network). SAMSUNG-1016, ¶¶[0088]-[0089]. For example, Cole describes a scenario where a file synchronization is usually performed on a local network, and completion of this activity is deferred until an equivalent network becomes available. SAMSUNG-1016, ¶[0089]. Cole provides another example where a data intensive activity performed on a public WWAN is deferred until a local network is encountered. SAMSUNG-1016, ¶[0088].

FIG. 2

SIM SELECTION BY TYPE OF COMMUNICATION TASK	
PHONE CALL	BY GROUP
SMS	SIM 2
E-MAIL	SIM 1
INTERNET ACCESS	SIM 1

200 {

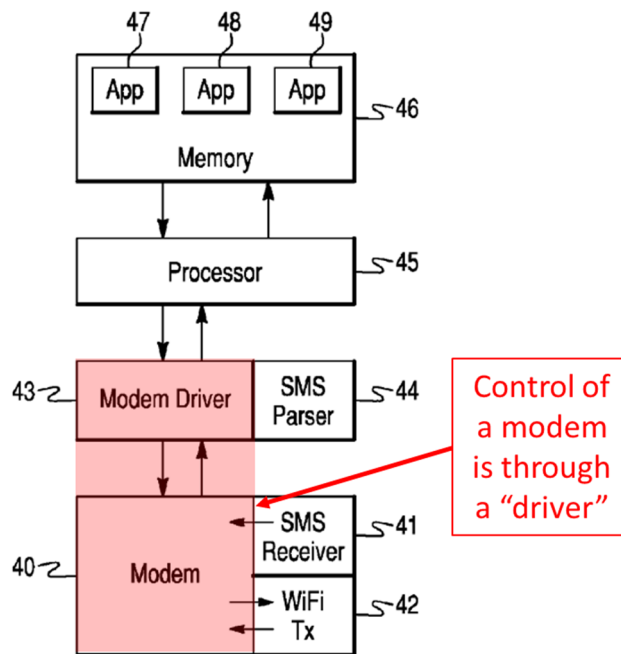
Applications are assigned to a SIM

SAMSUNG-1017, FIG. 2.

[12] The wireless end-user device of claim 1, the connection manager configured to prompt the WWAN modem to connect to a selected access network and send credentials associated with the selected one of the first and second service profiles to the selected access network.

114. Chiu's connection manager scans available networks, and once a network connection is selected, the connection manager "uses its stored profile to activate the detected connection using the network configuration information associated with the connection type of the available network connection." SAMSUNG-1006, 13:27-14:6. Recall from [2.1] that USIMs and connection profiles are associated with credentials (e.g., a "secret key K"). SAMSUNG-1005, ¶[0030]; *see above*, [2.1]. Once a selection has been made, the connection manager 240 "communicates this information to the wireless adaptation layer 235 which switches data flow to the appropriate network driver 270." *Id.* By selecting the appropriate network driver, Chiu's connection manager "***prompt[s] the WWAN modem to connect to a selected access network.***" SAMSUNG-1006, 13:27-14:6; SAMSUNG-1024, ¶¶[0035]-[0039], FIG. 4. As shown in FIG. 4 below, the modem driver "provide[s] a data and command interface between the processor 45 and the modem 40." *Id.*

Fig. 4



SAMSUNG-1024, FIG. 4.

115. A POSITA would have recognized and found obvious that the network driver provided operational control of the WWAN modem because network drivers were used to control wireless modems in wireless devices. SAMSUNG-1024, ¶¶[0035]-[0039], FIG. 4. Indeed, Papineau explains that modems “communicate with [a] processor 45 through a modem driver 43” and that “[d]ata and instructions intended for the modem are sent to the modem driver 43 which formats the data and instructions in a manner suitable for the modem 40.” *Id.*

116. Additionally, Jheng’s “secret key K” which is “available only to the USIM and the AuC” is used to generate an authentication token that is transmitted and used to authenticate the mobile station to the network upon connection.

SAMSUNG-1005, ¶[0030]; SAMSUNG-1014, 141. Thus, and as discussed above in [1.2], a POSITA would have recognized and found obvious that “*credentials associated with the selected one of the first and second service profiles*” would have been sent to the “*selected access network*” by the connection manager as this would have been part of the device’s mutual authentication with the network. SAMSUNG-1005, ¶[0030]; SAMSUNG-1014, 141. For example, Jheng’s “secret key K” which is “available only to the USIM and the AuC” is used to authenticate the mobile station to the network upon connection. SAMSUNG-1005, ¶[0030]; SAMSUNG-1014, 141.

X. GROUND 1B/2B: CLAIMS 3-4 ARE OBVIOUS OVER JHENG IN VIEW OF CHIU AND COLLINS (WITH OR WITHOUT RAO)

A. The combination of Jheng, Chiu, and Collins (with or without Rao)

117. It would have been obvious to a POSITA to combine the teachings of Jheng-Chiu/Jheng-Chiu-Rao (hereinafter collectively referred to as the “**JCR system**”) and Collins to incorporate Collins’ techniques of monitoring data usage and synchronizing or providing data usage information from the TIC to the CIS for at least the reasons noted below. SAMSUNG-1008, ¶¶[0025], [0035]-[0045], [0049]-[0050], FIGS. 1-3.

118. First, Collins’ techniques enhance the security of JCR’s wireless network. For example, Collins provides a means to alert a service provider to fraud

and security issues, which would have beneficially minimized security risks and reduced potential loss of revenue. SAMSUNG-1008, ¶¶[0012], [0016], [0038], [0042]-[0045], [0047], [0065], [0090]-[0091]. Collins discloses that the CIS can detect “fraudulent use pattern[s]” by comparing the TIC reported usage with usage identified by the network operator. SAMSUNG-1008, ¶¶[0129]-[0130]. By continually synchronizing usage between a device and the network operator, the CIS can timely alert the operator to indications of fraud (e.g., the cloning of SIM credentials). *Id.*

119. Second, Collins’ techniques of monitoring data usage would have provided implementation details for determining billing related to the data usage of the combination device, as disclosed by Jheng. SAMSUNG-1005, ¶[0057]; SAMSUNG-1008, ¶¶[0025], [0037], [0039], [0041], [0049]-[0050], FIGS. 1, 3. For example, Collins’ techniques provide a means for determining data usage local to the device, similar to Jheng, and the monitoring data usage with a remote CIS would help ensure accurate billing for data usage in the JCR system. SAMSUNG-1008, ¶¶[0025], [0035]-[0045], [0049]-[0050], FIGS. 1-3.

120. Jheng, Chiu, Rao and Collins are analogous art to the ’055 patent, which is generally directed to “a services policy communication system and method” for controlling wireless network usage by a mobile device in a wireless network. SAMSUNG-1001, Abstract, 8:44-67, 48:47-49:13, 82:54-59. Indeed, Jheng

generally describes transmitting “mobile originated (MO) request[s] by a mobile station with a first subscriber identity card and a second subscriber identity card,” Chiu generally describes “systems and methods for providing smart connection management of portable devices within a network communication system,” Rao generally describes “a remote access architecture for providing peer-to-peer communications and remote access connectivity,” and Collins generally describes a “risk control system that is used to control communications systems, such as mobile radio telephone, fixed digital communications, internet peer-to-peer communications and other systems, features and services.” SAMSUNG-1005, ¶¶0007]; SAMSUNG-1006, 1:1-4; SAMSUNG-1007, Abstract, ¶¶0004]; SAMSUNG-1008, Abstract, ¶¶0001]. Accordingly, the prior art references are all directed to the same field of wireless network communications. *Id.*

121. Additionally, as explained below in more detail, combining Jheng-Chiu/Jheng-Chiu-Rao and Collins would have been obvious at least because such a combination would have merely involved (1) combining prior art elements according to known methods to yield predictable results; and the (2) use of known techniques to improve similar devices in the same way.

122. Incorporating Collins’ data usage provision techniques into the dual-SIM phone or USIMs in the JCR system would have been predictable and foreseeable with a reasonable expectation of success at least because Collins’s TIC

application “can reside in ...[a] secure storage device (SIM/USIM or similar).” SAMSUNG-1008, ¶¶[0011]-[0022], [0039]; SAMSUNG-1005, ¶[0030]. Further, Collins discloses that its methods can be used in a “dual-SIM terminal,” such as Jheng’s mobile device. SAMSUNG-1008, ¶[0126], FIG. 4.

123. The combination of Collins with the JCR system would also have been predictable because Jheng discloses similar functionality (e.g., analyzing the charging information) to Collins’ TIC suggesting that the Jheng dual-SIM phone would have modified to implement local data usage monitoring, as taught by Collins, through routine skill of one in the art. SAMSUNG-1005, ¶[0057]. Indeed, the implementation of Collins’ data usage synchronization techniques would have involved only routine coding ability that would have been well within a POSITA’s capability (e.g., coding the functions of Collins’ TIC and CIS as machine readable code to be executed by the combination device’s processors). For example, the TIC would have been capable of being embodied as executable functions that provide an output (e.g., incrementing a service count) in response to a detected input (e.g., the detection of transmitted data). It would have been well within the ability of POSITA to code such functions, as a POSITA would have been exposed to various suitable programming languages throughout their education. *See above*, §IV. Collins itself corroborates the ability to embody the TIC as executable code (e.g., “Java,” which

would have been within a POSITA's general knowledge). SAMSUNG-1007, ¶[0039]; *see also id.*

124. Further, logging service data was well known before the '055 Benefit Date, as evidenced by other publications. SAMSUNG-1023, 189-191. For example, the Symbian operating system logged services used by the device to determine data consumption. SAMSUNG-1023, 189-191.

B. Analysis

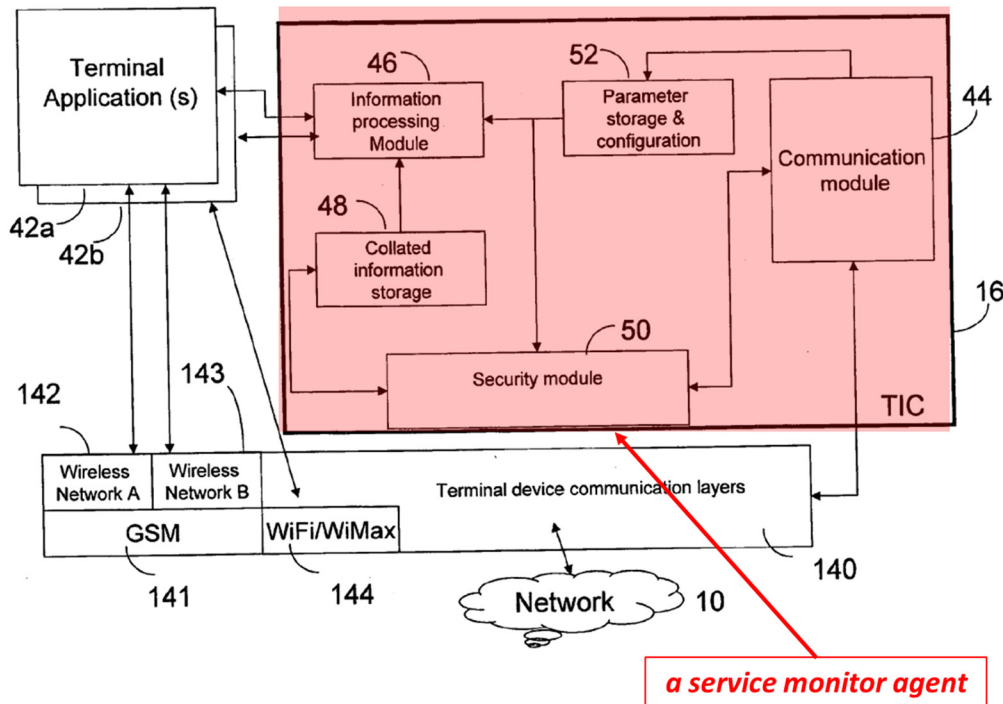
[3] The wireless end-user device of claim 1, further comprising a service monitor agent to record network service usage categorized by sub-account for different wireless networks, including separate service usage counts associated with each of the first service plan and the second service plan.

125. The '055 patent describes that a “service monitor agent 1696 maintains a history and provides reports or summary reports of which networks in addition to the networks controlled by the service controller 122 to which the device has connected.” SAMSUNG-1001, 55:54-56:8. Also, “[i]n some embodiments,” the service monitor agent monitors “application usage,” “multimedia file usage,” “the device user interface, application, and content discovery history,” and “advertisements provided to the user on the device 100.” SAMSUNG-1001, 56:9-43. Further, the '055 patent describes that “[a]s will be appreciated by those of ordinary skill in the art, the service monitor agent 1696 can monitor a wide variety of activities performed by the device/user of the device and/or based on other

information related to the device 100.” *Id.* Accordingly, the feature “*a service monitor agent to record network service usage*” should be interpreted to include at least one of the aforementioned examples. SAMSUNG-1001, 55:54-56:43.

126. Collins’ Terminal Information Collector (TIC) 16 collects usage information relating to “each activity or session that occurs through the network,” for example, “URLs of websites visited” and “addresses and sizes of received and sent SMS messages” (e.g., at least network and application usage (“*network service usage*”)). SAMSUNG-1008, ¶¶[0025], [0037], [0039], [0041], [0049]-[0050], [0120]-[0123], FIGS. 1, 3-4 (FIG. 4 reproduced below depicting a TIC collecting usage information for a plurality of networks). A POSITA would have understood that Collins’ TIC 16 is an agent that monitors network service and thus would have rendered obvious a “*service monitor agent.*”

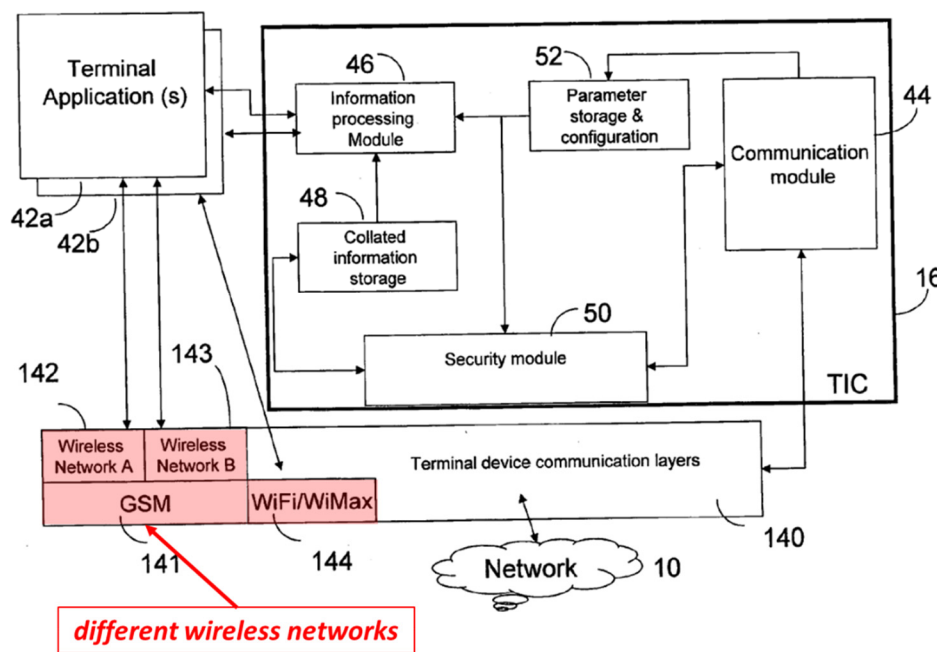
FIG 4.



SAMSUNG-1008, FIG. 4.

127. Collins discloses that each network is associated with an operator which has a central information server (CIS) that receives usage information from each device's TIC. SAMSUNG-1008, ¶¶[0035]-[0045], FIG. 2. The usage information is collected for *each* network, for example, “a GSM layer 141 and a WiFi/WiMax 144” (“*usage categorized by sub-account for different wireless networks*”). SAMSUNG-1008, ¶¶[0120]-[0127], FIG. 4 (reproduced below). Accordingly, it would have been obvious to a POSITA that each user's account would have a sub-account that records the usage information for the user for a particular wireless network.

FIG 4.



SAMSUNG-1008, FIG. 4.

128. Collins explains that distinguishing networks is important for “revenue assurance arbitrage,” such that an operator can determine that “that [its] service, although available, is not being selected.” *Id.* Further, Collins’s methods can be used in a “dual-SIM terminal” (e.g., JCR’s mobile station) that includes a TIC for each network operator. SAMSUNG-1008, ¶[0126]. And recall from [1.2] and [1.3], that each USIM is associated with a fare plan. SAMSUNG-1005, ¶¶[0056]-[0060], FIG. 10; Because each USIM and service plan is associated with an operator and each TIC reports usage associated with its network and USIM to the appropriate network operator, it would have been obvious to a POSITA that JCR+Collins renders obvious “*usage categorized by sub-account ... including separate service*

usage counts associated with each of the first service plan and the second service plan". SAMSUNG-1008, ¶¶[0058]-[0060], [0064] (describing that the TIC "collate[s] the information in counters" on the device, an aggregation of total service usage (a "*count*")), [0126], FIG. 4.

[4] The wireless end-user device of claim 3, wherein for at least one of the first and second service plans, the wireless end-user device synchronizes a local service usage count with a network-based service count.

129. As discussed above in [3], Collins discloses that each network is associated with an operator which has a CIS that receives usage information from each device's TIC. SAMSUNG-1008, ¶¶[0008], [0035]-[0045], [0061], [0092], FIG. 2. Each TIC reports "information relating to each activity or session that occurs through the network" ("*a local service usage count*") to the CIS, which records the information ("*a network-based service count*"). SAMSUNG-1008, ¶¶[0041]-[0048], [0058]-[0060], [0064]. In Collins, the information collected by the TIS and associated CIS is synchronized to determine their similarity, and to the extent the consumption of data differs between the TIS and its associated CIS, "the CIS can raise an event alarm" ("*the wireless end-user device synchronizes a local service usage count with a network-based service count*"—the TIC reporting to the CIS). SAMSUNG-1008, ¶[0092]. Collins explains that the synchronization of data between the TIC and CIS is important for "fraud detection, revenue assurance and legal interception," which were all known concerns in wireless networks that would

have been obvious to address through synchronization before the '055 Benefit Date. *Id.* Additionally, as explained in [3] above, each USIM has a TIC, and therefore Collins' techniques would have been performed “*for at least one of the first and second service plans.*” SAMSUNG-1008, ¶¶[0120]-[0127], FIG. 4; *see above*, [3].

XI. GROUND 1C/2C: CLAIM 5 IS OBVIOUS OVER JHENG IN VIEW OF CHIU AND CAMILLERI (WITH OR WITHOUT RAO)

A. The combination of Jheng, Chiu, and Camilleri (with or without Rao)

130. It would have been obvious to a POSITA to combine the teachings of Camilleri with the JCR system such that a PAM integrated into each of the device USIMs would switch the USIMs between LS and RS sub-modules, and at least one USIM sub-module in the dual-SIM combination device would have been associated with a MVNO for at least the reasons noted below. SAMSUNG-1005, ¶[0033], FIG. 1; SAMSUNG-1009, ¶¶[0040]-[0048].

131. First, Camilleri's PAM and SIM sub-modules would have increased the versatility of the USIMs of the JCR dual-SIM phone by allowing a user to combine multiple sets of SIM parameters into a single USIM (e.g., RS and LS sub-modules). SAMSUNG-1009, ¶¶[0041]-[0046]. Configuring USIMs to store multiple SIM sub-modules would have allowed the user to configure their device for more networks than would have been possible without these sub-modules (e.g., a dual-SIM device would have been able to be configured for four networks). *Id.*

132. Second, MVNOs “introduc[e] more competition in the wireless and/or cellular marketplace, greatly benefiting end-users” by facilitating “more competitive lower pricing” e.g., through lower international call tariffs and roaming charges. SAMSUNG-1009, ¶¶[0044], [0047]. To ensure that the JCR device would remain competitive in a world with MVNOs that provide comparable service to the consumer at a lower cost, the techniques of the combination device would have been made to be compatible with these MVNOs. *Id.* Due to the emergence of these network operators, a POSITA would have reasonably expected that at least one MVNO would have issued a SIM to a customer using the JCR device. *Id.*

133. Third, a POSITA would have been motivated to include MVNO compatibility (e.g., the ability to use a USIM issued by a MVNO) in the JCR system because such a modification would have resulted in additional revenue for the operators of core networks associated with these MVNOs. For example, Thanh discloses that the “MVNO has to pay to the [Mobile Network Operator (MNO)] for both outgoing and incoming calls.” SAMSUNG-1022, 3-5. The MNO would have been able to negotiate favorable terms as the MVNO “may rely almost totally on the MNO’s facilities.” *Id.*

134. Jheng, Chiu, Rao, and Camilleri are analogous art to the ’055 patent, which is generally directed to “a services policy communication system and method” for controlling wireless network usage by a mobile device in a wireless network.

SAMSUNG-1001, Abstract, 8:44-67, 48:47-49:13, 82:54-59. Indeed, Jheng generally describes transmitting “mobile originated (MO) request[s] by a mobile station with a first subscriber identity card and a second subscriber identity card,” Chiu generally describes “systems and methods for providing smart connection management of portable devices within a network communication system,” Rao generally describes “a remote access architecture for providing peer-to-peer communications and remote access connectivity,” and Camilleri generally describes “connecting a wireless device and a wireless network using a subscriber identity module (SIM).” SAMSUNG-1005, ¶[0007]; SAMSUNG-1006, 1:1-4; SAMSUNG-1007, Abstract, ¶[0004]; SAMSUNG-1009, Abstract, ¶¶[0001], [0013]-[0015]. Accordingly, the prior art references are all directed to the same field of wireless network communications. *Id.*

135. Additionally, as explained below in more detail, combining Jheng-Chiu/Jheng-Chiu-Rao and Camilleri would have been obvious at least because such a combination would have merely involved (1) combining prior art elements according to known methods to yield predictable results; and the (2) use of known techniques to improve similar devices in the same way.

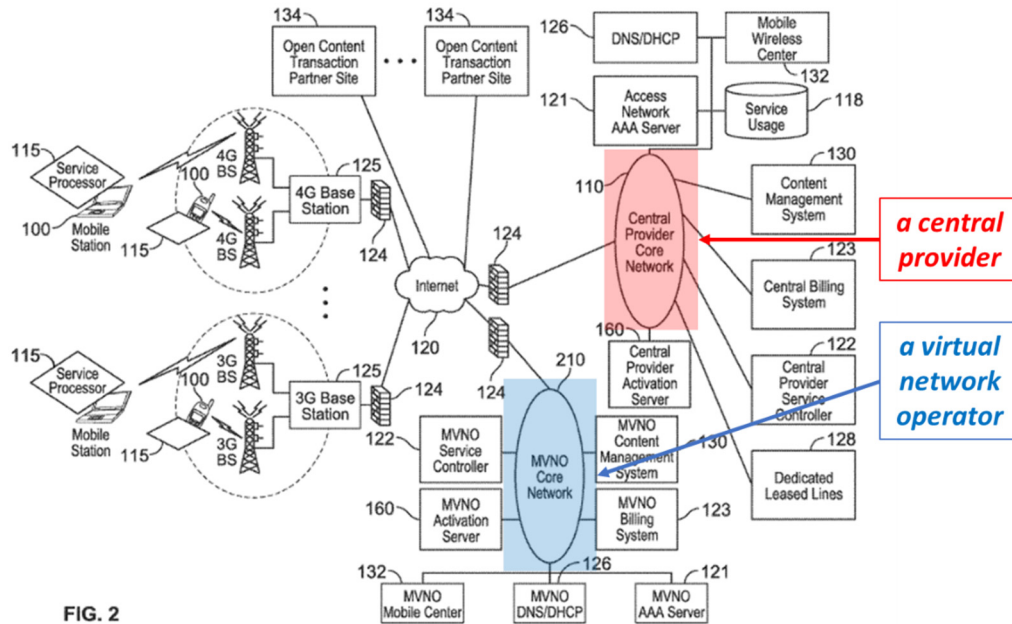
136. Providing MVNO compatibility in the JCR system would have been predictable and foreseeable with a reasonable expectation of success because MVNOs were well established by the '055 Benefit Date. SAMSUNG-1005, ¶[0033],

FIG. 1; SAMSUNG-1009, ¶¶[0040]-[0048]; SAMSUNG-1022, 3. For example, Thanh confirms that the presence of MVNOs “goes back to the early nineties” and describes various MVNO business models known in the industry before the ’055 Benefit Date. SAMSUNG-1022, 3-5. Additionally, Camilleri explicitly discloses that its PAM is implemented within a SIM, the same structure already present within the JCR dual-SIM phone. SAMSUNG-1009, ¶[0041].

B. Analysis

[5] The wireless end-user device of claim 1, wherein the first service plan is associated with a central provider that operates a WWAN access network, and the second service plan is associated with a virtual network operator.

137. The ’055 patent generally describes Mobile Virtual Network Operators (“MVNO”). SAMSUNG-1001, 9:38-42, 14:44-48, 20:9-16. The ’055 patent also describes that the central provider network “generally refers to the access network required to connect the device to other networks.” SAMSUNG-1001, 9:19-21. The ’055 patent depicts the central provider as a “core network.” *See, e.g.,* SAMSUNG-1001, FIG. 2.



SAMSUNG-1001, FIG. 2.

138. Jheng’s access networks are used to access “core networks” (a plurality of “*central provider[s]*”) and in combination with Camilleri, at least one of these networks would have been operated by an “MVNO” (“*a virtual network operator*”), as described above in the preceding section. SAMSUNG-1005, ¶[0033], FIG. 1; SAMSUNG-1009, ¶¶[0044], [0046]-[0047]; SAMSUNG-1001, 25:49-57 (describing that a “central provider network” is a “core” network). In the combined JCR-Camilleri system, Camilleri’s MVNO provides a SIM to the user, and thus the fare plan associated with the SIM (as discussed above in [1.2]) is associated with the MVNO (“*the second service plan is associated with a virtual network operator*”). SAMSUNG-1005, ¶¶[0056]-[0060]; SAMSUNG-1009, ¶[0044]; *see above*, [1.2]. A USIM is also associated with the other core network, and would have similarly

included a fare plan (also as discussed above in [1.2]) (“*the first service plan is associated with a central provider that operates a WWAN access network*”). *Id.*

XII. GROUND 1D/2D: CLAIM 8 IS OBVIOUS JHENG IN VIEW OF CHIU AND BAJKO (WITH OR WITHOUT RAO)

A. The combination of Jheng, Chiu, and Bajko (with or without Rao)

139. It would have been obvious to a POSITA to combine the teachings of Bajko with the JCR system to implement Bajko’s common service profile on the JCR device. SAMSUNG-1010, ¶¶[0014], [0039]-[0041], FIG. 4. A POSITA would have been motivated to include the teachings of Bajko with the JCR device because, as Bajko discloses, any one subscription may contain “a plurality of public and private identities.” SAMSUNG-1010, ¶[0039]. A POSITA would have recognized and found obvious that a common service profile would have been a convenient way to store the connection profile information that was common to both USIMs in JCR, or connection profile selection criteria that was not expected to change. SAMSUNG-1010, ¶¶[0014], [0039]-[0041], FIG. 4; SAMSUNG-1006, 4:19-5:2, 5:30-6:7, 6:23-29, 7:22-27, 8:26-9:10, 9:25-10:11, 10:16-20, 14:7-18, FIG. 2.

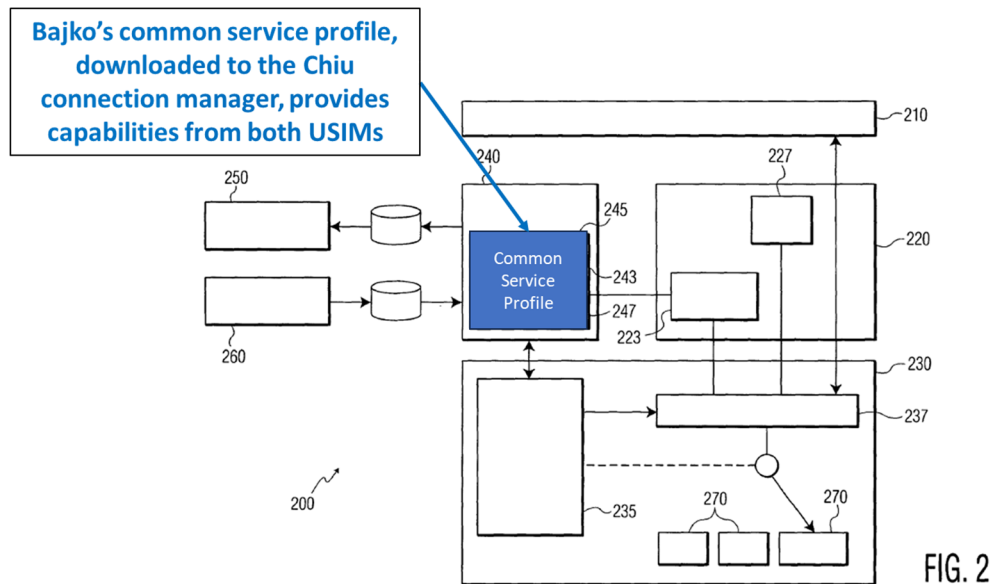
140. Jheng, Chiu, Rao, and Bajko are analogous art to the ’055 patent, which is generally directed to “a services policy communication system and method” for controlling wireless network usage by a mobile device in a wireless network. SAMSUNG-1001, Abstract, 8:44-67, 48:47-49:13, 82:54-59. Indeed, Jheng generally describes transmitting “mobile originated (MO) request[s] by a mobile

station with a first subscriber identity card and a second subscriber identity card,” Chiu generally describes “systems and methods for providing smart connection management of portable devices within a network communication system,” Rao generally describes “a remote access architecture for providing peer-to-peer communications and remote access connectivity,” and Bajko generally describes “a communication system wherein a subscription is allowed to have multiple registrations to control aspects of the system.” SAMSUNG-1005, ¶[0007]; SAMSUNG-1006, 1:1-4; SAMSUNG-1007, Abstract, ¶[0004]; SAMSUNG-1010, ¶¶[0001]-[0002]. Accordingly, the prior art references are all directed to the same field of wireless network communications. *Id.*

141. Additionally, as explained below in more detail, combining Jheng-Chiu/Jheng-Chiu-Rao and Bajko would have been obvious at least because such a combination would have merely involved (1) combining prior art elements according to known methods to yield predictable results; and the (2) use of known techniques to improve similar devices in the same way.

142. Incorporating a common service profile into the dual-SIM phone of Jheng-Chiu/Jheng-Chiu-Rao would have been predictable and foreseeable with a reasonable expectation of success because the JCR device already provides the infrastructure to enforce network service policies, and the addition of a common profile simply adds an additional source of these policies without substantively

changing their underlying function or purpose. SAMSUNG-1006, 4:19-5:2, 5:30-6:7, 6:23-29, 7:22-27, 8:26-9:10, 9:25-10:11, 10:16-20, 14:7-18, FIG. 2; SAMSUNG-1010, ¶¶[0014], [0039]-[0041], FIG. 4. For example, Chiu's connection manager stores connection profiles that can be downloaded from external sources. SAMSUNG-1006, 10:21-30, 13:27-31, FIG. 2; SAMSUNG-1010, ¶¶[0014], [0039]-[0041], FIG. 4. Thus, it would have been obvious for the connection manager to store a common service profile that included features common to both or multiple USIMs of the JCR dual-SIM phone, thus negating the need for USIMs to store duplicative information and ensuring the device always had access to common services (regardless of what USIM was in use). *Id.* Further, the implementation of a common service profile would have involved only routine coding ability that would have been well within a POSITA's capability (e.g., coding the instructions of the profile as machine readable code for execution by a processor). For example, Chiu discloses that profiles can be coded in Extensible Markup Language ("XML"), a well-known language that would have been part of a POSITA's general knowledge. SAMSUNG-1006, 7:25-27; *see, e.g.*, SAMSUNG-1029, 5.



SAMSUNG-1006, FIG. 2.

B. Analysis

[8] The wireless end-user device of claim 1, wherein the at least one adaptive service policy control agent applies network service policies from a superset profile that provides capabilities from each of the first and second service profiles.

143. The '055 patent explains that a “*superset profile*” is a “profile that provides the combined capabilities of two or more service profiles.” SAMSUNG-1001, 69:4-6.

144. Similarly, Bajko discloses a “common service profile” (“*a superset profile*”) that includes capability information such as services specified by service profiles stored on multiple SIM cards. SAMSUNG-1010, ¶¶[0039]-[0043]. Because the two USIM cards in JCR include the superset profile indicating common feature that refer to common services provided by the services associated with both

USIMs, it would have been obvious to a POSITA that the JCR-Bajko combination renders obvious “*capabilities from each of the first and second service profiles.*” SAMSUNG-1010, ¶¶[0014], [0039]-[0041], FIG. 4. An example hierarchy of Bajko’s subscriptions is shown below in FIG. 4. SAMSUNG-1010, FIG. 4.

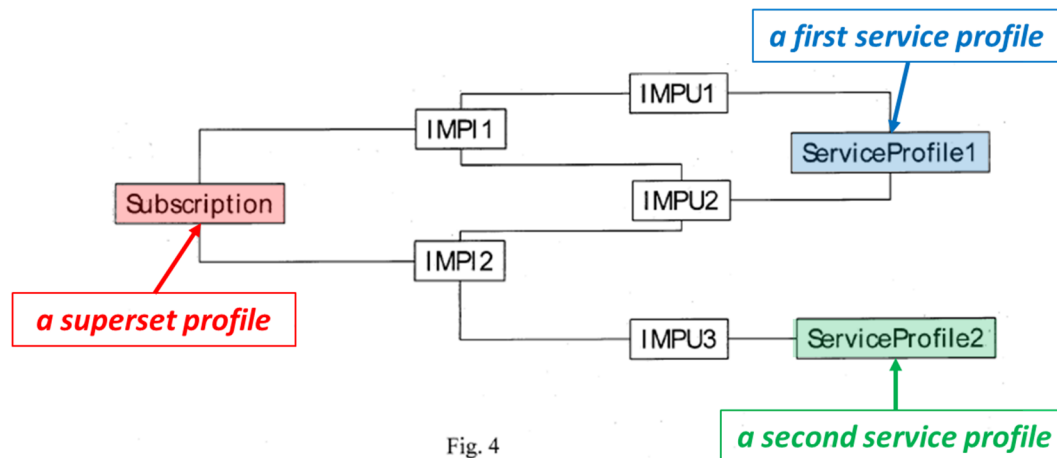


Fig. 4

SAMSUNG-1010, FIG. 4.

145. As discussed above in [1.5], Chiu’s wireless adaptation layer (“*at least one adaptive service policy control agent*”) switches the active network driver in response to instructions from the connection manager determined from the active connection profile’s selection criteria and configuration parameters. SAMSUNG-1006, 4:29-5:2, 6:8-22, 10:16-20, 13:4-12:18³. Bajko’s common subscription profile

³ Additionally, as discussed above in [1.5], Rao’s remote access client (“*at least one adaptive service policy control agent*”) also applies policies for applications,

would have included selection criteria from both the first and second USIMs for services and capabilities common to both (e.g., a network that is a home network for both USIMs, or common subscriptions). SAMSUNG-1010, ¶¶[0014], [0039]-[0041], FIG. 4. Accordingly, when making network selections for common services, the JCR connection manager and wireless adaptation layer would have enforced policies (“*applies network service policies*”) based on common selection criteria from the common service profile (“*at least one adaptive service policy control agent applies network service policies from a superset profile that provides capabilities from each of the first and second service profiles*”). SAMSUNG-1010, ¶¶[0014], [0039]-[0041], FIG. 4; *see above*, §XII.A, §IX.C.[1.4]-[1.5].

XIII. GROUND 1E/2E: CLAIM 11 IS OBVIOUS OVER JHENG IN VIEW OF CHIU AND LIU (WITH OR WITHOUT RAO)

A. The combination of Jheng, Chiu, and Liu (with or without Rao)

146. It would have been obvious to a POSITA to combine the teachings of Liu with the JCR system such that USIMs on the combination device would have included a template manager system to load SIM templates for the USIM in response to commands from the connection manager (enforcing a policy to load a SIM

and Bajko’s superset profile would have additionally specified policies common to multiple applications (e.g., policies for a group of “background” applications).

SAMSUNG-1007, ¶[0182]; *above* §IX.C.[1.5].

template for a particular network). SAMSUNG-1006, 4:19-5:2, 5:30-6:7, 6:23-29, 7:22-27, 8:26-7:10, 9:25-10:11, 10:16-20, 14:7-18, FIG. 2; SAMSUNG-1030, ¶¶[0017]-[0022], [0040]-[0041], FIGS. 1-3.

147. First, SIM templates would have enabled a user of the JCR device to compartmentalize the storage of their USIM, as taught by Liu. SAMSUNG-1030, ¶¶[0019]-[0022]. In addition to providing additional means for roaming prevention, SIM templates would have allowed a user to store SIM information particular to a network for multiple networks on a single USIM (e.g., a “phone book” for a specific roaming network), providing greater convenience to the user. *Id.*

148. Second, Liu’s templates would have increased the versatility of the USIMs of the JCR dual-SIM phone by allowing a user to combine multiple sets of SIM parameters into a single USIM. SAMSUNG-1030, ¶¶[0017]-[0022], FIG. 1. Configuring USIMs to store multiple SIM templates would have allowed the user to configure their device for more networks than would have been possible without these templates. *Id.*

149. Jheng, Chiu, Rao, and Liu are analogous art to the ’055 patent, which is generally directed to “a services policy communication system and method” for controlling wireless network usage by a mobile device in a wireless network. SAMSUNG-1001, Abstract, 8:44-67, 48:47-49:13, 82:54-59. As described in Sections IX.A and IX.B, Jheng, Chiu, and Rao are directed to wireless network

communications. Liu generally describes “rendering more portable telephone service in a telecommunication network.” SAMSUNG-1005, ¶[0007]; SAMSUNG-1006, 1:1-4; SAMSUNG-1007, Abstract, ¶[0004]; SAMSUNG-1030, ¶[0004]. Accordingly, the prior art references are all directed to the wireless network communications field. *Id.*

150. Additionally, as explained below in more detail, combining JCR and Liu would have been obvious at least because such a combination would have merely involved (1) combining prior art elements according to known methods to yield predictable results; and the (2) use of known techniques to improve similar devices in the same way.

151. Implementing a SIM template manager on the USIMs of the JCR dual-SIM phone to load SIM templates in response to instructions from the connection manager would have been predictable and foreseeable with a reasonable expectation of success because Liu describes that its SIMs adhere to well established GSM standards that (1) are compatible with the combination and (2) which a POSITA would have been generally aware of (e.g., GSM 11.11, discussed above in Ground 1A). SAMSUNG-1030, ¶¶[0025]-[0028]; *see generally* SAMSUNG-1015. Additionally, Liu’s template manager system is configured to accept commands to load a particular SIM template (“SIM command”), and the JCR connection manager is also configured to provide instructions to other programs in response to detected

networks (e.g., the wireless adaptation layer). SAMSUNG-1006, 4:19-5:2, 5:30-6:7, 6:23-29, 7:22-27, 8:26-7:10, 9:25-8:11, 10:16-20, 14:7-18, FIG. 2; SAMSUNG-1030, ¶¶[0017]-[0022], [0040]-[0041], FIGS. 1-3.

152. In the JCR-Liu system, SIM template manager systems resident on each USIM would have loaded SIM templates in response to instructions from the JCR connection manager. SAMSUNG-1006, 4:19-3:2, 5:30-4:7, 6:23-29, 7:22-27, 8:26-7:10, 9:25-8:11, 10:16-20, 14:7-18, FIG. 2; SAMSUNG-1030, ¶¶[0017]-[0022], [0040]-[0041], FIGS. 1-3.

B. Analysis

[11] The wireless end-user device of claim 1, further comprising a Subscriber Identity Module (SIM), the adaptive service policy control agent located at least in part on the SIM.

153. Jheng discloses at least one USIM in its dual-SIM phone (“***a Subscriber Identity Module (SIM)***”). SAMSUNG-1005, ¶¶[0030]-[0035]; *see above*, [1.2]. For the reasons explained above in §XIII.A, it would have been obvious to a POSITA that the JCR-Liu USIMs would have included a SIM template manager (an “***adaptive service policy control agent located at least in part on the SIM***”⁴) to load

⁴ The SIM template manager is an additional example of an “***adaptive service policy control agent***,” in addition to the wireless adaptation layer and remote access client discussed above in Grounds 1A and 1B. *Above*, §IX.C.[1.5]-[1.6].

SIM templates in response to commands from the connection manager (e.g., when a network corresponding to a SIM template is encountered). SAMSUNG-1006, 4:19-5:2, 5:30-6:7, 6:23-29, 7:22-27, 8:26-9:10, 9:25-10:11, 10:16-20, 14:7-18, FIG. 2; SAMSUNG-1030, ¶¶[0017]-[0022], [0040]-[0041], FIGS. 1-3. For example, Liu describes that when traveling to a country with a different network, a SIM template can be selected for service in that area, such that “incoming or outgoing calls are at local rates.” SAMSUNG-1030, ¶¶[0019]-[0021].

154. The SIM template manager includes all of the features of an “*adaptive service policy control agent*,” as previously discussed in [1.5]-[1.6] above. Above, §IX.C.[1.5]-[1.6]. For example, the SIM template manager enforces a policy to load a particular SIM template in response to the selection of a network, dictated by the connection profile of the USIM (“enforce network service policies associated with the selected one of the first and second service profiles”). SAMSUNG-1030, ¶¶[0017]-[0022], [0040]-[0041]. Further, these policies are enforced at an interface that provides services to applications (e.g., the “application layer 206” of the USIM—“the enforced network service policies including policies enforced at an application service interface on network data connections for selected applications resident on the device”). SAMSUNG-1030, ¶[0040], FIG. 2. For example, Liu describes that application services include Internet of Data (“IOD”) and Short Message Service

(“SMS”) applications that use the network data connections described above. SAMSUNG-1030, ¶¶[0019]-[0039]; *above*, §IX.C.[1.5]-[1.6].

XIV. GROUND 1F/2F: CLAIM 13 IS OBVIOUS OVER JHENG IN VIEW OF CHIU AND BROWN (WITH OR WITHOUT RAO)

A. The combination of Jheng, Chiu, and Brown (with or without Rao)

155. It would have been obvious to a POSITA to combine the teachings of Brown with the JCR system such that USIMs on the combination device would have been activated and deactivated as needed, as explained in detail below. SAMSUNG-1012, ¶¶[0018], [0020], [0024], [0032]-[0034].

156. First, the activation and deactivation of SIM credentials “allows the mobile phone or other electronic device to be adaptable to different criteria, e.g., different markets or regions, by allowing a particular set of subscription parameters to be activated on the SIM 15, depending on the market or region in which the SIM 15 is to be used.” SAMSUNG-1012, ¶[0018]. Accordingly, if a service provider wished to re-configure a USIM with a different fare plan for a particular region, a USIM using Brown’s techniques could have been deactivated, re-programmed, and then reactivated—negating the need for the user to acquire a new physical USIM. SAMSUNG-1012, ¶[0033].

157. Second, because the USIM allows for the activation and deactivation of credentials, as corroborated by 3GPP TS 31.102, a POSITA would have

recognized and found obvious that this would have been an efficient way to restrict a user's access to the network for security reasons (e.g., a user was suspected of fraud, as discussed above with respect to Collins). SAMSUNG-1005, ¶[0033], FIG. 1; SAMSUNG-1009, ¶¶[0040]-[0048]; SAMSUNG-1014, 15-17; *see above*, §X.A.

158. Jheng, Chiu, Rao, and Brown are analogous art to the '055 patent, which is generally directed to “a services policy communication system and method” for controlling wireless network usage by a mobile device in a wireless network. SAMSUNG-1001, Abstract, 8:44-67, 48:47-49:13, 82:54-59. Indeed, Jheng generally describes transmitting “mobile originated (MO) request[s] by a mobile station with a first subscriber identity card and a second subscriber identity card,” Chiu generally describes “systems and methods for providing smart connection management of portable devices within a network communication system,” Rao generally describes “a remote access architecture for providing peer-to-peer communications and remote access connectivity,” and Brown generally describes “subscriber identity module (SIM) cards for portable electronic devices such as mobile and wireless telephones.” SAMSUNG-1005, ¶[0007]; SAMSUNG-1006, 1:1-4; SAMSUNG-1007, Abstract, ¶[0004]; SAMSUNG-1012, ¶¶[0001]-[0002]. Accordingly, the prior art references are all directed to the same field of wireless network communications. *Id.*

159. Additionally, as explained below in more detail, combining Jheng-Chiu/Jheng-Chiu-Rao and Brown would have been obvious at least because such a combination would have merely involved (1) combining prior art elements according to known methods to yield predictable results; and the (2) use of known techniques to improve similar devices in the same way.

160. The activating and deactivating of USIMs on the JCR dual-SIM phone would have been predictable and foreseeable with a reasonable expectation of success because 3GPP TS 31.102, which a POSITA would have been aware of examples of credentials that could be activated and deactivated on the USIM to provide or rescind service (e.g., the “IMSI” or keys associated with the USIM). SAMSUNG-1005, ¶[0033], FIG. 1; SAMSUNG-1009, ¶¶[0040]-[0048]; SAMSUNG-1014, 15-17. Additionally, Brown discloses that USIMs can be activated and deactivated using a “terminal interface,” and Jheng already provides such an interface for user interaction with USIMs (the MMI). SAMSUNG-1005, ¶[0057], FIG. 11; SAMSUNG-1012, ¶[0034]. Further, the implementation of procedures to activate and reactivate USIMs would have involved only routine coding ability that would have been well within a POSITA’s capability (e.g., coding the functions into the secure memory of the USIM for execution by the USIM internal processor). In fact, Brown discloses explicitly that such capability can be programmed into USIMs. SAMSUNG-1012, ¶[0035].

161. In the JCR-Brown system, SIMs on the combination device could be activated and deactivated, either by the user at will or automatically when a USIM is installed in the JCR device, for example, to replace or restrict a USIM's fare plan, as taught in Brown. SAMSUNG-1012, ¶¶[0018], [0020], [0024], [0032]-[0035].

B. Analysis

[13] The wireless end-user device of claim 2, configured to, when the second service plan is inactive, suspend the second device credentials, and when the second service plan is reactivated, reactivate the second device credentials.

162. Brown discloses that parameters such as IMSI, subscription parameters (e.g., a telephone number) can be deactivated and reactivated. SAMSUNG-1012, ¶¶[0005], [0015]-[0016], [0018], [0020], [0024], [0032]-[0034], FIG. 1. In the JCR-Brown combination, a POSITA would have found obvious that credentials contained within a second USIM connection profile (e.g., a secret key K, IMSI, or phone number—“*the second device credentials*”), associated with a service plan (“*the second service plan*”) could be activated and reactivated with the service plan (“*suspend the second device credentials, and when the second service plan is reactivated, reactivate the second device credentials*”). SAMSUNG-1005, ¶¶[0006], [0029]-[0030], [0032], [0038], [0042], [0051]; SAMSUNG-1012, ¶¶[0019], [0020], [0032]-[0034], FIG. 1; SAMSUNG-1001, 123:8-45; *see above*, [1.2], [2.1]-[2.2]. For example, when a user removed the second USIM from the device, the second fare plan would have been deactivated “automatically,” as taught

in Brown. SAMSUNG-1012, ¶[0035]. Upon reinstalling the USIM, the USIM would have automatically activated the second fare plan “upon SIM power-up,” as taught in Brown. *Id.* In another example, the user would have deactivated or activated the second USIM manually. SAMSUNG-1012, ¶[0034].

XV. CONCLUSION

163. For all the reasons I have noted in the foregoing paragraphs, claims 1-13 of the '055 Patent are obvious in view of the references discussed above.

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

APPENDIX A

Patrick Gerard Traynor

Professor

Associate Chair for Research in CISE

John and Mary Lou Dasburgh Preeminent Chair in Engineering

Department of Computer & Information Science & Engineering (CISE)

University of Florida

E301 CSE Building, PO Box 116120

Gainesville, FL 32611 USA

traynor@cise.ufl.edu

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

Table of Contents

EDUCATIONAL BACKGROUND	4
EMPLOYMENT HISTORY	4
CURRENT FIELDS OF INTEREST	4
I. TEACHING	6
A. Courses Taught	6
B. Continuing Education	6
C. Curriculum Development	6
D. Individual Student Guidance	7
E. Teaching Honors and Awards	11
II. RESEARCH AND CREATIVE SCHOLARSHIP	12
A. Thesis	12
B. Published Journal Papers (Refereed)	12
C. Published Books and Parts of Books	14
D. Edited Proceedings	14
E. Conference Presentations	14
E.1. Conference Presentations with Proceedings (Refereed)	14
E.2. Conference Presentations with Proceedings (Non-Refereed)	20
E.3. Conference Presentations without Proceedings	20
F. Other	20
F.1. Submitted Journal Papers	20
F.2. Refereed Research Reports	20
F.3. Software	20
F.4. Published Papers (Non-Refereed)	21
F.5. Books in Preparation	21
F.6. Workshops and External Courses	21
G. Research Proposals and Grants (Principal Investigator)	22
H. Research Proposals and Grants (Contributor)	24
I. Research Honors and Awards	25
III. SERVICE	27
A. Professional Activities	27
A.1. Memberships and Activities in Professional Societies	27
A.2. Conference Committee Activities	27
B. On-Campus Committees	28
B.1. University of Florida	28
B.2. Georgia Tech	29
C. Special Assignments	29
D. Ph.D. Examining Committees	29
E. External Member of M.S. Examining Committee	33
F. Consulting and Advisory Appointments	33
G. Civic Activities	33
IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION	34
A. Honors and Awards	34
B. Invited Conference Session Chairmanships	34
C. Professional Registration	34
D. Patents	34
E. Editorial and Reviewer Work for Technical Journals and Publishers	35
F. Expert Witness Services	37
V. OTHER CONTRIBUTIONS	39
A. Seminar Presentations (Invited Papers and Talks at Meetings and Symposia)	39

B. Special Activities	43
---------------------------------	----

EDUCATIONAL BACKGROUND

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

EMPLOYMENT HISTORY

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

CURRENT FIELDS OF INTEREST

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

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

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

I. TEACHING

A. Courses Taught

Semester/Year	Course Number & Title	Number of Students	Comments
Fall 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

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

company to potential investors.

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

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

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

D. Individual Student Guidance

1. Research Scientists Supervised

None.

2. Ph.D. Students Graduated

Chaitrali Amrutkar Georgia Institute of Technology

Fall 2009–Fall 2013

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

Jasmine Bowers University of Florida

Fall 2015–Summer 2020

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

Henry “Hank” Carter Georgia Institute of Technology

Fall 2010–Spring 2016

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

Italo Dacosta Georgia Institute of Technology

Fall 2008–Summer 2012

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

David Dewey Georgia Institute of Technology

Fall 2011–Summer 2015

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

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

Nolen Scaife University of Florida
Fall 2014–Spring 2019
Developed techniques to detect credit card skimming. First: Assistant Professor at the University of Colorado Boulder. Now: Director, Global Cyber Intelligence at Walmart

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

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

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

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

2. Ph.D. Students Supervised

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

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

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

Ryon Kennedy University of Florida
Fall 2020–Present
Finding vulnerabilities in cellular core networks via fuzzing.

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

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

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

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

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

3. Ph.D. Students - Other

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

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

Eric (Yu) Liu Georgia Institute of Technology
Fall 2008
Research on the spread of malware through cellular infrastructure.

Chaz Lever Georgia Institute of Technology
Fall 2011–Spring 2014
Developing techniques to measure the spread of malware in cellular networks. Left Georgia Tech to create a startup.

Frank Park Georgia Institute of Technology
Fall 2008–Spring 2010
Research on multi-factor authentication using cellular phones. Left program after failing comprehensive exam to join startup.

Ferdinand Schober Georgia Institute of Technology
Fall 2009–Summer 2010
Developed mechanisms for smart networks and smart mobile devices to fight infection and provide remote remediation. Returned to Microsoft.

4. M.S. Students Supervised

Chaitrali Amrutkar Georgia Institute of Technology
Fall 2008–Spring 2009
Research on improving performance of security critical functions in IMS cellular core. Completed her Ph.D with me at GT.

Logan Blue University of Florida
Fall 2015–Spring 2016
Investigated problems of cellular and network security.

David Dewey Georgia Institute of Technology
Fall 2009–Spring 2010
Research on security issues caused by transitive trust assumptions in the Windows COM infrastructure. Completed his Ph.D. with me at GT.

Christopher Grayson Georgia Institute of Technology

Fall 2012–Fall 2013

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

Young Seuk Kim Georgia Institute of Technology

Fall 2012–Fall 2013

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

Daniel Komaromy Georgia Institute of Technology

Fall 2008–Summer 2009

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

Nigel Lawrence Georgia Institute of Technology

Fall 2011–Spring 2012

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

Philip Marquardt Georgia Institute of Technology

Fall 2009–Present

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

Fall 2015–Spring 2016

Research on connecting telephone calls to the larger authentication infrastructure.

Nilesh Nipane Georgia Institute of Technology

Fall 2008–Spring 2010

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

Walter “Nolen” Sciafe Georgia Institute of Technology

Spring 2012–Spring 2014

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

Tyler Tucker University of Florida

Fall 2018–Spring 2021

Evaluating the security of Bluetooth radios.

5. M.S. Special Problems Students

Siddhant Deshmukh University of Florida

Fall 2016–Present

Developed tools for analysis of mobile digital financial services.

Chinmay Gangakhedkar Georgia Institute of Technology

Spring 2009

Research on multi-factor authentication using mobile phones.

Christopher Grayson Georgia Institute of Technology
Spring 2013

Research on continuous authentication using mobile phones.

Aarushi Karnany University of Florida
Fall 2016–Present

Developed tools for analysis of mobile digital financial services.

Rohit Matthews Georgia Institute of Technology
Spring 2011

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

Ashwin Narasimhan Georgia Institute of Technology
Spring 2009

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

Aamir Poonawalla Georgia Institute of Technology
Spring 2010

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

Erin Reddick Georgia Institute of Technology
Fall 2008–Fall 2009

Research on IPTV security with GTRI.

Lalanthika Vasudevan Georgia Institute of Technology
Spring 2009

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

6. Undergraduate Special Problems Students

Ethan Shernan Georgia Institute of Technology
Spring 2014

Developed an infrastructure for detecting billing bypass fraud attacks.

Young Seuk Kim Georgia Institute of Technology
Fall 2011–Spring 2012

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

Dane Van Dyck Georgia Institute of Technology
Summer 2009

Research on virtualization support for mobile phones.

E. Teaching Honors and Awards

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

II. RESEARCH AND CREATIVE SCHOLARSHIP

A. Thesis

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

B. Published Journal Papers (Refereed)

1. Cassidy Gibson, Vanessa Frost, Katie Platt, Washington Garcia, Luis Vargas, Sara Rampazzi, Vincent Bindschaedler, Patrick Traynor, and Kevin Butler. Analyzing the Monetization Ecosystem of Stalkerware. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2022.
2. Bradley Reaves, Luis Vargas, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, and Kevin Butler. Characterizing the Security of the SMS Ecosystem with Public Gateways. *ACM Transactions on Privacy and Security (TOPS)*, 22(1), 2018.
3. Patrick Traynor, Kevin Butler, Jasmine Bowers, and Bradley Reaves. FinTechSec: Addressing the Security Challenges of Digital Financial Services. *IEEE S&P Magazine*, 15(5):85–89, 2017.
4. Nolen Scaife, Henry Carter, Rachel Jones, Lyrissa Lidsky, and Patrick Traynor. OnionDNS: A Seizure-Resistant Top-level Domain. *International Journal of Information Security (IJIS)*, 2017.
5. Bradley Reaves, Jasmine Bowers, Nolen Scaife, Adam Bates, Arnav Bharatiya, Patrick Traynor, and Kevin Butler. Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World. *ACM Transactions on Privacy and Security (TOPS)*, 2017.
6. Henry Carter and Patrick Traynor. OPFE: Outsourcing Computation for Private Function Evaluation. *International Journal of Information and Computer Security (IJICS)*, 2017.
7. Stephan Heuser, Bradley Reaves, Praveen Kumar Pendyala, Henry Carter, Alexandra Dmitrienko, William Enck, Negar Kiyavash, Ahmad-Reza Sadeghi, and Patrick Traynor. Phonion: Practical Protection of Metadata in Telephony Networks. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2017.
8. Bradley Reaves, Jasmine Bowers, Sigmond A. Gorski III, Olabode Anise, Rahul Bobhate, Raymond Cho, Hiranava Das, Sharique Hussain, Hamza Karachiwala, Nolen Scaife, Byron Wright, Kevin Butler, William Enck, and Patrick Traynor. *droid: Assessment and Evaluation of Android Application Analysis Tools. *ACM Computing Surveys (CSUR)*, 2016.
9. Chaitrali Amrutkar, Young Seuk Kim, and Patrick Traynor. Detecting Mobile Malicious Webpages in Real Time. *IEEE Transactions on Mobile Computing (TMC)*, To Appear 2016.
10. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Outsourcing Secure Two-Party Computation as a Black Box. *Journal of Security and Communication Networks (SCN)*, To Appear 2016.
11. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Secure Outsourced Garbled Circuit Evaluation for Mobile Devices. *Journal of Computer Security (JCS)*, 24(2):137–180, 2016.
12. Adam Bates, Kevin Butler, Micah Sherr, Clay Shields, Patrick Traynor, and Dan Wallach. Accountable Wiretapping -or- I Know They Can Hear You Now. *Journal of Computer Security (JCS)*, 23(2):167–195, 2015.
13. Henry Carter, Chaitrali Amrutkar, Italo Dacosta, and Patrick Traynor. For Your Phone Only: Custom Protocols for Efficient Secure Function Evaluation on Mobile Devices. *Journal of Security and Communication Networks (SCN)*, 7(7):1165–1176, 2014.

14. Chaitrali Amrutkar, Patrick Traynor, and Paul van Oorschot. An Empirical Evaluation of Security Indicators in Mobile Web Browsers. *IEEE Transactions on Mobile Computing (TMC)*, 14(5), 2015.
15. Andrew Harris, Seymour Goodman, and Patrick Traynor. Privacy and Security Concerns Associated with Mobile Money Applications in Africa. *Washington Journal of Law, Technology & Arts*, 8(3), 2013.
16. Italo Dacosta, Saurabh Chakradeo, Mustaque Ahamad, and Patrick Traynor. One-Time Cookies: Preventing Session Hijacking Attacks with Stateless Authentication Tokens. *ACM Transactions on Internet Technology (TOIT)*, 12(1), 2012.
17. Cong Shi, Xiapu Luo, Patrick Traynor, Mostafa Ammar, and Ellen Zegura. ARDEN: Anonymous netwoRking in Delay tolErant Networks. *Journal of Ad Hoc Networks*, 10(6):918–930, 2012.
18. Patrick Traynor. Characterizing the Security Implications of Third-Party EAS Over Cellular Text Messaging Services. *IEEE Transactions on Mobile Computing (TMC)*, 11(6):983–994, 2012.
19. Italo Dacosta, Vijay Balasubramaniyan, Mustaque Ahamad, and Patrick Traynor. Improving Authentication Performance of Distributed SIP Proxies. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 22(11):1804–1812, 2011.
20. Patrick Traynor, Chaitrali Amrutkar, Vikhyath Rao, Trent Jaeger, Patrick McDaniel, and Thomas La Porta. From Mobile Phones to Responsible Devices. *Journal of Security and Communication Networks (SCN)*, 4(6):719 – 726, 2011.
21. Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters. Secure Attribute-Based Systems. *Journal of Computer Security (JCS)*, 18(5):799–837, 2010.
22. Patrick Traynor, Kevin Butler, William Enck, Kevin Borders, and Patrick McDaniel. malnets: Large-Scale Malicious Networks via Compromised Wireless Access Points. *Journal of Security and Communication Networks (SCN)*, 2(3):102–113, 2010.
23. Patrick Traynor. Securing Cellular Infrastructure: Challenges and Opportunities. *IEEE Security & Privacy Magazine*, 7(4), 2009.
24. Kevin Butler, Sunam Ryu, Patrick Traynor, and Patrick McDaniel. Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 20(12):1803–1815, 2009.
25. Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Mitigating Attacks On Open Functionality in SMS-Capable Cellular Networks. *IEEE/ACM Transactions on Networking (TON)*, 17(1), 2009.
26. Patrick Traynor, Michael Chien, Scott Weaver, Boniface Hicks, and Patrick McDaniel. Non-Invasive Methods for Host Certification. *ACM Transactions on Information and System Security (TISSEC)*, 2008.
27. Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. *Journal of Computer Security (JCS)*, 16(6):713–742, 2008.
28. Patrick Traynor, Raju Kumar, Heesook Choi, Sencun Zhu, Guohong Cao, and Thomas La Porta. Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks. *IEEE Transactions on Mobile Computing (TMC)*, 6(6), 2007.

C. Published Books and Parts of Books

1. Andrew Harris, Frank S. Park, Seymour Goodman, and Patrick Traynor. *Emerging Privacy and Security Concerns for Digital Wallet Deployment*. Privacy in America: Interdisciplinary Perspectives. Scarecrow Press, July 2011.
2. Kevin Butler, William Enck, Patrick Traynor, Jennifer Plasterr, and Patrick McDaniel. *Privacy Preserving Web-Based Email*. Algorithms, Architectures and Information Systems Security, Statistical Science and Interdisciplinary Research. World Scientific Computing, November 2008.
3. Patrick Traynor, Patrick McDaniel, and Thomas La Porta. *Security for Telecommunications Networks*. Number 978-0-387-72441-6 in Advances in Information Security Series. Springer, August 2008.

D. Edited Proceedings

None.

E. Conference Presentations

E.1. Conference Presentations with Proceedings (Refereed)

1. 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.
2. 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.
3. 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.
4. 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.
5. 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%).
6. 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%).
7. 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%).
8. 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%).

9. 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.
10. Imani Sherman and Daniel Delgado and Juan Gilbert and Jaime Ruiz and Patrick Traynor. Characterizing User Comprehension in the STIR/SHAKEN Anti-Robocall Standard. In *Proceedings of the Annual Research Conference on Communications Information and Internet Policy (TPRC 49)*, 2021.
11. 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%).
12. 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%).
13. 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.
14. 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%).
15. Joseph Choi, Dave Tian, Grant Hernandez, Christopher Patton, Benjamin Mood, Thomas Shrimpton, Patrick Traynor, and Kevin Butler. A Hybrid Approach to Secure Function Evaluation Using SGX. In *Proceedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS’19)*, 2019. (Acceptance Rate: 17.0% for full papers).
16. 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).
17. 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%).
18. 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%).
19. 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%).
20. 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%).

21. 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%).
22. 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%.
23. 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%.
24. Dave (Jing) Tian, Grant Hernandez, Joseph Choi, Vanessa Frost, Christie Raules, Kevin Butler, Patrick Traynor, Hayawardh Vijayakumar, Lee Harrison, Amir Rahmati, and Mike Grace. AT-tention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2018. Acceptance Rate: 19.0%.
25. 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%).
26. 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%).
27. 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%).
28. 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%).
29. 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%).
30. 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%).
31. 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%).
32. 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%).
33. 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%).

34. 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%).
35. 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%).
36. 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%).
37. 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%).
38. Nolen Scaife, Henry Carter, and Patrick Traynor. OnionDNS: A Seizure-Resistant Top-level Domain. In *Proceedings of the IEEE Conference on Communications and Network Security (CNS)*, 2015. (Acceptance Rate: 28.1%).
39. 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%).
40. 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%).
41. 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%).
42. 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%).
43. 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%).
44. 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%).
45. 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%).
46. 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).
47. 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%).

48. 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).
49. 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).
50. 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%).
51. 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%).
52. 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%).
53. 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%).
54. 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%).
55. 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%).
56. 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%).
57. Vijay Balasubramaniyan, Aamir Poonawalla, Mustaque Ahamad, Michael Hunter, and Patrick Traynor. PinDrOp: Using Single-Ended Audio Features to Determine Call Provenance. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2010. (Acceptance Rate: 17.2%).
58. 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%).
59. 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%).
60. 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%).

61. 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%).
62. 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%).
63. 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%).
64. 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%).
65. 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%).
66. 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%).
67. 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%).
68. 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%).
69. 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).
70. 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%).
71. 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%).
72. 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%).
73. 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%).

74. 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%).
75. 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%).
76. 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%).
77. 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%).
78. 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. Testing Audio Deep Fake Detectors

Sponsor: Bank of America

Investigator(s): Patrick Traynor (PI), Kevin Butler

Amount: \$274,000 over 2 years

Awarded: August 2021

2. 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

3. 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

4. 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

5. 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

6. Workshop: Addressing the Technical Security Challenges of Emerging Digital Financial Services

Sponsor: NSF Secure and Trustworthy Cyberspace

Investigator(s): Patrick Traynor (PI), Kevin Butler

Amount: \$50,000 over 1 year

Awarded: September 2017

7. 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

8. 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

9. **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
10. **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
11. **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
12. **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
13. **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
14. **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
15. **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
16. **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
17. **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

18. **Characterizing and Mitigating Device-Based Attacks in Cellular Telecommunications Networks**
Sponsor: NSF Trustworthy Computing
Investigator(s): Patrick Traynor (PI) and Jonathon Giffin
Amount: \$450,000 over 3 years
Awarded: July 2009

2. Pending

Removed for external version.

H. Research Proposals and Grants (Contributor)

1. Approved and Funded

1. **SaTC: Frontier: Securing the Future of Computing for Marginalized and Vulnerable Populations**
Sponsor: NSF SaTC
Investigator(s): Kevin Butler (PI), Patrick Traynor, Tadayoshi Kohno, Franz Roesner, Apu Kapadia, Eakta Jain.
Amount: \$7,500,000 for 5 years
Awarded October 2022
2. **ROCKY: Reliable Obfuscated Communications Kit for everYone**
Sponsor: DARPA Resilient Anonymous Communication for Everyone (RACE) – Broad Agency Announcement
Investigator(s): Thomas Shrimpton (PI), Patrick Traynor, Kevin Butler, Vincent Bindschaedler, Nadia Heninger
Amount: \$1,600,000 over 4 years
Awarded May 2019
3. **WiFiUS: Collaborative Research: SELIOT: Securing Lifecycle of Internet-of-Things**
Sponsor: NSF CNS WiFiUS
Investigator(s): Gene Tsudik (PI), Patrick Traynor
Amount: \$300,000 for 2 years
Submitted December 2016
4. **Cloud-based Oblivious Spectrum Mapping and Allocation**
Sponsor: NSF CNS EARS
Investigator(s): John Shea (PI), Tan Wong, Patrick Traynor
Amount: \$532,952 for 2 years
Submitted May 2016
5. **DURIP: Developing Research Capability in Cyber-Physical Systems at the University of Florida**
Sponsor: Small
Investigator(s): Kevin Butler (PI), Patrick Traynor, My Thai
Amount: \$200,000 for 2 years
Submitted: June 2015
6. **Securing the New Converged Telephony Landscape**
Sponsor: NSF TWC: Small
Investigator(s): Mustaque Ahamad (PI) and Patrick Traynor
Amount: \$500,000 for 3 years
Submitted: December 2012

7. **Facilitating Free and Open Access to Information on the Internet**
 Sponsor: NSF Trustworthy Computing
 Investigator(s): Nick Feamster (PI), Wenke Lee, Patrick Traynor, Hans Klein, Roger Dingledine, Michael Freedman and Edward W. Felten
 Amount: \$1,500,000 for 4 years
 Awarded: June 2011
8. **Monitoring Free and Open Access to Information on the Internet**
 Sponsor: Google Focus Program
 Investigator(s): Nick Feamster (PI), Wenke Lee, Mustaque Ahamad, Patrick Traynor, Henry Owen, Ellen Zegura, Zvi Galil
 Amount: \$1,000,000 for 2 years
 Awarded: November 2011
9. **Dynamic-attribute-based Disclosure of Health Information in Emergency Care Scenarios**
 Sponsor: Health Systems Institute (HSI) Seed Grant Program
 Investigator(s): Doug Blough (PI), Mustaque Ahamad, Patrick Traynor and Jim Jose
 Amount: \$50,000 over 1 year
 Awarded: August 2009
10. **Federal Cyber Service Scholarships at Georgia Tech**
 Sponsor: NSF SFS Scholarships
 Investigator(s): Seymour Goodman (PI), Patrick Traynor
 Amount: \$1,250,682 over 5 years
 Awarded: June 2009
11. **Security for IMS-Enabled Converged Applications**
 Sponsor: US Department of Defense
 Investigator(s): Mustaque Ahamad (PI), Patrick Traynor (PI), Michael Hunter, Russ Clark
 Amount: \$146,121 for 1 year
 Awarded: August 2008

2. Pending

Removed for external version.

I. Research Honors and Awards

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

9. Pennsylvania State University Alumni Association Dissertation Award, 2007
10. Pennsylvania State University CSE Graduate Research Assistant Award, 2007
11. AT&T Wireless Fellowship, 2005

III. SERVICE

A. Professional Activities

A.1. Memberships and Activities in Professional Societies

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

A.2. Conference Committee Activities

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

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

B. On-Campus Committees

B.1. University of Florida

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

B.2. Georgia Tech

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

C. Special Assignments

None.

D. Ph.D. Examining Committees

Ph.D. Examining Committees

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

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

External Member of Ph.D. Research Committee

None.

External Member of Ph.D. Examining Committee

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

Ph.D. Thesis Proposal Committees

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

Ph.D. Qualifying Exam Committees—Georgia Tech

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

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

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

E. External Member of M.S. Examining Committee

M.S. Thesis Defense Committees None.

F. Consulting and Advisory Appointments

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

G. Civic Activities

None.

IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION

A. Honors and Awards

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

B. Invited Conference Session Chairmanships

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

C. Professional Registration

None.

D. Patents

1. 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. *Epic Games, Inc. & Anor v Google LLC & Ors - Federal Court of Australia Proceeding NSD 190 of 2021:* Expert witness for the Defense (via Corrs Chambers Westgarth). Status: Ongoing. *January 2023 - Present.*
2. *Telefonaktiebolaget LM Ericsson vs Apple, Inc:* Expert witness for the Defendant, Non-Infringement and Invalidity (via WilmerHale LLP). Status: Settled. *February 2022 - December 2022.*
3. *Wepay Global Payments, LLC v. Bank of America N. A.:* Expert Witness for the Defendant (via WilmerHale LLP) Status: Dismissed. *September 2022 - November 2022.*
4. *Apple vs. R.N Nehushtan Trust Ltd.:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Status: Submitted to PTAB. *August 2022 - Ongoing.*
5. *Apple/Microsoft vs. Zipit Wireless:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Status: Settled. *May 2021 - November 2022.*
6. *Blackberry Inc v MobileIron, Inc:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Verdict: Settled. *January 2021 - March 2021.*
7. *Apple Inc v Seven Networks, LLC:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Verdict: Three of four petitions instituted by PTAB. Fourth rejected via discretion, case settled. *August 2019 - November 2020.*
8. *mSIGNIA, Inc. v. InAuth, Inc.:* Expert Witness for the Defendant for Inter Partes Review, Non-Infringement and Invalidity (via Quinn Emanuel Urquhart and Sullivan, LLP). Verdict: Dismissed with prejudice. *October 2017 - December 2018.*
9. *Huawei v. T-Mobile:* Expert Witness for the Defendant for Non-Infringement (via WilmerHale LLP, Alston & Bird LLP) Verdict: Settled *June 2016 - December 2017.*
10. *Telefonaktiebolaget LM Ericsson v Apple:* Expert Witness for the Defendant for Non-Infringement, Invalidity (via WilmerHale LLP). Verdict: Settled *June 2015 - December 2015.*
11. *Mayfonk v Nike:* Expert Witness for the Plaintiff for Infringement (via Paul Hastings). Verdict: Settled. *June 2015 - November 2015.*

12. *Maxim Integrated Products v Bank of the West*: Expert Witness for the Defendant for Non-Infringement (via Paul Hastings LLP). Verdict: Dismissed with prejudice. *January 2014 - August 2014*.
13. *Maxim Integrated Products v Comerica Inc, et al*: Expert Witness for the Defendant for Non-Infringement (via McKenna, Long & Aldridge LLP). Verdict: Settled. *June 2014 - August 2014*.
14. *William Grecia v. Apple Inc. et al*: Expert Consultant for the Defendant for Invalidity (via Kirkland & Ellis LLP). Verdict: Closed in initial pleadings, dismissed with prejudice. *July 2014 - August 2014*.
15. *Intertrust Technologies Corp. v. Apple Inc.*: Expert Consultant for Defendant for Invalidity and Non-Infringement (via Kirkland & Ellis LLP). Verdict: Settled. *October 2013 - February 2014*.
16. *Maxim Integrated Products v KeyCorp Bank*: Expert Witness for the Defendant for Non-Infringement (via Calfee, Halter & Griswold LLP) Verdict: Settled. *April 2013 - June 2013*.
17. *Intellectual Ventures LLC vs. Check Point; et al.*: Expert Consultant for the Plaintiff for Infringement (via Susman Godfrey LLP), Verdict: Infringement on 2 of 4 patents. *October 2012 - February 2015*.

V. OTHER CONTRIBUTIONS

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

1. 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.
2. 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.
3. 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.
4. The State of Voice Cloning Technology. Federal Trade Commission (FTC) Workshop on Voice Cloning Technologies, January 2020. Washington, DC.
5. 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.
6. 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.
7. 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.
8. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. Bank of America - Colloquium Series, March 2019. Charlotte, NC.
9. 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.
10. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. University of Maryland - Distinguished Colloquium, February 2019. College Park, MD.
11. Responsible Finance for the Digital Client. Foromic Conference, October 2018. Barranquilla, Colombia.
12. Panel: Authentication Challenges for New Interfaces, Devices, and Wireless Networks. ACM Conference on Security and Privacy in Wireless and Mobile Networks, June 2018. Stockholm, Sweden.
13. Sonar: Detecting SS7 Redirection Attacks Via Call Audio-Based Distance Bounding. CyberSecurity@KAIST Workshop - KAIST, June 2018. Daejeon, South Korea.
14. 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.
15. Panel: The Future of Cybersecurity. SEC Academic Conference - Auburn University, May 2018. Auburn, AL.
16. Sound Principles: Verifying Voice Commands in an IoT World. IoT Security Workshop - Aalto University, September 2017. Helsinki, Finland.

17. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Eurecom Institute, September 2017. Sophia Antipolis, France.
18. Panel: Infrastructure Stability. ITU-T Focus Group Digital Financial Services, December 2016. Geneva, Switzerland.
19. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. ETH Zurich, December 2016. Zurich, Switzerland.
20. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. University of Richmond, October 2016. Richmond, Virginia.
21. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Indiana University, September 2016. Bloomington, Indiana.
22. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Aalto University Computer Science Department Forum, August 2016. Helsinki, Finland.
23. 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.
24. Updated Mobile Money Vulnerability Report. International Telecommunications Union Digital Financial Services Working Group Workshop, May 2016. Washington, DC.
25. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. UF Eye Opener Discovery Breakfast - University of Florida, May 2016. Gainesville, FL.
26. 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.
27. 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.
28. 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.
29. Chasing Telephony Security: Where the Wild Things... Are? University of Florida - Department Colloquium, January 2014. Gainesville, FL.
30. Chasing Telephony Security: Where the Wild Things... Are? Verizon Wireless RNC/Data Center, October 2013. Alpharetta, GA.
31. Chasing Telephony Security: Where the Wild Things... Are? University of Waterloo - CrySP Speaker Series on Privacy, October 2013. Waterloo, ON, Canada.
32. Analyzing Malicious Traffic in Cellular Networks. GSM Association's (GSMA) Mobile Malware Community Workshop, July 2013. Mountain View, CA.
33. Threats to Mobile Devices. US Federal Trade Commission (FTC) Public Forum - Invited Speaker, June 2013. Washington, D.C.
34. Chasing Telephony Security: Where the Wild Things... Are? University of Wisconsin - Madison, Security Seminar, March 2013. Madison, WI.

35. 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.
36. Chasing Telephony Security: Where the Wild Things... Are? Stanford Security Seminar, March 2013. Stanford, CA.
37. Chasing Telephony Security: Where the Wild Things... Are? University of California, Berkeley, Security Group, March 2013. Berkeley, CA.
38. Chasing Telephony Security: Where the Wild Things... Are? Carnegie Mellon University CyLab Seminar, February 2013. Pittsburgh, PA.
39. Chasing Telephony Security: Where the Wild Things... Are? University of Oregon Department of Computer Science Colloquium, November 2012. Eugene, OR.
40. 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.
41. Needles and Haystacks: Digging for Ground Truth on Mobile Malware. ZISC Workshop on Secure Mobile and Cloud Computing, ETH Zurich, June 2012. Zurich, Switzerland.
42. Panel: Advice for Early Career Faculty. CRA Career Mentoring Workshop, February 2012. Washington, D.C.
43. Research Challenges in Cellular and Mobile Network Security. US-China Software Workshop (Co-Sponsored by NSF and NSFC), September 2011. Beijing, China.
44. Mobile Security: Understanding Risks to Critical Infrastructure. Invited Talk: US Department of State East African Workshop on Cyberspace Security, July 2011. Nairobi, Kenya.
45. Tomorrow's Issues: Solving the Mobile Security Threat. Invited Talk: Centre for Secure Information Technologies (CSIT) Queen's University, March 2011. Belfast, Northern Ireland.
46. PinDr0p: Using Single-Ended Audio Features to Determine Call Provenance. Invited Talk: MITRE Corporation, March 2011. Burlington, MA.
47. Defeating Session Hijacking Attacks with Disposable Web Credentials. Invited Talk: Facebook, February 2011. Palo Alto, CA.
48. Understanding the Disruptive Potential of Malware in Cellular Networks. Invited Talk: RSA Conference, February 2011. San Francisco, CA.
49. Panel: Voice Security – Now Just a False Sense of Security and Privacy. Invited Panelist: Mobile Security Symposium, February 2011. San Francisco, CA.
50. Understanding the Disruptive Potential of Malware in Cellular Networks. Invited Talk: Concordia University, May 2010. Montreal, QC, Canada.
51. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Qualcomm Research, March 2010. San Diego, CA.
52. 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.
53. Considerations for EAS Over Cellular Text Messaging Services. 3G Americas Webinar, July 2009.

54. University Telephony Research Panel. Conference on Principles, Systems and Applications of IP Telecommunications (IPTCOMM), July 2009.
55. The Evolving Mobile Landscape: Emerging Security Threats. Mobile Security eConference, SC Magazine, June 2008.
56. Characterizing the Impact of Rigidity on the Security of Cellular Networks. University of Washington, February 2009. Seattle, WA.
57. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Microsoft Research, February 2009. Redmond, WA.
58. Next Year's Problems. Secure Computing (SC) Magazine Webinar, November 2008.
59. Panel: Embedded Systems and their Increasing Impact on Infrastructure Security. Workshop on Embedded Systems Security (WESS), October 2008.
60. Can you DoS me now? Security Issues in Cellular Networks. Georgia Institute of Technology, September 2008. Atlanta, GA.
61. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Georgia Institute of Technology, April 2008. Atlanta, GA.
62. Characterizing the Impact of Rigidity on the Security of Cellular Networks. AT&T Research Labs, April 2008. Florham Park, NJ.
63. Characterizing the Impact of Rigidity on the Security of Cellular Networks. University of Arizona, March 2008. Tucson, AZ.
64. Cellular Networks Security Panel. USENIX Security Symposium, August 2007. Boston, MA.
65. malnets:Large-Scale Malicious Networks via Compromised Access Points. The Pennsylvania State University - ACM Club Invited Speaker, October 2006. State College, PA.
66. malnets:Large-Scale Malicious Networks via Compromised Access Points. The University of Michigan, October 2006. Ann Arbor, MI.
67. Exploiting Open Functionality in SMS-Capable Cellular Networks. The University of Michigan, October 2006. Ann Arbor, MI.
68. Exploiting Open Functionality in SMS-Capable Cellular Networks. High Technology Crime Investigation Association (HTCIA), September 2006. Pittsburgh, PA.
69. Trends in Security: Critical Engineering in the Large. Schlumberger Innovate IT! Workshop, May 2006. Cambridge, MA.
70. Exploiting Open Functionality in SMS-Capable Cellular Networks. InfraGard Pittsburgh Chapter General Meeting, September 2006. Pittsburgh, PA.
71. 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-ransomware-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 Burrell. WABE NPR - Mobile Web Browsers Full of Security Risks, Tech Professor Finds. <http://wabe.org/post/mobile-web-browsers-full-security-risks-tech-professor-finds>, December 2012.

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 - http://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.