

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Gregory G. Raleigh et al. Attorney Docket Nos.: 39843-0183IP1, 39843-0183IP2
U.S. Patent No.: 9,609,510
Issue Date: March 28, 2017
Appl. Serial No.: 14/208,236
Filing Date: March 13, 2014
Title: AUTOMATED CREDENTIAL PORTING FOR MOBILE DEVICES

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: 7 February 2025

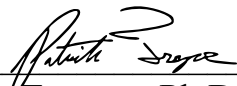
By: 
Patrick Traynor, Ph.D.

Table of Contents

| | | |
|-------|--|-----|
| I. | QUALIFICATIONS AND BACKGROUND INFORMATION..... | 4 |
| II. | LEGAL PRINCIPLES..... | 11 |
| | A. Anticipation | 11 |
| | B. Obviousness..... | 11 |
| III. | OVERVIEW OF CONCLUSIONS FORMED | 13 |
| IV. | BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE '510 PATENT | 14 |
| V. | INTERPRETATIONS OF THE '510 PATENT CLAIMS AT ISSUE..... | 15 |
| VI. | THE '510 PATENT..... | 16 |
| | A. Overview of the '510 Patent..... | 16 |
| | B. Prosecution History of the '510 Patent..... | 18 |
| VII. | OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES . | 20 |
| | A. Overview of Salmela | 20 |
| | B. Overview of Rishy-Maharaj | 24 |
| | C. Combination of Salmela and Rishy-Maharaj | 25 |
| | D. Overview of Bennett..... | 28 |
| | E. Combination of Salmela, Rishy-Maharaj, and Bennett..... | 30 |
| | F. Overview of FCCReg | 32 |
| | G. Combination of Salmela, Rishy-Maharaj, Bennett, and FCCReg..... | 34 |
| | H. Overview of Ionescu..... | 37 |
| | I. Combination of Salmela, Rishy-Maharaj, and Ionescu..... | 40 |
| | J. Overview of Sigmund..... | 42 |
| | K. Combination of Salmela, Rishy-Maharaj, and Sigmund..... | 44 |
| | L. Overview of Johansson..... | 47 |
| | M. Combination of Salmela, Rishy-Maharaj, and Johansson..... | 49 |
| | N. Overview of Slavov | 52 |
| | O. Combination of Salmela, Rishy-Maharaj, and Slavov | 54 |
| | P. Overview of Gupta | 56 |
| | Q. Combination of Salmela, Rishy-Maharaj, and Gupta..... | 58 |
| VIII. | MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '510 CLAIMS UNPATENTABLE | 60 |
| | A. The Salmela-Rishy-Maharaj Combination Renders Claims 1-3, 6-7, 11, 14-25, 28-33, 35-39, 41-43, and 45-48 Obvious | 60 |
| | B. The Salmela-Rishy-Maharaj-Bennett Combination Renders Claims 21, 23, and 25 Obvious | 150 |

| | | |
|-----|---|-----|
| C. | The Salmela-Rishy-Maharaj-Bennett-FCCReg Combination Renders Claims 26-27 Obvious | 152 |
| D. | The Salmela-Rishy-Maharaj-Ionescu Combination Renders Claims 12-13 Obvious..... | 155 |
| E. | The Salmela-Rishy-Maharaj-Sigmund Combination Renders Claims 4-5 and 8-10 Obvious..... | 156 |
| F. | The Salmela-Rishy-Maharaj-Johansson Combination Renders Claim 40 Obvious..... | 162 |
| G. | The Salmela-Rishy-Maharaj-Slavov Combination Renders Claim 34 Obvious..... | 165 |
| H. | The Salmela-Rishy-Maharaj-Gupta Combination Renders Claim 44 Obvious..... | 166 |
| IX. | CONCLUSION | 168 |

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 Appendix A, includes a list of publications on which I am a named author. It contains further details regarding my experience, education, publications, and other qualifications to render an expert opinion in connection with this proceeding.

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

- U.S. Patent No. 9,609,510 (EX1001), and excerpts of its accompanying prosecution history (EX1002)
- U.S. Publication No. 2009/0217364 (“Salmela”) (EX1004)
- U.S. Publication No. 2013/0165075 (“Rishy-Maharaj”) (EX1005)
- U.S. Publication No. 2010/0029273 (“Bennett”) (EX1006)
- U.S. Publication No. 2012/0236760 (“Ionescu”) (EX1007)
- U.S. Publication No. 2010/0222024 (“Sigmund”) (EX1008)
- U.S. Publication No. 2010/0177663 (“Johansson”) (EX1009)
- U.S. Patent No. 9,191,394 (“Novak”) (EX1010)
- U.S. Publication No. 2009/0253409 (“Slavov”) (EX1011)
- Federal Communications Commission (FCC) Regulation (2010), *available at*, <https://www.govinfo.gov/content/pkg/FR-2010-06-22/pdf/2010-15073.pdf> (“FCCReg”) (EX1012)
- U.S. Publication No. 2011/0130119 (“Gupta”) (EX1013)
- U.S. Publication No. 2008/0122796 (“Jobs”) (EX1014)
- Samsung Galaxy SII Mobile Phone User Manual (2011), *available at* <https://ringtones.specialtyansweringservice.net/wp-content/uploads/2014/08/manuals/samsung-galaxys2-userguide.pdf> (EX1015)

- iPhone User Guide For iPhone OS 3.1 Software (2009), *available at*
https://cdsassets.apple.com/live/6GJYWVAV/user/ma616_iphone_ios3_1_user_guide.pdf (EX1016)
- Architecture and Enablers for Optimized Radio Resource Usage in Heterogeneous Wireless Access Networks (2009), *available at*
https://www.researchgate.net/publication/224371987_Architecture_and_Enablers_for_Optimized_Radio_Resource_Usage_in_Heterogeneous_Wireless_Access_Networks_The_IEEE_19004_Working_Group (EX1017)
- Characterizing Radio Resource Allocation for 3G Networks (2010), *available at* https://www.cs.columbia.edu/~lierranli/coms6998-7Spring2014/papers/RRC3G_imc2010.pdf (EX1018)
- Operating System Implications of Fast, Cheap, Non-Volatile Memory (2011), *available at*
https://www.usenix.org/legacy/events/hotos11/tech/final_files/Bailey.pdf (EX1019)
- iPod touch User Guide for iOS 5.1 Software (2012), *available at*
https://cdsassets.apple.com/live/6GJYWVAV/user/ma1627_ipod_touch_ios_5_user_guide.pdf (EX1020)
- Samsung Galaxy SIII 4G LTE Smartphone User Manual (2013), *available at*
<https://downloadcenter.samsung.com/content/UM/202101/20210101045744>

723/ATT_SGH-I747_Galaxy_SIII_English_User_Manual_KK_NE4_F1.pdf

(EX1021)

- U.S. Publication No. 2009/0249247 (“Tseng”) (EX1022)
- U.S. Patent No. 7,280,818 (“Clayton”) (EX1023)
- U.S. Patent No. 8,923,824 (“Masterman”) (EX1024)
- Jacob et al., *Memory Systems: Cache, DRAM, Disk* (2007) (“Jacob”) (EX1027)
- U.S. Publication No. 2012/0185636 (“Leon”) (EX1028)
- U.S. Patent No. 8,060,748 (“Johansson-748”) (EX1029)
- U.S. Publication No. 2006/0258289 (“Dua”) (EX1030)
- European Telecommunications Standards Institute (ETSI) Technical Specification 23.003 v8.11.0 (2011), *available at* https://www.etsi.org/deliver/etsi_ts/123000_123099/123003/08.11.00_60/ts_123003v081100p.pdf (EX1031)
- Control Servers in the Core Network (2000), *available at* <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=1247211968f9167dbc5e7ea896bd910762e57ba7> (EX1032)
- Wireless Application Protocol (WAP) Architectural Overview (2001), *available at* https://www.openmobilealliance.org/release/Push/V2_1-20051122-C/WAP-250-PushArchOverview-20010703-a.pdf (EX1033)

II. LEGAL PRINCIPLES

A. Anticipation

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

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

B. Obviousness

18. I have been informed that a patent claim is invalid as "obvious" under 35 U.S.C. § 103 in light of one or more prior art references if it would have been obvious to a POSITA, taking into account (1) the scope and content of the prior art,

(2) the differences between the prior art and the claims, (3) the level of ordinary skill in the art, and (4) any so called “secondary considerations” of non-obviousness, which include: (i) “long felt need” for the claimed invention, (ii) commercial success attributable to the claimed invention, (iii) unexpected results of the claimed invention, and (iv) “copying” of the claimed invention by others. For purposes of my analysis, and at the direction of counsel, I have applied the March 14, 2013 filing date of the provisional application listed on the face of the ’510 Patent as the date of invention in my obviousness analyses, although in many cases the same analysis would hold true even at an earlier time than March 14, 2013.

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 1-3, 6-7, 11, 14-25, 28-33, 35-39, 41-43, and 45-48 of the '510 Patent are obvious over Salmela in view of Rishy-Maharaj.
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 21, 23, and 25 of the '510 Patent are obvious over Salmela in view of Rishy-Maharaj, and further in view of Bennett.
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 26-27 of the '510 Patent are obvious over Salmela in view of Rishy-Maharaj, further in view of Bennett, and further in view of FCCReg.
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 12-13 of the '510

Patent are obvious over Salmela in view of Rishy-Maharaj, and further in view of Ionescu.

- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 4-5 and 8-10 of the '510 Patent are obvious over Salmela in view of Rishy-Maharaj, and further in view of Sigmund.
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claim 40 of the '510 Patent is obvious over Salmela in view of Rishy-Maharaj, and further in view of Johansson.
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claim 34 of the '510 Patent is obvious over Salmela in view of Rishy-Maharaj, and further in view of Slavov.
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claim 44 of the '510 Patent is obvious over Salmela in view of Rishy-Maharaj, and further in view of Gupta.

IV. BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE '510 PATENT

21. Based on the foregoing and upon my experience in this area, a person of ordinary skill in the art (“POSITA”) relating to the subject matter of the ’510 Patent by the Critical Date (March 14, 2013) would have had (1) a bachelor’s degree in computer science, computer engineering, electrical engineering, or a related field, and (2) 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 ’510 PATENT CLAIMS AT ISSUE

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

Petitioner that I should use March 14, 2013 as the point in time for claim interpretation purposes.

VI. THE '510 PATENT

A. Overview of the '510 Patent

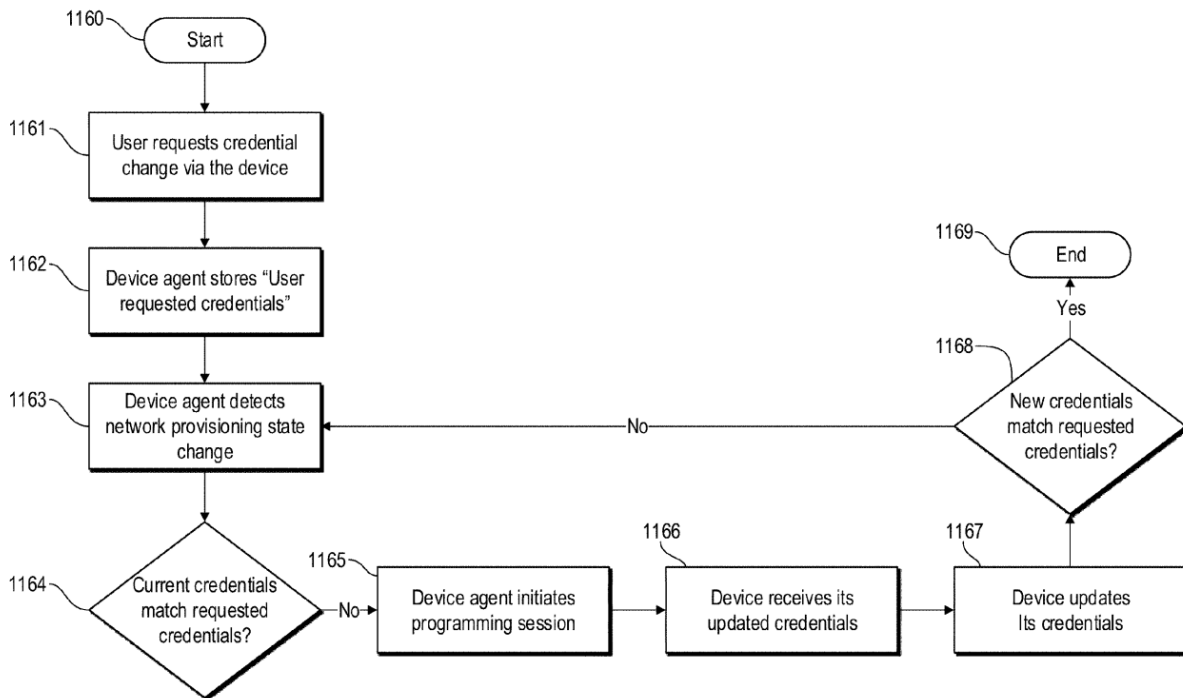
24. The '510 Patent describes techniques for automatically updating credentials stored by a mobile device. EX1001, 5:10-6:57, 6:4-7:15, 9:4-10:56, 11:20-12:44. The mobile device uses these stored credentials to gain access to wireless access networks. EX1001, 5:21-6:57. I noticed that examples of credentials providing wireless network access include an international mobile subscriber identity (IMSI), a phone number, and an internet protocol (IP) address, among many other examples. EX1001, 5:21-48, 9:59-10:8. The '510 Patent explains that:

Disclosed herein are systems, devices, and methods that provide for the updating of device credentials after a phone number port without user intervention. In some embodiments, the mobile device detects a network provisioning state change (e.g., detects that the device credentials are to be updated) and automatically initiates a programming session with a programming server to enable the device to obtain the desired credentials without the intervention of the user. Automation of this process ensures that the updating of credentials occurs when necessary and without user intervention. One of the benefits of this process is that it can reduce calls to a customer care center because this process helps to ensure that the device does not enter into a state in which it cannot interact with the network system and, as a result, appear to be unusable to the end user.

EX1001, 7:1-15

25. Another notable feature of the system is that a user of the mobile device can input a request to update the device's stored network access credentials through a user interface. EX1001, 7:28-68, 10:57-67, FIG. 3. According to the '510 Patent, the mobile device can also detect a "network provisioning state change" based on a denial of network access, which can indicate a need for the credentials on the device to be updated. EX1001, 9:4-35, 10:57-11:27. Based on receiving the user request and detecting the network provisioning state change, the mobile device can initiate a process to update network access credentials. EX1001, 11:28-12:44, FIG. 3. This process is depicted below in FIG. 3:

FIG. 3



EX1001, FIG. 3.

26. One notable feature of the process depicted above in FIG. 3 is that the mobile device performs several actions upon detecting a network provisioning state change. EX1001, 11:38-12:33. I noticed that these actions include (1) determining whether current credentials match user requested credentials, initiating a programming session with a network element, (2) receiving updated credentials, and (3) determining whether the updated credentials match the user requested credentials. EX1001, 11:38-12:33. The '510 Patent explains that credentials can be updated “automatically” and “without informing the subscriber” in some embodiments. EX1001, 12:34-35. Consequently, apart from the initial step of receiving a user request to update credentials, it is clear that wireless device can automatically perform the rest of the credential update process without user participation. EX1001, 10:57-12:44.

B. Prosecution History of the '510 Patent

27. I noticed that the Examiner mailed just one office action during original examination of the '510 Patent. EX1002, 28-33. In this office action, the original claims were rejected as allegedly being obvious in view of a single reference—Novak (EX1010)—which is not a subject of any of the grounds that I analyzed for this Petition. EX1002, 30-31. None of the references that I considered for Grounds 1A-1H were analyzed or even mentioned in the office action.

28. In one brief section of the office action, the Examiner also took official notice that (1) “a particular credential, that may be updated, associated with a particular client using a wireless device has been common knowledge within the wireless communication network art,” and that (2) “error reports associated with data transfers have been common knowledge in the art, as are wireless devices placing a voice call associated with land lines.” EX1002, 31. The applicant conceded that the above-identified facts “may be known generally” in its response to the office action. EX1002, 24-26.

29. The applicant’s response to the office action included at least two notable amendments to independent claims 1 and 47. EX1002, 15-23. In one of these amendments, the applicant clarified that the one or more credentials are for “authorizing” the wireless device to “use a wireless access network to access one or more services.” EX1002, 15-23. Specifically, I noticed that the applicant asserted that “all reasonable interpretations of this phrasing limit the credentials to those that a wireless device uses to gain authorization to use a wireless access network” and “the credentials may not authorize the access of all services over the wireless access network, but they authorize access to at least one service.” EX1002, 24. In another one of these notable amendments, the applicant clarified that the “determine,” “initiate,” “obtain,” and “assist” steps recited in the independent claims are

performed “automatically” in response to detecting the network-provisioning state change. EX1002, 15-23.

30. Shortly after the applicant submitted its amendments and remarks in response to the office action, the Examiner allowed all pending claims. EX1002, 6-13. The Examiner generically alleged in a notice of allowance mailed January 12, 2017 that “the prior art, either alone or in combination, does not disclose Applicant’s inventive claim language,” but did not otherwise address any specific claim features in the reasons for allowance. EX1002, 11. A second notice of allowance mailed February 15, 2017 acknowledged consideration of a pair of information disclosure statements that the applicant had filed after the first notice, but the second notice otherwise maintained the allowable subject matter. EX1002, 1-5.

31. Despite this history of prosecution before the Examiner, it is apparent that the ’510 Patent never should have been allowed. This is demonstrated below in my analysis of Grounds 1A-1H which are based on references that were never analyzed by the Examiner as part of a rejection. As demonstrated by this Petition, the prior art teaches and renders obvious each of the Challenged Claims.

VII. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES

A. Overview of Salmela

32. Salmela describes techniques for automatically updating credentials on a wireless device, much like the ’510 Patent. EX1004, [0003]-[0012], [0020]-[0027].

Salmela explains that “[s]ecure and convenient management of subscription credentials [stood] as an ongoing challenge in the field of wireless communications” by the critical date of the ’510 Patent. EX1004, [0003]. One reason that credential provisioning is a challenge in the telecommunications industry is that a home operator must issue credentials to grant a wireless device access to a network, and revoke or cause such credentials to expire when access for the wireless device is no longer authorized.

33. For example, I noticed that according to Salmela, “subscription credentials ... link the device to a given network service provider (home operator) and allow it to authenticate itself to the operator’s home network, and to any number of visited networks, subject to roaming agreements, etc.” EX1004, [0003]. In acknowledging the challenges of provisioning wireless devices with credentials for network access, Salmela specifically recognizes that it can be difficult for device owners to manually update subscription credentials when they “chang[e] subscription plans, and particularly when changing home operator affiliations.” EX1004, [0009]. To address this issue, Salmela proposes a credential updating process that is automatically triggered upon detecting that subscription credentials currently provisioned on a wireless device result in “a failure to gain network access.” EX1004; [0027], *generally* [0020]-[0027], FIG. 2.

34. As a solution to the telecommunications industry problem of granting and revoking access of a wireless device to a network, Salmela explains that “[r]ather than delivering a fully provisioned device to [a] purchaser, one approach to provisioning provides for the sale and/or distribution of preliminarily provisioned devices.” EX1004; [0006]. For example, the manufacturer can pre-provision the device with “temporary access credentials.” EX1004; [0006]. Because of this preliminary provisioning, Salmela’s wireless device is configured to “revert[] from subscription credentials to temporary access credentials, in response to detecting an access failure.” EX1004, [0010].

35. Such network access failure can occur when the device’s current subscription credentials expire or are otherwise no longer valid to authenticate the device on the network under the subscription plan that the device had been operating on previously. EX1004, [0010]. This can result from the device owner having changed subscription plans to a new home operator. EX1004, [0010]. According to Salmela, “[t]he device [then] uses [] temporary access credentials to gain temporary network access,” and if “the device determines [that] it needs new subscription credentials,” it “uses the temporary access to obtain them.” EX1004, [0010], *see also*, [0011]-[0013], [0020]-[0028], [0031], FIGS. 1-2, 4. I noticed that Salmela’s process for obtaining new subscription credentials involves (1) determining that new subscription credentials are needed, (2) initiating a programming session with a

credentialing server if it is determined that new subscription credentials are needed, (3) obtaining the new subscription credentials from the credentialing server, and (4) downloading the new subscription credentials to a secure element in a memory of the device. EX1004, [0024], [0025], [0041].

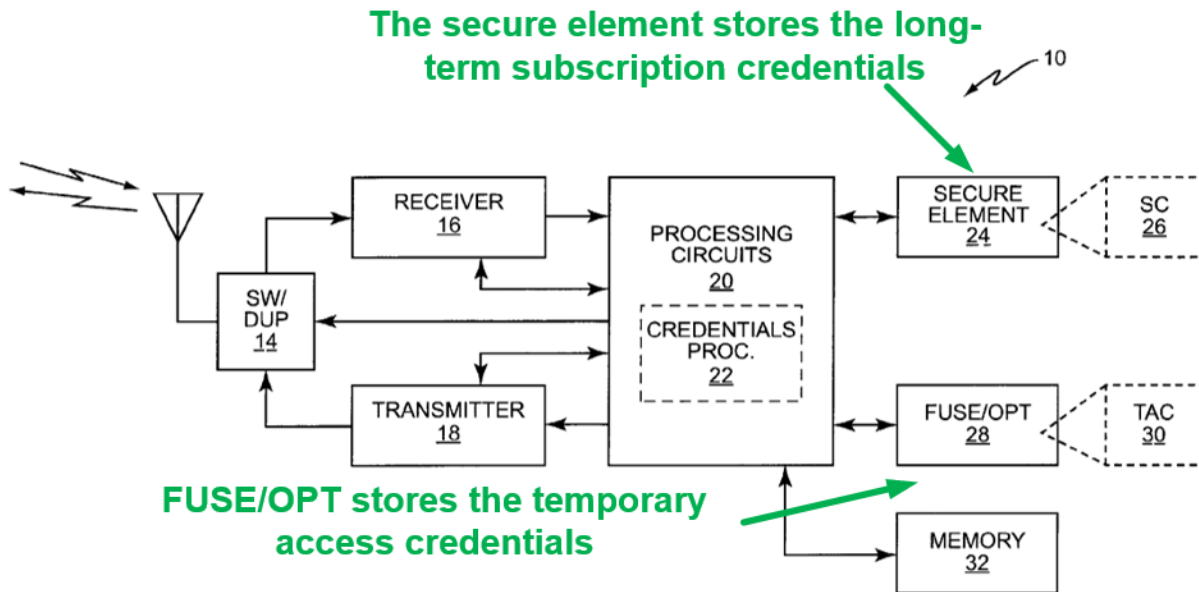


FIG. 1

EX1004, FIG. 1.

36. Because Salmela’s device can execute this automatic process for updating credentials, “a device owner” of Salmela’s wireless device can “change subscriptions without having to first update the affected device.” EX1004, [0050]. In particular, when a device owner changes subscriptions, I noticed that each device associated with the changed subscription automatically updates its own credentials by performing Salmela’s process of detecting network access failure, reverting to temporary credentials, and updating to new credentials associated with the changed

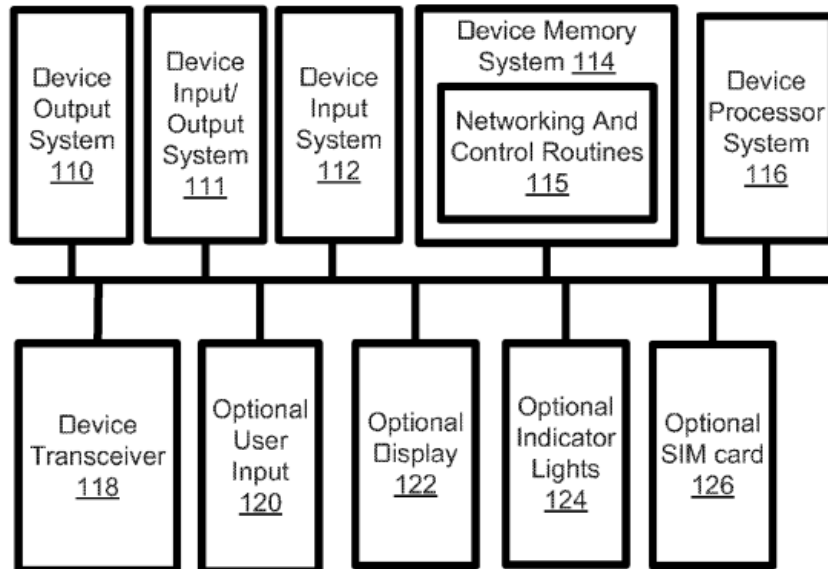
subscription. EX1004, [0011] (“To the extent that any subscription agreement change invalidates device-held subscription credentials, each such device will detect access failure with its current subscription credentials and revert to temporary access credentials and contact a registration service or other entity to determine if new subscription credentials are needed.”), [0024], [0025], [0041].

B. Overview of Rishy-Maharaj

37. Rishy-Maharaj describes techniques for updating credentials on a wireless device according to a user-selected subscription plan, which is similar to Salmela and the ’510 Patent. EX1004, [0010]-[0012]; EX1005, [0028]-[0036]. Although Salmela does not describe in detail how the user initiates a request to change subscription plans or the home operator, Rishy-Maharaj clearly describes that a user can make a request through a user interface of a wireless device (e.g., by selecting a subscription plan through a user interface of the wireless device from a list of options displayed on the user interface). EX1005, [0108]-[0121]. For instance, I noticed that Rishy-Maharaj explains that the user interface of a wireless device can “list services...for the user to select,” thus allowing “the user to select a plan.” EX1005, [0112]; *see also* (“[T]he user may select the subscription plan and network that best suits the user.”). Moreover, Rishy-Maharaj’s user interface includes a “device output system,” a “device input system,” an “optional user input,” and an

“optional display,” elements that alone or in combination represent a user interface.

The user interface of Rishy-Maharaj is depicted below in FIG. 1B:



EX1005, FIG. 1B.

EX1005, [0058]-[0060], [0066], [0067], FIG. 1B.

C. Combination of Salmela and Rishy-Maharaj

38. Based upon my knowledge and experience in the field and my review of Salmela and Rishy-Maharaj, it is clear that Salmela discloses that the owner of one or more wireless devices can request to update a subscription plan used by those devices to access the wireless access network(s) of an affiliated home operator. EX1004, [0008] (“the device owner can select and activate subscriptions”), [0009] (“changing subscription plans”), [0011] (“an owner ... can change subscription agreements”), [0053] (“changing subscription information”), Abstract (“new home operator”); *supra*, §VII.A. Even if it is the case that Salmela does not expressly

disclose how the device owner submits a request to update the subscription plan of a wireless device (e.g., through a user interface of the wireless device), Rishy-Maharaj demonstrates that one known option was to input the request through a user interface of an affected wireless device. EX1005, [0111]-[0112]; *supra*, §VII.B. It would have been obvious to apply Rishy-Maharaj's teachings to Salmela such that Salmela's wireless device receives a user selection through a user interface, as taught by Rishy-Maharaj. In doing so, Salmela's device owner would select to activate or change subscriptions through a user interface of a wireless device, thereby prompting each of the user's devices associated with the selected subscription plan to automatically obtain new subscription credentials as needed upon detecting a failure to gain network access with their current subscription credentials, according to the processes disclosed in Salmela.

39. As a *first* reason, a POSITA would have recognized that implementing Salmela's wireless device to include a "user interface" (e.g., user input 120) as suggested by Rishy-Maharaj would be advantageous in allowing a user to activate or change subscription plans on the wireless device itself without requiring the user to interact with other devices or with a call center. EX1005, [0058]-[0060], [0066], [0067], FIG. 1B. This would result in the process of activating or changing subscriptions more convenient to the user by reducing the time, burden, and

resources that would otherwise be necessary for the user to activate or change subscriptions. EX1005, [0066].

40. As a *second* reason, implementing Salmela's wireless device to include a "user interface" (e.g., display 122) as suggested by Rishy-Maharaj would allow the wireless device to provide information to the user in a manner that would conveniently guide the user's selection of a subscription plan. EX1005, [0067]. For example, Rishy-Maharaj explains that the wireless device can be advantageously "used for displaying information to the user about how to operate wireless device 102, about available local networks, prompts for proceeding through the process of selecting a local network, and/or adding funds to an established subscription." EX1005, [0067]. In the Salmela-Rishy-Maharaj combination, this information displayed by the wireless device would aid the user in selecting a subscription plan on a single device.

41. As a *third* reason, implementing Salmela's wireless device to include a "user interface" (e.g., display 122) as suggested by Rishy-Maharaj would have been obvious as a predictable application of a known technique (e.g., enabling selection of a subscription plan through a user interface of a wireless device) to a known system as taught by Salmela to achieve merely predictable results.

42. As a *fourth* reason, it would have been obvious for a POSITA to implement Salmela's wireless device with a user interface as suggested by Rishy-

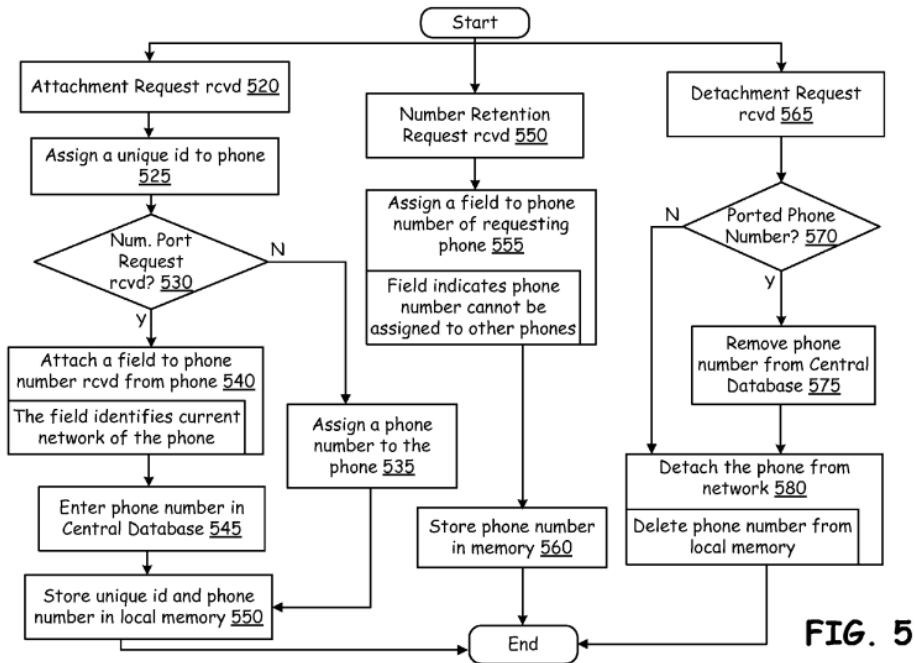
Maharaj because doing so represents one of a finite number of predictable solutions for receiving a user selection from a user. For example, because a user interface provides a practical and easy way for a user to make a request (e.g., by making a selection from a list of options on a screen), the user interface is a predictable solution. Furthermore, a POSITA would have appreciated that a request to change subscription plans for a wireless device could be made through a user interface of the wireless device itself, using another device, or by relaying the request to a third-party (e.g., a call center, retail outlet, or other agent of a network service provider). It is clear that a POSITA would have been driven toward the first option in many cases for the reasons discussed above, including to promote user convenience in a straightforward manner.

43. A POSITA would have reasonably expected success implementing the Salmela-Rishy-Maharaj combination because it was well known before the Critical Date of the '510 Patent for wireless devices to have user interfaces including hardware capable of executing software and performing the functions described above. EX1004, [0021], [0030].

D. Overview of Bennett

44. Bennett describes a “wireless phone” that can execute a “network switching application” for allowing the wireless phone to retain a phone number or obtain a new phone number when switching from a current service provider network

to a new service provider network, much like Salmela which describes techniques for changing a home operator associated with a wireless communication device. EX1006, [0008], [0009], [0021], [0023]-[0025]. For example, I noticed that Bennett's wireless phone can receive a user request to switch service provider networks via the user interface of the wireless phone. Alternatively, Bennett's wireless phone can determine to switch networks automatically without user input. EX1006, Abstract, [0021]-[0028], [0048]-[0054], FIG. 1, FIG. 7. Bennett's wireless phone automatically sends a network attachment request to an alternative network and sends a phone number retention request to a home network based on determining to switch from the home network to the alternative network. Notably, this allows the wireless phone to "port" its phone number to the alternative network while preventing the home network from assigning the number to another phone. EX1006, [0025]-[0028], [0042]-[0045] FIG. 1, FIG. 5. Alternatively, Bennetts' wireless phone can receive a new phone number by sending a network attachment request to the alternative network without requesting to port a current phone number. EX1006, [0025]-[0028], [0042]-[0045] FIG. 1, FIG. 5. An example process for switching service provider networks is depicted below in FIG. 5:



EX1006, FIG. 5.

E. Combination of Salmela, Rishy-Maharaj, and Bennett

45. As I described above in connection with Ground 1A, Salmela discloses techniques for automatically updating subscription credentials for a wireless device when the device fails to gain network access using its current subscription credentials, and the device detects this failure. *Supra*, §VII.A. Additionally, Salmela’s device automatically updates credentials when a user has requested to change subscription plans or the home operator network for the device—thus prompting a situation where the current subscription credentials are no longer valid for achieving access to the network. *Supra*, §VII.A.

46. Salmela explains that its subscription credentials allow the wireless device to authenticate itself on a wireless access network. Salmela identifies an

international mobile subscription identity (IMSI) as one prominent example of subscription credentials. EX1004, [0012], [0023]. Salmela does not limit the application of its techniques to just IMSI-based embodiments, but instead recognizes that its “methods and apparatuses may be implemented in a variety of system and device types.” EX1004, [0057]. To the extent Salmela does not expressly identify other suitable subscription credentials, however, it is clear that a POSITA would have known of other such credentials—such as a non-IMSI phone number used to route calls to a phone—as evidenced by Bennett. *Supra*, §VII.D. For example, Bennett describes techniques that “allow[] a phone to retain its number while switching from a current network to another network,” where the phone number is specifically “one that is dialed by a calling party” to reach the phone.¹ EX1006, [0021].

¹ A POSITA would have understood the phone numbers described in Bennett to be phone numbers that can be dialed to reach the device associated with those numbers. For example, the phone numbers described in Bennett may be a mobile station international subscriber directory number (MSISDN) in a global system for mobile communications (GSM) network or a mobile directory number (MDN) in a code division multiple access (CDMA) network.

47. To the extent that Patent Owner argues that a “phone number” should be limited to a dialable phone number (e.g., an MSISDN), it is clear that multiple reasons would have led a POSITA to implement Salmela’s subscription credentials to include a dialable phone number in accordance with Bennett’s suggestion (e.g., MSISDN or MDN). For example, an ability to update a dialable phone number of Salmela’s device 10 would have beneficially allowed the device 10 to be reached at a new phone number under a new subscription plan, including a phone number that the user ported from another device. Furthermore, wireless phones were also conventionally assigned dialable phone numbers in addition to an IMSI before the Critical Date. The ’510 Patent’s own description of background technology recognized that a “phone number” was a known credential for authenticating a mobile device in a wireless access network. EX1001, 5:21-45. It is clear that a POSITA would have reasonably expected success implementing the combination given the common use of dialable phone numbers by the Critical Date of the ’510 Patent.

F. Overview of FCCReg

48. FCCReg includes a set of final rules promulgated by the Federal Communications Commission (FCC) that are published in the Federal Register (Vol. 75, No. 119) dated June 22, 2010. *See* EX1012. I have been informed that the federal register is where rules are published before being codified into law as part of the

Code of Federal Regulations (CFR). Specifically, FCCReg includes rules relating to “Local Number Portability Porting Interval and Validation Requirements” and “Telephone Number Portability.” *See* EX1012. FCCReg explains that the FCC “adopted standardized data fields for simple number porting to streamline the port process and enable service providers to accomplish simple *wireline-to-wireline* and *intermodal* ports,” meaning that FCCReg’s rules cover phone number porting for both landline phones and wireless phones. EX1012, 1. For example, FCCReg expressly discloses that the term “intermodal ports” refers to “the porting of numbers from wireline providers to wireless providers, and vice versa.” EX1012, 1. FCCReg also acknowledges that number portability dates back to at least 1934, and that the FCC has since passed regulations for number porting “between wireline providers,” “between wireless providers,” and for “intermodal porting.” EX1012, 1. Thus, FCCReg describes regulations for porting phone numbers between wireline devices (wireline-to-wireline ports), between wireless devices, and also porting phone numbers between wireline devices and wireless devices (wireline-to-wireless ports and wireless-to-wireline ports). EX1012, 1, 11.

49. FCCReg therefore confirms that it was well-known by 2010 for phone numbers to be ported between wireless phones, between wireless phones and landlines, and between landlines—such that the Federal government saw fit to promulgate regulations concerning these ports. *See* EX1012. For example, FCCReg

provides that “[a]ll telecommunications carriers required by the commission to port telephone numbers must complete a simple wireline-to-wireline or simple intermodal port request within one business day,” and also acknowledges that the FCC has “established obligations for...porting between wireless providers, and intermodal porting.” EX1012, 1, 11. This means that FCCReg demonstrates that at least as early as June 2010, telecommunications carriers were required by law in the United States to port a number between wireless devices and to port a number from a landline to a wireless device. EX1012, 1, 11. It is apparent that these obligations for porting between wireless providers would cover a port from a first wireless device associated with a first wireless carrier to a second wireless device associated with a second wireless carrier. EX1012, 1, 11. Additionally, FCCReg’s obligations and requirements for carriers to support intermodal ports clearly establish that service providers were required to port a number from a landline associated with a wireline carrier to a wireless device associated with a wireless carrier by 2010. EX1012, 1, 11.

G. Combination of Salmela, Rishy-Maharaj, Bennett, and FCCReg

50. As I described above in the overview of Bennett (§VII.D, *supra*), Bennett describes a “wireless phone” that retains an existing phone number or obtains a new phone number when the phone switches between service providers—that is, when a single wireless phone maintains or replaces its original number.

EX1006, [0023] (The phone has two options when the phone switches to a new network...A first of the two options is to receive a new phone number from the new network...A second of the two options is to retain the phone number issued by the home network), *see also* [0008], [0009] (“issues a new phone number to the cellular phone”), [0021], [0023]-[0025]. To the extent Salmela, Rishy-Maharaj, and Bennett do not expressly disclose examples where a wireless phone obtains a new phone number from another wireless device or from a land line, these features would have been obvious when further considering the teachings of FCCReg given the detailed explanation of the kinds of devices that phone numbers can be ported between. EX1012, 1 (explaining that the FCC has regulated porting “between wireless providers” and porting “from wireline providers to wireless providers”), 6 (acknowledging that wireless providers believe the “wireless-to-wireless” porting process to be efficient and cost saving), 11 (detailing requirement for service providers to complete “wireline-to-wireless ports” within set periods of time). Based on my review of Salmela, Rishy-Maharaj, Bennett, and FCCReg, multiple reasons would have led a POSITA to implement the device 10 of the Salmela-Rishy-Maharaj-Bennett combination with landline-to-wireless and wireless-to-wireless number porting in accordance with FCCReg’s suggestion.

51. As a *first* reason, a POSITA would have been motivated to implement the device 10 of the Salmela-Rishy-Maharaj-Bennett combination further in

accordance with FCCReg’s suggestion to support porting numbers from landlines and other wireless devices because doing so would allow a user to maintain a number from an older mobile phone or landline on a new mobile phone. This would ensure that callers would still be able to reach the user by calling the same number after the port occurs, with the calls reaching the new mobile phone instead of the older mobile phone or land line. Similarly, the user would not need to distribute a new phone number to be reached by contacts.

52. As a *second* reason, a POSITA would have been motivated to implement the device 10 of the Salmela-Rishy-Maharaj-Bennett combination with FCCReg’s requirement to permit reuse of phone numbers. For example, because a phone number includes only seven digits after the area code, each phone number within an area code must include a unique combination of seven numbers—meaning that unique phone numbers can be scarce especially for area codes corresponding to high-population areas. Therefore, it is beneficial to enable porting so that phone numbers are re-used, ensuring that everyone within an area code can have a unique phone number.

53. As a *third* reason, implementing device 10 of the Salmela-Rishy-Maharaj-Bennett combination with FCCReg’s suggestion to enable number porting from other wireless devices and landlines would have been obvious as a predictable application of a known technique (e.g., enabling number porting) to a known system

as taught by the Salmela-Rishy-Maharaj-Bennett combination to achieve merely predictable results. It is clear that a POSITA would have reasonably expected success implementing the combination given the common use of dialable phone numbers by the Critical Date of the '510 Patent. Furthermore, because FCCReg promulgates standards for communication, a POSITA would have been motivated to comply with the regulations of FCCReg in designing a wireless device for use in telecommunications networks.

H. Overview of Ionescu

54. Ionescu describes techniques for establishing an emergency communication session using a mobile device. EX1007, [0011]-[0013], [0034]-[0042], FIG. 4. I noticed that one example technique disclosed by Ionescu involves a mobile device that initiates an emergency communication session based on receiving a user input through a user interface. EX1007, [0035]. For example, the user can dial of “911” on a keypad or touchscreen to initiate a voice call, or the user can send a text message, or any other emergency request. EX1007, [0035], Cl. 7 (“the emergency communication session is a voice call or a text message”), [0018]. Ionescu explains that the mobile device can initiate the emergency communication session with a preferred network (e.g., an IP network or a circuit-switched (CS) network) based on receiving the user request to establish the emergency communication session. EX1007, [0036], [0037].

55. Ionescu expressly discloses that the mobile device can determine whether an emergency communication session initiated by a user was successfully initiated. EX1007, [0036] (explaining that “the mobile device attempts to initiate a communication session via the IP network” and “a test is made to determine whether the session has been successfully started and connectivity achieved with an emergency responder”), *see also* [0037]. The mobile device attempts to connect to another network if the initiation is unsuccessful. EX1007, [0036] (“The system then ceases use of the IP-based network, and attempts access using the CS network.”), *see also* [0037]. Ionescu’s process for detecting network access failures is illustrated below in FIG. 4:

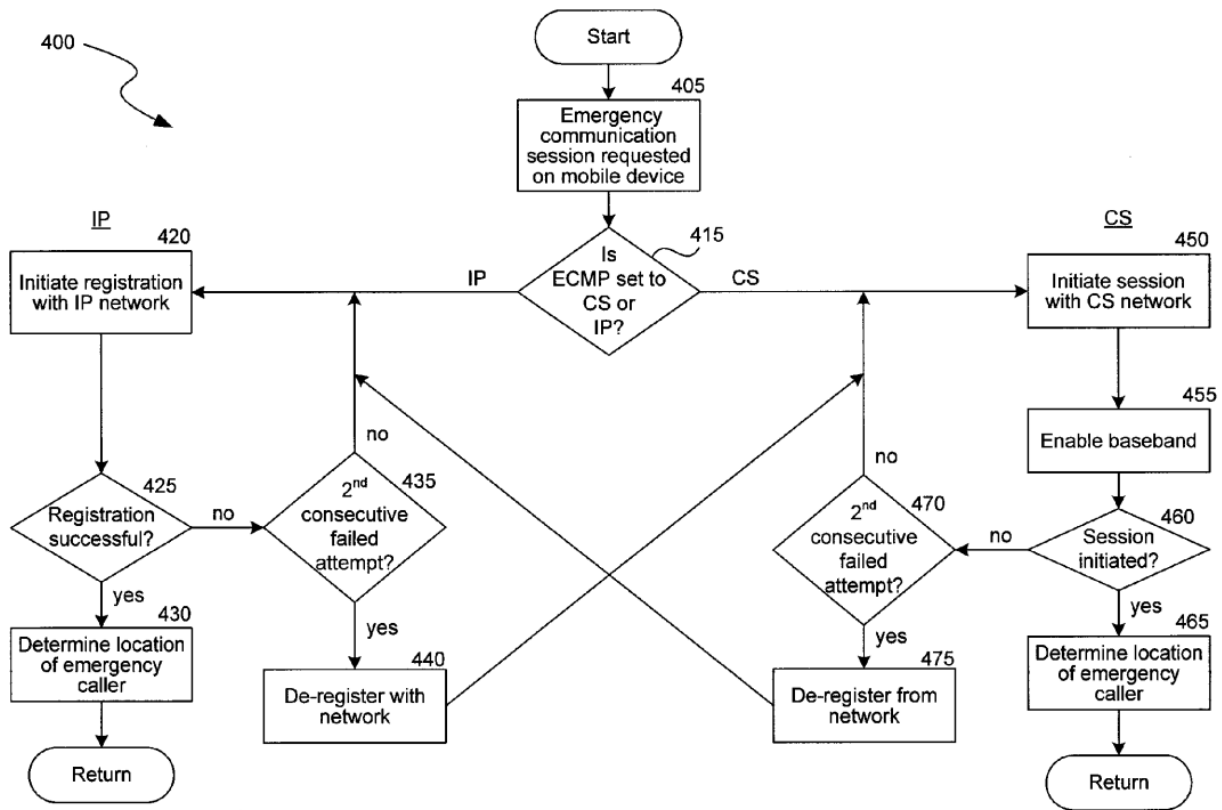


Fig. 4

EX1007, FIG. 4.

56. Ionescu's techniques therefore involve a wireless device attempting to establish an emergency communication session by placing a voice call or sending a text message, identifying a network access failure by determining that the emergency communication session was not established, and performing actions based on identifying the network access failure. EX1007, [0011]-[0013], [0034]-[0042], FIG. 4. Ionescu explains that the access attempts are made by the mobile device, the network access failure is detected by the mobile device, and the actions are performed by the mobile device. EX1007, [0034]-[0037], FIG. 4.

I. Combination of Salmela, Rishy-Maharaj, and Ionescu

57. Salmela discloses that device 10 can detect a failure to gain network access using current subscription credentials 26. EX1004, [0020]-[0027], FIGS. 1-2. In response to detecting this failure, Salmela's device 10 can initiate a process to update the current subscription credentials 26. EX1004, [0020]-[0027], FIGS. 1-2. Even if Salmela does not expressly disclose examples where device 10 detects the failure to gain network access based on a failed attempt to place a voice call or a failure to send a text message, it is clear that these features nonetheless would have been obvious in view of Ionescu. Multiple reasons would have prompted a POSITA to implement Salmela's device 10 in accordance with Ionescu's suggestions for detecting a failure to place a voice call or send a text message before the alleged invention of the '510 Patent.

58. As a *first* reason, a POSITA would have understood that implementing Salmela's device 10 to detect a network access failure by detecting a failure to place a call or send a text would predictably provide a way for device 10 to detect network access failure based on communication modes that device 10 commonly uses the network to achieve. For example, a "cellular communication device" such as device 10 would routinely use subscription credentials 26 to access a network to place voice calls or send text messages. EX1004, [0021]. Detecting a failure to access this

network based on failing to place a voice call or send a text message is predictable in the context of cellular phones.

59. As a *second* reason, in examples where a user requests to change wireless access networks, a POSITA would have been prompted to use Salmela's process to automatically update subscription credentials 26 in response to detecting a failure to place a phone call or send a text message because these network changes often result in situations where current subscription credentials are insufficient to place calls or send text messages over the new network. Detecting network access failure based on detecting a failure to place a voice call or send a text message would thus be a predictable way for device 10 to determine that subscription credentials need to be replaced.

60. As a *third* reason, implementing Salmela's device 10 to detect network access failure based on failed voice calls and texts would have been obvious to a POSITA because a common feature of cellular communication devices such as Salmela's device 10 is an ability to make emergency communications such as the calls and texts described in Ionescu. It would have been obvious for a POSITA to apply Ionescu's voice call and text message failure detection teachings in the context of Salmela's automatic credential update process.

61. As a *fourth* reason, implementing Salmela's device 10 to detect network access failure based on failed voice calls and texts as suggested by Ionescu

would have been obvious as a predictable application of a known technique to a known system as taught by Salmela to achieve merely predictable results. Furthermore, there are a finite number of ways to detect network access failure—two prominent examples being failed calls and failed texts—so it would have been obvious to try implementing device 10 with Ionescu’s suggested techniques for detecting failed calls and failed texts.

62. Considering the predictable electrical/network and software components involved in the combination and the relatively advanced state of the art at the time, a POSITA would have reasonably expected success applying Ionescu’s teachings for detecting a failure to gain network access based on failed voice calls or texts to Salmela before the Critical Date. Indeed, Salmela indicates that there are “multiple methods of detecting a failure to gain network access,” thus acknowledging that its techniques are not limited by the specific examples disclosed therein. EX1004, [0033], [0057]-[0058]. This means that Ionescu’s proposal to detect network access failures based on failed voice calls and texts is consistent with the multiple detection methods contemplated in Salmela.

J. Overview of Sigmund

63. Sigmund describes a mobile device 118 that includes a password-protected voicemail service which allows a user to access voicemails upon entering the correct password. EX1008, [0003]-[0008], [0028]-[0040], FIGS. 1-3. Notably,

Sigmund discloses a process for the user to reset the password for the voicemail service by initiating the reset through a user interface. EX1008, [0032]-[0035], FIG. 2. Specifically, the user inputs a password reset request to a user interface to initiate the password reset (e.g., by selecting an option displayed on the user interface). EX1008, [0041]-[0057], FIGS. 4-5. In response to receiving the request to reset the password, the mobile device 118 can execute a process to automatically update the password for the voicemail service. This process is depicted below in Sigmund's FIG. 2:

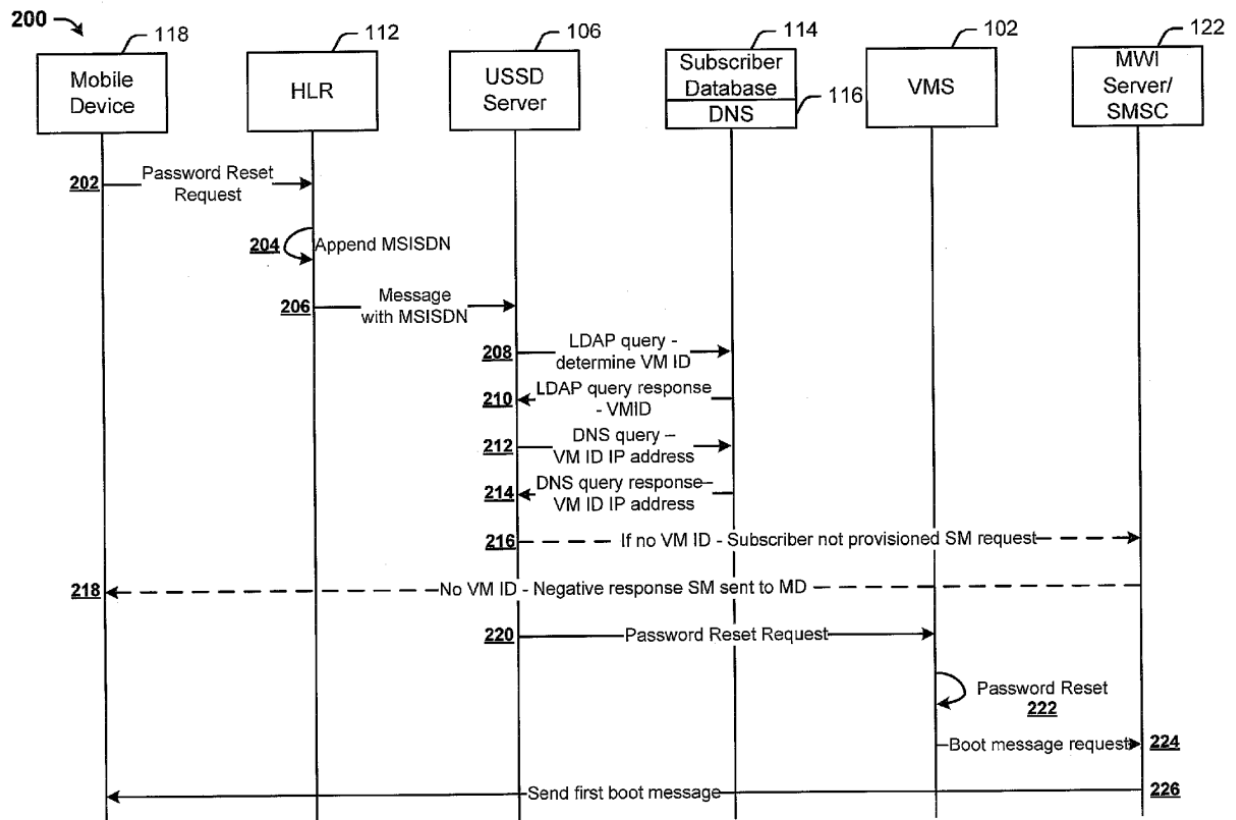


FIG. 2

EX1008, FIG. 2.

64. Sigmund's process to update the voicemail password involves mobile device 118 displaying notifications to the user in certain situations. EX1008, [0032]-[0036], FIG. 2. In one example, mobile device 118 can display a "short message" indicating that the subscriber is not provisioned for voicemail service and therefore the voicemail password cannot be reset—thus indicating that a process to reset the voicemail password has failed. EX1008, [0034], FIG. 2. I also noticed that Sigmund's mobile device 118 can display a message confirming that the password reset was successful by informing the subscriber of a new default password resulting from the successful password reset. EX1008, [0035], [0039], FIGS. 2-3. Sigmund further describes notifications "to reset a voicemail password after a voicemail account is enabled" and "as a cue or reminder to setup a voicemail box prior to receipt of incoming voice messages." EX1008, [0036].

K. Combination of Salmela, Rishy-Maharaj, and Sigmund

65. The Salmela-Rishy-Maharaj combination provides a process by which Salmela's device 10 automatically updates subscription credentials stored on the device 10 in response to detecting a network access failure and receiving a user's request to update a subscription plan for the device 10. EX1004, [0020]-[0027], FIGS. 1-2; EX1005, [0058]-[0069]; [0108]-[0121], FIG. 1B, FIG. 2. Sigmund describes notifications that can be displayed on a user interface in connection with the process to update credentials, even if the Salmela-Rishy Maharaj combination

lacks disclosure of these notifications. Consequently, it would have been obvious to implement device 10 of the Salmela-Rishy-Maharaj combination with the notifications of Sigmund.

66. As I described above in my overview of Sigmund (*Supra*, §VII.J), Sigmund discloses techniques for displaying notifications on a wireless device in a variety of circumstances—notably, in cases where a credential update process (e.g., a process to update the voicemail password) is successful and in cases where the credential update process is unsuccessful. EX1008, [0032]-[0037], FIG. 2. Multiple reasons would have prompted a POSITA to implement Salmela’s device 10 in accordance with Sigmund’s suggestion for causing notifications to be sent and displayed on a wireless device before the alleged invention of the ’510 Patent.

67. As a *first* reason, a POSITA would have understood presenting notifications through a user interface of Salmela’s device 10 that relate to Salmela’s credential updating process would enhance user satisfaction. Specifically, the notifications would advantageously inform the user of the status of the credential update and notify the user of particular milestones or events in the process. One benefit of these notifications would manifest in an example where device 10 obtains updated credentials to replace subscription credentials 26, the updated credentials later becoming invalid. In examples like this, providing a user with a notification indicating that an error has occurred or a process is underway to update the

credentials would present the user with information that is useful for determining whether the user needs to take additional steps to address the issue, such as rebooting device 10.

68. As a *second* reason, a POSITA would have understood that causing Salmela's device 10 to present notifications at different points in the process to update subscription credentials 26 would have been beneficial to assure the user of device 10 that the device is operating according to an intended process—removing possible doubts that the device 10 is performing automatic steps to ensure network connection. Notifications are commonly used in the field of cellular communication devices to provide information about the status of various processes and operations such as software updates, device reboot, application downloads, among others. A POSITA would have understood this.

69. As a *third* reason, a POSITA would have understood that causing Salmela's device 10 to present notifications at different points in the process to update subscription credentials 26 would have been useful to provide the user with information concerning a process that is important to the device's ability to connect to the wireless access network. A POSITA would have been motivated to provide the user with information relating to the credential update process so that the user is notified when access is granted or lost. This is because subscription credentials grant

device 10 with access to wireless access networks to receive voice, text, and data service.

70. As a *fourth* reason, it would have been obvious as a predictable application of a known technique (e.g., presenting notifications) to a known system as taught by Salmela to achieve merely predictable results by implementing Salmela's device to present notifications at different points in the process to update subscription credentials 26, as suggested by Sigmund . *KSR*, 550 U.S. at 417 (2007).

71. Considering the predictable electrical/network and software components involved in the combination and the relatively advanced state of the art at the time, it is clear that a POSITA would have reasonably expected success achieving the combination before the earliest effective filing date of the '510 Patent (Mar. 14, 2013).

L. Overview of Johansson

72. Johansson discloses a user equipment such as a mobile device that is able to communicate with a wireless access network (e.g., a "public communication services network") for the purpose of accessing one or more services. EX1009, [0038]-[0052], FIG. 2. For instance, I noticed that a user of Johansson's user equipment can purchase a subscription for the user equipment to use the wireless access network when the user equipment does not have a pre-established subscription with that network. EX1009, [0044]-[0050], FIG. 2. Johansson teaches

that the user equipment can use a temporary credential, referred to by Johansson as a temporal mobile station identifier (TMSI), to initially gain access to the network, a process that is very similar to Salmela and the '510 Patent which both describe temporary credentials that provide limited access. EX1009, [0047]-[0049], FIG. 2. An example process for obtaining a temporary credential is depicted below in Johansson's FIG. 3:

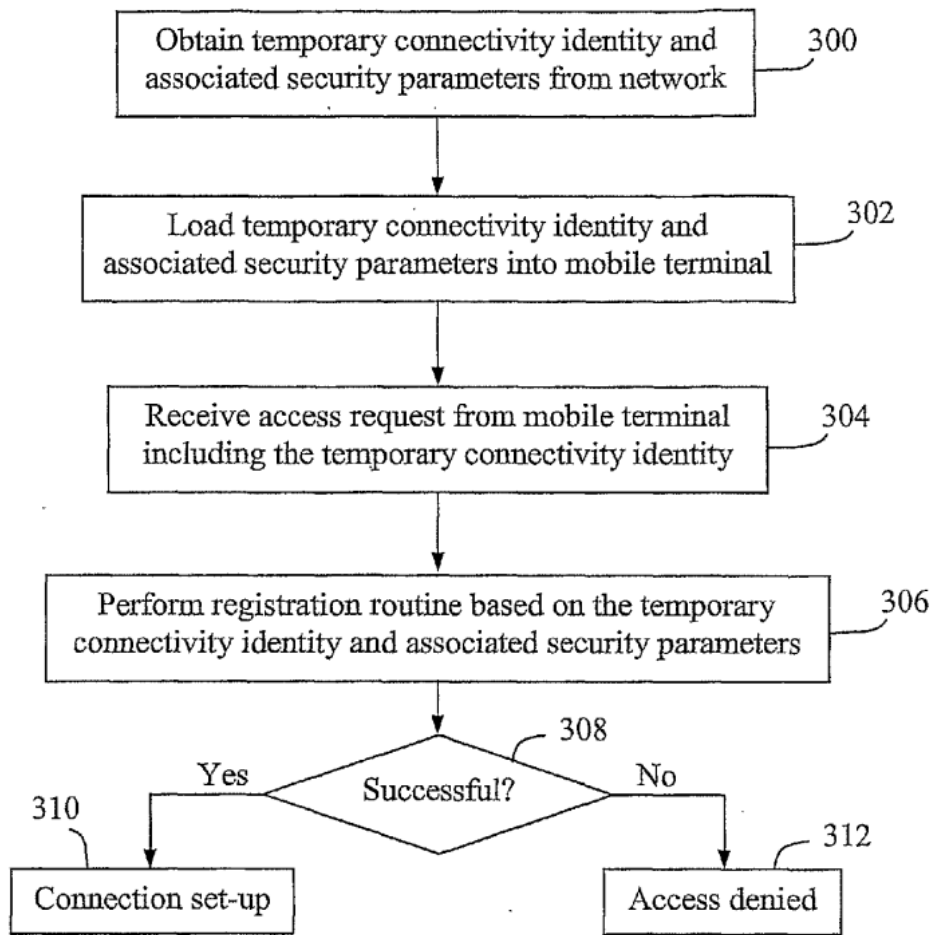


Fig. 3

EX1009, FIG. 3.

73. I noticed that Johansson’s user equipment receives the temporary credential from a connectivity providing unit 202 in communication with the user equipment. EX1009, [0047]-[0049], FIG. 2. That is, Johansson’s user equipment can receive the temporary credential from a device separate from the user equipment in some cases, rather than merely using a pre-provisioned temporary credential that is already stored in a memory of the user equipment. After receiving the temporary credential, Johansson’s user equipment can establish a connection with the wireless access network using the temporary credential. EX1009, [0050]-[0056], FIGS. 2-3.

M. Combination of Salmela, Rishy-Maharaj, and Johansson

74. Much like Johansson teaches using temporary credentials to achieve temporary access, Salmela explains that device 10 can revert to temporary access credentials 30. EX1004, [0020]-[0027]. Salmela’s credential reversion can establish temporary network access and initiate a programming session with a credentialing server to update subscription credentials 26. EX1004, [0020]-[0027], [0045], FIGS. 1-2. Specifically, Salmela explains that “[t]he temporary access credentials 30 may, for example, be burned into secure fuses or other secure OTP memory within the device 10, during its manufacture or initial configuration.” EX1004, [0023].

75. To the extent that Salmela does expressly disclose how the temporary access credentials 30 are loaded on device 10 during its initial configuration or in other suitable manners, Johansson discloses the conventional option of obtaining

temporary access credentials from a network system communicatively coupled to a wireless device, the network system being separate from the wireless device. *Supra*, §VII.L. Multiple reasons would have prompted a POSITA to implement Salmela's device 10 in accordance with Johansson's suggestions for obtaining temporary access credentials from a network system before the Critical Date of the '510 Patent.

76. As a *first* reason, implementing Salmela's device 10 to obtain temporary access credentials from a network system as suggested by Johansson would beneficially allow device 10 to achieve temporary access in cases where device 10 was not pre-provisioned with the correct temporary access credentials during manufacture of the device 10. In other words, a POSITA would have sought to implement device 10 with capabilities to obtain alternative temporary access credentials as taught by Johansson in cases where the correct credentials are not pre-provisioned in device 10, because the temporary access credentials 30 stored in the memory of device 10 are not necessarily valid for obtaining temporary access to every wireless access network that device 10 seeks to connect to. Obtaining temporary access credentials over-the-air from a network system would also allow device 10 to update the temporary access credentials as needed. This would be advantageous in cases where the original temporary access credentials expired, the original temporary access credentials were invalidated due to a leak to an

unauthorized user or other security breach, or where the original temporary access credentials were simply insufficient for connecting to a particular network.

77. As a *second* reason, a POSITA would have understood that allowing device 10 to receive temporary credentials from a network element would be beneficial in cases where a service provider seeks to strictly control temporary access to the service provider network by declining to issue temporary access credentials to wide swaths of wireless devices. For example, some service providers elect to distribute temporary access credentials from a connectivity providing unit rather than granting temporary access via pre-provisioned credentials, meaning that a POSITA would have been motivated to modify device 10 to receive temporary credentials from a network system in those situations. This would allow these service providers to work through the network system to provide temporary access to select devices, while withholding access to other devices.

78. As a *third* reason, obtaining temporary access credentials from a network system as suggested by Johansson would have been obvious as a predictable application of Johansson's known technique (e.g., receiving a temporary credential from a network system) to a known system as taught by Salmela to achieve merely predictable results.

79. Considering the predictable electrical/network and software components involved in the combination and the relatively advanced state of the art

at the time, it is clear that a POSITA would have reasonably expected success achieving the combination before the Critical Date.

N. Overview of Slavov

80. Similar to Salmela, Slavov describes a wireless device 100 that can use temporary credentials, referred to by Slavov as a “temporary device identifier,” to obtain “permanent” subscription credentials that provide access to a wireless access network. EX1011, [0005]-[0007], [0022]-[0028], FIGS. 1-2. Also similar to Salmela, Slavov’s permanent credentials offer more robust access to the network and the temporary credentials offer more limited access to the network. EX1011, [0026]. Slavov’s FIG. 2 depicts an “exemplary activation process” that allows wireless device 100 to register with home network 20 so that device 100 can download permanent subscription credentials that ensure continued access to the network:

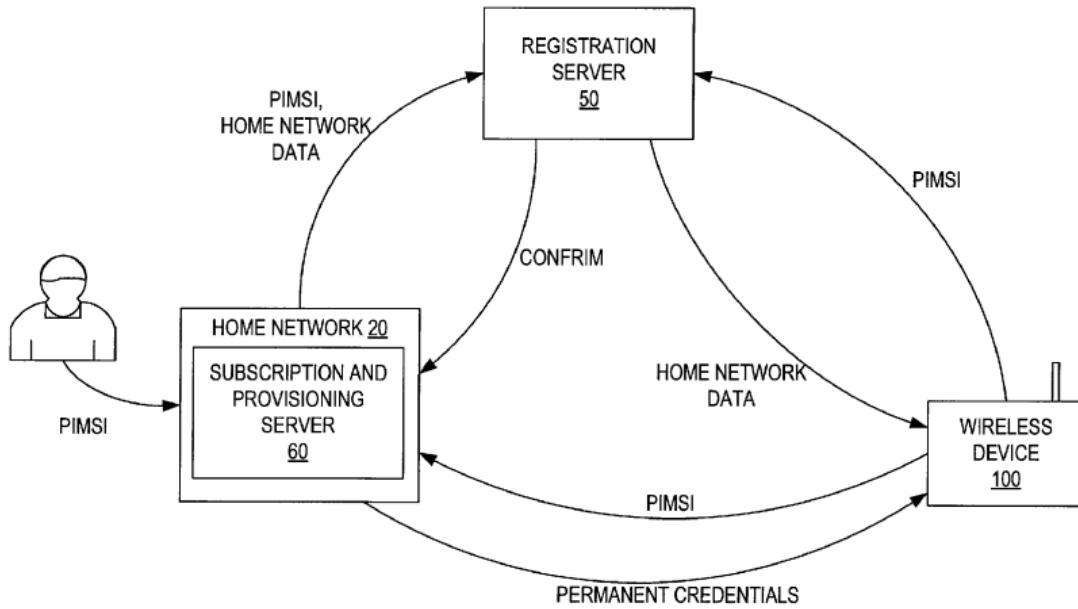


FIG. 2

EX1011, FIG. 2.

81. A user can subscribe wireless device 100 to the home network 20 through a web interface or website to register wireless device 100 with the home network 20. EX1011, [0024], [0049]. I noticed that this subscription process involves the user providing a temporary device identifier of wireless device 100 to home network 20. EX1011, [0026]. The wireless device 100 can also be pre-provisioned by the manufacturer with the same temporary device identifier that the user provides during the subscription process. EX1011, [0023], [0026].

82. Wireless device 100 can use the temporary device identifier to obtain permanent credentials for continued access to home network 20 as a result of the

user subscribing to home network 20 using the same temporary device identifier that is also pre-provisioned on wireless device 100. EX1011, [0026]-[0028]. That is, because the home network 20 received the temporary device identifier as part of subscription, the home network 20 can verify the wireless device 100 when the wireless device 100 contacts the home network 20 using the temporary device identifier.

O. Combination of Salmela, Rishy-Maharaj, and Slavov

83. The Salmela-Rishy-Maharaj combination provides a process that allows a wireless device—such as the device 10 of Salmela—to automatically update subscription credentials stored on the device 10 in response to receiving a request from a user through a user interface to update a subscription plan for the device 10. EX1004, [0020]-[0027], FIGS. 1-2; EX1005, [0058]-[0069]; [0108]-[0121], FIG. 1B, FIG. 2. Even if Salmela and Rishy-Maharaj do not expressly disclose that device 10 obtains information through a website as part of receiving this user request, Slavov discloses a feature for obtaining information through such a website. EX1011, [0024], [0049]. Multiple reasons would have prompted a POSITA to implement device 10 of the Salmela-Rishy-Maharaj combination in accordance with Slavov's suggested technique for a user to subscribe to a home network through a website before the alleged invention of the '510 Patent. For example, in the combination, the user interface described in Rishy-Maharaj could

predictably be a web-based interface with information about available subscription plans received from a website and presented on the device 10 through a web browser or other web portal or application. EX1005, [0111], [0112].

84. As a *first* reason, a POSITA would have appreciated that implementing device 10 according to Slavov's suggestion for permitting a user to subscribe to wireless services through a website would have advantageously allowed the user to subscribe to a new plan and request new subscription credentials through a standard web browser or other application on device 10, which is capable of loading a website. For example, the user could access a subscription portal through the website without needing to install special software on the device.

85. As a *second* reason, implementing device 10 according to Slavov's suggestion for permitting a user to subscribe to wireless services through a website would predictably allow device 10 to prompt the user to input certain information using the website. For example, device 10 could use the website for guiding the user to provide inputs through the user interface, including an input to subscribe device 10 to a home network.

86. As a *third* reason, implementing device 10 of the Salmela-Rishy-Maharaj combination so that a user can interact with device 10 through a website as suggested by Slavov would have been obvious as a predictable application of a known technique (e.g., using a website to subscribe to a home network) to a known

system as taught by the Salmela-Rishy-Maharaj combination to achieve merely predictable results. Furthermore, receiving a user input through a website represents one of a finite number of ways to receive user input, meaning that it would have been obvious to try an implementation where a wireless device receives user input through a website.

87. A POSITA also would have reasonably expected success implementing the Salmela-Rishy-Maharaj-Slavov combination. Indeed, wireless devices of the same or similar types as those described in the Salmela-Rishy-Maharaj combination permit internet browsing of websites. *See, e.g.*, EX1004, [0021] (“device 10 is a cellular communication device, such as a cellular radiotelephone, pager, PDA, computer or network access card”); EX1005, [0030] (“wireless device 102 may be any wireless electronic device capable of connecting to a network, such as a phone, personal desktop assistant (‘PDA’), laptop computer, tablet, or netbook, for example”). Wireless devices by the Critical Date of the ’510 Patent (e.g., March 14, 2013) commonly included interfaces, applications, network connectivity, internet browsing, and other capabilities sufficient to provide a website for prompting user input as taught in Slavov.

P. Overview of Gupta

88. Gupta discloses a wireless communication device 120 that is capable of making voice calls. EX1013, [0023]-[0043], FIGS. 1-2. For example, wireless

communication device 120 can communicate with a wireless communication station 130 over a wireless link in a way that supports voice call service to the wireless communication device 120. EX1013, [0023]-[0043], FIGS. 1-2. Specifically, Gupta describes a process for “staging” the wireless communication device 120. EX1013, [0017]-[0021], [0034]-[0044], FIGS. 1-2. Staging involves “preparing” wireless communication device 120 to use the wireless access network. EX1013, [0017], [0018], [0021]. Furthermore, in some cases, staging involves downloading software enabling wireless communication device 120 to operate in the wireless access network as part of configuring the wireless communication device 120. EX1013, [0017], [0018], [0021].

89. Gupta explains that wireless communication device 120 can initiate a voice call that is received by a base station represented by wireless communication station 130 and routed to a wide area network (WAN) gateway 140 (sometimes referred to as “network infrastructure 140”). EX1013, [0023], [0024], [0028]-[0032], [0034]-[0036], FIGS. 1-2. This voice call can be part of a process to “stage” the wireless communication device 120, thus preparing wireless communication device 120 to continue to use the network after staging is complete. EX1013, [0017]-[0021], [0034]-[0043], FIGS. 1-2. WAN gateway 140 can authenticate the wireless communication device 120 and relay encrypted staging data to wireless

communication device 120 responsive to receiving the voice call from wireless communication device 120. EX1013, [0034]-[0037], FIG. 2.

Q. Combination of Salmela, Rishy-Maharaj, and Gupta

90. Device 10 of the Salmela-Rishy-Maharaj combination can automatically initiate a programming session with a network element based on detecting a network-provisioning state change as part of a process to obtain new subscription credentials from the network element, as I described above in my analysis of Ground 1A at Element [1i], *supra*. EX1004, [0020]-[0027], FIGS. 1-2. Gupta discloses the conventional option of authenticating a wireless device through the staging process such that the wireless device makes a voice call to a network element. EX1013, [0021], [0034]-[0043], FIG. 2, *supra*, §VII.P. Consequently, to the extent that Salmela does not expressly disclose that device 10 makes a voice call to initiate a programming session with a network element through a voice call, Gupta this feature. Multiple reasons would have prompted a POSITA to implement Salmela's device 10 in accordance with Gupta's suggestions for a wireless device to initiate a programming session by making a voice call before the Critical Date of the '510 Patent.

91. As a *first* matter, implementing device 10 of the Salmela-Rishy-Maharaj combination to initiate a programming session by making a voice call as suggested by Gupta would beneficially allow device 10 to automatically initiate a

process to provision itself when the user makes a call. For example, users often attempt to place voice calls when a wireless device connects to a new wireless access network—sometimes without the user’s knowledge that they are in a new network. It would be beneficial for Salmela’s device 10 to automatically initiate a programming session to provision itself by making a voice call to a network element so that the user receives seamless service.

92. As a *second* matter, a POSITA would have understood that allowing device 10 to initiate a programming session by making a voice call as suggested by Gupta would cause device 10 to initiate a programming session with a network element in a situation where a network-provisioning state change becomes apparent. For example, if device 10 places a voice call without being properly provisioned to use the wireless access network, implementing device 10 with Gupta’s voice call teachings would beneficially cause device 10 to initiate a process to provision itself when device 10 is not properly provisioned for voice calls.

93. As a *third* matter, initiating a programming session through making a voice call as taught by Gupta would have been obvious as a predictable application of Gupta’s known technique to a known system as taught by Salmela to achieve merely predictable results.

94. Considering the predictable electrical/network and software components involved in the combination and the relatively advanced state of the art

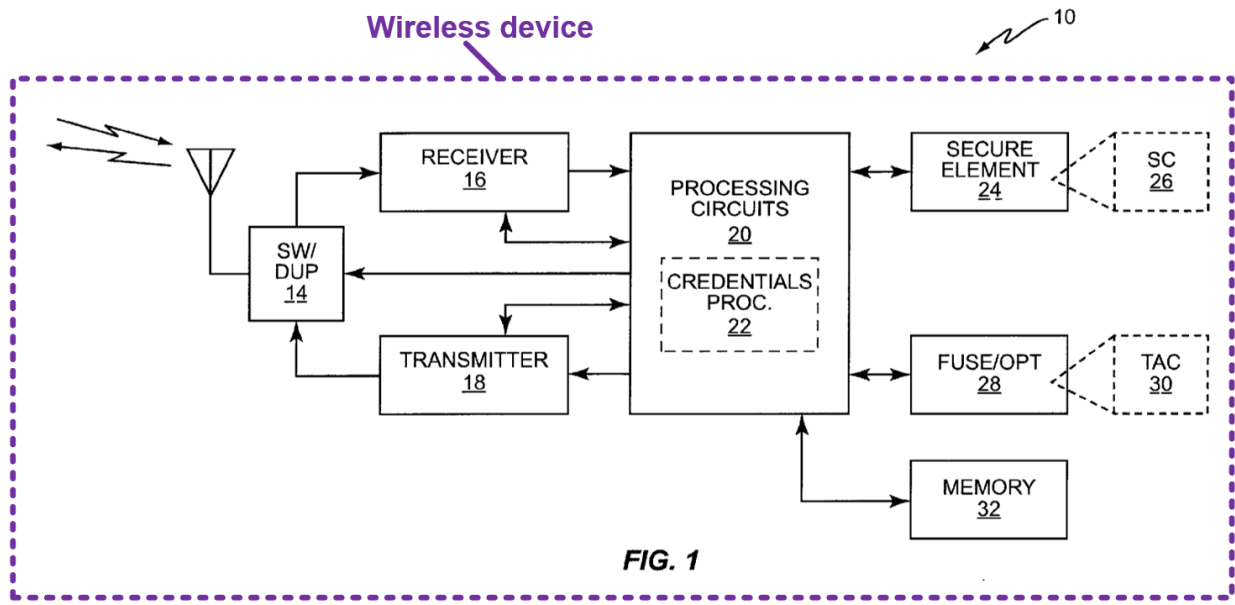
at the time, a POSITA would have reasonably expected success achieving the combination before the Critical Date.

VIII. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '510 CLAIMS UNPATENTABLE

A. The Salmela-Rishy-Maharaj Combination Renders Claims 1-3, 6-7, 11, 14-25, 28-33, 35-39, 41-43, and 45-48 Obvious

Element [1pre]: A wireless device, comprising:

95. To the extent the preamble is treated as a limitation, my review of Salmela and Rishy-Maharaj confirms that the Salmela-Rishy-Maharaj combination provides the claimed “wireless device.” For example, Salmela describes a “*wireless communication device 10*” in detail, sometimes referring to this wireless communication device as “device 10” or merely “device.” EX1004, [0002], [0010], [0020]-[0025], [0027]-[0029], [0033]-[0047]; FIG. 1. Salmela explains that wireless communication device 10 can be a “cellular communication device” in some embodiments. EX1004, [0021]. Furthermore, I noticed that Salmela’s wireless communication device 10 includes several components that clearly facilitate wireless communication including “one or more antennas 12, a switch and/or duplexer 14, a wireless signal receiver 16, and wireless signal transmitter 18.” EX1004, [0020], FIG. 1. An example of Salmela’s wireless communication device 10 is depicted below in FIG. 1:



EX1004, FIG. 1 (annotated).

Element [1a]: a user interface;

96. I noticed that Salmela clearly explains that wireless communication device 10 can be “a cellular communication device, such as a cellular radiotelephone, pager, PDA, computer.” EX1004, [0021]. By 2013, A POSITA would have recognized that all of these types of wireless devices commonly included a ***user interface*** by 2013. The fact that ***wireless devices*** included ***user interfaces*** by 2013 is corroborated by many sources published before 2013. *See, generally* EX1014 (describing numerous embodiments for implementing a user interface on a wireless device); EX1015, 10-15 (describing a mobile device that comprises a number of user interface elements including a touch screen, a menu key, a home key, a back key, and a search key); EX1016, 28-31 (describing a wireless mobile device that comprises a user interface including a “touchscreen”).

97. Salmela clearly acknowledges that a cellular handset user can “access subscribed services” through a home operator network. EX1004, [0004]. Accessing these “subscribed services” using a wireless device commonly involved, by 2013, interaction with a *user interface* on the wireless device (e.g., voice calls through a speaker and microphone, text messaging through a keypad and/or touchscreen, and internet browsing through a touchscreen). The fact that mobile devices commonly accessed subscribed services through user interaction with a user interface is corroborated by several references. EX1014, [0228]-[0300] (describing an application for a user to send text messages through a touchscreen of a user interface), [0544]-[0575] (describing an application for a user to make voice calls through a touchscreen of a user interface); EX1015, 30 (describing applications for use on a touch screen of a mobile device for sending text messages and emails); EX1016, 23 (describing applications that can be used on the touch screen of a mobile device for sending text messages and emails, making voice calls, and internet browsing).

98. It would have been obvious for a POSITA to implement a user interface in Salmela’s device based on the teachings of Rishy-Maharaj, to the extent Salmela does not expressly disclose that wireless communication device 10 includes a user interface. *Supra*, §VII.C. Rishy-Maharaj explains that wireless device 102 receives user inputs through a user interface of the device 102. EX1005, [0028]-[0046], [0108]-[0121], FIGS. 1A, 1B, 2. For example, wireless device 102 receives user

inputs for selecting subscription plans and managing credentials. EX1005, [0112] (“The wireless device 102 may also have an optional user input 120 to allow the user to select a plan.”).

99. It is apparent that wireless device 102 includes several user interface elements including a “device output system 110” and a “device input system 112.” EX1005, [0058]. I noticed, for example, that device output system 110 includes “a display system, a speaker system...and the like” which are common elements of user interfaces. EX1005, [0059]. Device input system 112 includes other common user interface elements including “a keyboard system...a mouse system, a track ball system...and the like.” EX1005, [0060]. Wireless device 102 of Rishy-Maharaj also includes “optional user input 120” and “optional display 122.” EX1005, [0058], [0066], [0067]. These parts of the *user interface* of Rishy-Maharaj’s wireless device 102 are depicted below in FIG. 1:

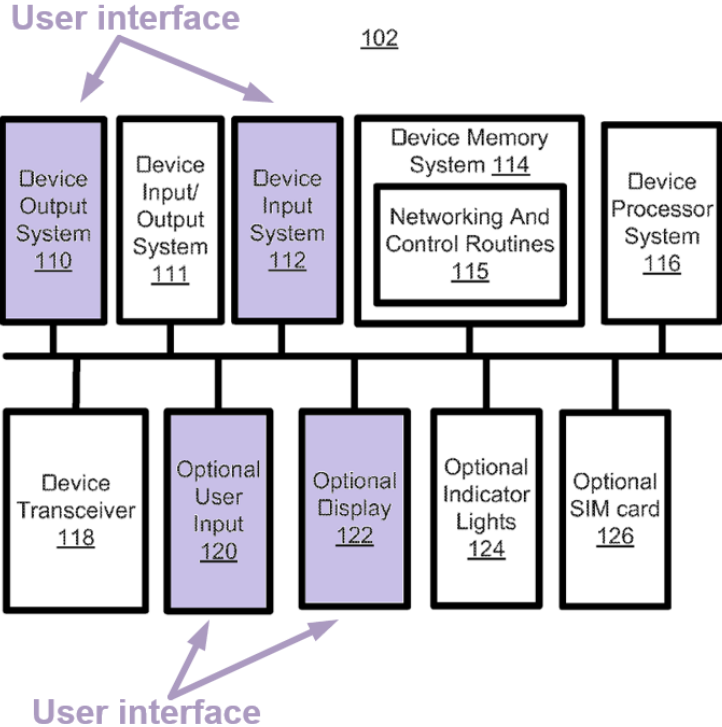


FIG. 1B

EX1005, FIG. 1B (annotated).

100. For at least the reasons that I discussed above in my analysis of the Salmela-Rishy-Maharaj combination (*see* §VII.C), it would have been obvious and a POSITA would have been motivated to implement Salmela’s device 10 to include a user interface as taught in Rishy-Maharaj. Indeed, based on the corroborating references that I mentioned above, it is apparent that numerous wireless devices included a use interface by 2013. It would have been obvious for a POSITA to modify Salmela’s device 10 to include a user interface as taught by Rishy-Maharaj so that device 10 includes this well-known feature. Furthermore, the Salmela-Rishy-Maharaj combination, a user would beneficially be permitted to perform tasks such

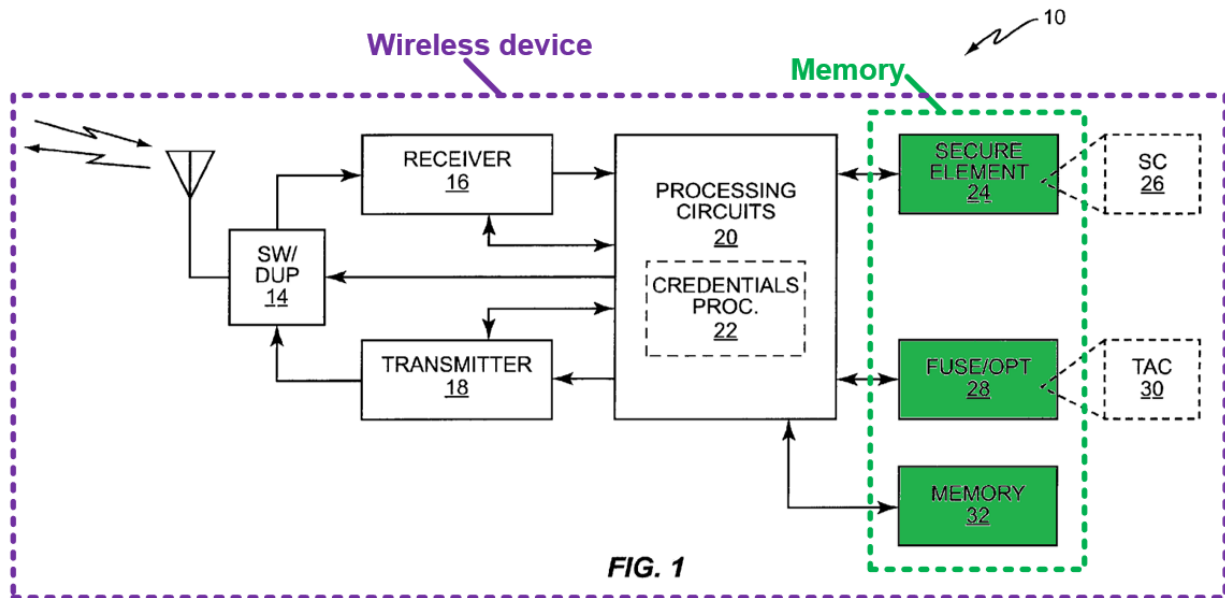
as activating or changing a subscription plan through the user interface of the wireless device.

Element [1b]: memory configured to store:

101. I noticed that Salmela's device 10 includes a ***memory*** having a secure element 24, a fuse/one-time-programmable (OTP) memory element 28, and a memory 32. EX1004, [0020], [0023], [0025], FIG. 1. It is clear that any one or combination of these three ***memory*** components could represent the ***memory*** of independent claim 1. This is because each of the ***memory*** components described by Salmela can ***store*** information such as wireless device credentials.

102. For example, Salmela discloses that secure element 24 can "***store*** subscription credentials (SC) 26," Salmela discloses that fuse/OTP memory element 28 can "***store*** temporary access credentials (TAC) 30," and Salmela discloses that memory 32 can "include one or more memory devices, for ***storing*** working data, computer program instructions, and configuration information." EX1004, [0020]. My opinion here is corroborated by numerous references published before 2013 that each describe a wireless device including a ***memory*** that can ***store*** information. EX1014, [0095]-[0098] (describing a "portable multifunction device" configured for wireless communication that includes a "memory 102" configured for storing information), EX1015, 11, 12, 43, 44 (describing a wireless mobile phone including a "memory card" to "expand available memory space), EX1016, 146 (describing a

“storage capacity” of a wireless mobile phone). The memory of Salmela’s device 10 is depicted in FIG. 1, which is reproduced below. Cf. EX1001, 10:14-10:56 & FIG. 2 (explaining that the memory may provide for partitioned or integrated storage of subscription and interim credentials).



EX1004, FIG. 1 (annotated).

Element [1c]: one or more credentials associated with the wireless device, the one or more credentials for authorizing the wireless device to use a wireless access network to access one or more services, and

103. Salmela explains that the *memory* of device 10, which represents a *wireless device* as I described above in connection with Element [1pre], *supra*, is configured to store *one or more credentials* associated with the device 10. EX1004, [0010]-[0012], [0020], [0022]-[0025], FIG. 1. For example, secure element 24 stores subscription credentials 26 and fuse/OTP memory element 28 stores temporary access credentials 30. EX1004, [0020], [0022]-[0025]. Salmela’s subscription

credentials 26 and temporary access credentials 30 either together or individually represent *one or more credentials* that are associated with device 10. Salmela's *one or more credentials* are depicted below in FIG. 1:

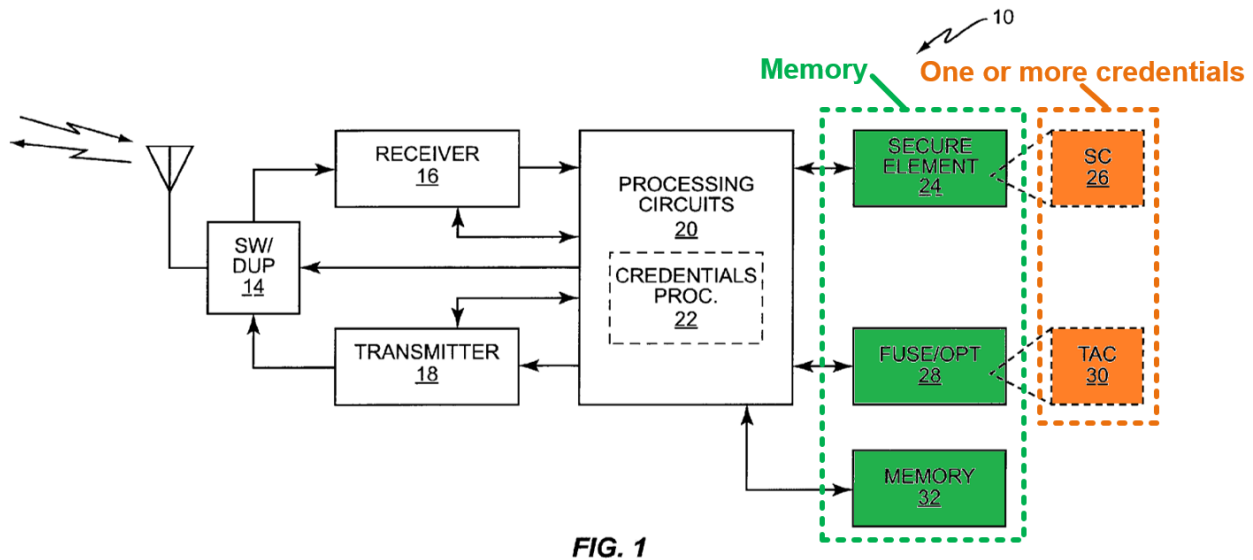


FIG. 1

EX1004, FIG. 1 (annotated).

104. Even though subscription credentials 26 are illustrated in FIG. 1 as being outside of secure element 24 and temporary access credentials 30 are illustrated as being outside of fuse/OTP memory element 28, Salmela clearly teaches that subscription credentials 26 are stored by secure element 24 and temporary access credentials 30 are stored by fuse/OTP memory element 28. EX1004, [0020]. Furthermore, according to Salmela, subscription credentials 26 and temporary access credentials 30 both *authorize* Salmela's wireless communication device 10 to use a *wireless access network* to access *one or more services*, thus making it apparent that subscription credentials 26 and temporary access credentials 30 are

both *associated* with device 10. EX1004, [0010]-[0012], [0020], [0022]-[0025]. For instance, Salmela expressly discloses that subscription credentials 26 are “for gaining network access” and that temporary access credentials 30 are “for gaining temporary access.” EX1004, [0022], *see also* [0012] (“the temporary access credentials are ‘generic’ credentials that allow temporary, limited network access”), [0025] (“uses those temporary access credentials 30 to gain temporary network access”). It is apparent that Salmela’s “network access” provides device 10 access to a *wireless access network* such as a home network and/or a visited network. EX1004, [0010], [0028], [0030]-[0032].

105. For example, Salmela explains that device 10 can use subscription credentials 26 and temporary access credentials 30 to access home network 40 and visited network 46. EX1004, [0028], [0030]-[0032], FIG. 3. Salmela’s home network 40 includes both of a radio access network (RAN) 42 and a core network (CN) 44. EX1004, [0028], FIG. 3. Similarly, Salmela’s visited network 46 includes RAN 48 and CN 50. EX1004, [0028], FIG. 3. The term “radio access network (RAN)” indicates that a *wireless device* can communicate wirelessly with the RAN to reach a *wireless access network* including the RAN. Thus, one or both of home network 40 and visited network 46 can represent a *wireless access network* that can communicate with device 10—a *wireless device*.

106. *Wireless access networks* including home networks and/or visitor networks can provide *one or more services* to device 10, such as wireless data service. EX1004, [0004], [0028], [0031]-[0033]. For example, access to the home and visited networks allows device 10 to connect to the internet and access the services of other networks and servers communicably coupled to the home and visited networks. EX1004, [0028] (“provide communicative coupling to one or more additional networks 52, such as the Internet”). It is clear that temporary access credentials 30 also authorize the device 10 to gain access to a wireless access network to utilize services for obtaining new long-term subscription credentials 26. EX1004, [0028] (“for the purpose of acquiring new subscription credentials”).

Element [1d]: a target credential; and

107. As I described above in my overview of Salmela (§VII.A, *supra*), Salmela discloses techniques for automatically updating subscription credentials 26 on a device 10. EX1004, [0003]-[0012], [0020]-[0027]. Specifically, I noticed that Salmela explains in detail how device 10 can determine that new subscription credentials are needed by comparing “first information” corresponding to the subscription credentials 26 currently held by device 10 with “second information” corresponding to subscription credentials “that are considered by [a] registration service to be current for the wireless communication device 10.” EX1004, [0044]; *see also*, [0041] (“[C]ommunicating with the registration service to determine

whether new subscription credentials are needed comprises receiving a hash value from the registration service, generating a hash value based on the current subscription credentials as held by the wireless communication device 10, and determining that new subscription credentials are needed by detecting a mismatch between the hash values.”). One situation in which the first and second information may differ is when the user has previously requested to change to a subscription plan that requires new subscription credentials that have not yet been loaded on device 10—thus meaning that device 10 must be provisioned with the new subscription credentials to receive access according to the new subscription plan. EX1004, [0041], [0044].

108. Salmela explains that the “first information” can be a “hash value” or “time stamp” of the subscription credentials 26 currently held by device 10. EX1004, [0041], [0044]. The “second information” of Salmela can likewise include a “hash value” or “time stamp” of subscription credentials that the registration service considers current for device 10. EX1004, [0041], [0044]. Because the first information and the second information can both include the same kind of data (e.g., both hash values or both time stamps), this makes it easier for device 10 to compare the first information and second information to determine whether there is a mismatch. It is clear that the hash value and/or time stamp of the underlying

subscription credential that the registration service considers to be current each correspond to and renders obvious a “*target credential*” as recited in Element [1d].

109. For example, I noticed that Salmela’s hash value and/or time stamp that is “considered by the registration service to be current for the wireless communication device 10” is very similar and analogous to examples of the “requested credential” and the “expected credential” (e.g., target credential) as described in the ’510 Patent specification.² For example, the ’510 Patent explains that the wireless device can receive a requested credential from an “application

² One thing that I noticed in my review of Salmela is that the term “target credential” is never used in the specification of the ’510 Patent. However, the descriptions of the “requested credential” (and the “expected credential”) in the specification generally align with the “target credential” in claim 1. This is especially apparent in FIG. 3, which depicts an operation 1164 where the device’s current credentials are compared with the requested credentials. EX1001, 11:28-37, FIG. 3. Element [1h] similarly refers to “determin[ing] that the particular credential does not match the target credential.” EX1001, 20:33-34. Similar uses of “requested credential” and “target credential” occur throughout FIG. 3 and claim 1, respectively. It is clear that the term “target credential” in claim 1 refers to the “requested credential” described in the specification of the ’510 Patent.

server or other network element” and that the requested credential may contain only “a subset of information about all of the one or more credentials that were requested to be changed.” EX1001, 11:1-19. In a similar way, Salmela’s device 10 receives the hash value and/or time stamp including a subset of information corresponding to the subscription credentials considered to be current for device 10 from the registration service, which is a remote server. I also noticed that the ’510 Patent’s disclosure at col. 11:32-37 is very clear that the requested credential (e.g., target credential) can be based on, but need not be identical to, the underlying updated credential (e.g., IMSI) that the device uses to authorize itself on a wireless network. *See* EX1001, 11:32-37 (describing the “requested credential” as a “configuration state indicator” as opposed to a phone number, ISDN, or the like).

110. I noticed in my review of Salmela that claim 1 does not require that the “target credential” and the underlying “updated credential” be identical, or even that the “target credential” and “updated credential” be similarly formatted. Even if claim 1 did require the updated credential and target credential to be identical (which it does not), it would have been obvious in the Salmela-Rishy-Maharaj combination for these credentials to be identical based on implementing device 10 to receive the underlying subscription credentials (e.g., IMSI) that the registration service considers current for device 10. This would allow for direct comparison at device 10 between the credentials considered to be current for device 10 and the subscription

credentials 26 currently held by the device (e.g., a direct IMSI comparison), rather than comparing time stamps or hash values.³ In this case, it is clear that the underlying subscription credentials considered by the registration service to be current for device 10 maps to and renders obvious the claimed “*target credential*.”

111. Furthermore, a POSITA would have been motivated to configure device 10 to receive and store the underlying credentials that the registration service considers current for device 10 in its original form in lieu of or in addition to a time stamp and/or hash value. This would facilitate a straightforward comparison of the credentials in their original form, as opposed to comparing credentials that are reduced to a different form for comparison (e.g., time stamps or hash values). This implementation would be beneficial to alleviate a burden on the remote server (e.g., registration server 54) of computing a hash or maintaining a time stamp for the credentials, thereby simplifying aspects of the registration service’s operations. This same burden would also be removed from device 10, which would not need to compute a hash value of the current subscription credentials 26 for a direct comparison of credentials.

³ It would have been obvious for device 10 to compute hash values of both sets of credentials locally for comparison as another predictable option.

112. A POSITA also would have also considered the choice of performing either a direct comparison of the credentials in their original form or a comparison of values associated with or derived from the credentials (e.g., hash values, time stamps) to be an obvious design choice for which a suitable option would be selected based on the needs and circumstances of a given application or design. Comparing credentials in their original form or comparing values uniquely representative of the credentials would have been understood by a POSITA as equivalent solutions. Each of these solutions would allow device 10 to determine whether it needs to update its current subscription credentials 26. EX1004, [0041], [0044]. It would have been obvious to a POSITA to pursue either a direct comparison of credentials or a comparison of representative values (e.g., time stamps and/or hash values) because Salmela itself contemplates a range of options for comparing the device's current credentials to a target credential to determine whether new subscription credentials are needed on the device. EX1004, [0043] (“**Broadly**, the wireless communication device 10 ... is configured to communicate with the registration service to determine whether new subscription credentials are needed.”); *generally*, [0040]-[0045].

113. Salmela also discloses that device 10 receives from the registration server 54 the hash value or time stamp for the credentials that the registration service considers current before comparing that information to the hash value or time stamp of the subscription credentials 26 currently held by device 10. EX1004, [0040],

[0041]. It is clear that a POSITA would have understood this to mean that the memory of device 10 stores the “second information” hash value or time stamp (e.g., target credential) at least temporarily upon receipt as the device 10 prepares to perform the comparison between the “first information” and “second information.” EX1004, [0040]-[0041], [0044] (“second information received from the registration service”). Based on my review of Salmela, it would have been obvious to store the second information or underlying subscription credentials that the registration service considers current in memory of device 10 for a period of time sufficient for device 10 to perform this comparison. My opinion here is corroborated, for example, by a 2008 textbook that describes a “cache” memory between a microprocessor and a “main memory” which allows the microprocessor to immediately access necessary data. EX1027, 40.

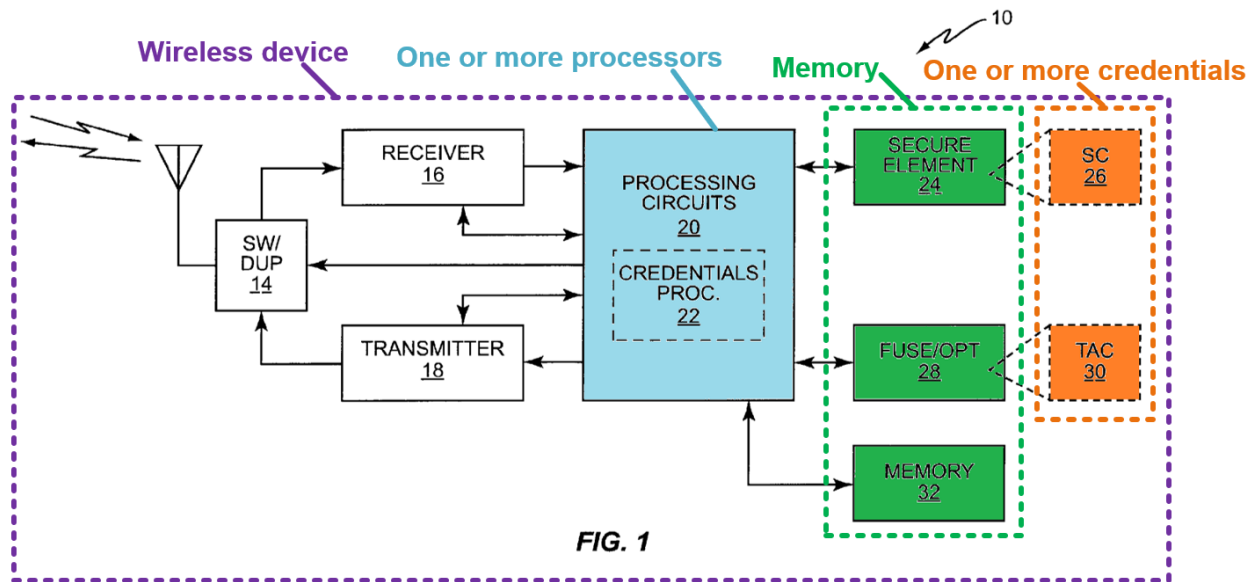
114. For example, it would have been obvious for Salmela’s device 10 to store the credentials or “second information” received from the registration server in registers, cache, random access memory, and/or or other memory of device 10 that conventionally make data available to a processor, as would occur for the device to 10 to perform the comparison described at paragraphs [0041] and [0044] of Salmela. EX1004, [0041], [0044], [0020] (memory 32 can “include one or more memory devices, for storing working data, computer program instructions, and configuration information”); *supra*, [1b]. As another example, it is clear that it would have been

obvious to store the target credential (e.g., hash value, time stamp, or underlying credential) received from the registration service in secure element 24 or a similar memory element to keep such information secure and to ensure it is available for subsequent use, similar to the storage of subscription credentials 26 in secure element 24 as disclosed in Salmela. EX1004, [0020].

115. Additionally, Salmela discloses and renders obvious storing the target credential that the registration service considers current in the secure memory element 24 when device 10 determines that its current subscription credentials 26 are no longer valid, as I describe in further below in my analysis of Element [1k], *infra*.

Element [1e]

116. Furthermore, Salmela's device 10 comprises ***one or more processors*** including processing circuits 20 and credentials processor 22. EX1004, [0020], [0024], [0026], [0027], FIG. 1. Each of these processing circuits 20 and credentials processor 22 can alone be considered ***one or more processors***, and processing circuits 20 and credentials processor 22 can together represent ***one or more processors***. The ***one or more processors*** of Salmela are depicted below in FIG. 1:



EX1004, FIG. 1 (annotated).

117. The *one or more processors* of Salmela including processing circuits 20 and/or credentials processor 22 can *execute one or more machine-executable instructions* that cause these *one or more processors* to perform actions. EX1004, [0020], [0024], [0026], [0027], FIG. 2. For instance, Salmela explains that “credentials processor 22 may be implemented via software executing in one or more microprocessor circuits used to implement the processing circuits 20.” EX1004, [0026]. This software represents *machine-executable instructions* that are *executed* by the *one or more processors*, because software includes a series of instructions (e.g., lines of code) that cause computers to perform actions when applied. I also noticed that credentials processor 22 itself can *execute machine-executable instructions*. See, e.g., EX1004, [0024] (“revert from the subscription credentials 26 to the temporary access credentials 30, responsive to detecting network access

failure”), [0034] (“controls or otherwise causes the device 10 to attempt a limited number of reattachments using its preferred network, and, if that fails, to attempt one or more additional reattachments to one or more non preferred networks”).

Element [1f]: obtain, through the user interface, an indication of a user request to replace a particular credential of the one or more credentials with the target credential,

118. In my review of Salmela, I noticed that a user of device 10, which Salmela refers to as a “device owner,” can request to activate or change subscription plans for one or more wireless devices including device 10. EX1004, [0008] (“the device owner can select and activate subscriptions”), [0009] (“changing subscription plans”), [0011] (“an owner ... can change subscription agreements”), [0053] (“changing subscription information”), Abstract (“new home operator”), [0007]. Each of the user’s device(s) associated with the new subscription plan can automatically obtain updated subscription credentials associated with the new subscription plan after detecting a network-provisioning state change based on the user submitting a request to change subscription plans. EX1004, [0003]-[0009], [0011], [0020]-[0027], [0050], FIG. 3.

119. It is clear that Salmela’s user’s request to change a subscription plan to a new home operator corresponds to and renders obvious “a user request to replace a particular credential of the one or more credentials with the target credential,” as recited in Element [1f]. By requesting that the device 10 operate under a new

subscription plan, the user is requesting that a subscription credential 26 currently held by device 10 (*a particular credential of the one or more credentials*) be replaced with a *target credential* associated with the new subscription plan. EX1004, [0003], [0010]-[0012]. This is because the new subscription plan requires a new credential for device 10 to be authorized to use a wireless access network of the home operator associated with the new subscription plan.⁴ EX1004, [0003], [0010]-[0012].

120. For example, Salmela discloses that subscription credentials 26 “generally remain valid for as long as the owner of the device 10 maintains a corresponding subscription agreement with the home network operator that issued

⁴ As discussed in the analysis of [1d], Salmela’s hash value or time stamp for the subscription credential that the registration service considers current, and the underlying subscription credential that the registration service considers current, all render obvious and alternatively map to the “*target credential*” in a manner consistent with the ’510 Patent’s description of such features. *Supra*, [1d].

Likewise, current subscription credential 26 on device 10 that would be replaced when the subscription is changed can be indicated by a hash value, time stamp, or the underlying credential 26 itself, each of which maps to and renders obvious a “*particular credential*” as claimed. EX1004, [0041], [0044].

the subscription credentials 26.” EX1004, [0022]. This means that when the user requests to change home operators by canceling a subscription plan with a prior home operator and activating a subscription plan with a new home operator, the user is requesting to replace a particular credential associated with the prior home operator with a target credential associated with the new home operator. EX1004, [0007]-[0009], [0022].

121. Even if Salmela does not expressly disclose that device 10 obtains an indication of its user request to update a subscription plan *through a user interface* of device 10, it is clear that this conventional option would have been obvious to a POSITA based on the teachings of Rishy-Maharaj. As described above in connection with [1a], I noticed that Rishy-Maharaj discloses a wireless device 102 including a user interface. EX1005, [0028]-[0046], [0058]-[0060], [0066], [0067], [0108]-[0121], FIGS. 1A, 1B, 2. Rishy-Maharaj also discloses that a “user may select [a] subscription plan ... that best suits the user”, and in particular, “[t]he wireless device 102 may [] have an optional user input 120 to allow the user to select a plan.” EX1005, [0112]; *see also*, [0108]-[0121], FIGS. 1B, 2.

122. As I described above in my analysis of the Salmela-Rishy-Maharaj combination (§VII.C, *supra*), it would have been obvious for a POSITA to implement Salmela in accordance with Rishy-Maharaj’s teaching such that the user in Salmela would submit a request to change subscription plans through a user

interface of his or her device 10. Making this modification would, among other reasons that I discussed in more detail above, enhance the user's convenience in selecting or changing a subscription plan.; *supra*, §VII.C. As a result, Salmela's device 10 in the combination would obtain, and based on the user's selection of a new subscription plan through the user interface, an indication of a user request to replace a *particular credential* (e.g., subscription credential 26) with the *target credential* (e.g., a new credential associated with the new subscription plan) as recited in [1f]. This is similar to example described in the '510 Patent. Cf. EX1001, 12:45-14:40 and FIGS. 4-13 (describing embodiments where the device obtains an *indication* of a user request to replace credentials based on actions as basic as the user tapping a "Transfer" button to initiate a number port).

Element [1g]: detect a network-provisioning state change, and based on the detected network-provisioning state change, automatically

123. Salmela clearly explains that wireless communication device 10 can detect a failure to gain network access using the current subscription credentials 26 stored in the *memory* of device 10—an event which Salmela refers to as an "access failure" or a "network access failure" in some cases. EX1004, [0010] ("reverts from subscription credentials to temporary access credentials, in response to detecting an access failure"), [0024] ("revert from the subscription credentials 26 to the temporary access credentials 30, responsive to detecting network access failure"), [0027], [0033]-[0035] ("detecting a failure to gain network access"), FIG. 4. , Based

on such detection, Salmela's device 10 *automatically* reverts from its current subscription credentials 26 to temporary access credentials 30 as part of an automated process for obtaining new subscription credentials associated with a new subscription plan. EX1004, [0010], [0024], [0025], [0027], [0033]-[0035], FIG. 4. The failure to gain network access detected by device 10 in Salmela represents *a network-provisioning state change* because the access failure indicates that the device 10 is no longer sufficiently *provisioned* with credentials necessary to provide network access. Examples of events that can cause this kind of network-provisioning state change include a subscription of device 10 to a home network lapsing and device 10 leaving a network area of the home network.

124. My opinion here is strengthened by the fact that the network access failure events described in Salmela are similar to several kinds of *network-provisioning state change* that are described by the '510 Patent. EX1001, 9:4-11 (describing how a mobile device can detect that it can no longer access a network using multiple different techniques), *see also* 11:20-27 (describing how denied network access events of the same kind disclosed in Salmela indicate network provisioning state changes).

125. Salmela describes in detail how device 10 detects a loss of network access. For example, Salmela discloses that device 10 can "detect access loss for its local (preferred) RAN" using subscription credentials 26. EX1004, [0033]. Based

on detecting this access loss, Salmela explains that device 10 can “attempt reconnection using its current subscription credentials 26.” EX1004, [0033]. If these reconnection attempts fail, device 10 can “scan for alternative access” through other networks and ultimately determine that there has been a failure to gain network access if device 10 is unable to secure alternative access using subscription credentials 26. EX1004, [0034], [0035]. Through these operations, it is clear that device 10 detects a “*network-provisioning state change*” indicating that current subscription credentials 26 are no longer usable by the device 10 to gain access to services on the wireless access network. The ’510 Patent similarly discloses that detection of a network-provisioning state change can include failed attempts to access a network and its services. EX1001, 11:20-27 (“There are a number of ways in which the device can detect the network provisioning state change, including...failed authentication with a network element, failed authorization for services.”)

126. Furthermore, it is apparent that device 10 performs actions to *automatically* check the validity of its current subscription credentials and obtain new subscription credentials based on detecting a failure to gain network access, EX1004, [0027], [0033]-[0035], [0037]-[0038], FIG. 2, FIG. 4; *infra*, Elements [1h]-[1k]. Some of these actions are illustrated below in FIG. 2, for example.

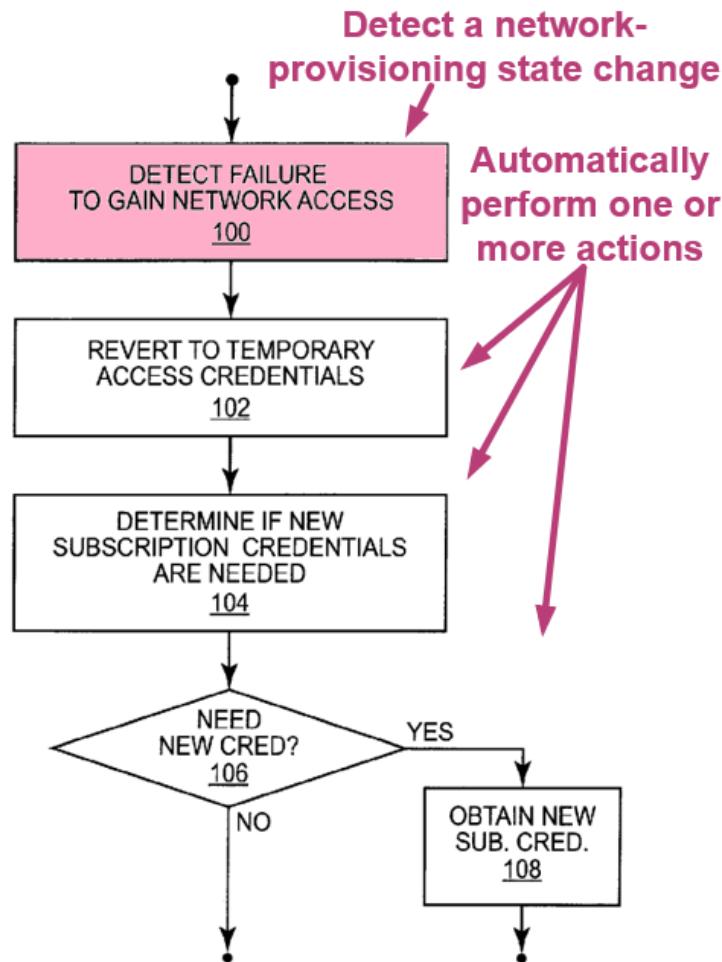


FIG. 2

EX1004, FIG. 2 (annotated).

Element [1h]: *determine that the particular credential does not match the target credential,*

127. As I described above in my analysis of Element [1f], *supra*, Salmela explains that a user can request to replace a *particular credential* (e.g., the current subscription credentials 26) with a *target credential* by requesting to change home operators for device 10. EX1004, [0003]-[0009], [0020]-[0027]. For example, when the user requests a change to a home operator associated with a network that cannot

be accessed using the current subscription credentials 26, such a request is a request to replace the subscription credentials 26 with new subscription credentials. Furthermore, because Salmela expressly discloses that the subscription credentials 26 “remain valid for as long as the owner of the device 10 maintains a corresponding subscription agreement with the home network operator that issued the subscription credentials 26,” this means that Salmela teaches that the current subscription credentials 26 become invalid when the user requests to update the current home network to a new home network. EX1004, [0022].

128. Such a switch from the current home network to a new home network would cause Salmela’s “registration service” to update the *target credential*—the credentials that the registration service considers “to be current” for device 10. EX1004, [0044]. Because Salmela’s registration service allows device owners and/or home network operators to “register” devices such as Salmela’s device 10 by maintaining the *target credential* associated with device 10, the switch from the current home network to a new home network would lead to the user and/or the new home network updating the *target credential* in the registration service. EX1004, [0030], [0044]. It is clear that updating the *target credential* in Salmela’s registration service would result in current subscription credentials 26 of device 10 no longer matching the *target credential* stored by the registration service. EX1004, [0020]-[0027], [0041], [0044]. Because of this mismatch, a network access failure would

occur in which device 10 is not able to access the new home network using the current subscription credentials 26, because the current subscription credentials 26 are associated with the old home operator and not the new home operator. EX1004, [0020]-[0027], [0041], [0044]. I discussed how device 10 can detect a **network-provisioning state change** by detecting such a failure to gain network access using the current subscription credentials 26 above in connection with Element [1g], *supra*.

129. Based on detecting a failure to gain network access using subscription credentials 26, device 10 **automatically** reverts to its temporary access credentials 30 so that device 10 can achieve limited access for retrieving a new subscription credential. EX1004, [0010], [0024] (“revert from the subscription credentials 26 to the temporary access credentials 30, responsive to detecting network access failure”), [0027] (“in response to detecting such failure, [] reverting from the current subscription credentials 26 to the temporary access credentials 30”), FIG. 2. Salmela explains that device 10 obtains temporary network access to connect with a registration server and determine whether new subscription credentials are available. EX1004, [0010], [0027] (“determining whether new subscription credentials are needed based on gaining temporary network access via the temporary access credentials”), FIG. 2.

130. As I described above in connection with Elements [1d] and [1f], Salmela’s device 10 can automatically identifies a need for new subscription

credentials by determining that its current subscription credential 26 (*particular credential*) does not match the subscription credential that the registration service considers to be current (*target credential*). EX1004, [0041], [0044]; *supra*, [1d], [1f]. Salmela describes options for determining this mismatch by comparing either hash values or time stamps respectively associated with the device's current subscription credential 26 and the credential that the registration service considers current, although it would have been equally obvious to directly compare the underlying credentials themselves.⁵ EX1004, [0041], [0044], *see also* [0020]-[0027]; *supra*, Elements [1d], [1f].

131. A process for *automatically* determining that new credentials are needed based on detecting a *network-provisioning state change* is depicted below in FIG. 2 of Salmela:

⁵ Recall that Salmela's hash values, time stamps, and underlying credentials (e.g. IMSI) all provide alternative forms of the claimed "*particular credential*" and "*target credential*" consistent with disclosures in the '510 Patent itself. *Supra*, [1d], [1f].

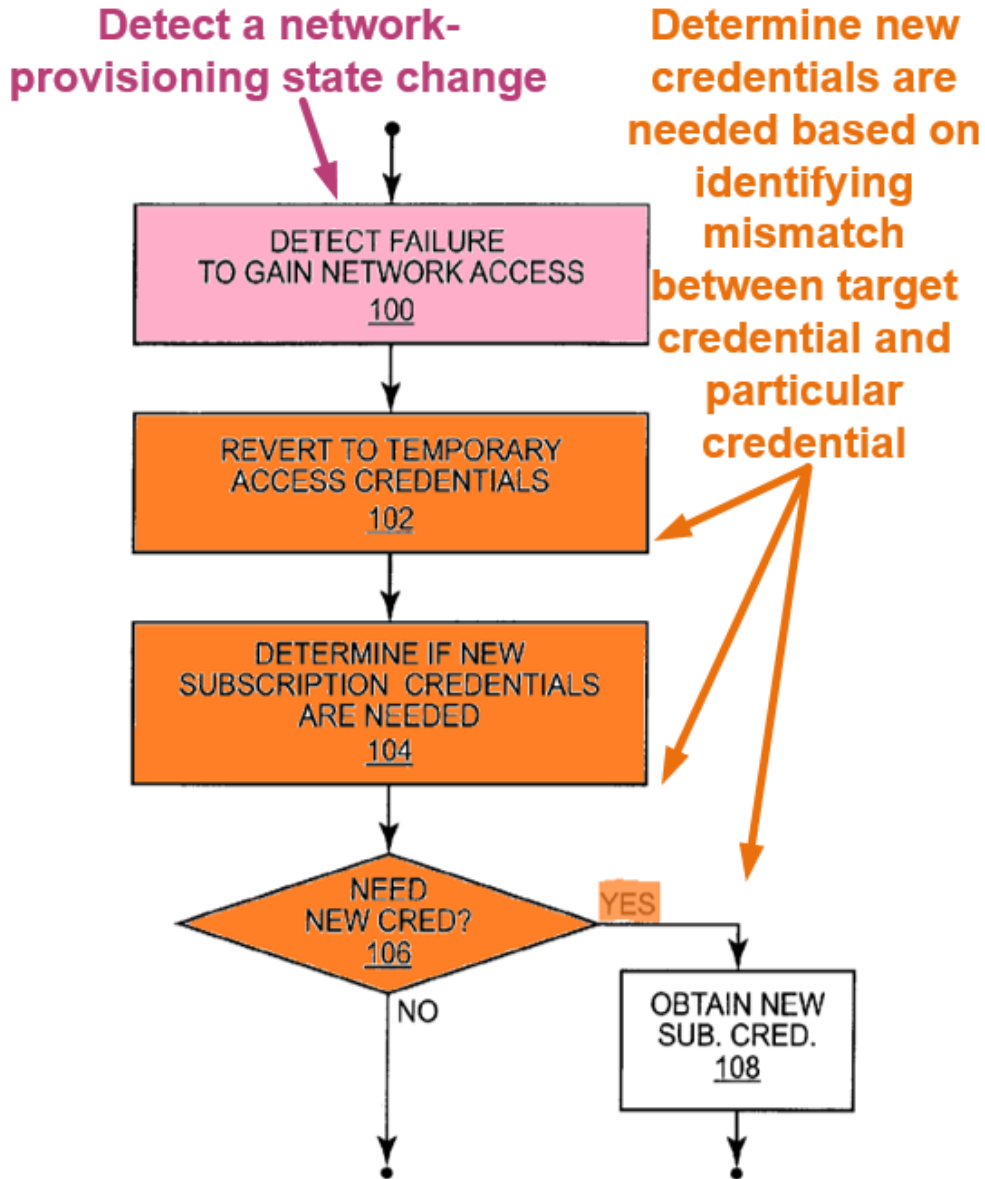


FIG. 2

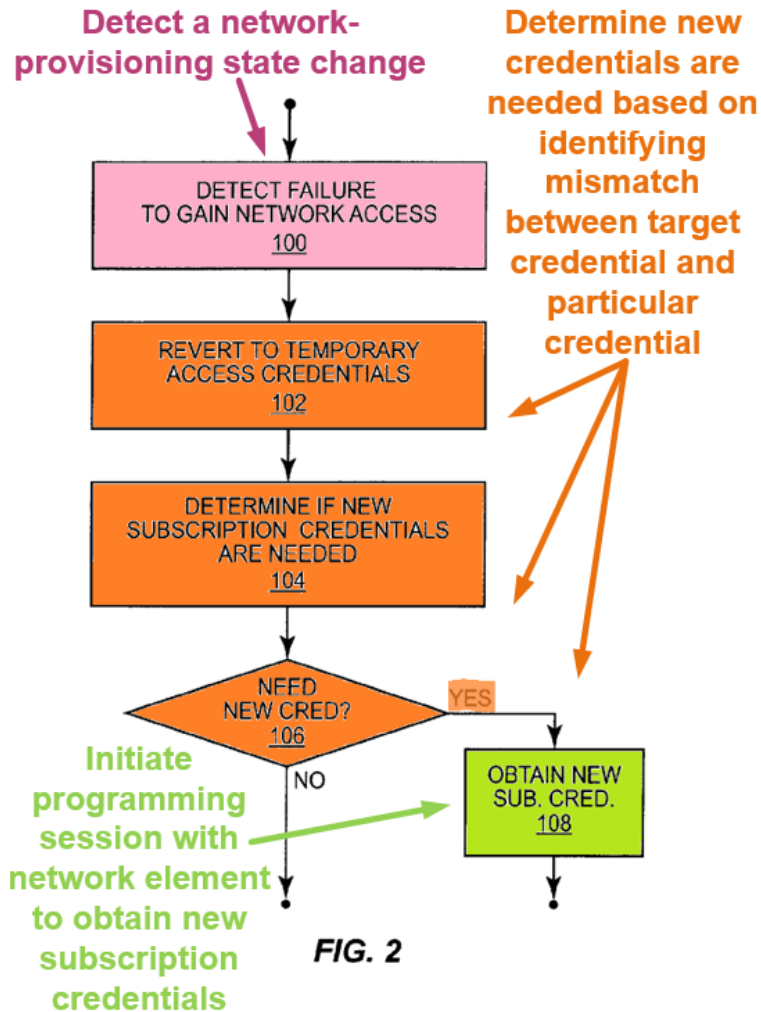
EX1004, FIG. 2 (annotated).

132. Furthermore, because Salmela's *particular credential* and *target credential* can, in some examples, both comprise an IMSI, it is clear that device 10 could simply determine that the *particular credential* does not match the *target credential* by determining that the IMSI corresponding to the particular credential is

not the same as the IMSI for the target credential. My opinion here is corroborated by the fact that an IMSI includes at least two constituent components (e.g., the mobile country code (MCC) and the mobile network code (MNC)) that together are unique to each home network. EX1031, 15. Thus, device 10 can determine whether its current subscription credentials 26 include an IMSI having an MCC and MNC corresponding to a home network of a newly selected home operator. If the MCC and MNC do not match in this way, it is apparent that device 10 could determine that the *particular credential* does not match the *target credential*.

Element [1i]: initiate a programming session with a network element communicatively coupled to the wireless device over the wireless access network,

133. It is apparent that Salmela's device 10 can *initiate a programming session* with a *network element* to obtain new subscription credentials. EX1004, [0025]-[0027]. As I describe in more detail below, device 10 *automatically* initiates this *programming session* based on detecting a *network-provisioning state change* (e.g., a network access failure). An example process for automatically initiating a programming session to obtain new subscription credentials is depicted below in Salmela's FIG. 2:



EX1004, FIG. 2 (annotated).

134. Salmela explains that as part of the process to *initiate* the *programming session* to obtain new subscription credentials, device 10 receives “network address information from the registration service that identifies a “credentialing server” from which the new subscription credentials are to be obtained.” EX1004, [0045], *see also* Claim 11 (“obtaining new subscription credentials for the wireless communication device comprises receiving network address information from the registration service that identifies a credentialing server from which the new subscription

credentials are to be obtained”). Salmela’s device 10 can initiate a programming session with the credentialing server identified by the network address information to obtain the new subscription credentials. EX1004, [0045] (“using the temporary network access to contact the credentialing server to obtain the new subscription credentials”), [0025]. This credentialing server represents a *network element* because servers are common network elements where information is stored. The fact that servers are network elements was corroborated by the Critical Date of the ’510 Patent. EX1032, 4 (describing a “control server” as being a “network element”).

135. Salmela explains that device 10 *automatically initiates* the *programming session* with the *network element* to obtain new subscription credentials based on detecting a *network-provisioning state change* (e.g., a network access failure). EX1004, [0011] (“devices [] *autonomously* detect problems with their current subscription credentials, and use their temporary access credentials to gain new/updated subscription credentials”), [0048] (“*automatic* acquisition of new subscription credentials”), [0025], claim 25 (“automatic acquisition of new Subscription credentials by a wireless communication device”).

136. Salmela’s credentialing server, which represents a *network element*, is communicatively coupled to device 10 over the *wireless access network* that includes home network 40 and/or visiting network 46. For example, Salmela explains that “the credentialing server is, in one or more embodiments, an entity

in...the CN of the service provider that issued the new subscription credentials.” EX1004, [0045]. It is well known in the telecommunications field that “CN” refers to “core network,” which an important part of a *wireless access network*. The core network can be accessed by a wireless device such as Salmela’s device 10 through a radio access network (“RAN”)—another important part of the *wireless access network*. EX1004, [0028], FIG. 3. The fact that CNs can be accessed through RANs is corroborated by several references published before 2013. EX1017, 6 (depicting a mobile terminal communicating with a CN through a RAN); EX1018, 2 (depicting a network architecture where a user equipment communicates with a core network through a radio access network).

137. Because Salmela explains that the credentialing server is part of the core network located within Salmela’s *wireless access network*, device 10 must communicate with the wireless access network to obtain the subscription credentials necessary to gain access to the wireless access network. EX1004, [0028], FIG. 3. This means that device 10 is *communicatively coupled* to the *network element* (e.g., credentialing server) over the *wireless access network*.

Element [1j]: obtain an updated credential from the network element, and

138. Through the *programming session* initiated with the *network element* (e.g., “credentialing server”), Device 10 can obtain an *updated credential* (e.g., “new subscription credentials”) from the credentialing server through the *programming*

session initiated with the credentialing server.⁶ EX1004, [0025], [0027], [0045] (“using the temporary network access to contact the credentialing server to obtain the new subscription credentials”), *see also* [0025] (“device 10...uses its temporary access to obtain new subscription credentials, which it may download”), [0027] (“obtaining new subscription credentials for the wireless communication device 10 via the temporary network access), FIGS. 2, 4. It is apparent that the updated subscription credential obtained from the credentialing server and associated with the new subscription plan replaces the current subscription credentials 26 stored on

⁶ The '510 Patent discloses—similar to Salmela—that the *updated credential* can be a target credential (referred to in the '510 Patent as an “expected credential” or “requested credential”), or the target credential can be a representation of the updated credential. EX1001, 9:16-19 (“mobile device 100 detects that a current device credential does not match the expected credential”), 9:47-49 (“delivers the new device credentials to the device”), 10:42-44 (“stores the expected credentials to be programmed to mobile device 100”), 12:19-22 (“the device compares the updated credentials with the expected credentials to determine if the credential update process...is complete”).

device 10 and associated with the prior subscription plan.⁷ Furthermore, Salmela teaches that device 10 obtains the *updated subscription credentials automatically* through a process that occurs in response to device 10 detecting of a network access failure that represents a *network-provisioning state change*. EX1004, [0011] (“devices [] *autonomously* detect problems with their current subscription credentials, and use their temporary access credentials to gain new/updated subscription credentials”), [0048] (“*automatic* acquisition of new subscription credentials”), [0025], claim 25.

Element [1k]: assist in storing, in memory, the updated credential as the particular credential.

⁷ In at least two instances, Salmela uses both of the terms “new” and “updated” to refer to subscription credentials obtained using temporary access credentials. EX1004, [0011] (“new/updated subscription credentials”), [0036] (“[t]he device 10 then uses that temporary network access to obtain new subscription credentials (Block 126), which comprises downloading a new or updated USIM”). Additionally, Salmela explains that “[o]nce the device 10 obtains new subscription credentials, they replace its previously current subscription credentials.” EX1004, [0036].

139. Salmela explains that device 10 “uses its temporary access to obtain new subscription credentials, which it may download to its secure element 24.” EX1004, [0025], *see also* [0036] (“Once the device 10 obtains new subscription credentials, they replace its previously current subscription credentials, and the newly obtained subscription credentials become the device’s current subscription credentials 26.”), [0046] (“replace or deactivate its formerly current subscription credentials ...”). As I described above in my analysis of Element [1b], *supra*, the memory of device 10 includes secure element 24. EX1004, [0020], [0025]. Therefore, it is clear that device 10’s processors assist in *storing* the *updated credential* (referred to by Salmela as “new subscription credentials”) in the *memory*. The *updated credential* automatically replaces the current subscription credentials 26 based on Salmela’s device 10 detecting a network access failure (*network-provisioning state change*). EX1004, [0011] (“devices [] *autonomously* detect problems with their current subscription credentials, and use their temporary access credentials to gain new/updated subscription credentials”), [0048] (“*automatic* acquisition of new subscription credentials”), [0025], claim 25.

Claim [2]: The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to: determine that the updated credential does not match the target credential, and based on the determination that the updated credential does not match the target credential, take an action.

140. As I described above in my analysis of Element [1e], *supra*, Salmela explains that device 10 includes **one or more processors** (e.g., processing circuits 20 and/or credentials processor 22) configured to **execute** one or more **machine-executable instructions**. EX1004, [0020], [0024], [0026], [0027], FIG. 1. Salmela also explains that device 10 can **automatically** obtain an **updated credential** (e.g., new/updated subscription credentials) to replace a **particular credential** (e.g., subscription credentials 26) based on detecting a failure to gain network access. EX1004, [0020]-[0027], FIG. 1, FIG. 2. Furthermore, as I describe above in my analysis of Element [1h], *supra*, device 10 obtains the **updated credential** based on determining that the **particular credential** does not match a **target credential**.

141. Salmela's process of checking subscription credentials and updating subscription credentials is a recurring process that occurs whenever current subscription credentials are unable to provide network access—and therefore need to be replaced. EX1004, [0010], [0024], FIG. 1, FIG. 2. For example, Salmela explains that “[D]evice 10 uses its subscription credentials 26 for gaining network access unless and until it is unable to gain access using those credentials. At that point, the device 10 advantageously reverts to its temporary access credentials 30.” EX1004, [0024], *see also* [0010] (“[A] wireless communication device reverts from subscription credentials to temporary access credentials, in response to detecting an access failure.”). Reverting from the subscription credentials 26 to the temporary

access credentials 30 can initiate process for (1) determining whether subscription credentials 26 need to be replaced, and (2) based on determining that replacement is necessary, replacing current subscription credentials 26 with new subscription credentials. EX1004, [0025], [0027]. Based on replacing the current subscription credentials 26 with new subscription credentials, Salmela's device 10 make the new subscription credentials the "current" subscription credentials, thus replacing the previous credentials that failed to gain network access. EX1004, [0036], [0046]; *supra*, Element [1k]. It is apparent that this same automatic process to replace subscription credentials occurs once again when Salmela's device 10 detects that the new subscription credentials (*updated credential*) fail to gain network access. EX1004, [0046] ("[T]he device 10 can replace or deactivate its formerly current subscription credentials and use the newly acquired subscription credentials as its newly current subscription credentials 26, to be used for subsequent network accesses, *while retaining its temporary access credentials 30 in case further reversions are needed.*"⁸).

142. As I explained above in my analysis of Element [1h], *supra*, Salmela teaches that device 10 can determine that first information (e.g., a hash value) corresponding to a *particular credential* (e.g., the current subscription credentials

⁸ Emphasis added.

26 stored by device 10) *does not match* second information (e.g., a hash value) corresponding to a *target credential* to determine that the *particular credential* does not match the *target credential*. EX1004, [0041], [0044]. Subsequently, device 10 can obtain an *updated credential* which replaces the *particular credential* to become the current subscription credential. EX1004, [0020]-[0027], [0033]-[0047], FIG. 1, FIG. 2, FIG. 4; *supra*, [1i]-[1k]. When device 10 replaces the previously current subscription credentials 26 (*particular credential*) with the new subscription credentials (*updated credential*) and determines that *updated credential* no longer provides access to the network, device 10 performs another comparison—this time between a hash value corresponding to the *target credential* and a hash value corresponding to the *updated credential* (which is now the current subscription credential 26) based on detecting that the *updated credential* has failed to gain network access. EX1004, [0027], [0041], [0049]-[0056]. A POSITA would have understood and it would have been obvious that device 10 would detect a mismatch between hashes for the *updated credential* and the *target credential* if the value of the target credential changes for any reason after the device begins using its *updated credential* as the current subscription credentials 26. The mismatch can also be determined based on comparison of time stamps or the underlying credentials, as I described in more detail above. *Supra*, [1d], [1k].

143. It is clear that the value of the *target credential* can change when the user makes a request to change the home operator or subscription plan associated with device 10, thereby causing the registration service to update the *target credential* according to the request.⁹ EX1004, [0010]-[0012], [0050], FIGS. 2, 4. Even if the user has not requested to activate a new subscription plan or to change the home operator and the target credential has not changed at the registration service, it would have been obvious to a POSITA that device 10 would still detect a mismatch between the hashes for the *updated credential* and the *target credential* if the hashes or the credentials themselves have been corrupted at device 10 (e.g., as a result of transmission or memory errors). Data corruption was well-known to occur in computer memory by 2013, as corroborated by at least one reference. EX1019, 4 (describing data corruption in computer memory).

144. Based on determining that the updated credential does not match the target credential, Salmela explains that device 10 can take an *action*, e.g., by

⁹ The '510 Patent explains that the target credential, sometimes referred to as the "expected credential" or the "requested credential," is not static. According to the '510 Patent, the value of the target credential can change whenever a new phone number or other credential is submitted as the target of a phone number or other credential porting process. EX1001, 9:11-27, 10:42-51, 7:1-15, FIG. 2.

“identify[ing] a credentialing server from which [] new subscription credentials are to be obtained, and using the temporary network access to obtain the new subscription credentials.” EX1004, [0045]; *see also* [0026], [0027]; *infra*, Claims [3], [6].

Claim [3]: The wireless device recited in claim 2, wherein the action is to communicate with the network element.

145. As I explained above in my analysis of Elements [1i] and [1j], Salmela explains that device 10 can initiate a ***programming session*** with a ***network element*** that Salmela refers to as a “credentialing server” for the purpose of obtaining an ***updated credential*** (e.g., new subscription credential) to replace a ***particular credential*** (e.g., current subscription credentials 26). EX1004, [0025], [0027], [0045]. Salmela explains that this ***updated credential*** becomes the current subscription credentials 26 that device 10 uses “unless and until it is unable to gain access using those credentials.” EX1004, [0024]. As I described above in my analysis of Claim [2], device 10 can detect that the ***updated credential*** fails to provide network access in a way that causes device 10 to determine that the ***updated credential*** does not match the ***target credential***. EX1004, [0024], [0027], [0033]-[0035], [0041]. Based on this determination, Salmela’s device 10 can communicate with the credentialing server to replace the ***updated credential***, just as device 10 previously communicated with credentialing server to replace the ***particular credential***. EX1004, [0045]. In other words, Salmela’s process to update current

subscription credentials 26 is repetitive, and current subscription credentials 26 can be replaced again even if the current subscription credentials 26 have already been replaced one or more times previously. Furthermore, it is clear that when device 10 communicates with the credentialing server to replace the updated credential, this communicating amounts to taking an *action* based on determining that the *updated credential* does not match the *target credential* as required by Claim [2].

Claim [6]: The wireless device recited in claim 2, wherein the action is to at least assist in restricting communications by the wireless device over the wireless access network.

146. As I described above in my analysis of Element [1h] and Claim [2], Salmela clearly explains that device 10 reverts from the current subscription credentials 26 to temporary access credentials 30 based on determining that the current subscription credentials 26 fail to provide network access. EX1004, [0010], [0024], [0027], FIG. 2; *supra*, Claim [2]. Because Salmela discloses that the process for updating current subscription credentials 26 is repetitive and that device 10 can use current subscription credentials 26 “for gaining network access unless and until it is unable to gain access using those credentials,” it is clear that reverting from subscription credentials 26 to temporary access credentials 30 would occur any time that the current subscription credentials 26 fail to provide network access. EX1004, [0024]. This includes situations like in Claim [2] where an *updated credential* (new subscription credentials) does not match a *target credential*.

147. Salmela explains that temporary access credentials 30 provide “temporary, limited network access” which represents a lesser, restricted form of access to the network as compared with the access provided by valid subscription credentials 26. EX1004, [0006], [0007] [0012], [0020], [0022]-[0024]. For example, temporary access credentials 30 allow the device to communicate with a registration server but may restrict access to other services that would be available by valid subscription credentials 26. EX1004, [0020]-[0027]. By reverting to the temporary access credentials 30, device 10 *at least assists* in *restricting communications* by device 10 over the *wireless access network* because reverting to temporary access credentials 30 restricts device 10 to the limited network access provided by temporary access credentials 30. EX1004, [0006], [0007] [0012], [0020]-[0027]. When device 10 detects that the *updated credential* does not match the *target credential*, Salmela explains that device 10 continues using the temporary access credentials 30 that offer limited network access, thus *assisting* in *restricting communications* by device 10. EX1004, [0045] (“using the temporary network access to contact the credentialing server”). Furthermore, it is clear that when device 10 reverts to the temporary access credentials 30, this reversion amounts to taking an *action* based on determining that the *updated credential* does not match the *target credential* as required by Claim [2].

Claim [7]: The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions

further cause the one or more processors to: determine that the updated credential matches the target credential, and based on the determination that the updated credential matches the target credential, take an action.

148. As I described above in my analysis of Elements [1g]-[1k], Salmela discloses that device 10 performs a process to automatically replace a ***particular credential*** with an ***updated credential*** by replacing current subscription credentials 26 with new subscription credentials. EX1004, [0020]-[0027], [0036], [0040], [0041], [0044]-[0047]. Salmela's disclosure makes it apparent that these new subscription credentials represent an ***updated credential*** that replaces formerly current subscription credentials 26 representing a ***particular credential***, and that the ***updated credential*** becomes the current subscription credentials 26 stored in secure element 24. EX1004, [0036], [0046] ("device 10 can replace or deactivate its formerly current subscription credentials and use the newly acquired subscription credentials as its newly current subscription credentials 26, to be used for subsequent network accesses"). Salmela also explains that that device 10 retains temporary access credentials 30 "in case further reversions are needed" when device 10 replaces current subscription credentials 26 with new subscription credentials. EX1004, [0046].

149. Indeed, Salmela explains that another reversion to temporary access credentials 30 occurs when the ***updated credential*** represented by the new subscription credentials fails to gain network access. For example, Salmela discloses

that (“[D]evice 10 uses its subscription credentials 26 for gaining network access unless and until it is unable to gain access using those credentials. At that point, the device 10 advantageously reverts to its temporary access credentials 30.”). EX1004, [0024]. This occurs even in cases where subscription credentials 26 represent “newly current subscription credentials” replacing “previously current subscription credentials.” EX1004, [0036]. Device 10 uses temporary access credentials 30 to determine whether the *updated credential* (e.g., the new current subscription credential 26 that replaced the formerly current subscription credential 26) must be replaced. EX1004, [0047]. Salmela explains that device 10 can determine whether a new subscription credential is needed based on comparing a hash value or other information about the *updated credential* (e.g., the new current subscription credential 26) with a hash value or other information about the *target credential* (e.g., subscription credentials considered by the registration service to be “current” for device 10). EX1004, [0041], [0044].

150. Furthermore, as I mentioned above in my analysis of Element [1h], an IMSI includes two constituent components (e.g., the MCC and the MNC) that together are unique to each home network. EX1031, 15. It would have been obvious as of the Critical Date of the ’510 Patent for Salmela’s device 10 to determine that the *updated credential* matches the *target credential* based on the MCC and MNC of the IMSI corresponding to the updated credential matching the MCC and MNC

of an IMSI considered by the registration service to be current for device 10. This would be an easy comparison for device 10 to make, especially when the MCC includes “three digits” and the MNC includes “two or three digits.” EX1031, 15.

151. It is apparent that device 10 *takes an action* to return to using the *updated credential* in cases where device 10 determines that the *updated credential* matches the *target credential*, for example based on comparing the hash values corresponding to the *updated credential* and the *target credential*. EX1004, [0047] (“If the device 10 receives no indication that new subscription credentials are needed, or otherwise cannot make such determination, it returns to using its current subscription credentials 26 and may continue with periodic access attempts using them. Additionally, or alternatively, it may alternate between using its temporary access credentials in attempts to determine whether there is a problem with its current subscription credentials 26, and using those subscription credentials 26 in regular access attempts.”). In other words, any time that the current subscription credentials 26 stored by the device 10 match the target credential (e.g., the subscription credentials that the registration service “considers to be current” for device 10), device 10 *takes an action* to return to using the current subscription credentials 26. EX1004, [0044], [0047]. It is apparent that a POSITA would have understood and it would have been obvious that device 10 would detect a match between the *updated credential* and the *target credential* in cases where the user has

not requested to activate a new subscription or to change home operators and the *target credential* held by the registration service has not changed since the device 10 began using the *updated credential*. EX1004, [0040]-[0044], [0053].

Claim [11]: The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that a registration attempt initiated by the wireless device has failed.

152. As I described above my analysis of Element [1g], Salmela discloses that device 10 can detect a *network-provisioning state change* based on determining that current subscription credentials 26 stored by device 10 fail to provide network access. EX1004, [0027] (“detecting a failure to gain network access using the current subscription credentials 26 held in the device 10”), [0024], [0033]-[0035], [0037], [0038]. Salmela teaches that in some cases, detecting a failure to provide network access involves determining that a registration attempt initiated by device 10 has failed. EX1004, [0010], [0024], [0027], [0033]-[0039], FIG. 2, FIG. 4, Claim 1, Claim 13. As an example, Salmela discloses that “[i]n ... detecting network access failure, the device 10 experiences a loss of its home network ... which may mean that the device 10 can communicate with a local RAN, but is not recognized or otherwise authenticated by its home network.” EX1004, [0037]. This lack of recognition of device 10 or other failure to authenticate with a home network would result from a failed registration attempt. This is because if device 10 fails to register with the registration service corresponding to the home network, the registration service

would not recognize the device 10 due to device 10 not being registered with the home network.

153. Salmela also explains that in other examples, the device 10 can detect failed network access resulting from access loss for its local RAN or from being “explicitly disconnected from its home network.” EX1004, [0033], [0038]. Such a disconnection from the home network would result from a failure of the device 10 to register with the home network. For example, when device 10 is not properly registered with the home network in Salmela’s “registration service,” subscription credentials 26 would not be “considered by the registration service to be current” for device 10, thus leading to device 10 not being able to access the home network that device 10 failed to register with. EX1004, [0044].

Claim [14]: The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that an attempt by the wireless device to authenticate with the network element has failed.

154. As I described above in my analysis of Element [1g], Salmela discloses that device 10 can determine that current subscription credentials 26 fail to provide network access, thus detecting a ***network-provisioning state change***. EX1004, [0027] (“detecting a failure to gain network access using the current subscription credentials 26 held in the device 10”), [0024], [0033]-[0035]. Salmela acknowledges that provisioning a wireless device with subscription credentials is known in the art, these subscription credentials allowing the device to authenticate itself to a home

operator for a given subscription. EX1004, [0003]. This means that when a device 10 detects that the current subscription credentials 26 of device 10 fail to provide access to a home operator network, device 10 likewise determines that an attempt by device 10 to *authenticate* with the *network element* has failed.

155. I noticed that Salmela explains that one example of detecting network access failure involves device 10 not being recognized “or otherwise *authenticated*” by its home network which includes the *network element* (e.g., the credentialing server). EX1004, [0037]. Furthermore, Salmela explains that “provisioning... includes securely storing subscription credentials in the device...and allow it to *authenticate* itself to the operator's home network.” EX1004, [0003]. From these disclosures of Salmela, it is clear that one way device 10 can detect a *network-provisioning state change* is by detecting a failure to *authenticate* with a *network element* of a home network.

Claim [15]: The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that an attempt by the wireless device to be authorized for a service has failed.

156. As I described above in connection with my analysis of Element [1g], Salmela discloses that device 10 can detect a *network-provisioning state change* based on determining that current subscription credentials 26 fail to provide network access. EX1004, [0024], [0027], [0033]-[0038]. For example, Salmela explains that device 10 can “detect access loss for its local (preferred) RAN” using the current

subscription credentials 26. EX1004, [0033]. Salmela also explains that based on detecting this access loss for the local RAN, device 210 can “attempt reconnection using its current subscription credentials 26—e.g., using its stored IMSI for some number of attempts.” EX1004, [0033]. Device 10 “scans for alternative access” to non-preferred networks in cases where the reconnection attempts are unsuccessful. EX1004, [0034]. If scanning for alternative access fails, device 10 detects a *network-provisioning state change* based on determining that subscription credentials 26 have failed to provide network access. EX1004, [0035]. Furthermore, Salmela discloses that a failure to gain network access can result from the device 10 not being “recognized or otherwise authenticated by its home network.” EX1004, [0037].

157. It is clear that these attempts to reconnect with the preferred network and connect with non-preferred networks represent *failed attempts* by device 10 to be *authorized* for the service(s) provided by these networks, such as voice services, data services, and/or Internet services. EX1004, [0003] (“network *service* provider (home operator)”), [0004] (“access subscribed services”), [0028] (“Internet”), [0033]-[0035], FIG. 3. Consequently, in cases where device 10 is unable to connect to the preferred and non-preferred networks using its current subscription credentials 26, a POSITA would have understood and it would have been obvious that device 10 has determined that an *attempt* by the device 10 to be *authorized* for *services* on these networks has *failed*.

Claim [16]: The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that a network access error has occurred.

158. As I described above in my analysis of Element [1g], Salmela discloses that device 10 can detect a ***network-provisioning state change*** based on determining that current subscription credentials 26 fail to provide network access by determining that a network access error has occurred. EX1004, [0024], [0027], [0033]-[0038]. This failure to provide network access constitutes, in many cases, a network access error that device 10 detects based on making unsuccessful attempts to use subscription credentials 26 for gaining network access. EX1004, [0024] (“device 10 uses its subscription credentials 26 for gaining network access unless and until it is unable to gain access using those credentials”), [0027] (“the method includes detecting a failure to gain network access using the current subscription credentials 26 held in the wireless communication device 10”), [0037] (“device 10 can communicate with a local RAN, but is not recognized or otherwise authenticated by its home network”), [0038] (“device 10 is explicitly disconnected from its home network...the home network sends signaling—e.g., a message—to the device 10 that indicates that the device’s subscription credentials are expired or otherwise invalid.”).

Claim [17]: The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises receiving a provisioning-state-change message.

159. As I described above in my analysis of Element [1g], Salmela discloses that device 10 can detect a ***network-provisioning state change*** based on determining that current subscription credentials 26 fail to provide network access. EX1004, [0024], [0027], [0033]-[0038]. Salmela explains that device 10 can identify a failure of subscription credentials 26 to provide network access by receiving a ***provisioning-state change message*** (e.g., a “failure message”) which indicates a network access failure. EX1004, Claim 14 (“the wireless communication device is configured to detect a failure to gain network access...based on receiving a failure message responsive to attempting to gain network access using the current subscription credentials”), *see also* Claim 2 (“wherein detecting a failure to gain network access using current subscription credentials held in the wireless communication device comprises receiving a failure message responsive to attempting to gain network access using the current subscription credentials”), [0038] (“home network sends signaling—e.g., a message—to the device 10 that indicates that the device’s subscription credentials are expired or otherwise invalid” and “device 10 recognizes such signaling as an explicitly indicated network access failure”). Salmela’s device 10 receiving this failure message amounts to device 10 detecting a ***provisioning-state change***, the message indicating that device 10 is no longer provisioned for network access using the current subscription credentials 26.

Claim [18]: The wireless device recited in claim 17, wherein the provisioning-state-change message comprises a text message.

160. As I described above in my analysis of Claim [17], *supra*, Salmela discloses that device 10 can receive a *provisioning-state change message* (referred to as a “failure message”) which indicates a network access failure. It would have been obvious for Salmela’s failure message to include *text* and therefore comprise a *text message*. One reason for this is that a “failure message” must include information that indicates the failure communicated by the message. It would have been obvious for this information to be in the form of *text* (e.g., numbers or characters) that indicates the existence of the failure and/or describes the failure because there are a limited number of ways to communicate a failure using a message and a *text message* is a prominent solution to achieve this. Implementing the failure message to include a text message would have been particularly obvious, for example, to provide a notification that would permit the failure message to be presented to and read by the user.

161. Even Salmela itself does not expressly disclose or render obvious implementing the failure message as a text message, it is clear that Rishy-Maharaj describes various conventional communication channels—including “short message service (“SMS”) protocols—that can be utilized for signaling between a wireless device and network elements including “short message service (“SMS”) protocols. EX1005, [0036], [0109], [0182]; *see also*, [0028]-[0035], [0108]-[0121]. SMS is widely known in the field to refer to protocols for text messaging. It would have

been obvious for a POSITA to use the SMS protocol communicate Salmela's network access failure message as a text message as suggested by Rishy-Maharaj.

162. For example, I noticed that Rishy-Maharaj teaches that “[i]n embodiments in which an unsubscribed-to network is used to initially gain a new subscription, the user may have to pay roaming charges to connect to the service fulfillment server system.” EX1005, [0036]. Rishy-Maharaj explains that one way to overcome this issue of roaming charges is to “use other channels to establish a subscription including...short message service (“SMS”) protocols.” EX1005, [0036]. Thus, it would have been obvious for a POSITA to cause device 10 to receive the *provisioning-state-change message* as a *text message* in order to avoid such roaming charges. It is also clear that using SMS-based text messages to alert device 12 of a network access failure also would have been obvious to try in view of the limited number of communication channels available to the wireless device, and further would have been obvious as a straightforward application of a conventional technique (e.g., SMS-based messaging) to a known system (e.g., Salmela's) to achieve merely predictable results.

Claim [19]: The wireless device recited in claim 17, wherein the provisioning-state-change message comprises a push message from a push server communicatively coupled to the wireless device over the wireless access network.

163. As I described above in my analysis of Claim [17], *supra*, Salmela discloses that device 10 can receive a *provisioning-state change message* (referred

to as a “failure message”) indicating a network access failure. For example, Salmela discloses that the “home network [can] send[] signaling—e.g., a message—to the device 10 that indicates that the device’s subscription credentials are expired or otherwise invalid” and “device 10 recognizes such signaling as an explicitly indicated network access failure.” EX1004, [0038]; *see also*, Claim 2, Claim 14. Salmela explains that the “failure message” described in paragraph [0038] and Claims 2 and 14 of Salmela is not requested by the device but is not requested by the device but is instead *pushed* from a server (*push server*) communicatively coupled to the *wireless device* over the *wireless access network* of the home operator. EX1004, [0028], FIG. 3.

164. In the field of telecommunications, “push” messages are understood to be sent from a server to a client device without a request from the client device to send the message. EX1033, 10 (“there is also ‘push’ technology...where there is no explicit request from the client before the server transmits its content”). In contrast, “pull” messages are sent by a server to a client device at the request of the client device. EX1033, 10 (“whereas ‘pull’ transactions of information are always initiated from the client, “push” transactions are server-initiated”). For example, a technical specification for the wireless application protocol (WAP) corroborates that as of 2001, wireless access network operators could send “push” messages to client devices (e.g., wireless devices) without the client devices requesting these messages.

EX1033, 5-11. Salmela's "failure messages" represent push messages because these failure messages are sent to the wireless device to notify the wireless device of a failure to gain network access even though the device did not request a notification in the event of a failure to gain access. EX1004, Claim 2, Claim 14.

165. My opinion here is also corroborated by multiple references indicating that it was well known for wireless devices to receive *push messages* from push servers by 2013. EX1015, 96 (describing a wireless device that "allows you to receive push messages from the network."); EX1016, 140 ("Push notifications are used by applications to alert you of new information, even when the application isn't running. Notifications differ depending upon the application, but may include text or sound alerts, and a numbered badge on the application's icon on the Home screen."); EX1020, 101 ("Push notifications appear in the Notification Center and alert you to new information, even when an app isn't running. Notifications vary by app, but may include text or sound alerts, and a numbered badge on the app icon on the Home screen."); EX1021, 81 (describing a wireless device that "allows you to receive push messages from the network.").

166. It would have been evident, or at least obvious to a POSTIA that a failure message is pushed to device 10 from a push server because Salmela's failure message is automatically sent from the home network to device 10 as an explicit indication of network access failure, as opposed to other instances where device 10

detects a provisioning state change as a result of the device's inability to communicate with the local RAN or inability to be authenticated over the local RAN. EX1004, [0033], [0037], FIG. 4. Furthermore, it would have been obvious to implement device 10 to use a push message due to the limited number of communication channels available to the wireless device, and further would have been obvious as a straightforward application of a known technique (e.g., push notifications) to a known system (e.g., Salmela's) to achieve merely predictable results.

Claim [20]: The wireless device recited in claim 17, wherein the provisioning-state-change message comprises a message received by an application program on the wireless device.

167. It is clear that Salmela's device 10 includes logic that enables device 10 to "recognize[]" a network-provisioning state change message (e.g., a network-access failure message) "as an explicitly indicated network access failure." EX1004, [0038]. Furthermore, Salmela explains that processing on device 10 is "implemented via software executing in one or more microprocessor circuits." EX1004, [0026]; *see also*, [0020] ("storing working data, computer program instructions"). It is apparent that a POSITA would have appreciated and found obvious that Salmela's software for receiving and processing the network-access failure message constitutes an ***application program*** on the wireless device (e.g., device 10). This is especially true because ***application programs*** commonly refer to "software" like that disclosed

in Salmela. EX1004, [0026] (“implemented via software executing in one or more microprocessor circuits”).

168. Another reason for my opinion here is that the ’510 Patent broadly describes “application” programs with reference to a range of different types of software including user applications (e.g., “browser”), operating system (OS) applications, and native applications. EX1001, 10:62-64. Rishy-Maharaj similarly confirms that it was a known and conventional option before 2013 to implement software such as Salmela’s as application programs. *See, e.g.*, EX1005, [0062] (describing “*applications* necessary to provide instructions to the network and control routines 115”). Furthermore, my opinion here is corroborated by numerous references confirming that text messaging applications were commonplace in wireless phones by the Critical Date of the ’510 Patent. EX1015, 91-97 (describing a messaging application for a wireless phone); EX1016, 23 (describing an application to “[s]end and receive SMS text messages”); EX1022, [0042] (describing a wireless device where messages including text messages can be “sorted by application”).

Claim [21]: The wireless device recited in claim 1, wherein the one or more credentials comprise a phone number.

169. As I described above in my analysis of Elements [1b]-[1c], Salmela’s device 10 includes a *memory* configured to store *one or more credentials* including subscription credentials 26 and temporary access credentials 30. EX1004, [0010]-

[0012], [0020], [0022]-[0025], FIG. 1. For example, I noticed that Salmela explains “the subscription credentials 26 comprise a downloadable Universal Subscriber Identity Module (USIM), which may include an international mobile subscriber identifier (IMSI).” EX1004, [0023], [0033] (“using its stored IMSI”), [0036] (“IMSI-based attachment”), FIG. 4. This disclosure is notable because a POSITA would have recognized that an IMSI represents a *phone number* consistent with the plain meaning of this term as used in the ’510 Patent. EX1004, [0021], [0023]. For example, a POSITA would have recognized that Salmela’s IMSI is a *phone number* that uniquely identifies device 10 (e.g., “a cellular radiotelephone”) and the USIM associated with device 10.¹⁰ EX1004, [0021], [0023].

¹⁰ One thing that I noticed in my review of the ’510 Patent is that the term “phone number” is not defined. The ’510 Patent also does not use the term “phone number” to refer to a specific type of credential or identifier known in the field. The specification of the ’510 Patent provides a lengthy list of credentials that a mobile device may use to authenticate with a wireless access network including a phone number, an IMSI, an MSID, an MSISDN, an MDN, among many others. EX1001, 5:21-43. I noticed, however, that the listed credentials are not mutually exclusive. For example, an MSISDN and an MDN are both numbers that a calling

Claim [22]: The wireless device recited in claim 1, wherein the one or more credentials comprise an international mobile subscriber identifier (IMSI), a mobile station identifier (MSID), a mobile station international ISDN number (MSISDN), a subscriber information module (SIM) identifier, an electronic serial number (ESN), a mobile equipment identifier (MEID), an international mobile equipment identity (IMEI), a device identifier, a subscriber identifier, a service account identifier, a media access control (MAC) address, an Internet protocol (IP) address, a token, a one-time token, a mobile directory number (MDN), a network access identifier (NAI), a user name, a password, access point name (APN) configuration information, an encryption key (Ki), a Wi-Fi service set identifier (SSID), a Wi-Fi network configuration, an IP address, or a combination of these.

170. As I described above in my analysis of Elements [1b]-[1c], Salmela's device 10 includes a *memory* configured to *store one or more credentials* including subscription credentials 26 and temporary access credentials 30. EX1004, [0010]-[0012], [0020], [0022]-[0025], FIG. 1. I noticed that Salmela expressly discloses that "the subscription credentials 26 comprise a downloadable Universal Subscriber

party may call to reach a device on cellular network, and both are often colloquially referred to as "phone numbers." The '510 Patent identifies these terms them alongside "phone number" and "IMSI" in the list of credentials. EX1001, 5:21-43. It is apparent in this context that a POSITA would have understood that the term "phone number" in the '510 Patent does not refer to a specific or particular type of number but instead broadly encompass a range of different numbers that identify or are associated with a wireless device including an IMSI.

Identity Module (USIM), which may include an *international mobile subscriber identifier (IMSI)*,” which means that Salmela’s *one or more credentials* comprise an *IMSI*. EX1004, [0023], *see also* [0033] (“the device 10 is configured to attempt reconnection using its current subscription credentials 26—e.g., using its stored IMSI”), [0036] (“IMSI-based attachment”), FIG. 4.

171. Furthermore, at least by the Critical Date of the ’510 Patent, an IMSI is understood in the field of telecommunications to be a *subscriber identifier*. As an initial matter, IMSI stands for *international mobile subscriber identity*, which clearly refers to a *subscriber identifier*. Furthermore, my opinion here is corroborated by a European telecommunications standard document published in 2011 which provides that an IMSI includes three constituent parts—including a *mobile subscriber identification number* (MSIN) that identifies a particular subscriber of a home operator network. EX1031, 15 (describing the MSIN as “identifying the mobile subscriber” within a network). Because it is clear that Salmela’s IMSI identifies a subscriber, the IMSI is a *subscriber identifier*.

Claim [23]: The wireless device recited in claim 1, wherein the target credential comprises a phone number.

172. As I described above in my analysis of Claim [21], *supra*, Salmela explains that “the subscription credentials 26 comprise a downloadable Universal Subscriber Identity Module (USIM), which may include an international mobile subscriber identifier (IMSI).” EX1004, [0023], [0033] (“using its stored IMSI”),

[0036] (“IMSI-based attachment”), FIG. 4. An IMSI is (or at least renders obvious) a phone number consistent with the plain meaning of this term as used in the ’510 Patent in that it is a number that uniquely identifies device 10 (e.g., “a cellular radiotelephone”) and its USIM. EX1004, [0021], [0023]; *supra*, Footnote 8. In the case where the subscription credentials 26 comprise an IMSI *phone number*, it is clear that a POSITA would have understood and it would have been obvious that the *target credential* would also include an IMSI *phone number* so that device 10 would be capable of comparing them to determine a match and to update the IMSI when a new subscription is available. EX1004, [0023], [0041], [0044].

Claim [24]: The wireless device recited in claim 1, wherein the target credential comprises an international mobile subscriber identifier (IMSI), a mobile station identifier (MSID), a mobile station international ISDN number (MSISDN), a subscriber information module (SIM) identifier, an electronic serial number (ESN), a mobile equipment identifier (MEID), an international mobile equipment identity (IMEI), a device identifier, a subscriber identifier, a service account identifier, a media access control (MAC) address, an Internet protocol (IP) address, a token, a one-time token, a mobile directory number (MDN), a network access identifier (NAI), a user name, a password, access point name (APN) configuration information, an encryption key (Ki), a Wi-Fi service set identifier (SSID), a Wi-Fi network configuration, an IP address, or a combination of these.

173. As I described above in my analysis of Element [1c], Salmela’s device 10 includes a *memory* configured to *store one or more credentials* including subscription credentials 26 and temporary access credentials 30. EX1004, [0010]-[0012], [0020], [0022]-[0025], FIG. 1. Salmela explains that device 10 engages in a process to automatically update a *particular credential* (e.g., current subscription

credentials 26) of the *one or more credentials* with new subscription credentials in response to detecting that the current subscription credentials 26 no longer provide network access. EX1004, [0022]-[0027], [0033]-[0038]. I noticed that this automatic update is done based on comparing the *particular credential* with a *target credential* as I explain in further detail above in my analysis of Element [1h]. In examples where the current subscription credential 26 includes an “*international mobile subscriber identifier (IMSI)*,” a POSITA would have understood and it would have been obvious that the *target credential* would also include an *IMSI* so that device 10 would be capable of comparing the *particular credential* and the *target credential* (both IMSIs) to determine whether a match exists, and to update the IMSI when a new subscription is available. EX1004, [0023], [0041], [0044].

174. Furthermore, at least by the Critical Date of the '510 Patent, an IMSI is understood in the field of telecommunications to be a *subscriber identifier*. As an initial matter, IMSI stands for *international mobile subscriber identity*, which clearly refers to a *subscriber identifier*. Furthermore, my opinion here is corroborated by a European telecommunications standard document published in 2011 which provides that an IMSI includes three constituent parts—including a *mobile subscriber identification number* (MSIN) that identifies a particular subscriber of a home operator network. EX1031, 15 (describing the MSIN as

“identifying the mobile subscriber” within a network). Because it is clear that Salmela’s IMSI identifies a subscriber, the IMSI is a *subscriber identifier*.

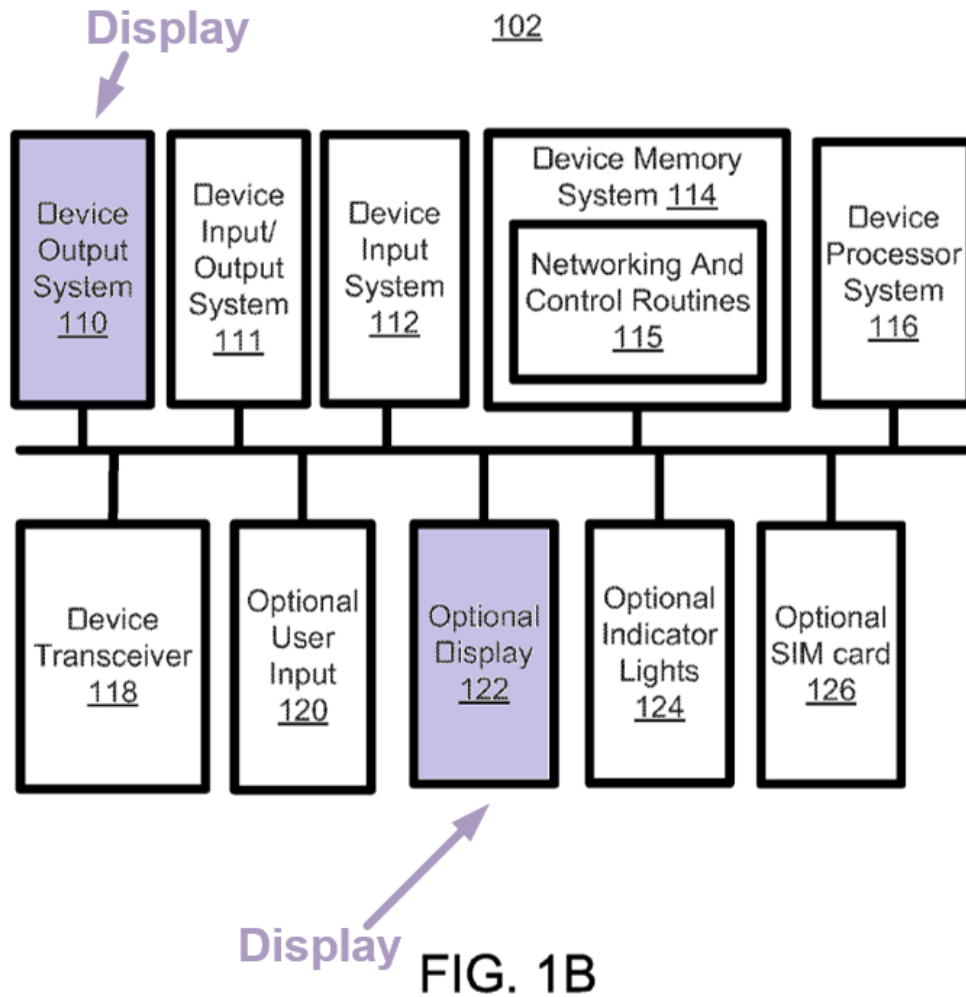
Claim [25]: The wireless device recited in claim 1, wherein the particular credential comprises a first phone number currently associated with the wireless device, and wherein the target credential comprises a second phone number.

175. As I described above in my analysis of Claims [21] and [23], Salmela clearly teaches that the current subscription credentials 26 (*particular credential*) comprise an IMSI representing a *first phone number* currently associated with device 10 (*wireless device*), and the representations of the new subscription credentials 26 (*target credential*) held by the registration service comprise another IMSI represent a *second phone number*. EX1004, [0023], [0041], [0044]. It is clear that the *target credential* represents, or at least renders obvious, a *second IMSI phone number* different from the *first IMSI phone number* of the current subscription credentials 26, for example, when the credentials have been updated in response to a requested change in subscription plans or a requested change in the home operator network. EX1004, [0010]-[0012], [0041], [0044]. This is because when the *particular credential* and the *target credential* are part of the same class of credential—an IMSI—the particular credential and the target credential can be compared to determine whether a mismatch exists.

Claim [28]: The wireless device recited in claim 1, wherein the user interface comprises a display.

176. As I described above in my analysis of Element [1a], *supra*, a POSITA would have been motivated to implement Salmela’s wireless communication device 10 with a user interface as taught by Rishy-Maharaj. EX1004, [0004], [0009], [0021]; EX1005, [0028]-[0046], [0108]-[0121], FIGS. 1A, 1B, 2; *supra* §VII.C. Salmela discloses types of wireless devices 10 that commonly included *displays* such as “a cellular radiotelephone, pager, [or] PDA” EX1005, [0021]. Furthermore, in the combination, Rishy-Maharaj also expressly discloses that the user interface can include a *display*, meaning that the *user interface* of the Salmela-Rishy-Maharaj combination comprises a *display*. EX1005, [0059] (“[t]he device output system 110 may include... a display system...”), [0067] (“optional display 122 may be any display capable of rendering images, including, by way of example, a monitor, laptop screen, net book screen, cellular phone, smart device, personal desktop assistant or projector”); *supra*, §VII.C.

177. Furthermore, displays were common on wireless devices by 2013, a fact which multiple references corroborate. EX1015, 21 (describing a “display screen” of a wireless device); EX1016, 20 (describing wireless device including a “touchscreen” that can display information). FIG. 1B of Rishy-Maharaj, which depicts the device output system 110 and optional display 122, is reproduced below:



EX1005, FIG. 1B (annotated).

Claim [29]: *The wireless device recited in claim 1, wherein the user interface comprises a speaker.*

178. As I described above in my analysis of Element [1a], *supra*, a POSITA would have been motivated to implement Salmela’s *wireless* communication *device* 10 with a *user interface* as taught by Rishy-Maharaj. EX1004, [0004] [0009], [0021]; EX1005, [0028]-[0046], [0108]-[0121], FIGS. 1A, 1B, 2. Salmela discloses wireless devices 10 that commonly include *speakers* such as “a cellular radiotelephone, pager,

[or] PDA” EX1005, [0021]. Additionally, in the combination, Rishy-Maharaj expressly discloses a *user interface* can including a *speaker*, meaning that the *user interface* of the Salmela-Rishy-Maharaj combination includes a *speaker*. EX1005, [0059] (“[t]he device output system 110 may include... a speaker system...”), [0160], FIG. 1B; *supra*, §VII.C. My opinion here is corroborated by multiple references which demonstrate that speakers were commonplace on wireless devices by 2013. EX2016, 20 (describing wireless device including a “speaker”); EX1022, [0068] (describing a “speaker” of a wireless device).The device output system 110 including a speaker, is reproduced below in FIG. 2B of Rishy-Maharaj:

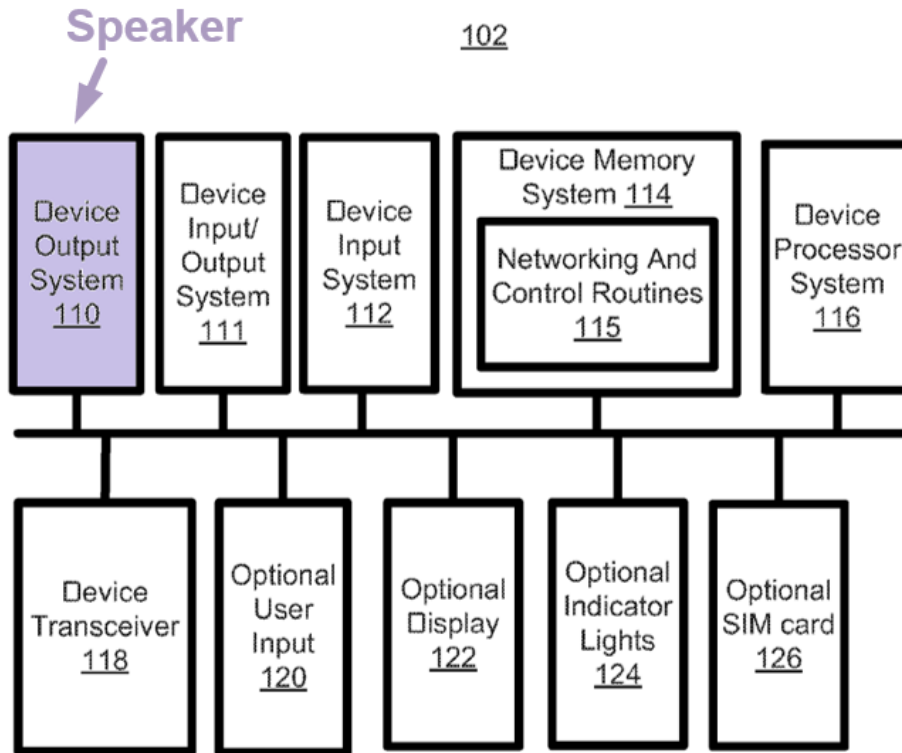


FIG. 1B

EX1005, FIG. 1B (annotated).

Claim [30]: *The wireless device recited in claim 1, wherein the one or more services comprise a voice service, a messaging service, or a data service.*

179. As I described in my analysis of Element [1c], Salmela discloses that the *one or more credentials* (e.g., subscription credentials 26 and temporary access credentials 30) associated with the *wireless device* (e.g., device 10) authorize the *wireless device* to use a *wireless access network* to access *one or more services*. EX1004, [0004] (“allowing the handset user to access subscribed *services*”), [0010]-[0012], [0020], [0022]-[0025], [0027]-[0032], FIG. 1, FIG. 3. For example, Salmela

explains that device 10 can subscription credentials 26 for accessing home network 40 and visited network 46, which are wireless access networks including RANs and CNs that provide *services* to connected devices—including Salmela’s device 10. EX1004, [0028], [0030]-[0032], FIG. 3. Salmela explains that these wireless access networks “communicative[ly] couple to one or more additional networks 52, such as the Internet” thereby providing the device 10 with access to Internet *data services*. EX1004, [0028]. Furthermore, a POSITA also would have understood and it would have been obvious that wireless access networks like those described in Salmela commonly provided voice, data, and/or messaging services that would ordinarily be utilized by a wireless device such as Salmela’s “cellular radiotelephone, page, [or] PDA.” EX1004, [0021]; *supra*, Claim [18] (describing SMS messaging service).

180. For example, Salmela that “the device 10 is a cellular communication device” in some embodiments. EX1004, [0021]. One class of cellular communication devices that uses credentials for accessing networks is “conventional 3G cellular telephones.” EX1004, [0004]. For example, 3G cellular telephones receive any one or combination of data service, voice service, and messaging service from wireless access networks such as home network 40 and visited network 46 that include RANs and CNs. Data service, voice service, and messaging service are staple services provided by wireless access networks including RANs and CNs, especially networks that operate in accordance with 3G and other 3GPP protocols.

This is corroborated by Rishy-Maharaj, which describes a wireless device that communicates with networks using internet data service. EX1005, [0035] (“wireless device 102 may communicate with other networks and devices using any wireless protocol including, for example, Wi-Fi, Wi-Max, 2G, 3G, 4G, 4G LTE, UMTS, other satellite communication, or radio via a transceiver”), [0065]. My opinion here is also corroborated by multiple references that describe 3GPP networks providing any one or combination of *voice service*, a *messaging service*, and *data service*. EX1018, 1-3 (describing 3GPP network that can provide “cellular data”); EX1032, 3 (“The connectivity layer is a pure transport mechanism that is capable of transporting any type of information via voice, data and multimedia streams.”).

Claim [31]: The wireless device recited in claim 1, wherein the one or more machine-executable instructions comprise an application program.

181. Salmela discloses that device 10 includes *one or more processors* including processing circuits 20 and credentials processor 22 that execute *one or more machine-executable instructions*, as I described above in my analysis of Element [1e] and Claim [20]. EX1004, [0020], [0024], [0026], [0027], FIG. 1, FIG. 2. For example, I noticed that Salmela explains device 10’s memory 32 can store “computer program instructions,” thus indicating that the processing circuits 20 and credentials processor 22 execute these *program* instructions to perform one or more actions. EX1004, [0020]. It would have been obvious to implement Salmela’s machine-executable program instructions as an application program for at least the

reasons described above in connection with Claim [20], *supra*. Cf. EX1001, 10:62-64 (broad range of example “application” programs in the ’510 Patent). Rishy-Maharaj similarly confirms that implementing software like Salmela’s as application programs was a known and conventional option before the Critical Date. EX1005, [0062] (describing “*applications* necessary to provide instructions to the network and control routines 115”), [0058].

Claim [32]: The wireless device recited in claim 1, wherein the one or more machine-executable instructions comprise an operating system (OS) component, an OS function, an OS service, a modem programming agent, a modem software or firmware agent, an over-the-air (OTA) mobile device parameter programming agent, an Open Mobile Alliance (OMA) agent, a secure communication agent configured to communicate number porting and number provisioning information, a software agent, a firmware agent, or a combination of these.

182. Salmela’s *machine-executable instructions* include instructions for “obtaining the subscription credentials 26 via over-the-air (OTA) provisioning.” EX1004, [0022]. This clearly renders obvious that Salmela’s device 10 includes an *OTA mobile device parameter programming agent* to enable device 10 to participate in OTA provisioning, because this programming agent would facilitate obtaining subscription credentials 26 via OTA provisioning. Salmela explains that “credentials processor 22 may be implemented via software executing in one or more microprocessor circuits used to implement the processing circuits 20,” which a POSITA would have understood to mean and found obvious that credentials processor 22 can be a *software agent*. EX1004, [0026]. Therefore, a POSITA would

have understood to this to mean, and would have found it obvious, that credentials processor 22 can be a *software agent*.

183. It was well known by the 2013 Critical Date of the '510 Patent that a wireless device communicating over a *wireless access network* includes an *operating system*. Several references corroborate this. EX1015, 5 (user manual explaining that a manufacturer is not responsible for modifications to the operating system of a wireless device); EX1016, 1 (describing a wireless device including operating system (OS) software); EX1021, 5 (explaining that “[t]he actual available capacity of the internal memory” of a wireless device “is less than the specified capacity because the operating system and default applications occupy part of the memory.”).

184. Rishy-Maharaj likewise discloses a wireless device 102 that includes a device processor system 116 that can “*execute instructions*” in networking control routines 115 stored in a device memory system 114. EX1005, [0063]. Rishy-Maharaj expressly discloses that these networking control routines 115 can “receive credentials to access the then subscribed-to network” and “access the network.” EX1005, [0063]. Rishy-Maharaj also discloses that in one embodiment, device processor system 116 is “communicatively coupled to...a wireless modem,” e.g., a *modem programming agent* or a *modem software or firmware agent*. EX1005, [0163].

Claim [33]: The wireless device recited in claim 1, wherein the user request comprises an indication of the target credential, a phone number, a user name, a password, an account number, a subscriber name, a company name, at least a portion of a billing address, at least a portion of a social security number, a personal identification number (PIN), or a combination of these.

185. As I described above in connection with my analysis of Element [1f], *supra*, and my analysis of the Salmela-Rishy-Maharaj Combination (*Supra*, §VII.C), it is apparent the teachings of Salmela in view of Rishy-Maharaj would have rendered obvious a ***wireless device*** configured to ***receive*** an indication of a ***user request*** to replace a ***particular credential*** with a ***target credential***. EX1004, [0003]-[0009], [0011], [0020]-[0027], [0033]-[0035], [0050]; EX1005, [0028]-[0046], [0058]-[0060], [0066], [0067], [0108]-[0121], FIGS. 1A, 1B, 2. For example, I noticed that Salmela and Rishy-Maharaj both describe how a user can submit a ***user request*** to activate or change a subscription plan. EX1004, [0003]-[0009], [0010]-[0011], [0050]; EX1005, [0066], [0067], [0112], [0113]. Rishy-Maharaj, for example, explains that “[t]he user may use the optional user input 120 to select [a] particular local network subscription that suits the user best.” EX1005, [0066], *see also* [0112] (“the user may select the subscription plan and network that best suits the user”).

186. Rishy-Maharaj explains that “[u]pon receiving the plan or subscription data, the wireless device 102 or its user may determine that there is a plan ... worth purchasing and decide to purchase it. The wireless device 102 may transmit the

subscriber ID and the plan selection to the SFSS to process the transaction,” thus explaining that the user’s request selecting a particular subscription plan includes the user’s ID. EX1005, [0230], *see also* FIG. 14 (depicting client device transmitting request including “SUBSCRIBER_ID, PLAN”), [0112]-[0113], [0126]-[0127], [0139]-[0140], [0153], FIGS. 4-5. It is clear that the Rishy-Maharaj’s “subscriber ID” represents a *user name* or *subscriber name*. Indeed, the terms “user name” and “subscriber name” both refer to login credentials or system identifiers that are similar to the “subscriber ID” of Rishy-Maharaj.

187. Furthermore, the user request also includes an indication of a *company name* of a service provider that operates the network for the subscription plan selected by the user, because the user’s request identifies a particular plan or network associated with a particular service provided. This means also that the user request includes an indication of the *target credential* associated with the selection. The request can also include an indication of an *account number* that can be charged for the subscription. EX1005, [0153] (“The transaction may include an acceptance of the terms of service of a particular service plan or some agreement to a transaction to add funds or credits to an account.”).

Claim [35]: The wireless device recited in claim 1, wherein obtaining the indication of the user request to replace the particular credential of the one or more credentials with the target credential comprises obtaining information associated with the user request through the user interface.

188. As I described above in my analysis of Element [1f], *supra*, and the overview of the Salmela-Rishy-Maharaj combination (*see* §V.A.3, *supra*), the teachings of Salmela in view of Rishy-Maharaj would have rendered obvious a *wireless device* that can *receive* an indication of a *user request* to replace a *particular credential* with a *target credential*. EX1004, [0003]-[0009], [0020]-[0027]; EX1005, [0058]-[0060], [0067], [0108]-[0121]. The Salmela-Rishy-Maharaj combination expressly provides that a wireless device can obtain *information* associated with a *user request* through a *user interface* of the device. EX1005, [0066] (“The user may use the optional user input 120 to select the particular local network subscription that suits the user best.”), [0112] (“The wireless device 102 may have an optional display 122 in order to list services and terms of service for the user to select. The wireless device 102 may also have an optional user input 120 to allow the user to select a plan.”). Each of these cited portions of Rishy-Maharaj describe user requests received through user interfaces that involve information.

Claim [36]: The wireless device recited in claim 1, wherein the network element comprises a programming server.

189. Salmela discloses that device 10 can initiate a *programming session* with a *network element* (e.g., a credentialing server) to obtain a new subscription credential from the *network element*, as I described above in my analysis of elements [1i]-[1j], *supra*. EX1004, [0025], [0027], [0045]. Salmela explains that the

credentialing server is a *network element* that performs substantially the same functions as the programming server described in the '510 Patent, including delivering new credentials to the wireless device. Cf. EX1001, 9:47-48 (“Programming server 1152 delivers the new device credentials to the mobile device 100.”), 7:6-8 (“programming server [] enable[s] the device to obtain the desired credentials”) with EX1004, [0045] (“credentialing server from which the new subscription credentials are obtained”). It is clear that a POSITA would have understood and found obvious that Salmela’s credentialing server comprises a *programming server*. One reason for this is that the new subscription credentials that device 10 obtains from the credentialing server *program* the device 10 to use a wireless access network according to a new subscription plan. EX1004, [0045]. Indeed, Salmela expressly discloses that device 10 can “download” the new subscription credentials to secure element 24 for use, meaning that device 10 is *programmed* with the new subscription credentials. EX1004, [0025].

Claim [37]: The wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises contacting the network element using at least a portion of the one or more credentials associated with the wireless device.

190. Salmela discloses that device 10 can *initiate a programming session* with a *network element* (e.g., a credentialing server) to obtain an updated subscription credential from the *network element*, as I described above my analysis

of Elements [1i]-[1j]. EX1004, [0025], [0027], [0045]. Salmela discloses that the *one or more credentials* stored in the *memory* of device 10 include temporary access credentials 30 that device 10 uses to *initiate* the *programming session*. EX1004, [0020]-[0027], FIG. 1; *supra*, [1c]. For example, Salmela discloses that “device 10 is configured to perform a reversion to its temporary access credentials 30, responsive to detecting a network access failure” and “determining whether new subscription credentials are needed...comprises *contacting a registration service via the temporary network access*.” EX1004, [0039], [0040]. After device 10 contacts Salmela’s registration service using the temporary access credentials 30, the registration service then provides network address information that “identifies a credentialing server from which the new subscription credentials are to be obtained.” EX1004, [0045]. Device 10 uses this “temporary network access” obtained with the temporary access credentials 30 “*to contact the credentialing server to obtain the new subscription credentials*.” EX1004, [0045]. Consequently, device 10 initiates the programming session with the credentialing server using *at least a portion* of the *one or more credentials* (e.g., temporary access credentials 30) associated with the *wireless device*.

Claim [38]: The wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises contacting the network element using a temporary credential.

191. For at least the reasons that I described above in connection with Claim [37], Salmela discloses that device 10 can *initiate* a *programming session* with a *network element* (e.g., a “credentialing server”) to obtain new subscription credentials from the *network element*. EX1004, [0025], [0027], [0045]; *supra*, [1i]-[1j], [37]. For example, Salmela expressly discloses that device 10 uses a *temporary credential* (e.g., a temporary access credential 30) to *contact* the *network element* (e.g., the credentialing server) as part of a process to *initiate a programming session* with the *network element*. EX1004, [0025] (“device 10...uses those temporary access credentials 30 to gain temporary network access”), [0045] (“using the temporary network access to contact the credentialing server to obtain the new subscription credentials”).

Claim [39]: The wireless device recited in claim 38, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to obtain the temporary credential from memory.

192. As described above in connection with Claims [37] and [38], Salmela discloses that device 10 can use a temporary credential (e.g., temporary access credentials 30) to secure temporary network access and to contact a network element (e.g., a credentialing server) that holds new subscription credentials for device 10. EX1004, [0020]-[0027], [0045]. One example of Salmela’s temporary access credentials 30 is a “preliminary international mobile subscriber identity (PIMSI).” EX1004, [0023]. Salmela explains that “device 10 includes a ‘credentials processor’

22 that is configured to revert from the subscription credentials 26 to the temporary access credentials 30, responsive to detecting network access failure.” EX1004, [0024]; *see also*, [0010], [0027]-[0028], [0035], [0038], [0047], FIG. 1. Salmela discloses that the temporary access credentials 30 are stored in the fuse/OTP memory element 28 of Salmela’s device 10. EX1004, [0020], [0023], FIG. 1.

193. A computer processor like Salmela’s credential processor 22 are configured to obtain data and instructions from memory to enable the processor to perform operations or other processing on the data according to the retrieved instructions. EX1004, [0020] (“working data, computer program instructions”). This is especially true given the fact that Salmela discloses a separate one or more processors and memory—meaning that the one or more processors would need to obtain the temporary access credentials from the memory to use these credentials as disclosed by Salmela. EX1004, [0020] A POSITA thus would have understood and it would have been obvious that Salmela’s credentials processor 22 obtains the temporary access credentials 30 from fuse/OTP memory element 28 when reverting from the subscription credentials 26 to the temporary access credentials 30.

Claim [41]: The wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises contacting the network element using a default credential.

194. Salmela discloses that device 10 can *initiate a programming session* with a *network element* (e.g., a credentialing server) to obtain a new subscription

credential from the *network element*, as I described above in connection with Elements [1i]-[1j] and Claims [37]-[38], *supra*. EX1004, [0025], [0027], [0045], FIG. 1. Salmela discloses that device 10 *initiates* this *programming session* using temporary access credentials 30, which represent *a default credential* stored in the *memory* of device 10. EX1004, [0020]-[0027], FIG. 1. For example, Salmela explains that “determining whether new subscription credentials are needed...comprises *contacting a registration service* via [] *temporary network access*.” EX1004, [0039], [0040], [0045]. After device 10 contacts the registration service using the temporary access credentials 30, the registration service then provides network address information that “identifies a credentialing server from which the new subscription credentials are to be obtained.” EX1004, [0045]. Device 10 uses *temporary access credentials* 30 and the network address information to “obtain the new subscription credentials” from the credentialing server (*network element*). EX1004, [0045].

195. It would have been obvious that temporary access credentials 30 constitute a *default credential* of device 10. For example, Salmela teaches that device 10 reverts by default to temporary access credentials 30 anytime that subscription credentials 26 cannot gain network access. EX1004, [0024] (“revert from the subscription credentials 26 to the temporary access credentials 30, responsive to detecting network access failure”), [0025] (“device 10 thus

(automatically and autonomously) switches from its provisioned subscription credentials 26 to its temporary access credentials 30, and uses those temporary access credentials 30 to gain temporary network access”). Indeed, temporary access credentials 30 can be “burned into secure fuses or other secure OTP memory within the device 10, during its manufacture or initial configuration” thereby rendering the temporary access credentials 30 available to the device 10 as the *default credentials* when temporary network access is needed. EX1004, [0023], [0020].

Claim [42]: The wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises communicating with the network element over the wireless access network.

196. As I described above in connection with Element [1i], Salmela discloses an embodiment where the *network element* (e.g., “credentialing server”) is an entity of the core network (CN) of a *wireless access network*, such as CN 44 of home network 40 or CN 50 of visited network 46. EX1004, [0028], [0045] (“an entity in or operating under control of the CN”); *supra*, [1i]. Salmela also discloses that device 10 can *initiate* a *programming session* with the credentialing server to obtain a new subscription credential. EX1004, [0025], [0027], [0045]; *supra*, [1i]. Consequently, to *initiate* a *programming session* with Salmela’s network element (e.g., “credentialing server”)—which is part of a CN in a *wireless access network*—it would have been obvious to a POSITA for device 10 to communicate with the credentialing server *over a wireless access network* such as the home network of the

service provider that issued the new subscription credentials (e.g., home network 40) or another network that serves as a “preliminary” or “registration” operator. EX1004, [0028]-[0029], *see also* [0045].

Claim [43]: The wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises communicating with the network element over a Wi-Fi network.

197. Salmela discloses that device 10 can *initiate a programming session* with a *network element* (e.g., a credentialing server), as I described above in connection with Element [1i]. EX1004, [0025], [0027], [0045]. To the extent Salmela does not expressly disclose that device 10 *initiates the programming session* by communicating with the network element *over a Wi-Fi network*, it is clear that this feature would have been obvious based on the teachings of Rishy-Maharaj. For example, I noticed that Rishy-Maharaj discloses that “wireless device 102 may communicate with other networks and devices using any wireless protocol including, for example, Wi-Fi.” EX1005, [0035]. Furthermore, Rishy-Maharaj discloses that “the wireless device may connect to the SFSS 108 via a routing network” and “[t]he routing network may be any type of network including...a Wi-

Fi network.”¹¹ EX1005, [0109]; *see also*, [0036], [0065], [0075], [0089], [0187]. Each of these disclosures involves a *wireless device* communicating with a *network element* over a *Wi-Fi network*.

198. Implementing Salmela’s system in accordance with Rishy-Maharaj’s suggestion for communicating with a credentialing server over a Wi-Fi network such that device 10 in the Salmela-Rishy-Maharaj combination would communicate over a Wi-Fi network to initiate the programming session with the credentialing server would have been obvious to a POSITA. For example, A POSITA would have been motivated to configure device 10 to communicate with the credentialing server over a Wi-Fi network in a way that improves device 10’s ability to retrieve updated credentials when other types of networks (e.g., cellular networks) are limited or unavailable and to avoid roaming charges that could otherwise be incurred by communicating on certain networks (e.g., visitor networks). EX1005, [0037]-[0038], [0187]. A POSITA would also have reasonably expected success implementing these features in the combination because Wi-Fi networks were ubiquitous by the Critical Date and wireless devices commonly communicated over Wi-Fi networks

¹¹ The SFSS 108 of Rishy-Maharaj is a credentialing server that wireless device 102 communicates with to retrieve credentials. EX1005, [0041]-[0042], [0049]-[0050], [0108]-[0118].

by this time. My opinion here is corroborated by multiple pre-2013 references that describe Wi-Fi capable wireless devices. EX1014, [0100] (describing a wireless device including RF circuitry for communicating over Wi-Fi networks); EX1015, 19 (describing wireless device including “Built-in Bluetooth and Wi-Fi technology”); EX1016, 40 (describing a wireless device that “connects to the Internet using either a Wi-Fi network or a cellular data network”). I also noticed that Salmela does not restrict the types of networks that device 10 is able to communicate over. EX1004, [0028], [0031], [0057] (“may be implemented in a variety of systems and device types”).

Claim [45]: The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to at least assist in restricting communications over the wireless access network until the updated credential has been obtained.

199. As I described above in my analysis of Claim [6], *supra*, Salmela discloses that device 10 reverts from the current subscription credentials 26 to temporary access credentials 30 based on determining that the current subscription credentials 26 fail to provide network access. EX1004, [0010], [0024], [0027], FIG. 2. Salmela discloses that device 10 uses this temporary network access to determine if new subscription credentials are needed. EX1004, [0027]. If new credentials are indeed necessary, device 10 uses the temporary network access to if obtain the new subscription credentials. EX1004, [0027]. When device 10 obtains the new

subscription credentials, Salmela discloses that these new credentials replace the former subscription credentials and become the current subscription credentials that device 10 uses to gain access. EX1004, [0046].

200. According to Salmela, temporary access credentials 30 provide “temporary, limited network access” which is a lesser form of access to the network as compared with the access provided by valid subscription credentials 26. EX1004, [0006], [0007] [0012], [0020], [0022]-[0024]. This means that by reverting to the temporary access credentials 30 until new subscription credentials are received, the processors of device 10 *at least assist* in *restricting communications* by device 10 over the *wireless access network* until the *updated credential* has been obtained. For example, because device 10 reverts to the temporary access credentials 30 which offer limited access, device 10 assists in restricting device 10 to communicating according to the limited network access.

Claim [46]: The wireless device recited in claim 1, wherein the target credential comprises a configuration state indicator.

201. As I described above in in my analysis of Elements [1d] and [1h], *supra*, Salmela’s device 10 determines whether it needs new subscription credentials by comparing information about its current subscription credentials to a *target credential* such as “a time stamp or hash value for subscription credentials that are considered by the registration service to be current for the wireless communication device 10.” EX1004, [0044], [0041]. It is clear that Salmela’s *target credential*

indicates a *configuration state* of the device 10 by identifying which credentials the network has currently configured for device 10 to be able to access the wireless network associated with the device 10's active subscription plan. In this regard, Salmela's target credential is substantially similar to the configuration state indicator tersely mentioned in the '510 Patent itself. *Cf.* EX1001, 11:32-37 ("the requested credential may be a configuration state indicator, and the device inspects the configuration state indicator to determine if the device expected additional credential updates associated with the credential change request"). For example, Salmela's device 10 likewise inspects the time stamp or hash value to determine if updated subscription credentials associated with the user's earlier credential change request are expected. EX1004, [0044], [0041]. For example, the time stamp and hash value indicate a configuration state by conveying whether device 10's current configuration with its current subscription credentials is valid or if device 10's configuration should be updated with new subscription credentials. EX1004, [0044], [0041].

202. Moreover, it is apparent that Salmela discloses a registration server configured to receive a "bootstrap request" when accessed by a wireless device, the wireless device gaining temporary network access by reverting to temporary access credentials 30. EX1004, [0046]. In other words, the temporary access credentials 30 represent bootstrap credentials that device 10 uses in a bootstrap configuration state.

Whether the device 10 uses the subscription credentials 26 or the temporary access credentials 30 thus indicates a *configuration state* of device 10. Salmela clearly teaches that temporary access credentials 30 correspond to a “bootstrap” *configuration state* while subscription credentials 26 correspond to a normal “non-bootstrap” *configuration state*,¹² meaning that use of subscription credentials 26 indicates the non-bootstrap configuration state and use of temporary access credentials 30 indicates the bootstrap configuration state.

203. In some cases, device 10 uses a hash value or timestamp for the *target credential* to determine whether a new subscription credential is needed to replace the current subscription credential 26. EX1004, [0041], [0044]. The *target credential* can be indicative of a normal “non-bootstrap” configuration state when it serves as a benchmark for subscription credentials 26 that device 10 uses for long-term access to the network.

Element [47pre]: A non-transitory computer-readable storage medium storing one or more machine-executable instructions that, when executed by one or more processors of a wireless device, cause the one or more processors to:

¹² I noticed that the '510 Patent refers to term “configuration state” as a “bootstrap state.” EX1001, 11:38-65. I also noticed that the '510 Patent also teaches that “bootstrap credentials” are those that “provide the mobile device with limited access to the network.” EX1001, 9:4-35.

204. The Salmela-Rishy-Maharaj combination provides this claim element for at least the same reasons described above in connection with elements [1pre], [1e]. *See supra*, [1pre], [1e]; *see also* EX1004, [0020] (“The device 10 also includes a memory 32, which may include one or more memory devices, for storing working data, computer program instructions, and configuration information.”), [0026] (“software executing in one or more microprocessor circuits used to implement the processing circuits 20”), FIG. 1.

Element [47a]: obtain, through a user interface, an indication of a user request to replace a particular credential of one or more credentials, for authorizing the wireless device to use a wireless access network to access one or more services, with a target credential;

205. The Salmela-Rishy-Maharaj combination provides this claim element for at least the same reasons described above in connection with Elements [1c], [1f], [1d]. *See supra*, Elements [1c], [1f], [1d].

Element [47b]: detect a network-provisioning state change; and based on the detected network-provisioning state change, automatically

206. The Salmela-Rishy-Maharaj combination provides this claim element for at least the same reasons described above in connection with Element [1g]. *See supra*, Element [1g].

Element [47c]: determine that the particular credential does not match the target credential,

207. The Salmela-Rishy-Maharaj combination provides this claim element for at least the same reasons described above in connection with Element [1h]. *See supra*, Element [1h].

Element [47d]: initiate a programming session with a network element communicatively coupled to the wireless device over a wireless access network,

208. The Salmela-Rishy-Maharaj combination provides this claim element for at least the same reasons described above in connection with Element [1i]. *See supra*, Element [1i].

Element [47e]: obtain an updated credential from the network element, and

209. The Salmela-Rishy-Maharaj combination provides this claim element for at least the same reasons described above in connection with Element [1j]. *See supra*, Element [1j].

Element [47f]: assist in storing, in memory, the updated credential as the particular credential.

210. The Salmela-Rishy-Maharaj combination provides this claim element for at least the same reasons described above in connection with Element [1k]. *See supra*, Element [1k].

Claim [48]: The wireless device of claim 1, wherein the memory configured to store the one or more credentials comprises a protected memory that does not allow direct user modification of the particular credential.

211. Salmela discloses that device 10 includes a *memory* configured to *store one or more credentials* including subscription credentials 26 and temporary access credentials 30, as I described above in connection with Elements [1b]-[1c], *supra*.

EX1004, [0020], [0023], [0025], FIG. 1. It is apparent that the current subscription credentials 26 provide a *particular credential* that device 10 can replace if the current subscription credentials 26 do not match a *target credential*. EX1004, [0020]-[0027], [0033]-[0041]. Salmela explains that the secure element 24, the part of Salmela's *memory* that stores current subscription credentials 26, is a *protected memory*. EX1004, [0020], FIG. 1. Because subscription credentials 26 provide access to wireless access networks (e.g., home network 40 and/or visited network 46) that subscribers ordinarily pay to access and that would create substantial disruption in the ability to connect to a network if the credentials 26 were compromised, it would have been obvious to implement Salmela's secure memory 24 to prevent direct user modification of the subscription credentials 26 stored therein.

212. A POSITA would have sought to configure the secure memory 24 in this manner to ensure users could not tamper with the subscription credentials to gain improper access to a subscriber network. Preventing direct user modification of information in secure memory 24 is consistent with conventional security features of secure memories by the Critical Date of the '510 Patent, as corroborated by several pre-2013 references that discuss tamper-resistant memories. EX1028, [0050] (describing “[a] tamper-resistant, secure portable computer memory device with variable data transmission rate”); EX1029, 3:1-3 (“many mobile phone devices

include tamper-resistant memory”); EX1030, [0109] (describing a mobile device including “tamper resistant” memory).

B. The Salmela-Rishy-Maharaj-Bennett Combination Renders Claims 21, 23, and 25 Obvious

Claim [21]: The wireless device recited in claim 1, wherein the one or more credentials comprise a phone number.

213. As I discussed above in my analysis of Ground 1A at Element [1b], *supra*, Salmela explains that device 10 includes a *memory* that can *store one or more credentials* including subscription credentials 26—such as an IMSI—and temporary access credentials 30— such as a preliminary IMSI (PIMSI). EX1004, [0003]-[0012], [0020]-[0027], FIG. 1. To the extent Salmela does not disclose that the *one or more credentials* stored by device 10 include a dialable *phone number* (e.g., an MSISDN) which can be called to reach the device 10, it is apparent that Bennett provides this feature. Bennett discloses a wireless device configured as a cellular phone that can store a dialable *phone number*. EX1006, [0008], [0009], [0021]-[0023]. In the predictable Salmela-Rishy-Maharaj-Bennett combination, Salmela’s device could store *one or more credentials* including a dialable *phone number*. *Supra*, §VII.E.

Claim [23]: The wireless device recited in claim 1, wherein the target credential comprises a phone number.

214. To the extent Salmela does not disclose that the *target credential* stored by device 10 includes a dialable *phone number*, Bennett provides this feature. *Supra*,

§§VII.D-E. As I described above in connection with Elements [1d], [1h]-[1k], *supra*, Salmela discloses that device 10 determines that a *particular credential* represented by current subscription credentials 26 does not match a *target credential* corresponding to subscription credentials “considered by the registration service to be current for...device 10.” EX1004, [0020]-[0027], [0041], [0044]. Based on this determination, device 10 based on this determination, obtains an *updated credential* to replace the *particular credential*. EX1004, [0020]-[0027], [0041], [0044]. Bennett further discloses the predictable option of switching dialable phone numbers on devices. EX1006, [0025]-[0028], [0042]-[0045] FIG. 1, FIG. 5.

215. According to the teachings of Salmela, the *target credential* of the wireless device would be of the same type as the current subscription credentials (*particular credential*) so that device 10 can compare the target credential with the subscription credential. EX1004, [0023], [0041], [0044]; *supra*, Ground 1A at Claim [23]. Therefore, the *target credential* in the Salmela-Rishy-Maharaj-Bennett combination would include a dialable *phone number* (e.g., a new phone number associated with a new subscription)—just as the *particular credential* includes a dialable phone number. EX1006, [0025]-[0028], [0042]-[0045] FIG. 1, FIG. 5; *supra*, §VII.E.

Claim [25]: The wireless device recited in claim 1, wherein the particular credential comprises a first phone number currently associated with the wireless device, and wherein the target credential comprises a second phone number.

216. As I described above in my analysis of Claims [21] and [23], *supra*, the Salmela-Rishy-Maharaj-Bennett combination renders obvious an example where a wireless device (e.g., device 10) stores current subscription credentials 26 representing a *particular credential* comprising a *first* dialable *phone number* currently associated with device 10, where representations of new subscription credentials 26 representing a *target credential* comprising a *second* dialable *phone number* are stored by a credentialing service. EX1004, [0023], [0041], [0044]; *supra*, §VII.E. In the predictable Salmela-Rishy-Maharaj-Bennett combination, the *second* dialable *phone number* representing the *target credential* would be different from the *first* dialable *phone number* representing the current subscription credentials 26 (*particular credential*). EX1004, [0010]-[0012], [0041], [0044]. This is true especially when device 10 automatically updates the subscription credentials 26 in response to a requested change in subscription plans or a requested change in the home operator network. EX1004, [0010]-[0012], [0041], [0044].

C. The Salmela-Rishy-Maharaj-Bennett-FCCReg Combination Renders Claims 26-27 Obvious

Claim [26]: The wireless device recited in claim 25, wherein the wireless device is a first wireless device, and wherein the second phone number is, prior to the user request to replace the particular credential with the target credential, associated with a second wireless device.

217. FCCReg describes a federal regulation that requires service providers to permit a *first wireless device* to update its phone number from a *first phone*

number to a *second phone number*, and FCCReg expressly discloses that service providers must support this number update when the *second phone number* is previously associated with a *second wireless device* different from the *first wireless device*. EX1012, 1-11. For example, FCCReg acknowledges that the FCC has passed regulations requiring service providers to support local number portability (LNP) in a way that allows “porting...between wireless providers.” EX1012, 1. A wireless provider supports *wireless devices* such as the “cellular radiotelephone” of Salmela, meaning that “porting...between wireless providers” can involve porting a *second phone number* from a *second wireless device* to a *first wireless device*, the *second phone number* replacing the *first phone number* at the *first wireless device*. EX1012, 1; EX1004, [0021].

218. One example port of between wireless devices would occur when a mother acquires a new wireless phone and gifts her old wireless phone to a son—who already has another wireless phone associated with another wireless service provider. According to the rules of FCCReg, wireless service providers would be required to support the son in porting his phone number from the son’s original phone to the gifted phone, thus replacing the mother’s number with the son’s number on the gifted phone. EX1012, 1. Likewise, FCCReg’s rules would require service providers to support the mother in porting her number from the gifted phone to the mother’s new wireless phone. EX1012, 1.

219. Thus, FCCReg indicates that porting a phone number from a wireless device associated with a first wireless service provider to another wireless device associated with a second service provider was well-known by 2010. Consequently, implementing device 10 of the Salmela-Rishy-Maharaj-Bennett combination with FCCReg’s suggestion to enable porting between wireless service providers would result in device 10 updating from a *first phone number* to a *second phone number* that was previously associated with a *second wireless device* associated with another service provider. EX1012, 1, 11.

Claim [27]: The wireless device recited in claim 25, wherein the second phone number is, prior to the user request to replace the particular credential with the target credential, associated with a land line.

220. The rules promulgated by FCCReg require service providers to support a *first wireless device* in updating its phone number from a *first phone number* to a *second phone number*, the *second phone number* being previously associated with a *land line*. EX1012, 1, 11. For example, FCCReg discloses that “[a]ll telecommunications carriers...must complete a...simple intermodal port request within one business day.” EX1012, 11. FCCReg expressly conveys that these “intermodal ports” include “wireline-to-wireless ports” in which a phone number is ported from a *land line* to a *wireless device*. One example where this kind of port occurs is when a father receives his daughter’s old wireless phone as a gift and decides to port his number from a landline to the gifted phone, thus replacing the

daughter's number with the landline number on the gifted phone. Consequently, it is clear that implementing the device 10 of the Salmela-Rishy-Maharaj-Bennett combination with the requirements of FCCReg would result in the device 10 updating from a *first phone number* to a *second phone number*, the *second phone number* being previously associated with a *land line*. EX1012, 11.

D. The Salmela-Rishy-Maharaj-Ionescu Combination Renders Claims 12-13 Obvious

Claim [12]: The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that an attempt by the wireless device to place a voice call has failed.

221. Ionescu expressly discloses techniques that a wireless device can use to determine that an attempt by the wireless device to place a *voice call* has *failed*, thus leading to a failure to establish a voice-based emergency communication session. EX1007, [0029], [0035] (“[A] user of a mobile device initiates an emergency communication session. The emergency communication session may be a voice call (e.g., a 911 call) ...”), [0036]-[0037] (“two consecutive failures to access the network ...”), Claim 7, FIG. 4; *supra*, §VII.H. For the reasons that I described above in my analysis of the Salmela-Rishy-Maharaj-Ionescu Combination (*supra*, §VII.I), it would have been obvious for a POSITA to implement Salmela's technique for detecting a failure to gain network access with the device 10 by determining that an attempt by the device 10 to place a voice call has failed as taught by Ionescu. *Supra*, §VII.I. This combination would predictably result in device 10 being able to

determine that device 10 has failed in an attempt to place a voice call and perform one or more actions based on this determination.

Claim [13]: The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that an attempt by the wireless device to send a text message has failed.

Ionescu expressly discloses techniques that a wireless device can use to determine that an attempt by the wireless device to send a ***text message*** has ***failed***, thus leading to a failure to establish a text-based emergency communication session. EX1007, [0029], [0035] (“[A] user of a mobile device initiates an emergency communication session. The emergency communication session may be ... a text message ...”), [0036]-[0037] (“two consecutive failures to access the network ...”), Claim 7, FIG. 4; *supra*, §VII.H. For the reasons that I described above in my analysis of the Salmela-Rishy-Maharaj-Ionescu Combination (*supra*, §VII.I), it would have been obvious for a POSITA to implement Salmela’s technique for detecting a failure to gain network access with the device 10 by determining that an attempt by the device 10 to send a text message has failed as taught by Ionescu. *Supra*, §VII.I. This combination would predictably result in device 10 being able to determine that device 10 has failed in an attempt to send a text message and perform one or more actions based on this determination.

E. The Salmela-Rishy-Maharaj-Sigmund Combination Renders Claims 4-5 and 8-10 Obvious

Claims [4], [5], [8], [9], [10]

Claim [4]: The wireless device recited in claim 2, wherein the action is to cause a notification to be presented through the user interface, wherein the notification reports an error.

Claim [5]: The wireless device recited in claim 2, wherein the action is to cause a notification to be presented through the user interface, wherein the notification reports that a procedure is in progress or has not been completed.

Claim [8]: The wireless device recited in claim 7, wherein the action is to cause a notification to be presented through the user interface, wherein the notification reports that the particular credential has been replaced by the target credential.

Claim [9]: The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to cause a notification to be presented through the user interface, the notification providing information about a status of the user request to replace the particular credential of the one or more credentials with the target credential.

Claim [10]: The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to cause a notification to be presented through the user interface, the notification requesting confirmation of the user request to replace the particular credential with the target credential.

222. Like device 10 of the Salmela-Rishy-Maharaj combination, Sigmund discloses a mobile device that can connect to a wireless access network for the purpose of receiving one or more services. EX1008, [0024]-[0031]; *supra* §VII.J. I noticed that Sigmund describes a “process...for handling a password reset request” from a user. EX1008, [0032]. This process involves notifying the user of various information such as, for example, whether the reset request is successful or unsuccessful. EX1008, [0032]-[0040], FIGS. 2-3; *supra* §VII.J. As I described above in my analysis of the Salmela-Rishy-Maharaj-Sigmund combination, it is

clear that a POSITA would have found it obvious cause a notification to be presented through a user interface (e.g., a display) of Salmela's device 10 in response to various events in Salmela's process for updating credentials, as taught by Sigmund. *Supra*, §VII.K.

223. Based on my review of Sigmund, it is also clear that a POSITA would have known that notifications were commonly employed by the Critical Date of the '510 Patent to perform a wide range of tasks—including to inform mobile device users about the status or results of processes performed on the mobile device. EX1008, [0036] (“A visual prompt can be presented to the subscriber as a cue or reminder ...”), see also [0024] (describing a wireless device as being configured for “visual voicemail”). It is apparent that a POSITA would have found it obvious to implement Salmela's device 10 with Sigmund's teachings to display notifications to the user at any point during the credential updating process. This includes displaying notifications in response to determining that the updated subscription credential does or does not match the target credential—any time that the device 10 performs the comparison between the *particular credential* (e.g., current subscription credentials 26) and the *target credential* (e.g., credentials that are “considered to be current” by the credentialing server). EX1004, [0041], [0044]; *supra*, Ground 1A at Claims [2] and [7]. My opinion here is corroborated by numerous pre-2013 references describing mobile devices that display notifications by 2013. EX1020, 29

(describing notifications displayed on a mobile device for new email, new text messages, calendar events, weather reports, and many other events); EX1021, 26 (describing “notification panel” of a mobile device that “shows information about processes that are running, notifications, and alerts); EX1022, FIGS. 2A-2D (depicting a mobile device that can display notifications for a variety of events including text messages, voice calls, and downloads); EX1023, FIGS. 4-8 (depicting various notifications that can be displayed on mobile device including warnings that available minutes are almost exhausted and information concerning incoming deposits to a bank account). In the combination, for example, Rishy-Maharaj confirms that the user interface of the wireless device is configurable to present notifications to the user during a credential updating process. EX1005, [0168] (“The display 702 is a component configured to show images and notifications in order to allow a user to understand the state of the wireless device ...”), [0130] (“wireless device 102 [is] notified that the subscription has been created ... and wireless device 102 prepare[s] to receive the credentials”).

224. From a POSITA’s general knowledge of well-known notification technology developed before the Critical Date of the ’510 Patent, as evidenced by Sigmund and other prior art references, a POSITA would have presented notifications based on the results of this matching operation. For example, such notifications would inform the user whether the device 10 has detected that new

subscription credentials are available, that the device 10 is in the process of obtaining new subscription credentials if available, and whether an error has been detected. It is clear that a POSITA would have expected users to find this information displayed in these notifications helpful because the information it would help the user better understand if his or her earlier request to update the subscription plan for the device 10 had been effected. The information would also help the user to determine whether device 10's failure to gain network access was related to the user's request or if it stemmed from a different problem unrelated to the user's request to update the subscription plan or home operator.

225. Claims [4], [5], [8], [9], and [10] each refer to notifications presented through the user interface of the device. These notifications report different a variety of different content presented to the user. All of this content appears to me to be informative in nature, and not functional to the operation of the wireless device. I have been informed that the limitations of claims [4], [5], [8], [9], and [10] are not entitled to patentable weight because these limitations amount to no more than non-functional printed matter. Because the limitations of claims [4], [5], [8], [9], and [10] have no functional or structural relationship to the wireless device, I understand that the limitations cannot distinguish the invention of the '510 Patent.

226. Even if the contents of the notifications described in claims [4], [5], [8], [9], and [10] were entitled to patentable weight—which I have been informed that

they do not—I believe that these claim limitations would have been obvious to a POSITA for the reasons I described above. For example, as recited in Claim [4], it would have been obvious for Salmela’s device 10 to report an error when the updated and target subscription credentials do not match, because this reporting would inform the user that the credential has been corrupted and/or a new credential is needed. This is especially true given that error reports were common before the alleged invention of the ’510 Patent. *Supra*, Ground 2A at Claim [2]. It would have been obvious to report that a credential update is in progress as recited in claim [5] when the updated and target credential do not match to inform the user that the device 10 is taking action to update the subscription and resolve the issue that led the device to fail to gain network access. EX1008, [0034]. Furthermore, as recited in claim [8], it would have been obvious to report that the particular credential has been replaced by the target credential when the updated and target credential do match to assure the user that no new subscription credentials are necessary at the current time since the subscription credentials were already updated successfully. *Supra*, Ground 2A at Claim [7].

227. As recited in claim [9], reporting a status of a user request to replace the particular subscription credential with the target credential would have been obvious to a POSITA so as to remind the user of a status of device 10’s attempts to obtain new subscription credentials. Finally, it would have been obvious to

implement device 10 to request confirmation that a user intended to request to replace a particular credential with a target credential, thus ensuring that the request was not in error and providing the user with an opportunity to cancel the request if it was initially mistakenly submitted. My opinion here is corroborated by references confirming that it was common by 2013 for mobile devices to provide notifications that prompt a user to decide whether to proceed with one or more courses of action. EX1023, FIG. 4 (depicting a mobile device notification that prompts a user to upgrade a mobile plan based on a call minute threshold approaching); EX1024, FIG. 4 (depicting a mobile device notification that prompts a user to view an “important email”).

F. The Salmela-Rishy-Maharaj-Johansson Combination Renders Claim 40 Obvious

Claim [40]: The wireless device recited in claim 38, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to obtain the temporary credential from a network system communicatively coupled to the wireless device.

228. Johansson describes techniques for using a mobile station (e.g., a wireless mobile phone) to obtain a ***temporary credential*** from a ***network system*** that is communicatively coupled to the mobile station. EX1009, [0045]-[0052], FIG. 2; *supra*, §VII.L. Specifically, I noticed that Johansson discloses that a connectivity providing unit 202 acquires a temporary connectivity identity (e.g., TMSI) and “pushes” this temporary connectivity identity to user equipment 200. EX1009,

[0047]-[0048]. Johansson explains that “each temporary connectivity identity is valid for a predetermined amount of connectivity which, as mentioned above, may be limited with respect to call/session time, lifetime and/or data/bandwidth amount,” meaning that Johansson’s temporary credentials are for situations like the ones I discussed above in §VII.M, *supra*, that involve a service provider strictly controlling access to the network (e.g., limited amount of bandwidth, limited amount of access time). EX1009, [0048]. Johansson’s connectivity providing unit 202 stores a temporary connectivity identity until the temporary connectivity identity is “pushed” to the mobile terminal 200 to provide temporary access. EX1009, [0049]. The connectivity providing unit 202 of Johansson represents a *network system* that is separate from Johansson’s user equipment representing a *wireless device*:

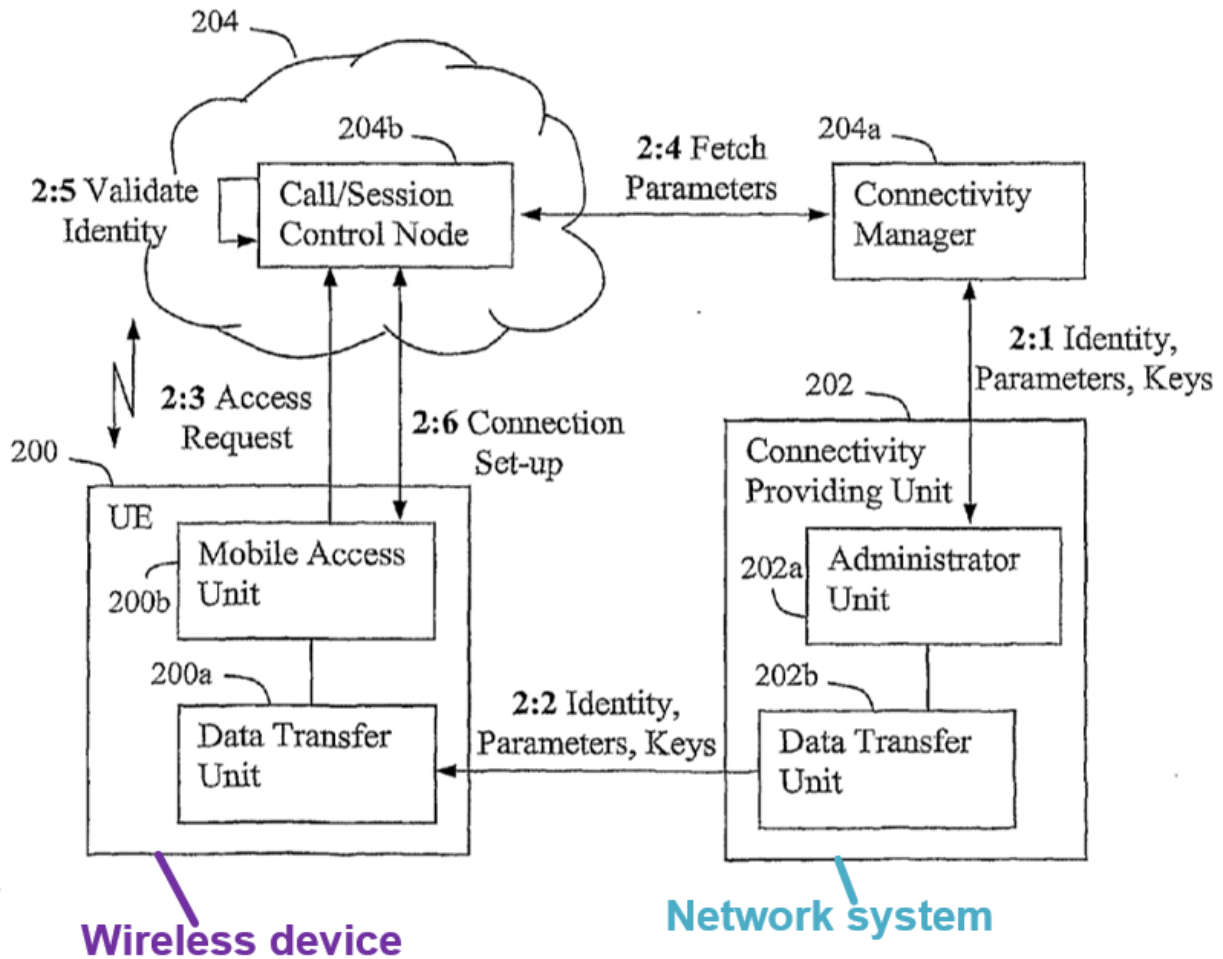


Fig. 2

EX1009, FIG. 2 (annotated).

229. Consequently, Johansson discloses that the user equipment obtains the temporary credential from the connectivity providing unit communicatively coupled to the user equipment. As I discussed above in my analysis of the Salmela-Rishy-Maharaj-Johansson combination (*Supra*, VII.M), it would have been obvious and a POSITA would have been motivated to implement device 10 according to Johansson's teachings such that it would obtain temporary access credentials 30 from a network system communicatively coupled to device 10.

G. The Salmela-Rishy-Maharaj-Slavov Combination Renders Claim 34 Obvious

Claim [34]: The wireless device recited in claim 1, wherein obtaining the indication of the user request to replace the particular credential of the one or more credentials with the target credential comprises obtaining information from a website.

230. The wireless device 100 of Slavov can use a temporary device identifier, such as a preliminary international mobile subscriber identity (PIMSI), to automatically obtain permanent subscription credentials for accessing a home network 20. EX1011, [0022]-[0028], [0049], FIGS. 1-2, 10. A user can subscribe wireless device 100 to home network 20 through a website before the wireless device 100 contacts home network 20 using the temporary device identifier. EX1011, [0049] (“The subscription and provisioning server 60 may provide a website accessible to device owners for subscribing to the services of the home network 20.”), *see also* [0024] (“The subscription and provisioning server 60 may provide a web interface that allows wireless device owners to subscribe to the services of the home network 20 after purchase of the wireless devices 100.”). The wireless device receives information about available subscriptions that the user can select, as described in Rishy-Maharaj, which can be obtained from a website, as described in Slavov. EX1011, [0024], [0049]; EX1005, [0110]-[0111]. Slavov’s website is similar to an internet server disclosed in Rishy-Maharaj, which is configured to communicate with wireless devices over an internet gateway. EX1005, [0216]-[220], FIG. 12. As

I described in my overview of the Salmela-Rishy-Maharaj-Slavov Combination (*Supra*, §VII.O), it would have been obvious to apply Slavov’s suggestion to receive user input through a user interface by obtaining information through a website. *Supra*, §VII.O. In the resulting Salmela-Rishy-Maharaj-Slavov combination, the device 10 would obtain the user request to replace the particular credential represented current subscription credential 26 with the target credential by obtaining information from a website based on the teachings of Slavov. *Supra*, Ground 1A at Element [1f].

H. The Salmela-Rishy-Maharaj-Gupta Combination Renders Claim 44 Obvious

Claim [44]: The wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises communicating with the network element through a voice call.

231. I noticed that Gupta discloses that a ***wireless device*** (e.g., wireless communication device 120) is able to communicate with a wireless communication station 130 via radiofrequency (RF) signals by making a ***voice call***. EX1013, [0017], [0021], [0034]-[0037], [0044]-[0051], FIG. 2, FIG. 3. This ***voice call*** can be received by a ***network element*** (e.g., network infrastructure 140) through the wireless communication station 130. EX1013, [0035] (“Method 200 begins when a wireless communication device 120 that needs to be staged transmits a call over the air that is received by a base station or access point and routed to network infrastructure

140”), FIG. 2. The network infrastructure 140 can authenticate the wireless communication device 120 and send “encrypted staging data” to wireless communication device 120 based on receiving the *voice call*. EX1013, [0036], [0037], FIG. 2. Thus, it is clear that the *voice call* placed by wireless communication device 120 *initiates a programming session* with a network infrastructure 140, and this programming session ultimately results in wireless communication device 120 being provisioned with “encrypted staging data.” EX1013, [0034]- [0037], FIG. 2. When the device 10 of the Salmela-Rishy-Maharaj combination is implemented with Gupta’s teachings for staging a wireless device that places a voice call, device 10 would place a voice call to initiate a programming session with a network element like Salmela’s credentials in a way that causes device 10 to be provisioned with new subscription credentials. EX1013, [0017], [0021], [0034]-[0037], FIG. 2, *supra*, §VII.Q.

IX. CONCLUSION

232. For all the reasons I have noted in the foregoing paragraphs, claims 1-48 of the '510 Patent are obvious in view of the references discussed above.

233. 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 | <i>August 2018–Present</i> |
| Associate Professor | University of Florida | <i>August 2014–July 2018</i> |
| Associate Professor | Georgia Institute of Technology | <i>March 2014–August 2014</i> |
| Assistant Professor | Georgia Institute of Technology | <i>2008–March 2014</i> |
| Research Assistant | Pennsylvania State University | <i>2004–2008</i> |
| Teaching Assistant | Pennsylvania State University | <i>2004</i> |

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. Attention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2018. Acceptance Rate: 19.0%.
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 Sherman, 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 Sherman, 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 Dingedine, Michael Freedman and Edward W. Felten
 Amount: \$1,500,000 for 4 years
 Awarded: June 2011
8. **Monitoring Free and Open Access to Information on the Internet**
 Sponsor: Google Focus Program
 Investigator(s): Nick Feamster (PI), Wenke Lee, Mustaque Ahamad, Patrick Traynor, Henry Owen, Ellen Zegura, Zvi Galil
 Amount: \$1,000,000 for 2 years
 Awarded: November 2011
9. **Dynamic-attribute-based Disclosure of Health Information in Emergency Care Scenarios**
 Sponsor: Health Systems Institute (HSI) Seed Grant Program
 Investigator(s): Doug Blough (PI), Mustaque Ahamad, Patrick Traynor and Jim Jose
 Amount: \$50,000 over 1 year
 Awarded: August 2009
10. **Federal Cyber Service Scholarships at Georgia Tech**
 Sponsor: NSF SFS Scholarships
 Investigator(s): Seymour Goodman (PI), Patrick Traynor
 Amount: \$1,250,682 over 5 years
 Awarded: June 2009
11. **Security for IMS-Enabled Converged Applications**
 Sponsor: US Department of Defense
 Investigator(s): Mustaque Ahamad (PI), Patrick Traynor (PI), Michael Hunter, Russ Clark
 Amount: \$146,121 for 1 year
 Awarded: August 2008

2. Pending

Removed for external version.

I. Research Honors and Awards

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

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

III. SERVICE

A. Professional Activities

A.1. Memberships and Activities in Professional Societies

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

A.2. Conference Committee Activities

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

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

B. On-Campus Committees

B.1. University of Florida

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

B.2. Georgia Tech

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

C. Special Assignments

None.

D. Ph.D. Examining Committees

Ph.D. Examining Committees

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

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

External Member of Ph.D. Research Committee

None.

External Member of Ph.D. Examining Committee

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

Ph.D. Thesis Proposal Committees

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

Ph.D. Qualifying Exam Committees—Georgia Tech

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

3. Xinyu Xing, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Wenke Lee.
4. Brad Reaves, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Patrick Traynor.
5. Chaz Lever, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Patrick Traynor.
6. Terry Nelms, College of Computing, Georgia Tech, Spring 2012.
Advisor: Professors Mustaque Ahamad and Roberto Perdesci.
7. Saurabh Chakradeo, College of Computing, Georgia Tech, Spring 2012.
Advisor: Professor Patrick Traynor.
8. Henry Carter, College of Computing, Georgia Tech, Spring 2012.
Advisor: Professor Patrick Traynor.
9. David Dewey, College of Computing, Georgia Tech, Spring 2012.
Advisor: Professor Jon Giffin.
10. Chaitrali Amrutkar, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Patrick Traynor.
11. Yacin Nadji, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Wenke Lee.
12. Yogesh Mundada, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Nick Feamster.
13. Hyojoon Kim, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Nick Feamster.
14. Ikpeme Erete, College of Computing, Georgia Tech, Spring 2011.
Advisor: Professor Alex Orso.
15. Chaitrali Amrutkar, College of Computing, Georgia Tech, Spring 2011.
Advisor: Professor Patrick Traynor.
16. Brendan Dolan-Gavitt, College of Computing, Georgia Tech, Spring 2011.
Advisor: Professor Wenke Lee and Professor Jon Giffin.
17. Sam Burnett, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Nick Feamster.
18. Cong Shi, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Mostafa Ammar and Professor Ellen Zegura.
19. Partha 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, Byungsook 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 Burress. WABE NPR - Mobile Web Browsers Full of Security Risks, Tech Professor Finds. <http://wabe.org/post/mobile-web-browsers-full-security-risks-tech-professor-finds>, December 2012.

27. Mark Huffman. Consumer Affairs - Georgia Tech: mobile browsers fail safety test. <http://www.consumeraffairs.com/news/georgia-tech-mobile-browsers-fail-safety-test-120612.html>, December 2012.
28. Matthew J. Schwartz. Information Week - Blame Screen Size: Mobile Browsers Flunk Security Tests. <http://www.informationweek.com/security/mobile/blame-screen-size-mobile-browsers-flunk/240143999>, December 2012.
29. Jon Gold. Network World - Ga. Tech researchers: Mobile Browsers need better HTTPS indicators. <http://www.networkworld.com/news/2012/120512-mobile-browsers-264846.html>, December 2012.
30. United Press International. Study: Most mobile Web browsers unsafe. http://www.upi.com/Science_News/Technology/2012/12/05/Study-Most-mobile-Web-browsers-unsafe/UPI-73431354743353/#ixzz2EGtQsuLd, December 2012.
31. Suzanne Choney. Mobile browser woes can fool even experts: report. <http://www.nbcnews.com/technology/mobile-browser-woes-can-fool-even-experts-report-1C7451203>, December 2012.
32. Meghan Kelly. VentureBeat - 3 hot security startups to watch. <http://venturebeat.com/2012/02/27/3-security-startups-to-watch-at-the-2012-rsa-conference/>, February 2012.
33. Jacob Goodwin. Government Security News - RSA 2012 – Pindrop Security can distinguish a fraudulent phone call from a real one. <http://www.gsnmagazine.com/node/25721?c=communications>, February 2012.
34. Matt Liebowitz. Phone hack logs keystrokes from nearby computers. MSNBC.com - http://www.msnbc.msn.com/id/44993238/ns/technology_and_science-security/#.TqU5MNSjPh4, October 2011.
35. Jacob Aron. iPhone keylogger can snoop on desktop typing. New Scientist - <http://www.newscientist.com/article/dn21059-iphone-keylogger-can-snoop-on-desktop-typing.html>, October 2011.
36. iPhone Keylogger Can Snoop on Desktop Typing. Slashdot - <http://mobile.slashdot.org/story/11/10/18/2346222/iphone-keylogger-can-snoop-on-desktop-typing>, October 2011.
37. Robert Lemos. Smart Phones Could Hear Your Password. Technology Review - <http://www.technologyreview.com/computing/38913/?p1=A2>, October 2011.
38. Kevin McCaney. Bad vibrations: How smart phones could steal PC passwords. Government Computer News - <http://gcn.com/articles/2011/10/18/smart-phone-sensors-steal-keystrokes.aspx>, October 2011.
39. PhysOrg. Turning iPhone into spiPhone: Smartphones' accelerometer can track strokes on nearby keyboards. PhysOrg.com - <http://www.physorg.com/news/2011-10-iphone-siphone-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.