IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	David L. Brown	Attorney Docket No.:42342-0134IP1
U.S. Patent No.:	8,646,042	
Issue Date:	February 4, 2014	
Appl. Serial No.:	13/445,825	
Filing Date:	April 12, 2012	
Title:	HYBRID DEVICE HAVING A PERSONAL DIGITAL KEY AND RECEIVER-DECODER CIRCUIT AND METHODS OF USE	

DECLARATION OF DR. PATRICK TRAYNOR

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

QUALIFICATIONS AND BACKGROUND INFORMATION

1. My name is Patrick Gerard Traynor and I have been retained as an expert witness by Microsoft in the matter of Proxense, LLC vs. Microsoft Corporation. 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

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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).

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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 App. 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

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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 8,646,042 (MS-1001), and its accompanying prosecution history (MS-1002)
- U.S. Patent Publication No. 2007/0245157 A1 ("Giobbi-157") (MS-1005)
- U.S. Patent Publication No. 2004/0255139 A1 ("Giobbi-139") (MS-1006)
- U.S. Patent No. 9,042,819 ("Dua") (MS-1007)
- European Patent No. EP 1 536 306 A1 ("Broadcom") (MS-1008)
- Claim Construction Order, *Proxense, LLC v Samsung Electronics Co., Ltd*, 6:21-CV-00210-ADA, W.D. Tex., filed January 18, 2022 (MS-1009)
- Provisional Application No. 60/798,843 (MS-1010)

I. LEGAL PRINCIPLES

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.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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.

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 above and because I know of no indication from the patent owner or

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

others to the contrary, I have applied a date of December 6, 2007, 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 December 6, 2007.

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

II. 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, 5-6, 8-11, and 13-

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

14 of the ’042 patent are obvious over Giobbi-157 in view of Giobbi-139.

- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 1, 5-6, 8-11, and 13-14 of the ’042 patent are obvious over Giobbi-157 in view of Giobbi-139 and Dua.
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 10-11 and 13-14 the ’042 patent are obvious over Broadcom.

III. BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE ’042 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 ’042 Patent as of December 6, 2007 would have had (1) at least a bachelor’s degree in computer science, electrical engineering, or a related field, and (2) at least two years of experience in the field of encryption and security. 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.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

Moreover, I have taught, participated in organizations, and worked closely with many such persons over the course of my career.

IV. INTERPRETATIONS OF THE '042 PATENT CLAIMS AT ISSUE

23. I have been informed by Counsel and understand that the best indicator of claim meaning is its usage in the context of the patent specification as understood by one of ordinary skill. I further understand that the words of the claims should be given their plain meaning unless that meaning is inconsistent with the patent specification or the patent's history of examination before the Patent Office. Counsel has also informed me, and I understand that, the words of the claims should be interpreted as they would have been interpreted by one of ordinary skill at the time of the invention was made (not today). I have been informed by Counsel that I should use December 6, 2007 as the point in time for claim interpretation purposes.

24. I have been asked to provide my interpretation of the following terms of the '042 patent set forth below. In providing the following interpretations, I have carefully considered and applied the claim construction standard referred to in ¶23 above. Below, I offer my analysis of how a POSITA would have construed certain claim features of the '042 patent. My analysis also considers the constructions adopted in previous proceedings where family members of the '042 patent were asserted. MS-1009.

A. Hybrid Device

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

25. For the purposes of the present proceeding this term ("hybrid device") appears in claims 1, 5-6, and 8-11. The use of the term "hybrid device" is consistent with the use of the term in the specification of the '042 patent. *See, e.g.,* MS-1001, Abstract, 1:65-2:19. Previously in a related proceeding with a family member of the '042 patent, the court construed "hybrid device" to be "a device comprising an integrated personal digital key (PDK) and an integrated receiver-decoder circuit." MS-1009. Accordingly, because the '042 patent recites the use of a "PDK" and "RDC" in the "hybrid device" claims and given the consistency with the '042 patent specification, I believe the previous construction is consistent. MS-1001, Claim 1, 10. For purposes of this proceeding, I adopt this construction of "hybrid device," which, as noted above, was adopted in previous proceedings. MS-1009.

B. Personal Digital Key ("PDK")

26. For the purposes of the present proceeding, I believe this term, which appears in claims 1, 5-6, 8, 10, and 13-14, should be construed to mean "an operably connected collection of elements including an antenna and a transceiver for communicating with a RDC and a controller and memory for storing information particular to a user." This definition is consistent with the use of the term in the specification of the '042 patent. *See, e.g.*, MS-1001, 13:41-54. Accordingly, I adopt the construction of "personal digital key," which, as noted above, was adopted in previous proceedings. MS-1009.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

C. Receiver-decoder circuit ("RDC")

27. For the purposes of the present proceeding, I believe this term, which appears in claims 1, 5-6, 8, 10, and 13-14 should be construed to mean "a component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing." This definition is consistent with the use of the term in the specification of the '042 patent. *See, e.g.*, MS-1001, 7:10-22. Accordingly, I adopt the construction of "receiver-decoder circuit," which, as noted above, was adopted in previous proceedings. MS-1009.

V. THE '042 PATENT

A. Overview

28. The '042 Patent is directed to "a hybrid device" that includes a personal digital key (PDK) and a receiver-decoder circuit (RDC) coupled in communication with each other. MS-1001, Abstract, 1:20-26. The integrated PDK communicates wirelessly with an external RDC and the integrated RDC communicates wirelessly with at least one external PDK within its proximity zone. MS-1001, 3:62-4:20. The specification discloses that the integrated PDK is capable of storing local, secured financial information or secured biometric information for authenticating a user. MS-1001, 3:20-32, 16: 20-38. Similarly, the external PDK is also capable of storing information. MS-1001, 3:62-4:20. For example, in one embodiment, the integrated PDK carries credentials such as credit card or account information that are used to

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

enable services associated with the external RDC. MS-1001, 4:63-5:24; 8:30-49. A user can make a purchase with the hybrid device provided that they are in possession of the external PDK and in proximity to the hybrid device. If so, the external PDK wirelessly connects to the integrated RDC and authorizes the integrated PDK to enable a transaction by sharing credit card or account information with the external RDC. *Id*.

29. The '042 Patent claims priority to a number of provisional applications, the earliest of which was filed 12/6/2007. MS-1001, Cover.

B. Prosecution History

30. The '042 Patent was allowed after a single office action that presented only a double-patenting rejection. MS-1002, 380-386. During prosecution, the Examiner did not consider any of Giobbi-157, Giobbi-139, Dua, or Broadcom. *Id*.

VI. ANALYSIS OF GIOBBI-157, GIOBBI-157, AND DUA

31. Below, I analyze a first ground based on Giobbi-157 and Giobbi-139 ("the Giobbi references") and a second ground that additionally incorporates the disclosure of Dua. In the first ground [1A], I rely on the disclosure of the Giobbi references and explains why their disclosure, when interpreted in view of the general knowledge of a POSITA, renders obvious claims 1, 5-6, 8-11, and 13-14. In the second ground [1B], I rely on the same disclosure of the Giobbi references and explanation of obviousness as presented in the first ground [1A], but also turn to

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

Dua's disclosure to provide additional implementation examples. Because the use of the Giobbi references' disclosure and corresponding obviousness arguments are similar for both grounds [1A/1B], I discuss these grounds together for ease of presentation.

A. Overview of Giobbi-157

32. Giobbi-157 is directed at a system and method to "provide efficient, secure and highly reliable authentication for transaction processing and/or access control applications." MS-1005, Abstract, ¶¶[0011]-[0014]. The disclosure further explains that a "transaction includes enabling access to secure physical or digital assets (e.g., unlocking a door, opening a vault, providing access to a secured hard drive, etc.)." MS-1005, ¶[0063]. This process is accomplished using "secure and tamperproof memories" to store information for "identification and authentication." MS-1005, ¶[0036], *see also* ¶¶[0026]-[0029], [0035]-[0048]. Giobbi-157 is a continuation in part of a prior application and claims priority to five provisional applications. MS-1005, Cover, ¶[0002].

33. Giobbi-157 discloses a Personal Digital Key (PDK) that "stores one or more profiles (e.g., a biometric profile) in a tamperproof memory that is acquired in a secure and trusted process." MS-1005, ¶[0063], *see also* ¶¶[0026]-[0029], [0035]-[0048]. Giobbi-157 further teaches that the PDK may be integrated into an

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

electronic device, such as **a cellphone**. MS-1005, ¶[0035] ("a portable electronic device such as a cell phone"), *see also* ¶[0080], claims 27, 33.

34. Giobbi-157 teaches that its integrated PDK can communicate with a receiver-decoder circuit (RDC). MS-1005, ¶¶[0049]-[0058], [0064]. The RDC establishes a secure communication channel between the PDK and RDC, then sends "profile authentication requests to the PDK 102 requesting transmission of one or more stored profiles over the secure channel." MS-1005, ¶[0064]. In some examples, Giobbi-157 teaches that information stored on a PDK, such as fingerprint information, is transmitted to an external RDC located on a "Reader 108." MS-1005, ¶[0049]. An example of Giobbi-157's PDK and Reader configuration is shown in the annotated version of Figures 2 and 3 below.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

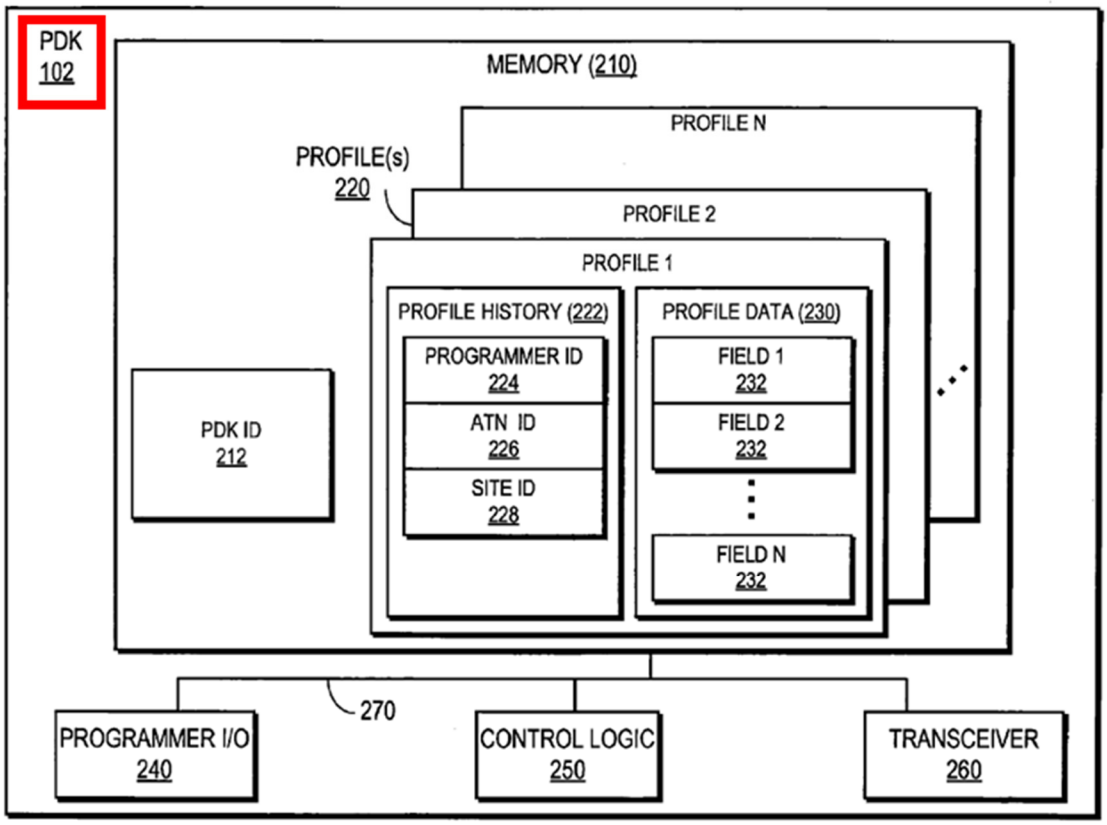


FIG. 2

MS-1005, FIG. 2[1].

[1] My annotations to the figures in my declaration are shown in color.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

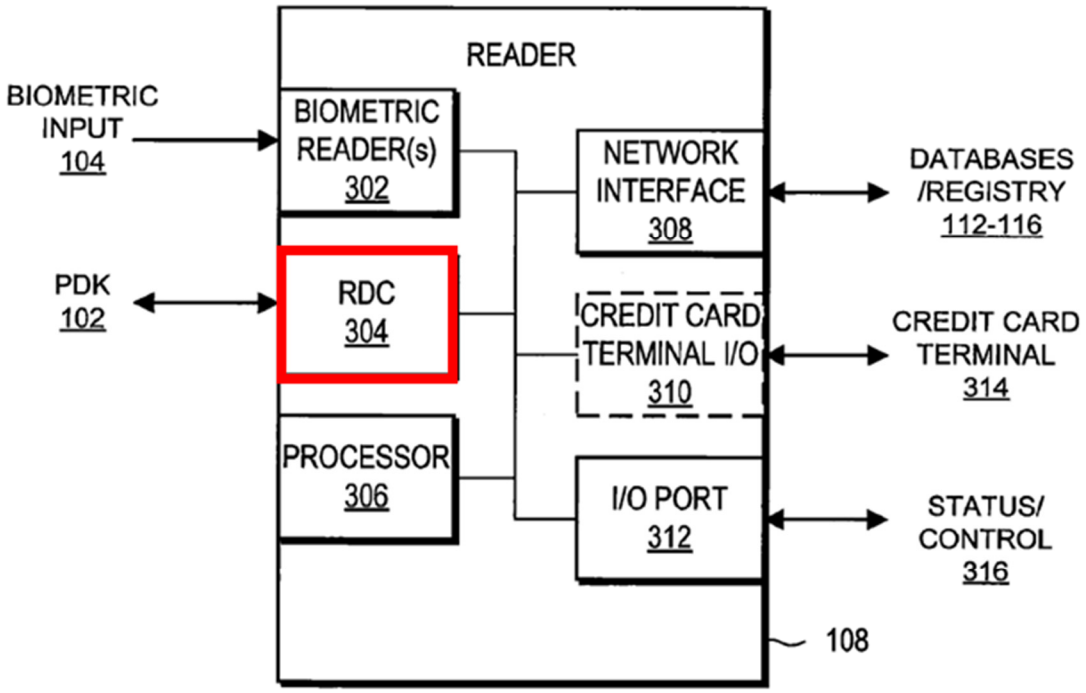


FIG. 3

MS-1005, FIG. 3.

35. Giobbi-157 teaches that its RDC can authenticate a PDK and then enable a "transaction," the "transaction includ[ing] enabling access to secure physical or digital assets (e.g., unlocking a door, opening a vault, providing access to a secured hard drive, etc.)." MS-1005, ¶¶[0057]-[0058], [0063], FIG. 4.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

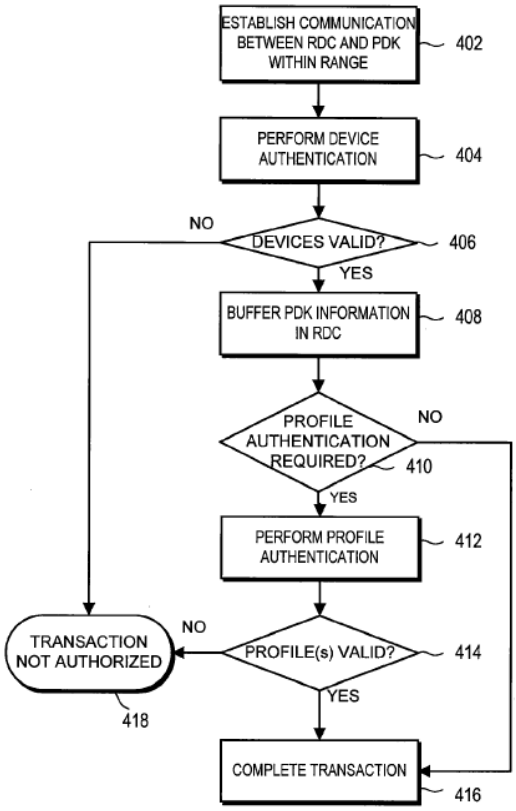


FIG. 4

MS-1005, FIG. 4.

36. Giobbi-157 also discloses that "the PDK can store other information such as credit/debit card information, bank information, or personal information in a memory for use in authorizing or completing a transaction." MS-1005, ¶¶[0011], [0063], [0065].

37. The Giobbi-157 provisional applications disclose several use cases of the PDK and RDC systems and detail both the process and components necessary to setup and operate a PDK and RDC system. MS-1010, pp. 2-14. The details include exemplary form factors for the PDKs and RDCs and explanations as to how a user

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

could incorporate these devices into a user's current devices to setup and operate a PDK and RDC system. *Id*.

B. Overview of Giobbi-139

38. Giobbi-139 shares the same goal of securing physical or digital access as Giobbi-157, disclosing a "Personal Digital Key Digital Content Security System" which prevents "unauthorized use and protect[s] the digital content stored on computers from being wrongfully accessed, copied, and/or distributed." MS-1006, Abstract, ¶[0010]. Like the Giobbi-157 publication, Giobbi-139 discusses the use of RDCs to communicate with PDKs to enable access and functions on devices. MS-1006, ¶¶[0010], [0071]-[0078]. The disclosure of Giobbi-139 further teaches that an RDC can be incorporated into **a cell phone** and that the RDC "is an integrated circuit able to process PDK-Key information, as well as encrypt/decrypt PDK-compliant digital content." MS-1006, ¶[0077], [0088] ("This embodiment involves integrating RDCs into…PDAs, cell phones [etc.]"); MS-1005, ¶[0035].

39. Giobbi-139 teaches the PDK and RDC relationship as being flexible and capable of being integrated with existing equipment. MS-1006, ¶¶[0087]-[0099]. Giobbi-139 also teaches that an RDC can be acquired independently and integrated into a device. MS-1006, ¶¶[0088]-[0090]. The integrated RDC could then be used to secure the device and can even "enable/disable" the device based on communication with a PDK. MS-1006, ¶¶[0087]-[0090]. When using a PDK to

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

secure a device with an integrated RDC, "[t]his security mechanism protects any data stored on such devices in the event they are ever stolen, left unattended, or even purposely 'disabled' to prevent access to sensitive content (i.e. preventing minors from accessing adult files, websites, etc.). MS-1006, ¶[0090]. When the associated PDK-Key(s) is not present, these devices and their storage means are locked and disabled." *Id*.

40. Giobbi-139 also discloses the scalability of RDC and PDK architecture. MS-1006, ¶¶[0091]-[0096]. For example, Giobbi-139 teaches that a user can "assign (or remove)" additional PDKs to a device with an integrated RDC. MS-1006, ¶¶[0092] ("Giving users the option to purchase and associate a PDK-Key at a later time, or importantly, assign a PDK-Key they already utilize for another PDK-based device. This allows a user to utilize a single PDK-Key to provide access to all their PDK based devices"), [0095].

41. Giobbi-139 further discloses a version of communication between a PDK and RDC that is not wireless. ¶¶[0041], [0071]-[0073]. Particularly, Giobbi-139 teaches alternative embodiments where an RDC and PDK are communicatively coupled to each other by a wired signal line:

> "In other alternative embodiments, the communication between the user's physical electronic key [i.e., PDK] and the playing device is not wireless. Rather, in one alternative embodiment, the user's physical electronic key [i.e., PDK] communicates the activation code to the

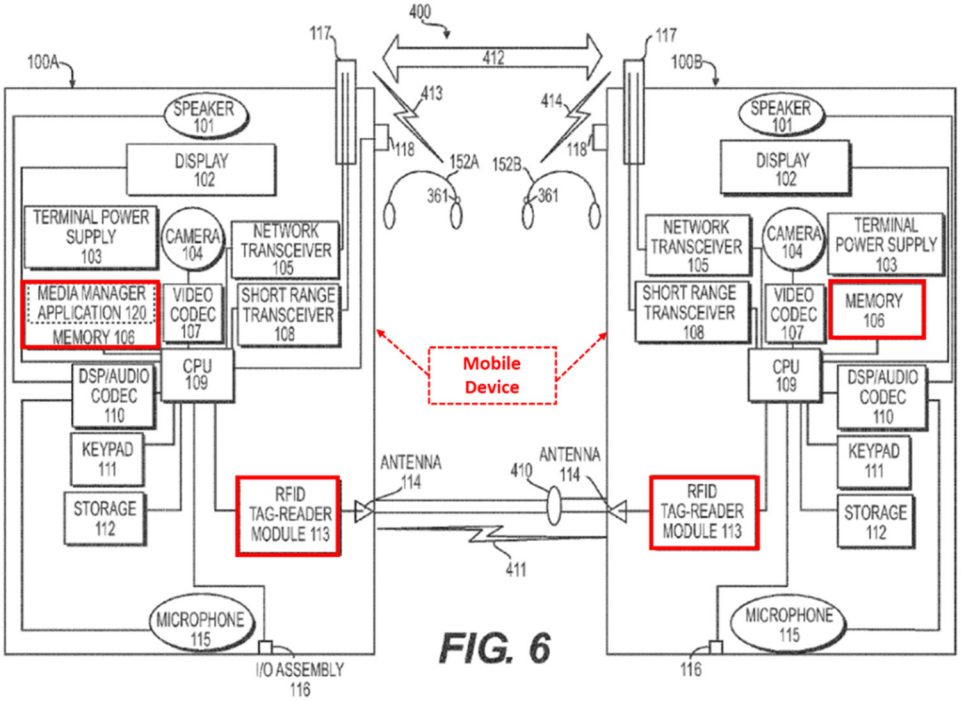
APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

playing device [i.e., the RDC on the playing device] via a transmission line such as a serial cable that plugs into the key at one end and the playing device at the other end. In another alternative embodiment, the key is a smart card or magnetic card into which the activation code is encoded, and the key is configured to physically fit into a card reader slot on the playing device."

MS-1006, ¶¶[0041], [0071]-[0073].

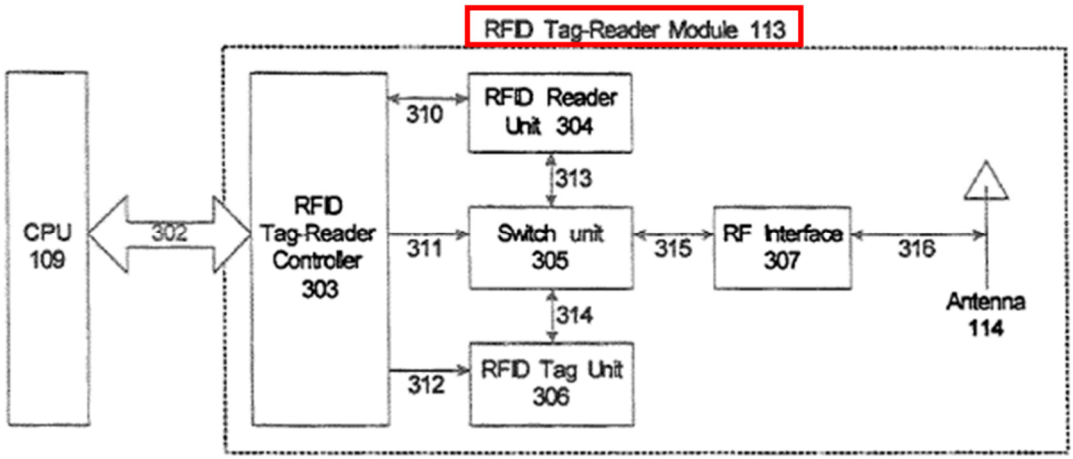
C. Overview of Dua

42. Dua discloses a wireless media player or related system (e.g., a cell phone) which establishes wireless connections with other devices to enable functions and exchange data. MS-1007, 6:46-65, FIG. 6. Dua's device is shown, for example, in annotated Fig. 6:



MS-1007, FIG. 6.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782



MS-1007, FIG. 4A.

43. Dua employs an RFID system to secure data and applications on its device using an RFID "electronic key" (e.g., for point-of-sale transactions). MS-1007, 12:51-64. Dua uses an RFID Tag as an electronic "key" and an RFID Reader as the electronic "lock." *Id*. Specifically, Dua discloses that its device uses RFID Tag-Reader Module (shown above in FIG. 4A), that includes both an RFID Reader Unit 304 and RFID Tag Unit 306. MS-1007, 13:22-48, FIGS. 4A, 6.

44. Dua's RFID Tag Unit 306 stores information necessary to gain access to an external device in an encrypted internal tag memory and transmits this information to an external Reader when establishing a connection. MS-1007, 13:9-18, 14:53-64, 15:42-56, 16:31-34. As shown in FIG. 4A above, Dua also discloses an integrated Reader Unit 304 for reading information transmitted by external Tag Units. MS-1007, 14:53-64, FIG. 4A.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

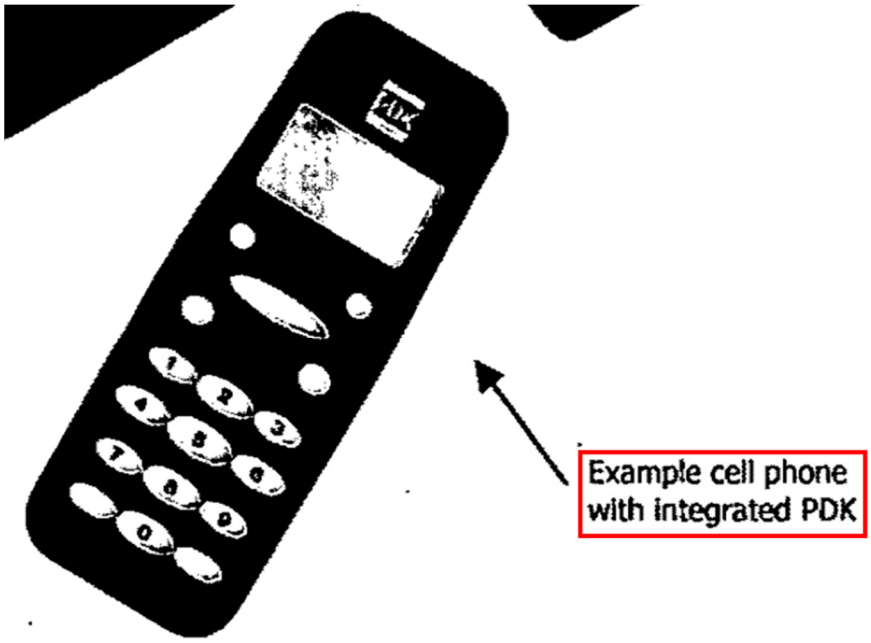
D. The Giobbi-157-Giobbi-139 combination

1. Giobbi-157 teaches integrating a PDK into a mobile device to enable a user to enjoy secure storage functionality via a commonly carried item

45. Giobbi-157 expressly and repeatedly discloses the portability of a PDK, emphasizing that a PDK can be carried by a user on their person and expressly teaches integrating the PDK into cell phones, PDAs, and other commonly carried items. MS-1005, ¶¶[0012], [0027], [0030], [0035] ("integrated into commonly carried items … such as a cell phone, [or PDA]"); MS-1010, p. 3, 14 ("[c]ell phones & PDAs with integrated PDKs … [represent] an obvious advance in convenience and simplicity over currently available alternatives"). Based on these teachings, a POSITA would have readily recognized that integration of PDKs into mobile devices, such as cell phones, provides the benefits of simplicity and convenience by, for example, providing a secure and local storage location for the user's biometric data. MS-1005, ¶¶[0012], [0027], [0030], [0035]. This integration enables a user who already carries a cell phone to enjoy the security benefits offered by Giobbi-157's system without having to carry a separate PDK. Indeed, these benefits include enabling the user to execute transactions with, for example, external RDCs (e.g., to enable access to an external, secure, digital or physical asset) where the transactions are secured by biometric verification while providing an individual with "a simple and efficient enrollment process that does not put an individual's highly personal

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

information at risk of identity theft or fraudulent use." MS-1005, ¶¶[0010], [0063]. The incorporated '157 provisional application provides an illustration of a cell phone with integrated PDK.



MS-1010, p. 28 (image cropped).

2. Giobbi '139 teaches integrating an RDC into a mobile device to provide enhanced security for the data stored on the mobile device.

46. Giobbi-139 teaches integrating an RDC into the same type of device disclosed in Giobbi-157 (e.g., a mobile device, such as a cell phone). MS-1006, ¶[0088]; MS-1005, ¶[0035]. Specifically, Giobbi-139 discloses the PDK and RDC architecture "to protect computers from unauthorized use and protect the digital content stored on computers from being wrongfully accessed, copied, and/or distributed." MS-1006, Abstract. Like Giobbi-157, Giobbi-139 teaches that the

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

PDK stores the data that authenticates a user via an RDC. MS-1006, ¶¶[0022]-[0044].

47. Giobbi-139 provides additional implementation details for its RDCs, noting that an RDC "is an integrated circuit able to process PDK-Key information, as well as encrypt/decrypt PDK-compliant digital content." MS-1006, ¶[0072]. Giobbi-139 also notes that its integrated RDC may communicate with a PDK wirelessly or through a physical connection. MS-1006, ¶¶[0022]-[0044]. Thus, Giobbi-139 teaches similar components as Giobbi '157, where an RDC can communicate with at least one PDK to grant digital or physical access. MS-1006, Abstract, ¶¶[0036]-[0037], [0088]-[0090]. Notably, Giobbi-139 identifies such a configuration as an "enhancement." MS-1006, ¶¶[0087]-[0088]. Giobbi-139 also discloses that it would have been desirable to include an RDC in a device holding data, such as a cell phone, to increase security by requiring a valid PDK to be used to permit access to the data. MS-1006, ¶[0088], FIG. 4. Given these teachings, a POSITA would have found it obvious and advantageous to integrate an RDC into Giobbi-157's cell phone to thereby enhance the security of the data stored on the cell phone.

48. Giobbi-139 additionally teaches a broader way to secure data on a cell phone and discloses that an RDC integrated into a cellphone can be used with a PDK to "effectively enable[]/disable[] the device itself." MS-1006, ¶¶[0088]-[0089].

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

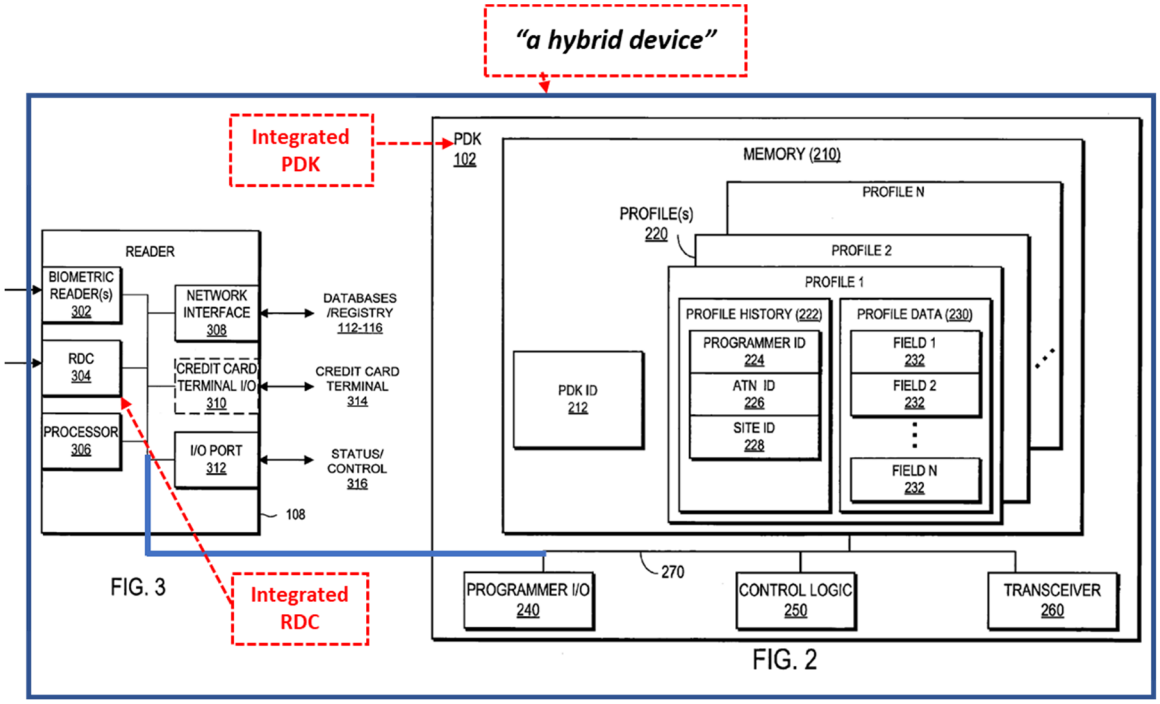
Giobbi-139 teaches that, "[t]his security mechanism protects any data stored on such devices in the event they are ever stolen, left unattended, or even purposely 'disabled' to prevent access to sensitive content (i.e. preventing minors from accessing adult files, websites, etc.)." MS-1006, ¶[0090]. In this configuration, the cell phone with the integrated RDC can enable or disable the device through authentication with a PDK. *Id*.

3. The combination of Giobbi-157 and Giobbi-139

49. Given the teachings of Giobbi-157 and Giobbi-139, a POSITA would have been motivated to integrate a PDK and RDC into the same mobile device (thus, creating a "***hybrid device***"). MS-1005, ¶¶[0012], [0027], [0030], [0035]; MS-1006, ¶¶[0022]-[0044]. As stated above, Giobbi-157 enumerates the advantages and motivations of incorporating a PDK into a mobile device. MS-1005, ¶¶[0035], [0080], claims 27, 33. For example, a user carrying the hybrid device would be able to be wirelessly authenticated with RDCs to securely complete transactions or gain access to physical or digital assets. Each RDC would be capable of communicating with the PDK's "secure and tamperproof memories," in which biometric authentication data is stored securely on the device in a format retrievable by an RDC. MS-1005, ¶¶[0036], [0064]. Additionally, Giobbi-139 teaches the benefits of integrating an RDC into this hybrid device. MS-1006, ¶¶[0087]-[0099]. For instance, a user can use an RDC integrated in the hybrid device to secure the data

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

within the hybrid device (cell phone) to thereby protect it from loss or theft. MS-1006, ¶[0091]. Further the RDC would allow other external PDKs to interact with the hybrid device. Accordingly, a POSITA would have recognized that a mobile device having an integrated RDC and PDK would provide increased security in accessing both assets internal to the mobile device and assets external to the mobile device. In this way, the mobile device would provide the same enhanced security as the disclosed PDK and RDC security architecture taught in both Giobbi-157 and Giobbi-139 for accessing internal and external assets.



MS-1005, FIGS. 2-3 (modified to incorporate Giobbi-139's teachings).

4. A POSITA would have found it obvious to integrate a PDK and RDC in a mobile device to enable secure access to assets

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

internal to the mobile device and assets external to the mobile device

50. A POSITA would have found it obvious to communicatively couple the integrated PDK and RDC within the mobile device with a physical connection based on Giobbi '139's teachings that a PDK can be connected to an RDC by a "transmission line such as a serial cable." MS-1006, ¶[0041]. By coupling the integrated PDK and RDC in this manner, assets internal to the mobile device (e.g., files, applications, etc.) can thereby be protected using the PDK-RDC techniques disclosed by Giobbi-157 and Giobbi-139. MS-1005, ¶¶[0012], [0027], [0030], [0035]; MS-1006, ¶¶[0022]-[0044].

51. For example, the mobile device may be equipped with or otherwise communicatively coupled to a biometric scanner that receives a biometric input from a user. MS-1005, ¶[0071] ("a biometric reader built into the PDK"). To authenticate the user, the integrated RDC securely accesses the valid biometric information from the integrated PDK or from an external PDK as taught by Giobbi-157 to thereby enable a comparison of the inputted biometric information with the valid biometric information stored in the PDK. MS-1005, ¶¶[0050], [0053], [0061]. A match results in a successful authentication, thereby enabling the user to access assets internal to the mobile device. A mismatch results in a failed authentication, preventing such access. MS-1005, ¶¶[0056], [0062]-[0063], [0070], [0072]. Consistent with the teachings of Giobbi-157 and Giobbi-139, the internal assets of the mobile device

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

would be protected from access by unauthorized users who would be unable to provide a biometric input that matches the valid biometric stored in the tamper proof memory of the integrated PDK of the mobile device or, in some implementations, of a PDK external to the mobile device.

52. A POSITA would have further recognized and found obvious that integrating a PDK and RDC into the same device would facilitate the Notary process disclosed by Giobbi-157 to initialize or otherwise securely edit the information securely stored in the integrated PDK. MS-1005, ¶¶[0050], [0053], [0061]. For example, Giobbi-157 discloses that a PDK can store information used in the verification of the PDK user. MS-1005, ¶¶[0011]-[0012], [0036]-[0039]. The information stored within the PDK is stored in profiles, which can be accessed and edited in a secure, auditable way. MS-1005, ¶¶[0012], [0036]-[0039], [0043]. Giobbi-157's "Notary" PDK is used to verify that authorized individuals are creating or editing information inside a PDK, and to maintain a history of changes to the PDK including the identity of the "Notary" PDK that was present during the change. MS-1005, ¶¶[0037], [0043]; MS-1010, p. 4. As shown in FIG. 2 of Giobbi-157, a PDK profile contains a history (Profile History 222) that includes the identification of the Authorized TruProx Notary PDK ID (ATN ID 225). MS-1005, FIG. 2. For an integrated PDK to record the ATN PDK ID into the profile history of the integrated PDK in a mobile device, an RDC can be used to (1) interface with and read the ATN

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

PDK, and (2) record the ATN PDK ID into the PDK. MS-1006, ¶¶[0022]-[0044]. Accordingly, a POSITA would have recognized the need for both a PDK and an RDC to be integrated into the same mobile device (a "***hybrid device***") and communicatively coupled together. MS-1005, ¶¶[0012], [0027], [0030], [0035]; MS-1006, ¶¶[0022]-[0044].

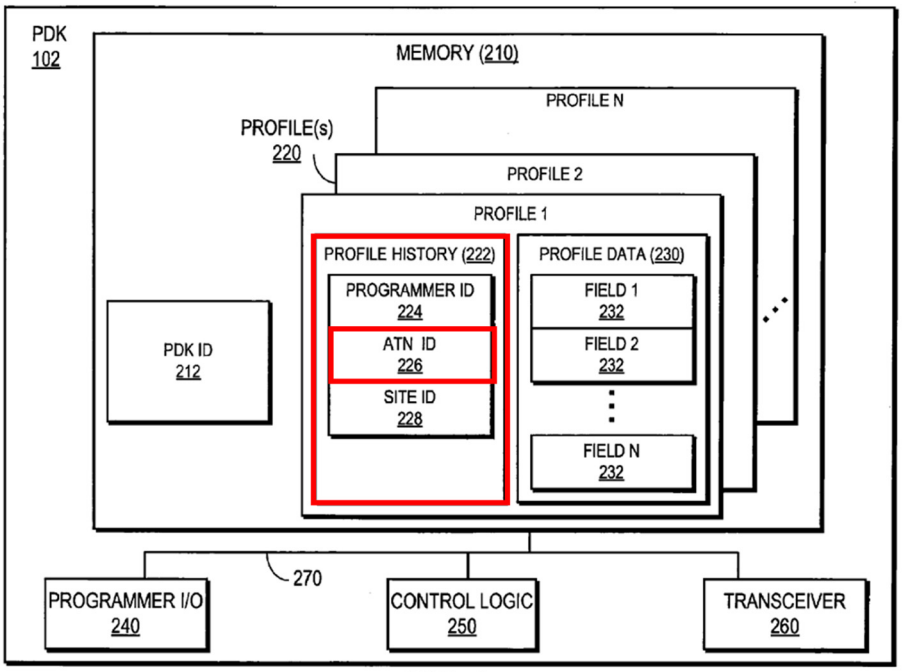


FIG. 2

MS-1005, FIG. 2.

53. In addition to using the integrated RDC to enable secure access to assets internal to the mobile device, a POSITA would have further recognized the benefit of using the integrated PDK to enable secure access to assets external to the mobile device. For example, as taught by Giobbi-139, the owner of the mobile device could separately use the integrated PDK of the mobile device to securely authenticate

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

themselves for the purpose of accessing all or portions of an external hard drive equipped with an RDC. MS-1006, ¶¶[0087]-[0090]. Moreover, as taught by Giobbi-157, the owner of the mobile device could separately use the integrated PDK of the mobile device to securely access physical items, such as a room or safe. MS-1005, ¶¶[0011]-[0012], [0063].

54. For at least the aforementioned reasons, a POSITA would have found it obvious to modify Giobbi-157's portable electronic device to include an RDC as taught by Giobbi-139 (thus creating a "***hybrid device***"). Combining Giobbi-157 and Giobbi-139 would have involved (1) combining prior art elements according to known methods to yield predictable results; (2) use of a known technique to improve similar devices (methods, or products) in the same way; and (3) applying a known technique to a known device ready for improvement to yield predictable results. Further, Giobbi-157 expressly teaches the integration of a PDK into a mobile device. MS-1005, ¶[0035], claim 27. Giobbi-139 expressly teaches the integration of a RDC into a mobile device. MS-1006, ¶[0088], claim 9, FIG. 4.

55. Specifically, a POSITA would have been motivated to integrate a PDK and RDC into a ***hybrid device*** by recognizing that (i) Giobbi-157 and Giobbi-139 are directed to similar operations having similar purposes (e.g., "provide efficient, secure, and highly reliable authentication for … access control applications" and "protect[ing] any data stored on such devices"; (ii) Giobbi-157 and Giobbi-139

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

describe similar structures for performing those operations (e.g., PDKs and RDCs); (iii) the techniques of Giobbi-157 and Giobbi-139 are compatible with each other, given that both were filed by the same applicant and describe similar techniques; and (iv) combining the techniques of Giobbi-157 and Giobbi-139 would have worked in the same manner already described in the references. MS-1005, ¶[0011]; MS-1006, ¶[0090].

E. The Giobbi-157-Giobbi-139-Dua combination

56. Dua further corroborates the teachings of the Giobbi references and provides implementation details for integrating an RDC and PDK into the same device. First, a POSITA would have recognized the similarity between 1) the RFID Tag in Dua and the PDK in Giobbi; and 2) the RFID Reader in Dua and the RDC in Giobbi. This is because, like RFID technology, Giobbi's PDK and RDC architecture require both components within proximity of each other. For example, two RFID tags without a reader would not be usable. Likewise, two PDKs without an RDC would not be usable. An RFID tag becomes usable when in range of an RFID reader, comparable to how a PDK is usable when in range of an RDC.

57. A POSITA would have been motivated to combine the teachings of the Giobbi references and Dua because, at least, these references are all in the same field of endeavor (e.g., incorporating proximity based enabling technology into mobile devices to allow secure data sharing and services). MS-1005, Abstract, ¶¶[0011]-

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

[0014]; MS-1006, Abstract, ¶[0010]; MS-1007, Abstract, 6:46-65, FIGS. 4A, 6.; MS-1001, Abstract, claim 1. Accordingly, with proximity enabling technology (RFID) like Dua integrating both transmitters (PDKs/RFID Tags) and receivers (RDCs/RFID Readers) into the same mobile device, a POSITA would have had a reasonable expectation of success integrating an RDC from Giobbi-139 into the Giobbi-157 device to create a hybrid device. *Id*. This reasonable expectation of success is further bolstered by the teachings of Dua, which, as discussed above, also teaches integrating an "RDC" and "PDK" into the same type of device. MS-1007, 13:19-14:64, Fig. 4A. More specifically, the media player of Dua includes an RFID Tag-Reader Module that is capable of functioning as both an RFID tag and an RFID reader. MS-1007, 3:1-9.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

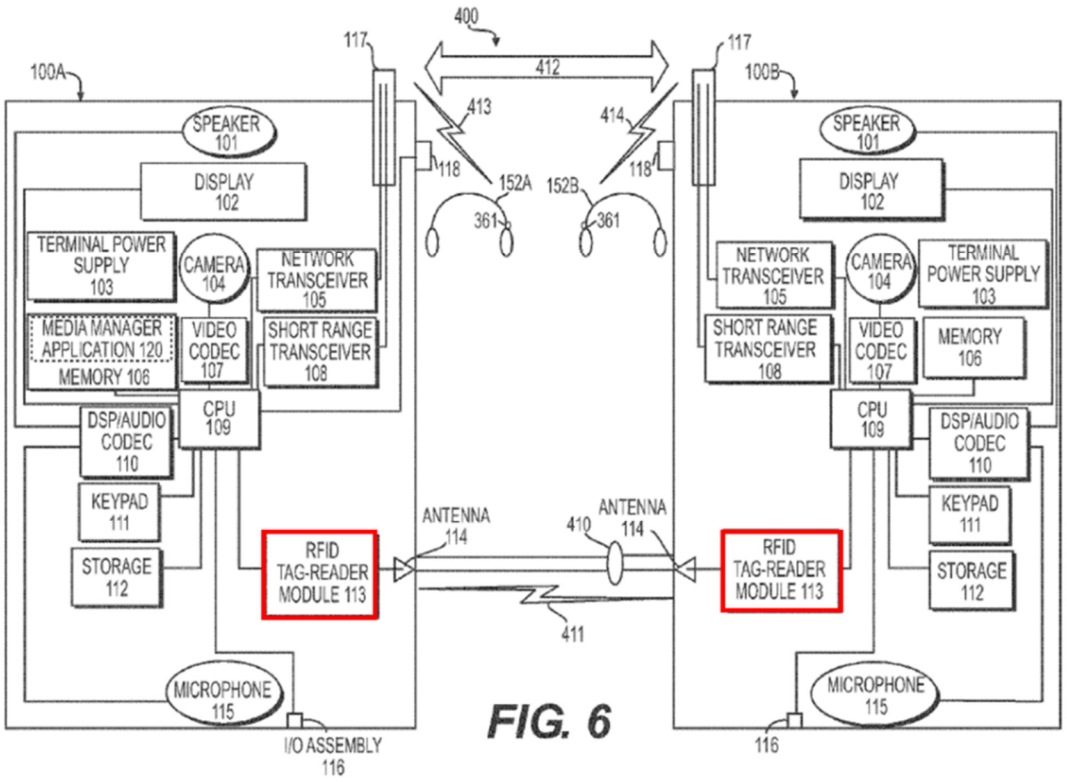
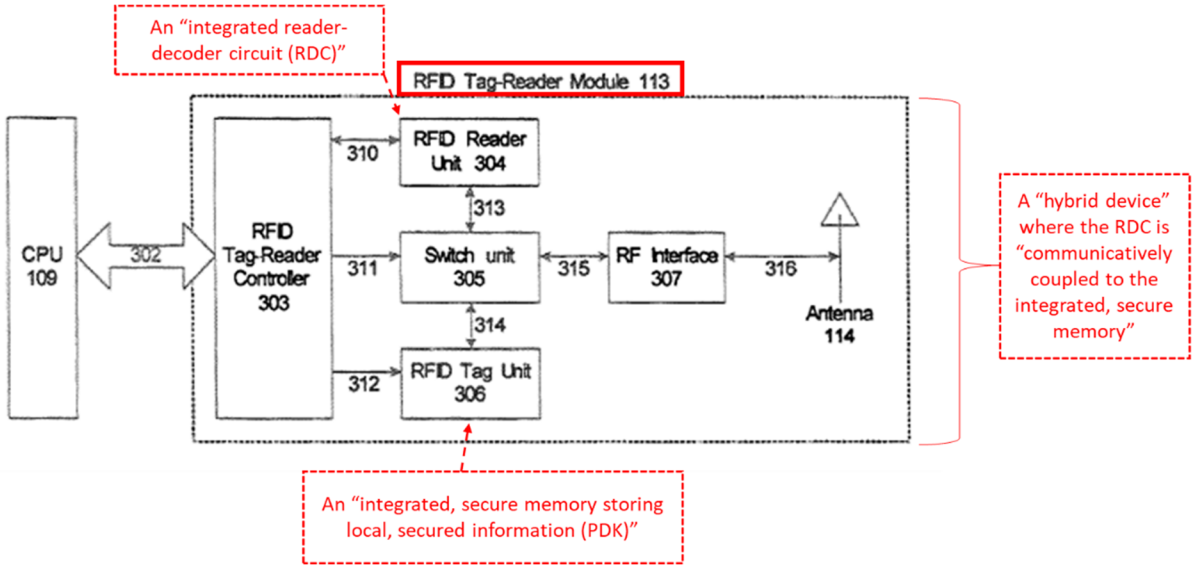


FIG. 6

MS-1007, FIG. 6.



MS-1007, FIG. 4A

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

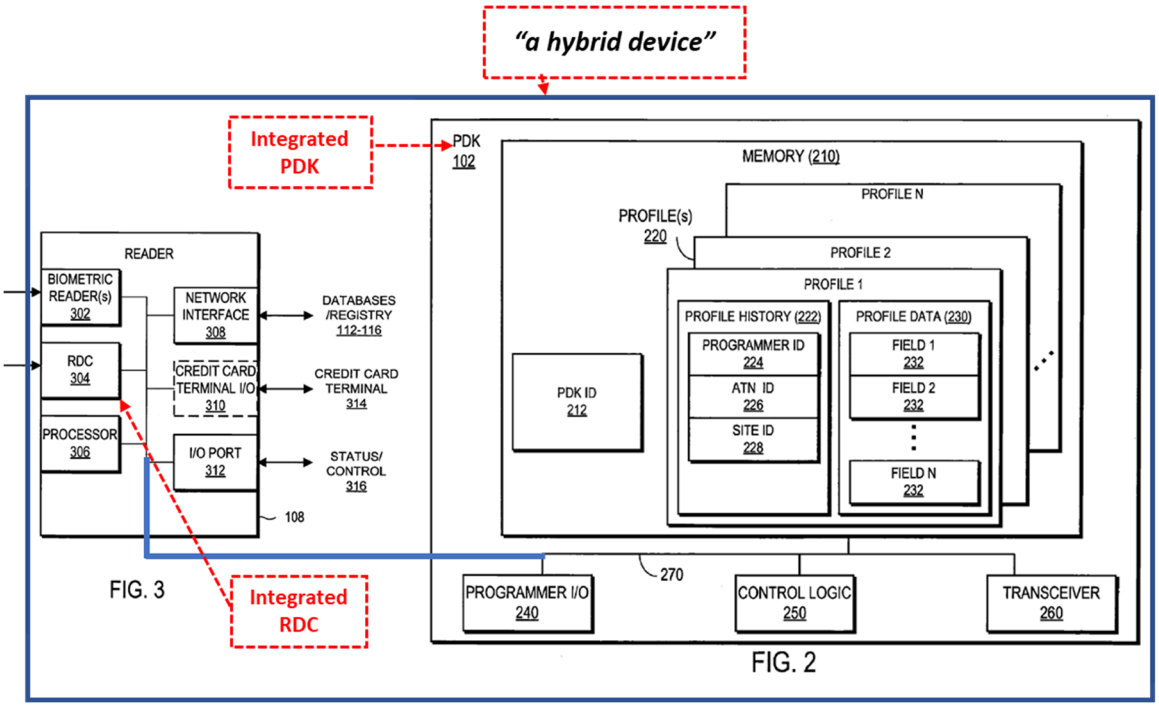
F. Analysis

[1.pre] A hybrid device comprising:

Grounds 1A/IB

58. To the extent the preamble is limiting, the combination of Giobbi-157 and-139 discloses a "***hybrid device***." MS-1005, ¶¶[0012], [0027], [0030], [0035]; MS-1006, ¶¶[0022]-[0044]. For example, Giobbi-157 discloses incorporating PDKs into different electronic devices, while Giobbi-139 discloses incorporating RDCs into different electronic devices. MS-1005, ¶¶[0012], [0027], [0030], [0035]; MS-1006, ¶¶[0022]-[0044]; *see supra,* §§VI.D.1-3. Accordingly for the reasons described in detail in Sections III.A.1-3 and 5 above, the combination of these two references renders obvious "a device comprising [a PDK] and an integrated [RDC]." *See supra,* §§IV.A, VI.D.3. As shown below in FIGS. 2-3, Giobbi-157's cell phone includes an integrated PDK. MS-1005, FIGS. 2-3. In the combination of Giobbi-157 and Giobbi-139, this integrated PDK communicates with an integrated RDC all within a ***hybrid device***. *Id*.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782



MS-1005, FIGS. 2-3 (modified to incorporate Giobbi-139's teachings).

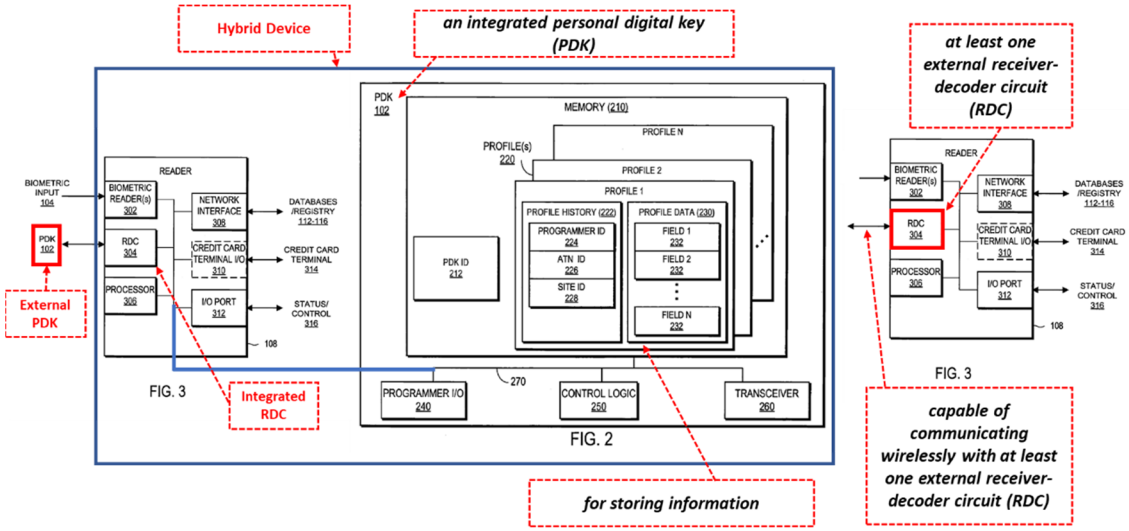
[1.1] an integrated personal digital key (PDK) for storing information and capable of communicating wirelessly with at least one exter-nal receiver-decoder circuit (RDC); and

Ground 1A

59. Giobbi-157 discloses a "***Personal Digital Key (PDK)***," which is an example of an ***integrated*** secure memory ***for storing information***. MS-1005, ¶[0011] ("A portable physical device, referred to herein as a Personal Digital Key or 'PDK,' ***stores*** one or more profiles (e.g., a biometric profile) ["***information***"] in a tamper-proof memory"). As discussed above, Giobbi-157 also discloses that its PDK is ***integrated*** into a hybrid device, such as a cell phone. MS-1005, ¶[0035] ("The PDK 102 can be standalone as a portable, physical device or can be integrated into

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

commonly carried items … such as a cell phone"); *see supra*, §VI.A, [1.pre]. Accordingly, the hybrid device of the Giobbi-157-Giobbi-139 combination includes an integrated PDK for storing information. Additionally, Giobbi-157's PDK stores information in local storage as the PDK is integrated into the hybrid device. MS-1005, ¶¶[0011], [0027]-[0028].



MS-1005, FIGS. 2-3 (modified to incorporate Giobbi-139's teachings).

60. Finally, Giobbi-157 teaches that PDKs "can wirelessly transmit [("***communicating wirelessly***")] the identification information including a unique PDK identification number and the biometric profile over a secure wireless channel for use in an authentication process," and that the RDC is specially designed to receive information from the PDK. MS-1005, ¶[0050]. For example, "[t]he RDC 304 provides the wireless interface to the PDK 102 [("***with at least one external receiver-decoder circuit (RDC)***")]. Generally, the RDC 304 wirelessly receives data

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

from the PDK 102 in an encrypted format and decodes the encrypted data for processing by the processor 306." MS-1005, ¶¶[0050], [0059] ("When a PDK 102 comes within range of a Reader 108, communication is automatically established 402 between the RDC 304 of the Reader 108 and the PDK 102."). Thus, a PDK by its definition can "***communicat[e] wirelessly with at least one external receiver-decoder circuit (RDC)***."

Ground 1B

61. Like Giobbi-157 and Giobbi-139, Dua uses an RFID system to secure data and applications on its hybrid device. MS-1007, 6:46-65, 12:51-64, 13:9-18, 14:53-64, 15:42-56, 16:31-34, FIGS. 4A, 6; *see supra* §VI.C Dua teaches that its RFID setup may act as an "electronic key" for point-of-sale transactions and uses an RFID Tag as an electronic "key" and an RFID Reader as the electronic "lock." *Id*. Accordingly, Dua's RFID Tag Unit 306 is another example of a "***PDK***" ***for storing information and capable of communicating wirelessly with at least one external receiver-decoder circuit (RDC)*** (RFID reader). This is because the RFID Tag Unit 306 stores information that it later conveys wirelessly to an RFID reader, just as the PDK wirelessly conveys information to the RDC.

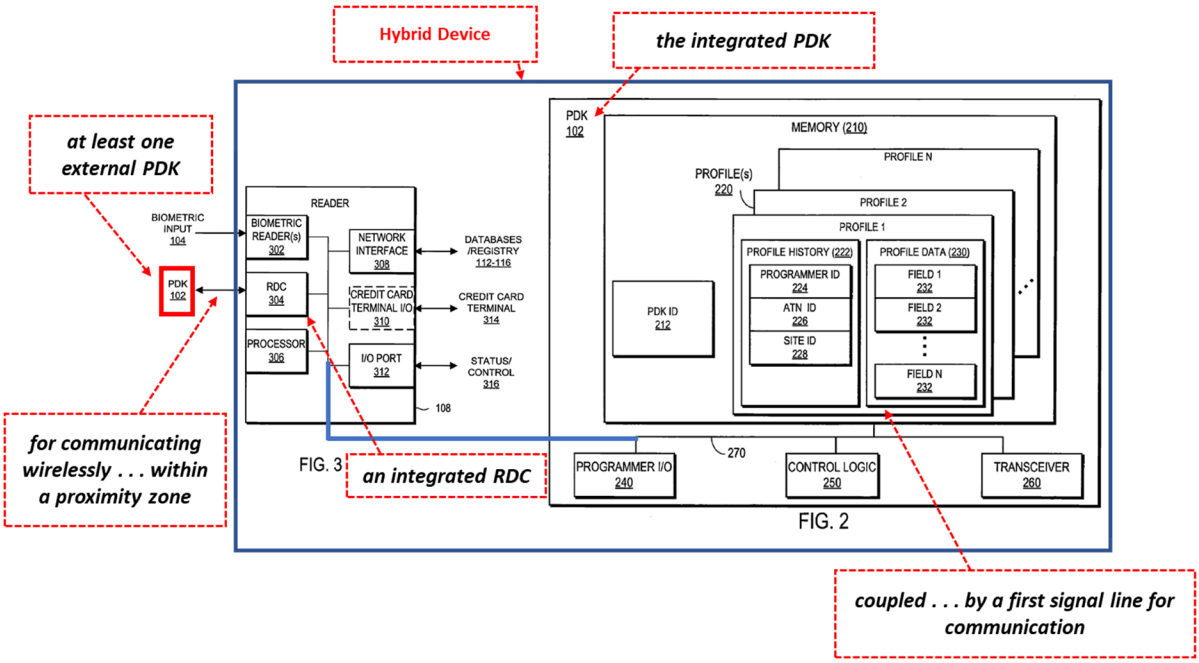
[1.2] an integrated RDC for communicating wirelessly with at least one external PDK within a proximity zone, the integrated RDC coupled to the integrated PDK by a first signal line for communication,

Ground 1A

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

62. The combination of Giobbi-157 and Giobbi-139 discloses "a component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing" as required by the district court's construction for "***an integrated RDC***." *See supra*, §§IV.C, VI.A-B, VI.D. In particular, Giobbi-157 teaches that "the RDC 304 wirelessly receives data from the PDK 102 in an encrypted format and decodes the encrypted data for processing." MS-1005, ¶[0050]. Giobbi-157 also discloses an integrated RDC "***communicating wirelessly with at least one external PDK within a proximity zone***." MS-1005, ¶¶[0026]-[0044] ("The Reader 108 wirelessly communicates with the PDK 102 when the PDK 102 is within a proximity zone of the Reader 108"); *see supra* §VI.A. As described above, the hybrid device includes an ***integrated RDC*** that is ***coupled to the integrated PDK by a first signal line for communication***. MS-1005, ¶¶[0012], [0027], [0030], [0035]; MS-1006, ¶¶[0022]-[0044]; *see supra*, §VI.D. An RDC is illustrated in FIG. 3 of Giobbi-157 below. MS-1005, FIG. 3.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782



MS-1005, FIGS. 2-3 (modified to incorporate Giobbi-139's teachings).

63. Giobbi-139 also discloses an integrated RDC "communicating wirelessly with the at least one external device within a proximity zone." MS-1006, ¶¶[0026]-[0044] ("The Reader 108 wirelessly communicates with the PDK 102 when the PDK 102 is within a proximity zone of the Reader 108").

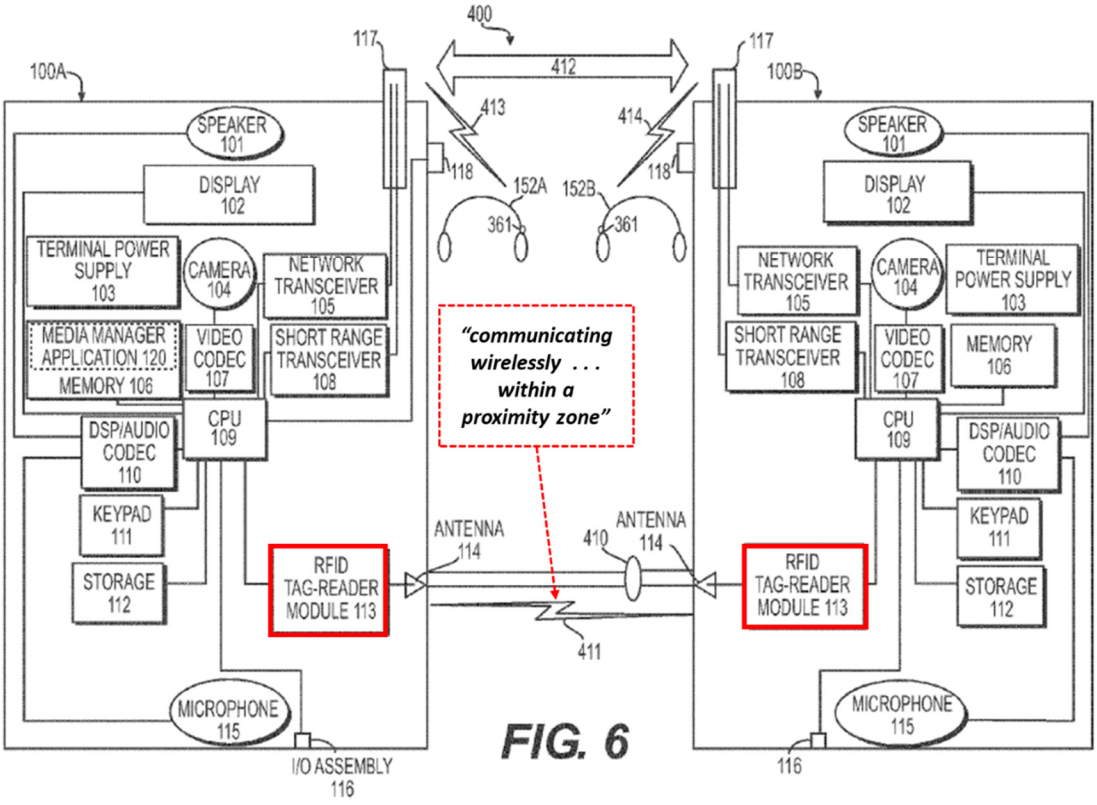
Ground 1B

64. Like Giobbi-157 and Giobbi-139, Dua uses a proximity (RFID) system to secure data and applications on its "hybrid device." MS-1007, 6:46-65, 12:51-64, 13:9-18, 14:53-64, 15:42-56, 16:31-34, FIGS. 4A, 6; *see supra* §VI.D. Dua teaches that its RFID setup may act as an "electronic key" for point-of-sale transactions and uses an RFID Tag (PDK) as an electronic "key" and an RFID Reader (RDC) as the electronic "lock." MS-1007, 12:60-61. FIG. 6 of Dua illustrates a hybrid device

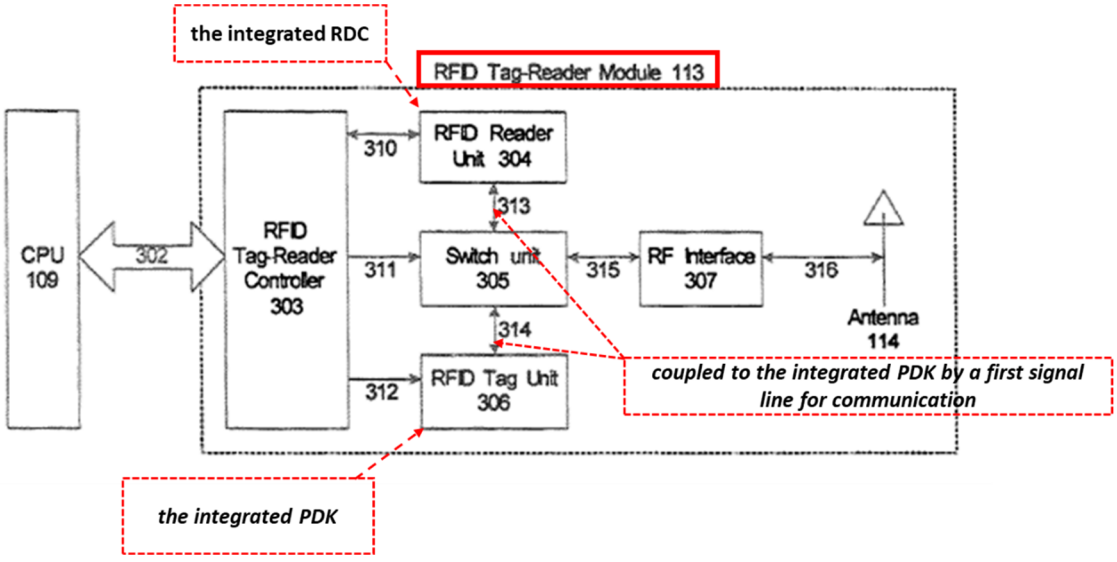
APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

that includes an RFID Tag-Reader Module (an "***integrated reader-decoder circuit (RDC)***" and an RFID Tag Unit 306 (the "***integrated . . .(PDK)***" of [1.1]). MS-1007, FIG. 6. As explained, the patent's disclosure of integrating PDKs and RDCs in a hybrid device is merely a recitation of technology commonly used in RFID applications, such as Dua's application, function, and service. *Id*. Accordingly Dua's Reader Unit 304 is another example of an "***integrated reader-decoder circuit (RDC)***" as the Reader Unit 304 also "***communicat[es] wirelessly with at least one external device within a proximity zone***" and is "***communicatively coupled to [an] integrated PDK***" (the RFID Tag Unit 306). MS-1007, 6:46-65, 12:51-64, 13:9-18, 14:53-64, 15:42-56, 16:31-34, FIGS. 4A, 6. This is because of the RFID reader, like the RDC, is configured to communicate wirelessly with an external component. In the case of the RFID reader, the external component is an RFID tag, and in the case of the RDC the external component is the PDK.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782



MS-1007, FIG. 6.



MS-1007, FIG. 4A.

[1.3] the integrated RDC coupled to at least one other component of the hybrid device by a second signal line,

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

Ground 1A

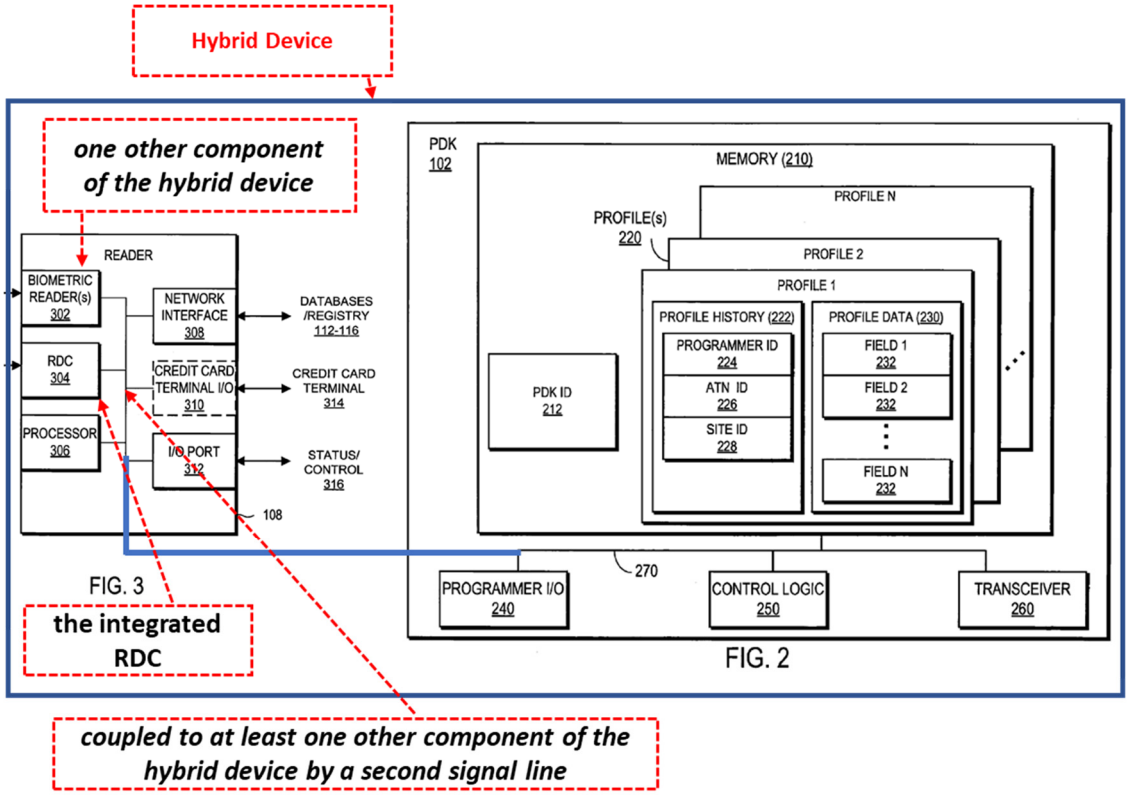
65. First, Giobbi-139 teaches that a device can be controlled utilizing signals that are sent from or controlled by the RDC within the device. MS-1006, ¶¶[0041], [0088]-[0089]. For example, a storage device ("***at least one other component***") "***of the hybrid device***" (such as a portion of the memory of a cell phone) can be controlled by a signal line from the RDC to the storage device ("***the integrated RDC coupled to at least one other component of the hybrid device by a second signal line***"). MS-1006, ¶¶[0041], [0088]-[0090]. Using the example of digital storage, Giobbi-139 teaches that the integrated RDC provides "multiple methods of securing digital content." MS-1006, ¶[0071]. For example, Giobbi-139 teaches that the "bus structure that provides the communications path between storage mechanisms and their hosting devices" is controlled to secure portions of a device. MS-1006, ¶¶[0078], [0089]. In this way a controller (under direction of an RDC) can control "access to the storage is enabled/disabled by interrupting the communications path, signaling to the hosting device that the storage is either "ready" or "busy," effectively enabling/disabling the device itself." MS-1006, FIG. 11-13; ¶¶[0078], [0089]. Giobbi-139 gives a specific example of the use case where "[t]he [hard]drive's controller 334 [(***at least one other component)***] is disabled whenever the PDK-Key 336 is not present." (in reference to FIGS 12 and 13) MS-1006, ¶[0078]. Therefore, a POSITA would have found obvious that in order to control an

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

application, function, or service on the device, "***a second signal line***" would connect the RDC to the "***at least one other component of the hybrid device***."

66. Alternatively, Giobbi-157 teaches that both RDCs and PDKs can include biometric readers ("***at least one other component of the hybrid device***"). MS-1005, FIG. 3, ¶¶[0030], [0048]-[0049], [0051]-[0052], [0071]. Indeed, Giobbi-157 shows the ***integrated RDC*** 304 ***coupled*** by ***a second signal line*** to the biometric reader 302 (***at least one other component of the hybrid device***) in FIG. 3. MS-1005, FIG. 3. The ***integrated RDC*** compares the biometric input at the biometric reader to the biometric profile data received from a PDK. MS-1005, FIG. 3, ¶¶[0030], [0048]-[0049], [0051]-[0052], [0071]. Therefore, a POSITA would have found it obvious that in order for the data of the biometric reader to be compared to the data of the PDK, the "***the integrated RDC [is] coupled to at least one other component of the hybrid device by a second signal line***."

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782



MS-1005, FIGS. 2-3 (modified to incorporate Giobbi-139's teachings).

67. Finally, both Giobbi-157 and Giobbi-139 teach a network interfacing component (***at least one other component of the hybrid device***) connected to an RDC, thus allowing the RDC to "relay" authorization information to an external device (Giobbi-157's "network interface 308" connected to the RDC 304 in FIG.3). MS-1006, ¶[0085]. For example, Giobbi-139 teaches that "Network-Level protection, File-Level Protection can be expanded to a network environment by employing a centralized software application/database called a PDK Document Controller (DC) 340 running on a server 342." MS-1006, ¶[0084]. "An RDC located in the requester's workstation 346 acquires information from the user's PDK-Key

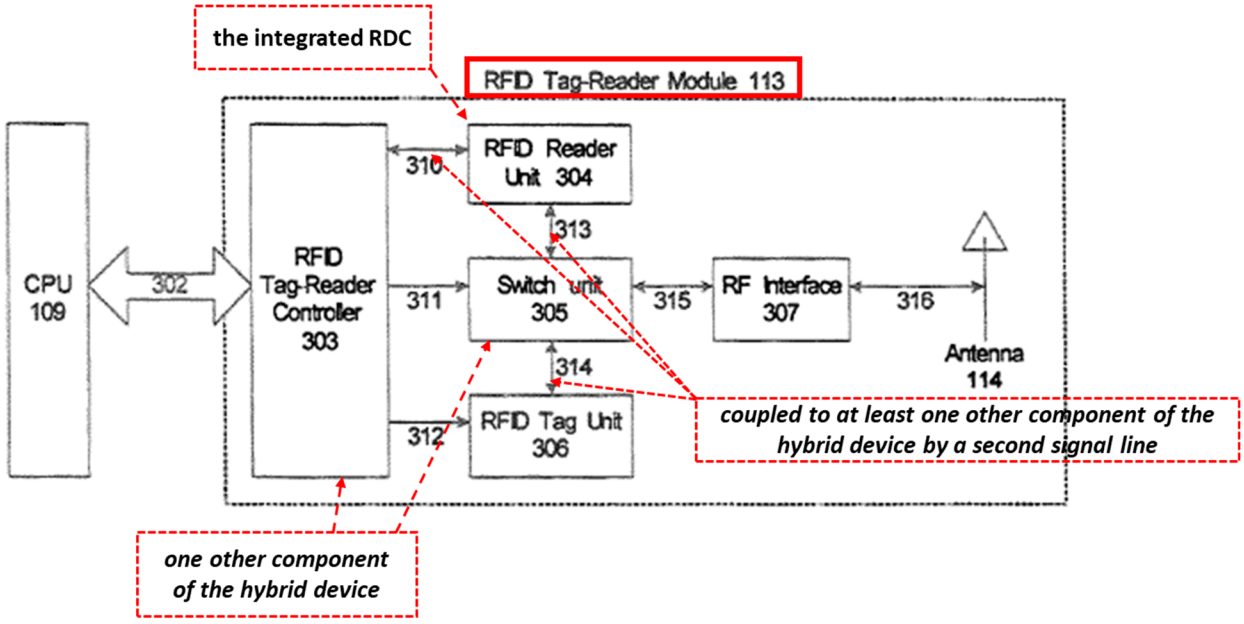
APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

344 and relays that information to the DC 340. The DC then enables appropriate access." MS-1006, ¶[0085]. Here the ***integrated RDC*** is ***coupled to at least one other component of the hybrid device*** (a network interface component) ***by a second signal line*** that allows communication with a component outside the hybrid device.

Ground 1B

68. FIG. 6 of Dua illustrates a hybrid device that includes an RFID Tag-Reader Module (an "RDC) Unit 306 (the "PDK"). MS-1007, FIG. 6. As explained, the patent's disclosure of integrating PDKs and RDCs in a hybrid device is merely a recitation of technology commonly used in RFID applications, such as Dua's application, function, and service. *Id*. It is obvious that ***the integrated RDC*** is ***coupled to at least one other component of the hybrid device by a second signal line***, so that the RDC can enable that component or for the mere fact that the RDC must be connected to a processor, transmitter, memory, or power to function in the mobile device. MS-1007, FIG. 4A. MS-1007, 6:46-65, 12:51-64, 13:9-18, 14:53-64, 15:42-56, 16:31-34, FIGS. 4A, 6. This connection from the RDC (RFID reader of Dua) to another component would have been obvious to a POSITA at least in so much that the RFID reader does some action after reading the RFID tag, such as authenticating the user, enabling a function, or providing information used elsewhere in the device.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782



MS-1007, FIG. 4A.

[1.4] one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and a service on one or more of the hybrid device and a device associated with the ex-ternal RDC.

Ground 1A/1B

69. Giobbi-157 discloses that, "[w]hen a PDK 102 comes within range of a Reader 108, communication is automatically established 402 between the RDC 304 . . . and the PDK 102 . . . when it enters a proximity zone of the [RDC]" MS-1005, ¶¶[0059-0063]. The RDC then requests profile data stored within the external PDK for authentication. MS-1005, ¶[0061]. If the profile data received from the external PDK is valid and authenticated, the ***integrated RDC*** "completes the transaction." MS-1005, ¶[0063]. A "transaction includes enabling access to secure physical or digital assets (e.g., unlocking a door, opening a vault, providing access

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

to a secured hard drive, etc.)" ("***enabling one or more of an application, a function, and service***"). MS-1006, ¶[0063]. More specifically, the external PDK can enable functions on ***the hybrid device***, including "effectively enabling/disabling the device itself." MS-1006, ¶[0089].

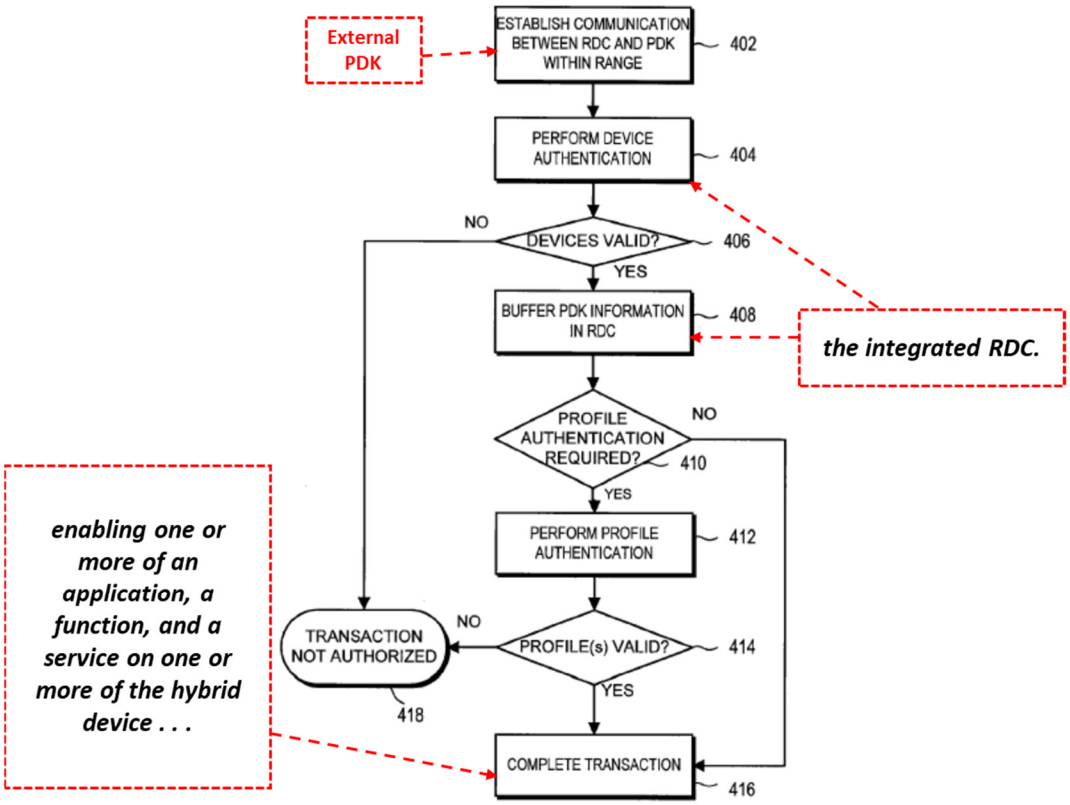


FIG. 4

MS-1005, FIG. 4.

70. Additionally, the integrated PDK of the hybrid device "***enabl[es] one or more of an application, a function, and service on. . . a device associated with the external RDC.***" MS-1005, Abstract, ¶[0011]. Transactions in Giobbi-157 are performed by transmitting authenticating information from a PDK ("***the integrated***

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

PDK" of the hybrid device) to an RDC (***the external RDC***), for example, when completing a withdrawal from an ATM (***a device associated with the external RDC***). MS-1005, ¶[0065]. An example authentication process and function enablement is shown below in FIG. 4.

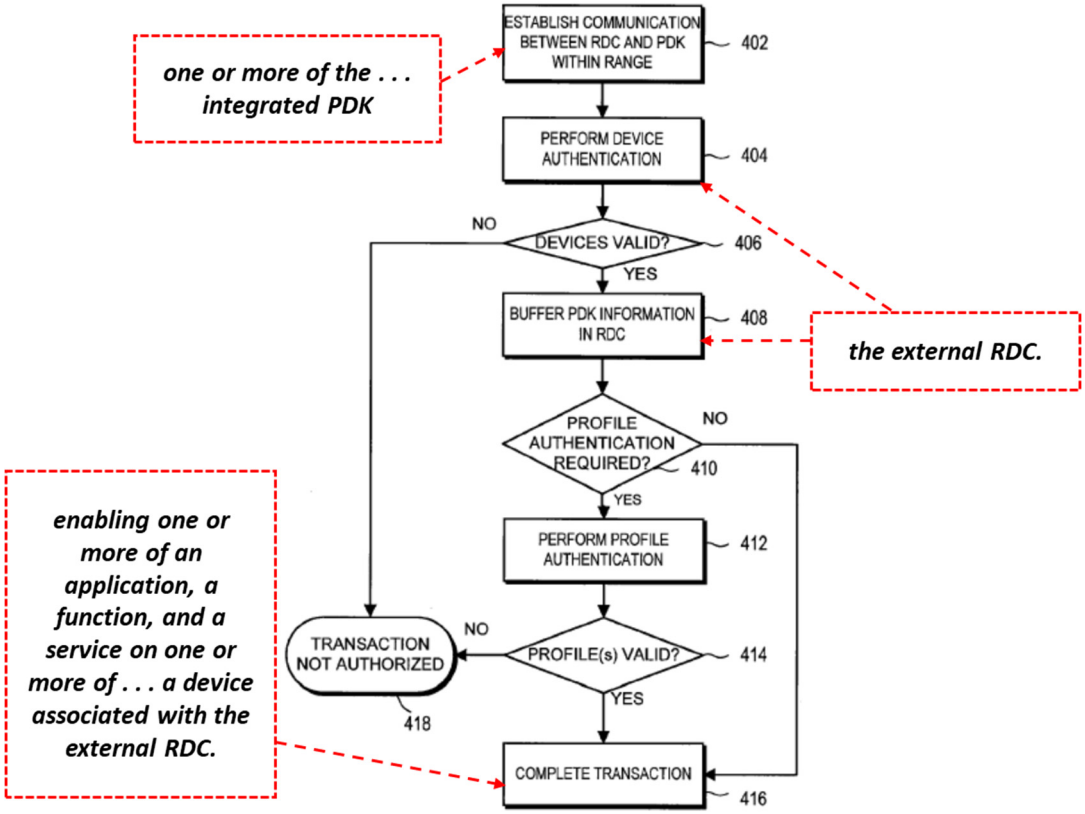


FIG. 4

MS-1005, FIG. 4.

71. Giobbi-157 explicitly teaches that the "transaction" in FIG. 4 "***enables one or more of an application, a function, and service***" when stating that "the transaction includes enabling access to secure physical or digital assets (e.g.,

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

unlocking a door, opening a vault, providing access to a secured hard drive, etc.)." MS-1005, ¶[0063].

72. Additionally, Giobbi-139 discloses a use case where an integrated RDC can be incorporated into cell phones, PDAs, and MP3 players. MS-1006, ¶[0088]; *see supra* §§VI.B, VI.D. If an authorized PDK is used in conjunction with the integrated RDC the application/function/service runs on the hybrid device, e.g., the hybrid device "plays the digital content," such as music ("***enables one or more of an application, a function, and service***"). MS-1006, ¶[0037].

[5] The hybrid device of claim 1, wherein the one or more of the hybrid device and the device associated with the external RDC are enabled subsequent to the external PDK entering the proximity zone of the integrated RDC and based on the information stored by one or more of the external PDK and the integrated PDK.

Ground 1A/1B

73. Claim 5 includes the limitation of claim 1 in that the enablement is the enablement "of an application, a function, [or] a service." *See supra* [1.4].

74. As discussed above, Giobbi-157 provides an example use of a Notary PDK used to initialize other PDKs, such as the PDK of the hybrid device. *See supra* §VI.D.4. The Notary PDK (***the external PDK***) when initializing the hybrid device's PDK would ***enter[]the proximity zone of the integrated RDC*** and provide the Notary PDK ID in "a process that is trusted, audited, and easily verified." MS-1005, ¶[0029], [0037], [0043]-[0044]. Then any subsequent use of the hybrid device to

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

enable functionality would be ***subsequent to the external PDK*** (Notary PDK) ***entering the proximity zone of the integrated RDC***.

75. Both Giobbi-139 and Giobbi-157 teach proximity-based enablement of applications, functions, and services on a ***device associated with an external RDC***. MS-1005, ¶¶[0030], [0059], [0062]; MS-1006, ¶¶[0036]-[0037], [0087]-[0090]. For example, Giobbi-157 teaches that "[w]hen a PDK 102 comes within range of a Reader 108 [a device with an integrated RDC], communication is automatically established 402 between the RDC 304 of the Reader 108 and the PDK 102." MS-1005, ¶[0059]. A user can then "initiate" or "trigger" a transaction for example, "[b]y supplying the biometric contact, the user indicates that the authentication and transaction process should proceed. For example, a PDK holder that wants to make a withdrawal from an Automated Teller Machine (ATM) equipped with a Reader 108 initiates the withdrawal by touching a finger to the Reader 108. The ATM then begins the transaction process for the withdrawal." MS-1005, ¶[0065]. Then, the RDC "transmits 604 profile authentication requests to the PDK 102 requesting transmission of one or more stored profiles over the secure channel" in order to authenticate the user ("***based on the information stored by one or more of the external PDK and the integrated PDK***"). MS-1005, FIG. 4, ¶¶[0064]-[0068]. If the transmitted profiles are valid, the transaction is completed at the ATM (***the***

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

device associated with the external RDC [is] enabled). MS-1005, FIG. 4, ¶¶[0064]-[0068].

76. Both Giobbi-139 and Giobbi-157 teach proximity-based enablement of applications, functions, and services on ***the hybrid device***. MS-1005, ¶¶[0049]-[0058], [0064]-[0068]. For example, a shop owner can carry a hybrid device and utilize the integrated PDK to enable functions within the store such as enabling a cash register or unlocking a storeroom. MS-1005, ¶¶[0049]-[0058], [0064]-[0068]. When a customer carrying a PDK (e.g., a hybrid device including a PDK external to the merchant's hybrid device) requests to initiate a purchase, the merchant can utilize the hybrid device to both receive input from the user (e.g., fingerprint, PIN, or password), and receive, via the integrated RDC, the external PDK's information to compare to the input to authenticate the customer. MS-1005, FIG. 3, 5, ¶¶[0049]-[0058], [0064]-[0068]. Thus, the ***hybrid device*** carried by the merchant is ***enabled*** to complete a purchase transaction ***subsequent to the external PDK*** of the customer ***entering the proximity zone of the integrated RDC*** of the merchant's hybrid device ***and based on the information stored by . . . external PDK*** (e.g., authentication information, credit card information).

77. Of note, both the external PDK and the integrated PDK can connect to the integrated RDC, as taught by Giobbi-157: "Thus, if multiple PDKs 102 enter the proximity zone, the Reader 108 automatically determines which PDKs 102 are valid

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

and buffers the received information from each valid PDK 102." MS-1005, ¶[0062]. In some cases, the enablement can occur automatically, based on proximity alone such as "situations where the mere presence of a PDK 102 [("***the external PDK***")] within range of the Reader 108 is by itself a clear indication of the PDK owner's desire to complete a transaction." MS-1005, ¶[0067]. Here, the RDC "detects the PDK 102 within range, authenticates the user [("***based on the information stored by . . . the external PDK***")], and executes a transaction." MS-1005, ¶[0067]. Alternatively, if using the ***integrated PDK***, the user of the hybrid device can "trigger" the authentication process to request profile information from the integrated PDK for the enablement of the hybrid device ***based on the information stored by . . . the integrated PDK***. Thus, a POSITA would have found obvious that with multiple PDKs having communications with the integrated RDC, the "transaction" is completed using information from either PDK. Giobbi-157 teaches that "completing 416 the transaction includes enabling access to secure physical or digital assets" [("***one or more of the hybrid device . . . are enabled***")]. and Giobbi-139 teaches that a PDK can "effectively enabling/disabling the device itself" ("***one or more of the hybrid device . . . are enabled***"). MS-1005, ¶[0063]; MS-1006, ¶[0089].

78. Therefore, a POSITA would have found it obvious that the hybrid device is enabled subsequent to the external PDK entering the proximity zone of the

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

integrated RDC and based on the information stored by one or more of the external PDK and the integrated PDK.

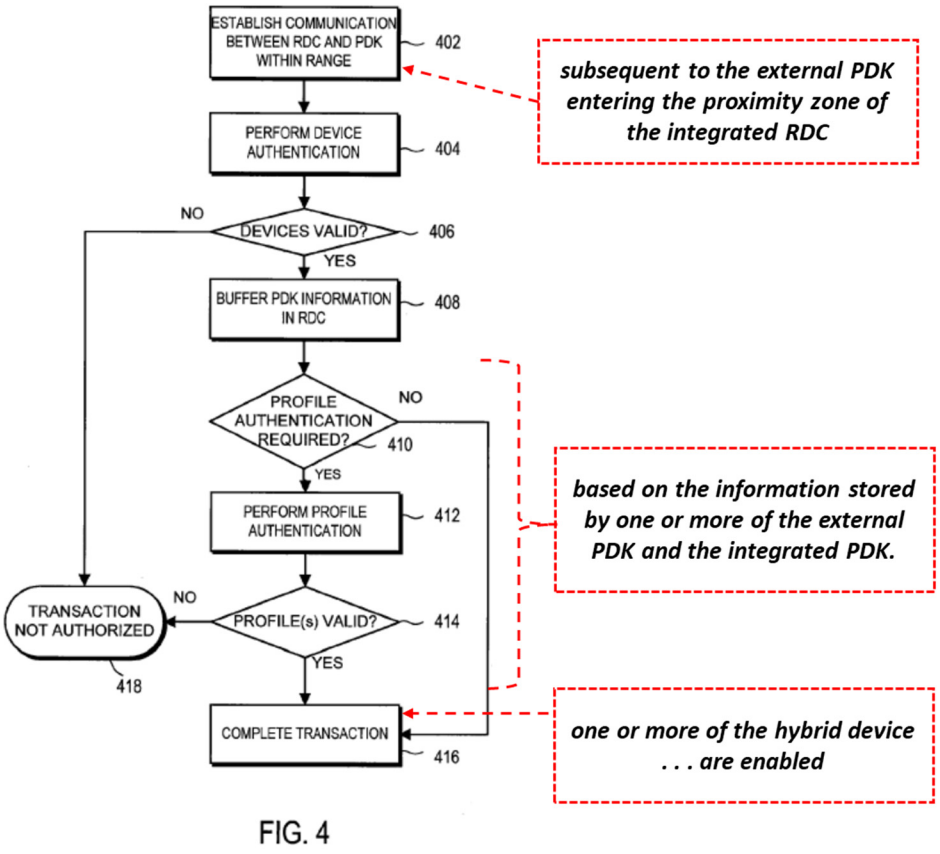


FIG. 4

MS-1005, FIG. 4.

[6] The hybrid device of claim 1, wherein the hybrid device is a cell phone and the hybrid device is enabled to provide cell phone service subsequent to the external PDK entering the proximity zone of the integrated RDC and based on the information stored by one or more of the external PDK and the integrated PDK.

Ground 1A/1B

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

79. *See supra* [5] (Any subsequent use of the hybrid device to enable functionality would be ***subsequent to the external PDK*** (Notary PDK) ***entering the proximity zone of the integrated RDC***.).

80. As discussed above, Giobbi-157 also discloses that its PDK is integrated into a hybrid device, such as a cell phone. MS-1005, ¶[0035] ("The PDK 102 can be standalone as a portable, physical device or can be integrated into commonly carried items … such as a cell phone"); *see supra*, §VI.A, [1.pre]. Giobbi-139 teaches integrating an RDC into the same type of device disclosed in Giobbi-157 (e.g., a mobile device, such as a cell phone). MS-1006, ¶[0088]; MS-1005, ¶[0035]. Therefore, a POSITA would have found obvious that by integrating each device according to their teachings, a hybrid device is created, ***wherein the hybrid device is a cell phone***.

81. Giobbi-139 teaches that the use of PDKs and RDCs can "effectively enabl[e]/disabl[e] the device itself," thus an ***external PDK enable***[s] ***a cell phone***. MS-1006, ¶[0089]. By enabling the cell phone, the device would then be able ***to provide cell phone service***. A POSITA would have found obvious that the enablement of the entire device would subsequently enable the device to ***provide cell phone service***. Alternatively, a POSITA would have found obvious that the integrated RDC connected to other components of the cell phone (such as a cellular modem), would control a component of the hybrid device to enable the device to

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

provide cell phone service. Thus, the hybrid device being ***enabled to provide cell phone service subsequent to the external PDK entering the proximity zone of the integrated RDC*** (hybrid device) ***and based on the information stored by one or more of the external PDK and the integrated PDK***," would have been obvious to a POSITA. *See supra* [5].

[8] The hybrid device of claim 1, wherein the integrated PDK communicates with the external RDC subsequent to the external PDK entering the proximity zone of the integrated RDC.

Ground 1A/1B

82. *See supra* [5] (Any subsequent use of the hybrid device to enable functionality would be ***subsequent to the external PDK*** (Notary PDK) ***entering the proximity zone of the integrated RDC***.).

83. Giobbi-157 teaches that when PDKs come within range of RDCs an initial communication occurs and the RDCs retain connected PDKs in buffer memory. MS-1005, ¶[0062]. Giobbi states that communications "are automatically initiated each time a PDK 102 enters the proximity zone of the Reader 108.Thus, if multiple PDKs 102 enter the proximity zone, the Reader 108 automatically determines which PDKs 102 are valid and buffers the received information from each valid PDK 102." MS-1005, ¶[0062]. Thus, a POSITA would have found obvious that ***the integrated PDK*** of the hybrid device ***communicates with the external RDC*** of a device (e.g., a credit card terminal, an ATM, a second hybrid

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

device) ***subsequent to the external PDK*** (the Notary PDK) ***entering the proximity zone of the integrated RDC*** (during initialization). MS-1007, FIGs. 4a, 4b, and 6; 18:60-22:6.

[9] The hybrid device of claim 1, comprising storage for inheritance information.

Grounds 1A/IB

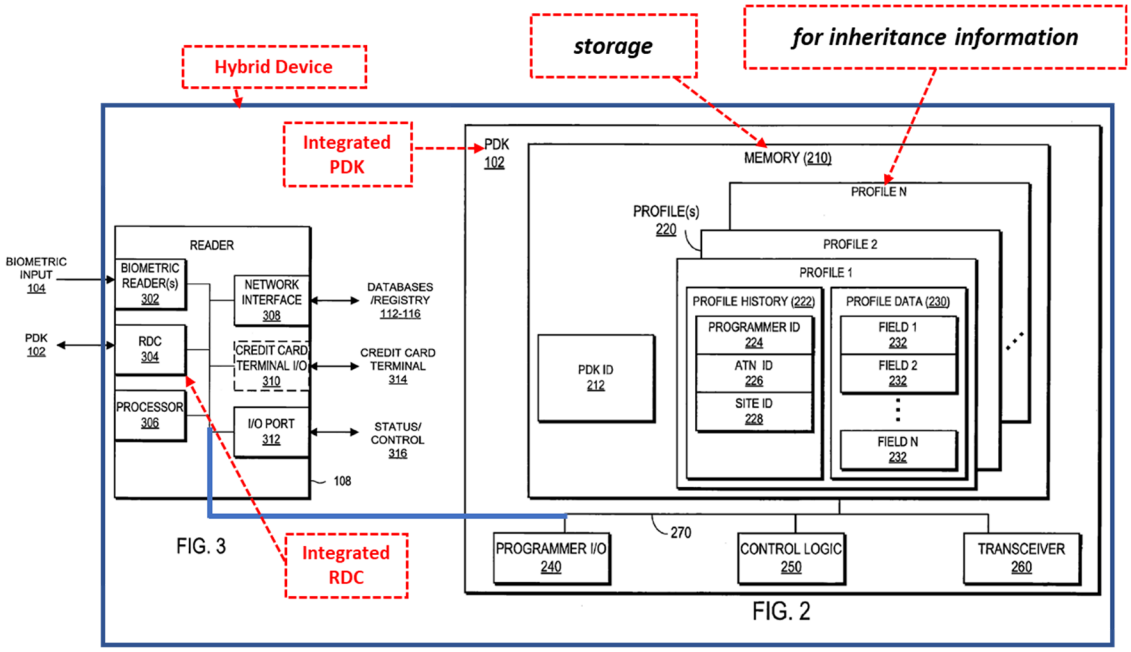
84. The '042 describes "inheritance" as the transfer of some information such as "authorization inheritance." MS-1001, C2: 52-55.

> Authorization inheritance is when a first device passes selected information to a second device and the second device then "inherits" that information for use. The use of the information can be a one-time use during the presence of the first device, multiple uses with or without the presence of the first device or permanent use.
> Furthermore, there are multiple types of inheritance including service inheritance, feature inheritance and personality inheritance. Service inheritance is authorization of the second device for any functionality provided by a given service. Feature inheritance is similar to service inheritance but for a limited set of features offered by a given service. Personality inheritance is where the preferences of a user or holder of a first device are shared with a user or holder of a second device. MS-1001, C17:46-60

85. The profile information within a PDK contains authentication information. MS-1005, ¶¶[0011]-[0012]. When the profiles are copied to another PDK, the other PDK effectively "inherits" the information from the first PDK, thereby enabling the second PDK to "inherit" the permissions of the first PDK. MS-

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

1005, ¶[0043]. Giobbi-157 teaches that a "user can make copies of the PDK 102 or move profiles from one PDK 102 to another once the PDK 102 is unlocked." MS-1005, ¶[0043]. Thus, a POSITA would have found obvious that 1) the storage within the PDK that is within ***the hybrid device compris[es] <u>storage</u> for inheritance information*** and 2) that when a profile is copied from one PDK to another—the information is inherited.



MS-1005, FIGS. 2-3 (modified to incorporate Giobbi-139's teachings).

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

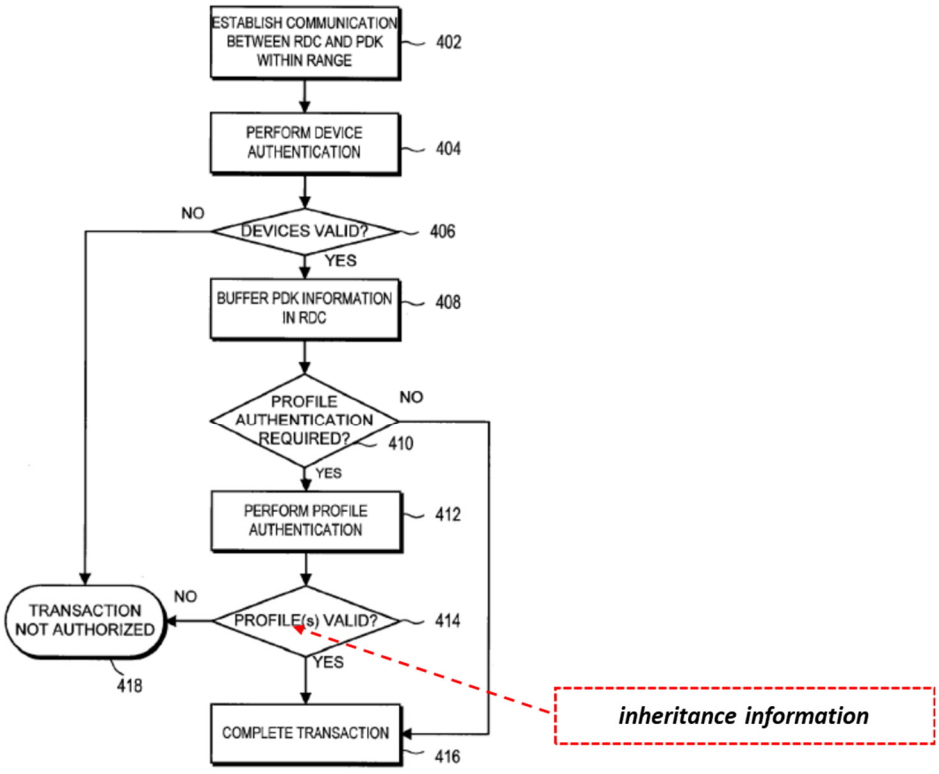


FIG. 4

MS-1005, FIG. 4.

[10.pre] A method comprising:

Grounds 1A/IB

86. *See supra* [1.pre]. Giobbi-157 discloses that its techniques can be implemented as a "method." MS-1005, Abstract, ¶[0011].

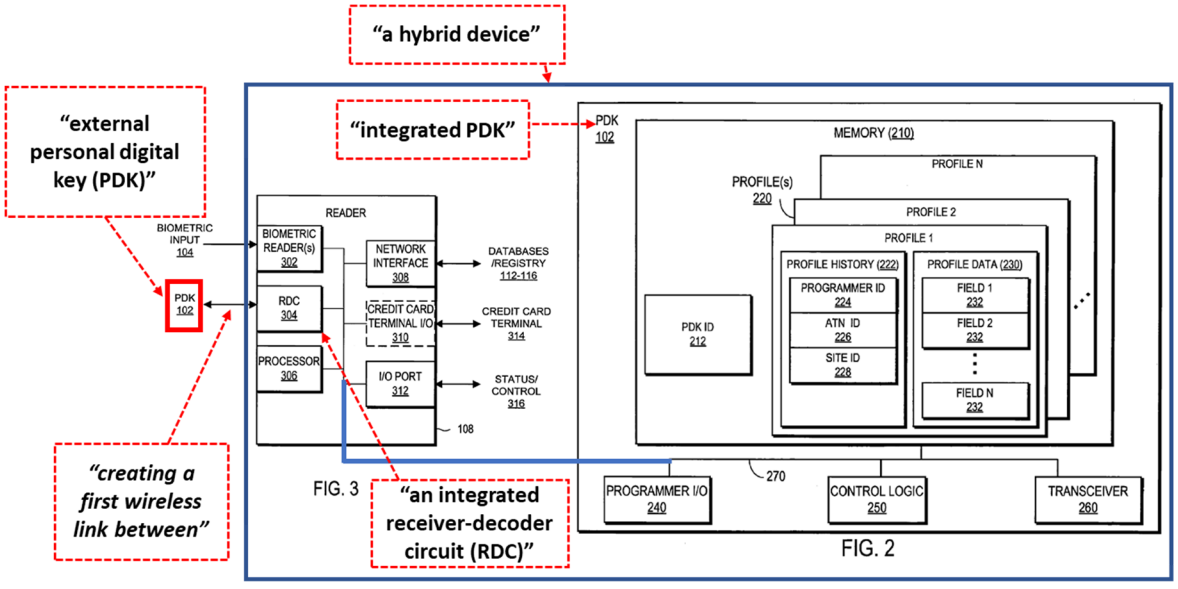
[10.1] creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external personal digital key (PDK), the hybrid device including an integrated PDK and the integrated RDC;

Grounds 1A/IB

87. As described above in [1.1] and [1.2], the Giobbi-157-Giobbi-139 combination includes both an RDC and a PDK ("***the hybrid device including an***

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

integrated PDK and the integrated RDC"). MS-1005, ¶¶[0011], [0027]-[0028], [0050]; *see supra* §VI.D, [1.1]-[1.2]. Additionally, Giobbi-157 discloses that, "[w]hen a PDK 102 [("***an external personal digital key (PDK)***")] comes within range . . . communication is automatically established 402 between the RDC 304 [("***integrated receiver-decoder circuit (RDC)***")] . . . and the PDK 102 . . . when it enters a proximity zone of the [RDC]" ("***creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external personal digital key (PDK)***"). MS-1005, ¶[0059]. Additionally, FIG. 1 of Giobbi-157 (which includes the Reader 103 and integrated RDC of FIG. 3) shows a contextual use of the Giobbi-157-Giobbi-139 combination hybrid device and the "external device[s]." MS-1005, FIG. 1.



MS-1005, FIGS. 2-3 (modified to incorporate Giobbi-139's teachings).

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

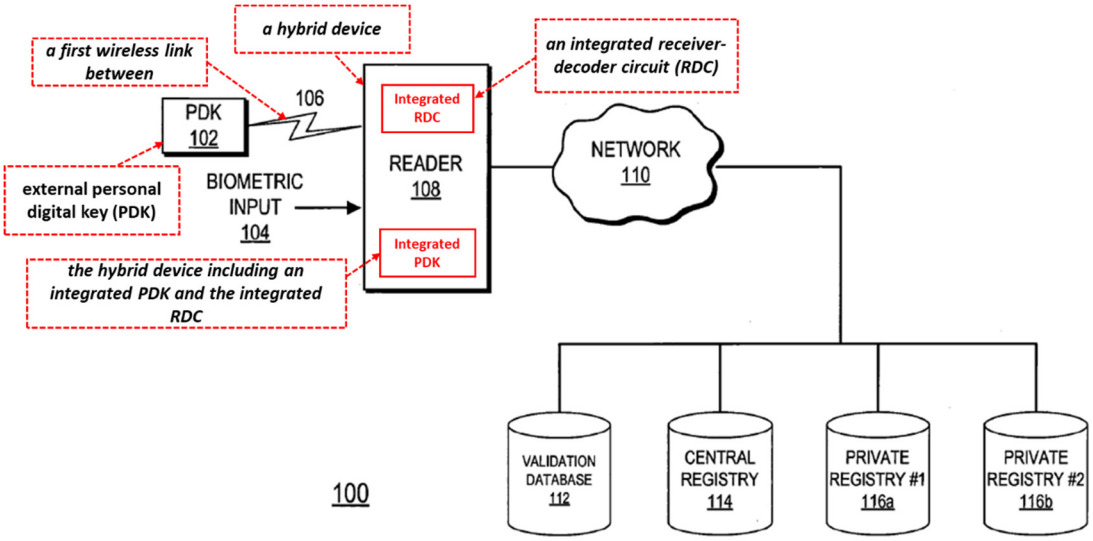


FIG. 1

MS-1005, FIG. 1 (modified to incorporate Giobbi-139's teachings).

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

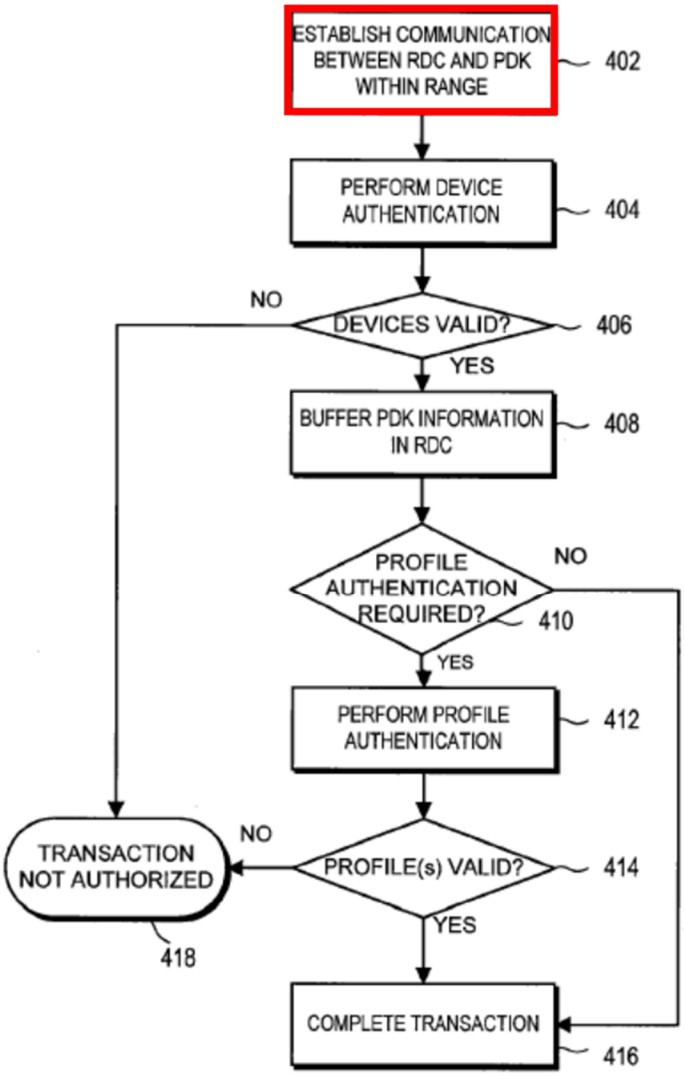


FIG. 4

MS-1005, FIG. 4.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

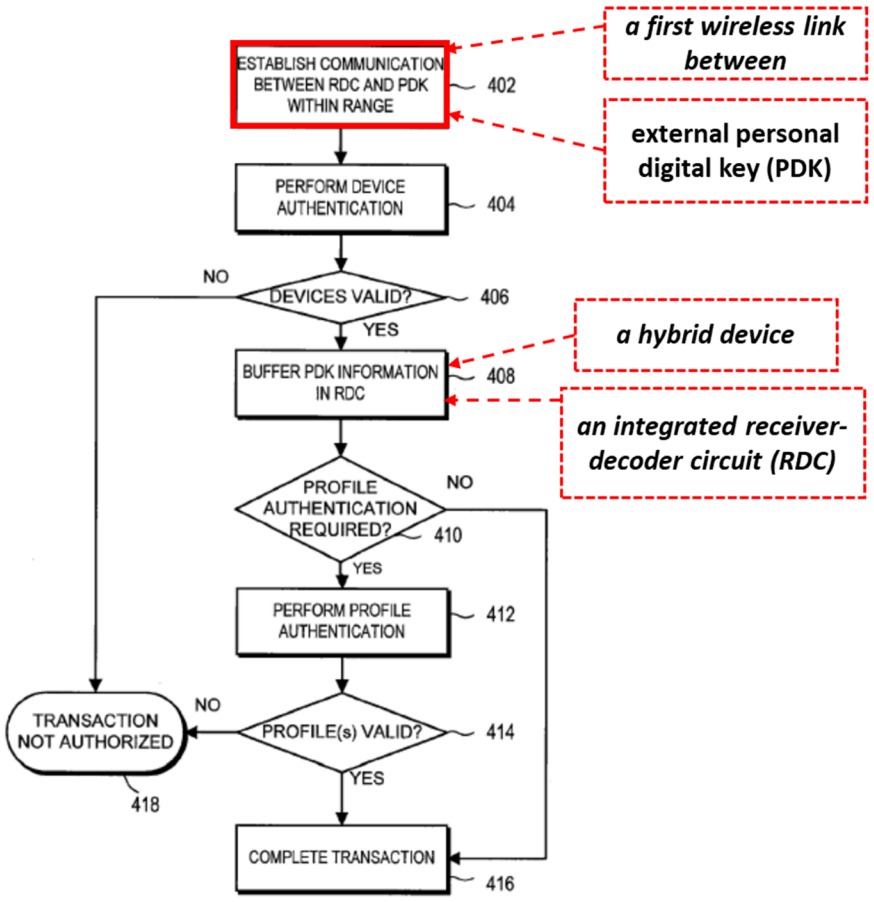


FIG. 4

MS-1005, FIG. 4.

[10.2] receiving a first signal at the integrated RDC via the first wireless link from the external PDK;

Grounds 1A/IB

88. Giobbi-157 discloses that, when an external "PDK 102 [("***the external PDK***")] comes within range of a Reader 108, communication [("***receiving a first signal . . . via the first wireless link***")] is automatically established 402 between the RDC 304[("***at the integrated RDC***"] . . . and the PDK 102 . . . when it enters a proximity zone of the [RDC]". MS-1005, ¶[0059], FIGS. 4-5; *see supra* [1.1], [1.2].

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

When in the proximity zone, the PDK and RDC are coupled by "a ***wireless link***." MS-1005, ¶[0059]. "The RDC 304 receives and analyzes 502 information from the PDK 102 [("***external PDK***")]" ("***receiving a first signal, at the integrated RDC via the first wireless link from the external device***"). MS-1005, ¶[0061]. Additionally, Giobbi-157 provides an example of establishing communication between a PDK and an RDC where "the communication is … initiated by the PDK 102 and acknowledged by the Reader 108" ("***receiving a first signal, at the integrated RDC, via the first wireless link, from the external device***"). MS-1005, ¶[0059].

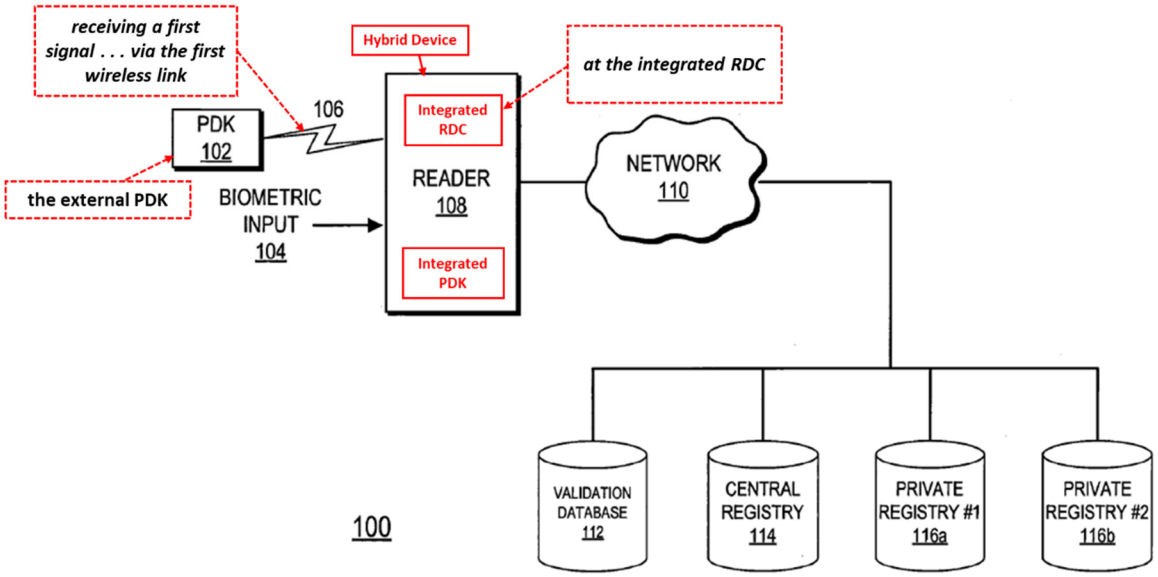


FIG. 1

MS-1005, FIG. 1 (modified to show the hybrid device of Giobbi-157/139).

89. Alternatively, a POSITA would have found obvious from the teachings of Giobbi-157/139, especially from FIG. 1 above and FIG. 4 below, that "[w]hen a

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

PDK 102[("***the external PDK***")] comes within range of a Reader 108 communication [("***receiving a first signal . . .via the first wireless link from the external PDK***")] is automatically established 402 between the RDC 304 [("***the integrated RDC***")], of the Reader 108 and the PDK 102." MS-1005, ¶[0059].

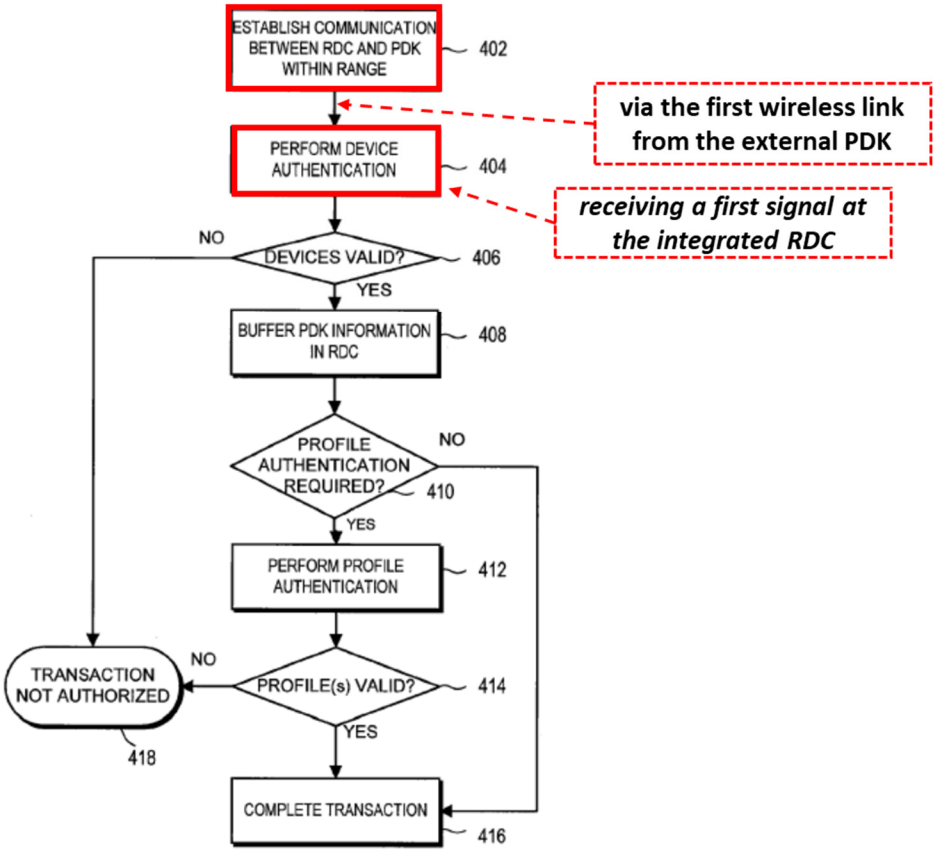


FIG. 4

MS-1005, FIG. 4.

[10.3] generating an enablement signal enabling one or more of an application, a function and a service on one or more of the hybrid device and a device associated with an external RDC; and

Grounds 1A/IB

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

90. As shown in Giobbi-157's FIG. 4, the wireless authentication process between the PDK and RDC "completes a transaction." MS-1005, FIG.4. A "transaction includes ***enabling*** access to secure physical or digital assets (e.g., unlocking a door, opening a vault, providing access to a secured hard drive, etc.)" ("***enabling one or more of an application, a function, and service on . . . a device associated with an external RDC***"). MS-1005, ¶[0063]. Moreover, Giobbi-139 states "access to the storage is ***enabled***/disabled by interrupting the communications path, signaling to the hosting device that the storage is either 'ready' or 'busy,' effectively ***enabling***/disabling the device itself" ("***enabling one or more of an application, a function, and service on . . . the hybrid device***"). MS-1006, ¶[0089]. Accordingly, a POSITA would have found obvious that "enabling access to secure physical or digital assets" (e.g., "unlocking a door" or "opening a vault" ("***one or more of an application, a function, and service***")) or "enabling/disabling the device itself" would require an electronic signal to be ***generated*** ("***an enablement signal***"). Specifically, a POSITA would have understood from the PDK/RDC architecture that when PDKs and RDCs communicate for the purpose of ***enabling one or more of an application, a function and a service on one or more of the hybrid device and a device associated with an external RDC***, that the ***enablement signal*** is first ***generated*** prior to transmission between the PDK and RDC.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

91. Additionally, Giobbi-157 discloses a "trigger" that can be required to allow a transaction to complete or continue. MS-1005, ¶[0065]. Giobbi-157 provides an example where a "biometric contact" ("***an enablement signal***") is ***generated*** by a biometric scanner, for "biometric authentication" of a service ("***enable[ing] one or more of an application, a function, and service***") and provides examples of triggers, to include: "the touch of a finger to a fingerprint scanner, the positioning of a face in front of a facial or retinal scanner, the receipt of a signature, the detection of a voice, the receipt of a DNA sample, RNA sample, or derivatives or any other action that permits the Reader 108 to begin acquiring the biometric input 104." *Id*. Giobbi-139 further teaches that signals between PDKs (either integrated or external) and RDCs can "enable/disable" functions on the device with the integrated RDC ("***enabling one or more of an application, a function and a service on one or more of the hybrid device***"). MS-1006, ¶[0089]-[0091]; *see supra* §VI.D. As seen in FIG. 4 below, because the RDC of the hybrid device or the external RDC can perform the "profile authentication" with the biometric input, the ***enablement signal*** can ***enable[] . . . on one or more of the hybrid device and a device associated with an external RDC***. MS-1005, FIG. 4.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

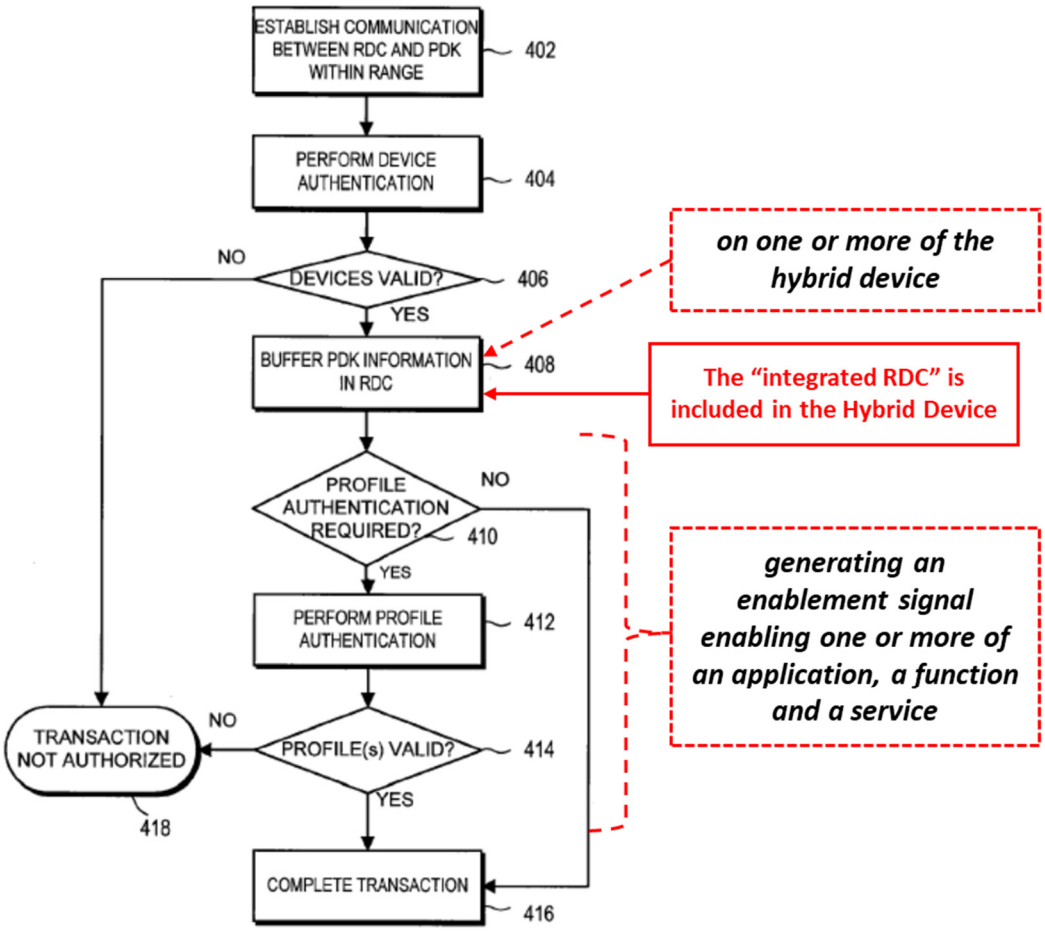


FIG. 4

MS-1005, FIGS. 4.

92. Furthermore, a POSITA would have found obvious from the teachings of Giobbi-139 that the connection between a PDK and RDC can authenticate or enable functionality associated with an RDC. MS-1006, ¶[0067]-[0069], [0087]-[0091] ("effectively enabling/disabling the device itself"). For example, Giobbi-157 teaches situations where the mere presence of a PDK 102 within range of the Reader 108 is by itself a clear indication of the PDK owner's desire to complete a transaction."

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

MS-1005, ¶[0067]. Thus, the generation of these communication signals between a PDK and RDC are the ***generat[ion]*** of ***an enablement signal enabling one or more of an application, a function and a service on . . . a device associated with an external RDC***").

[10.4] sending the enablement signal to one or more of the hybrid device and the device associated with an external RDC.

Grounds 1A/IB

93. As discussed above, Giobbi-157 discloses a wireless authentication process ("***sending the enablement signal***") between the PDK and RDC that "completes a transaction." MS-1005, FIG.4. The authentication is first performed after a PDK has connected to an RDC (either the hybrid device's integrated RDC or second device that includes an external RDC). ("***sending the enablement signal to one or more of the hybrid device and the device associated with an external RDC***."). MS-1005, ¶[0074], FIGS. 3, 7D; *see supra* [14.1]-[14.3]. Giobbi-157 teaches that authentication of a PDK is used for "authorizing a transaction to be processed at the Reader 108 [device containing an RDC]" ("***the hybrid device***" or "***the device associated with an external RDC.***"). MS-1005, ¶[0033], FIG. 3.

94. Giobbi-139 teaches that a PDK (external to the hybrid device) can enable functions on a device or the device itself. MS-1006, ¶¶[0088-0090]. For example, Giobbi-139 teaches that the authentication process can enable the playing of music on a device:

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

> In a preferred embodiment, the device continues to play the digital content only while the physical key [(PDK)] is sufficiently close to the device to communicate . . . If the physical key [(PDK)] is moved out of range, the device is no longer enabled to decrypt and play the digital content. MS-1006, ¶[0037].

95. Thus, a POSITA would have found obvious that an external PDK causes the RDC of the hybrid device to send the enablement signal to a component within the hybrid device itself to enable a function within the hybrid device (such as a cell phone) ("***sending the enablement signal to one or more of the hybrid device***"). *See supra* [1.3], [4]; MS-1006, ¶¶[0037], [0088-0090].

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

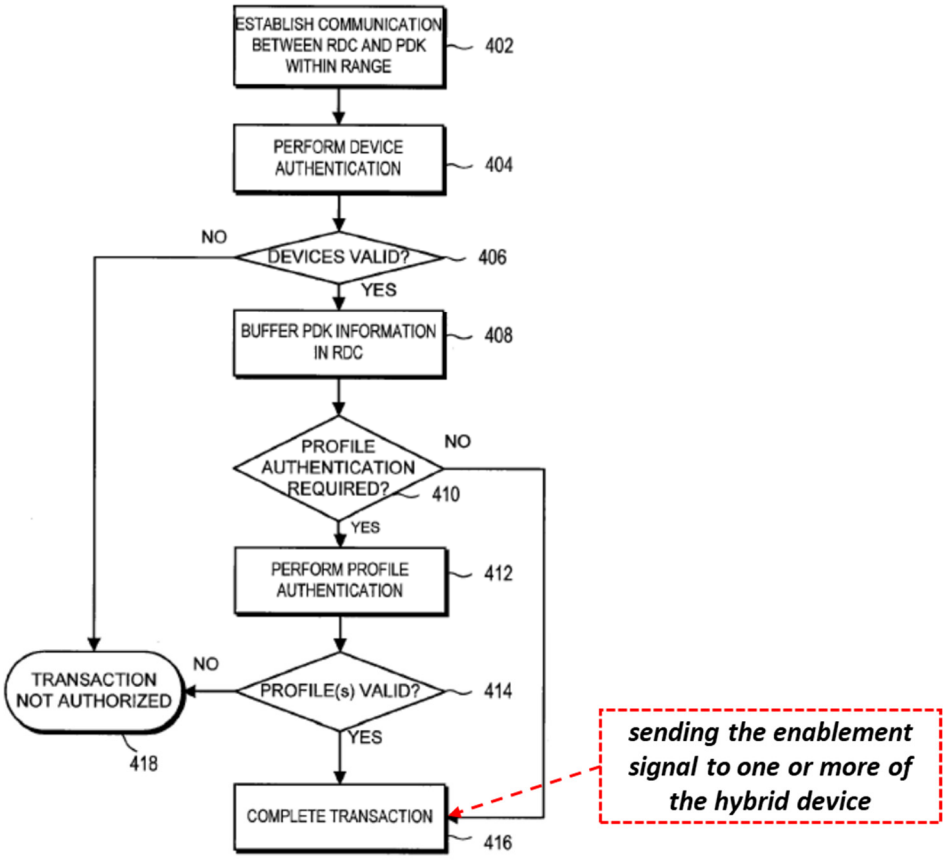


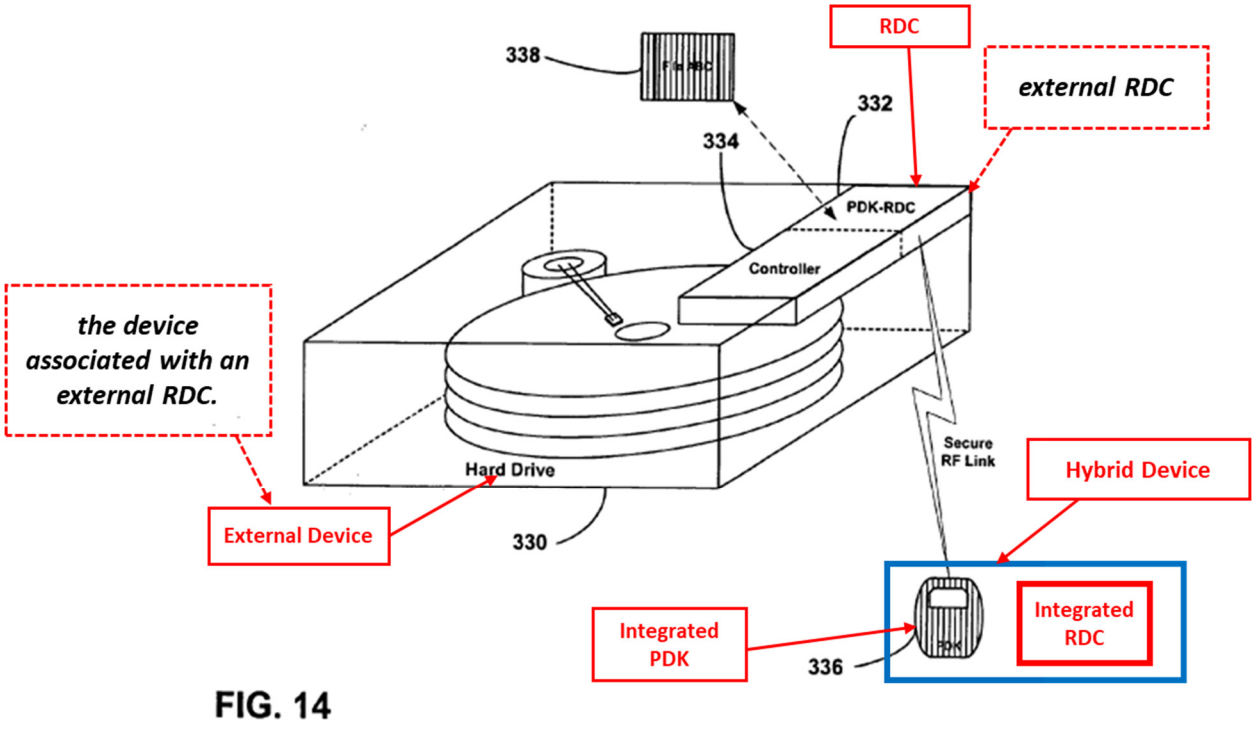
FIG. 4

MS-1005, FIG. 4.

96. Additionally, the hybrid device can use the integrated PDK to ***send[] the enablement signal to . . .the device associated with an external RDC*** and enable "an application, a function and a service" on the device associated with "***an external RDC***." MS-1005, ¶¶[0057], [0061-0063]; MS-1006, ¶¶[0037], [0088-0090]. For example, Giobbi-157 teaches that this can occur automatically, when "the mere presence of a PDK 102 within range of the Reader 108 is by itself a clear indication of the PDK owner's desire to complete a transaction." MS-1005, ¶[0067]. As seen

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

below in FIG. 14, Giobbi-139 also teaches this architecture such that, a hybrid device within range of an external RDC (through the integrated PDK) can "***send[] the enablement signal to one or more of . . .the device associated with an external RDC***" MS-1005, ¶¶[0057], [0061-0063]; MS-1006, ¶[0037], [0081-0083], [0088-0090]. A POSITA would have understood that the automatic communication and authentication of a PDK that completes the "transaction" would include ***sending the enablement signal to . . . the device associated with an external RDC***.



MS-1006, FIG. 14.

[11] The method of claim 10, wherein the hybrid device is a cell phone and the enablement signal is sent to the cell phone enabling one or more of a service, a feature and a functionality of the cell phone.

Grounds 1A/IB

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

97. *See supra* §VI.D, [6], [10.3], [10.4] ("***wherein the hybrid device is a cell phone***").

98. As discussed above, claim 10 recites "*sending the enablement signal to ... the hybrid device*." *See supra* [10.4]. Here, claim 11 recites a "cell phone" as an example of a "hybrid device." Thus, for the reasons stated above, "***the enablement signal is sent to the cell phone***" *(the "hybrid device")*. *See supra* [10.3]-[10.4].

99. Giobbi-139 teaches that a device including an RDC (the hybrid device cell phone) can be "effectively enabl[ed]/disabl[ed]" using a PDK ("***enabling one or more of a service, a feature and a functionality of the cell phone***"). MS-1006, ¶[0089]. Giobbi-157 teaches that the entire "system and method provide[s] efficient, secure and highly reliable authentication for transaction processing and/or access control ***applications***." MS-1005, ¶[0011]. Giobbi-157 further details the enablement of a "transaction" which "includes enabling access to secure physical or digital assets (e.g., unlocking a door, opening a vault, providing access to a secured hard drive, etc.)." ("***enabling one or more of a service, a feature and a functionality of the cell phone***")

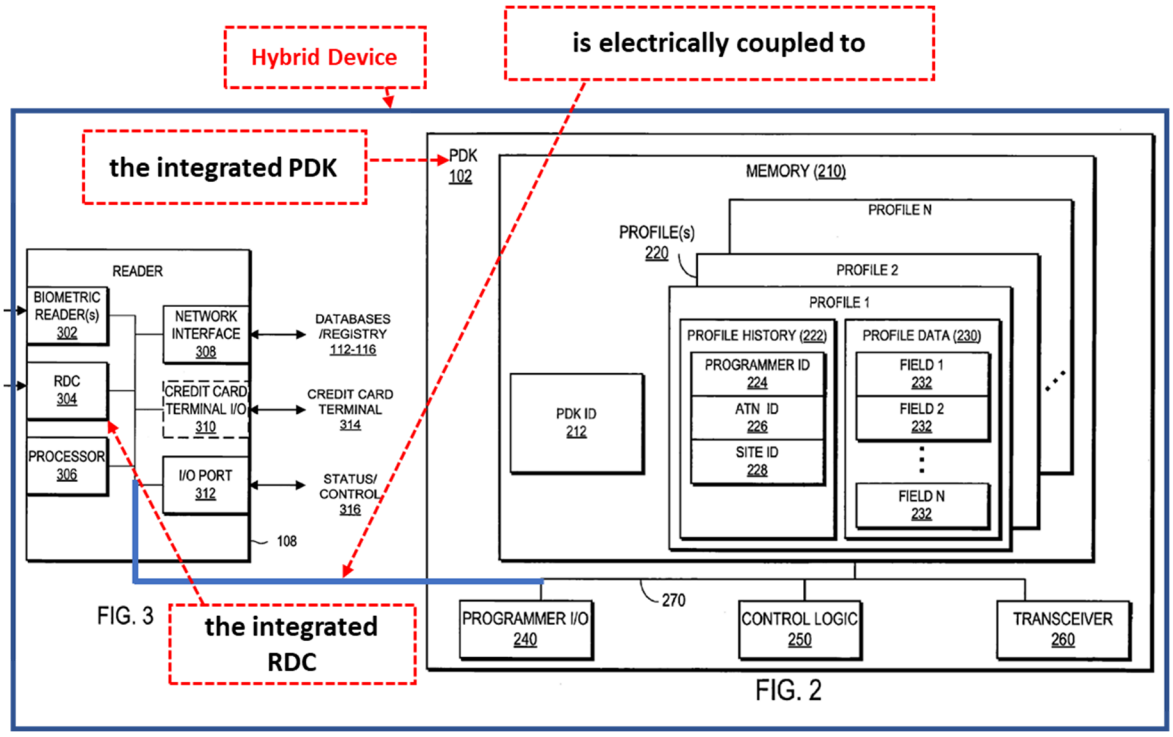
[13.1] The method of claim 10, wherein the integrated PDK is electrically coupled to the integrated RDC, and the method comprises:

Grounds 1A/IB

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

100. *See supra* [1.2] ("*the integrated RDC coupled to the integrated PDK by a first signal line for communication*"), [10.3]-[10.4] (*generating/sending an "enablement signal" on the hybrid device*)

101. The hybrid device includes an ***integrated PDK*** that ***is electrically coupled to the integrated RDC***. *See supra* [1.2]; §VI.D (explaining how an RDC is necessary to register Notary/Administrator PDK IDs into another PDK.)



MS-1005, FIGS. 2-3 (modified to incorporate Giobbi-139's teachings).

[13.2] sending the enablement signal from the integrated RDC to the integrated PDK;

Grounds 1A/IB

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

102. *See supra* [1.2] ("*the integrated RDC coupled to the integrated PDK by a first signal line for communication*"), [1.4] ("*the integrated RDC . . . enabling one or more of an application, a function, and a service on . . . the hybrid device . . .*")

103. *See supra* [5], [6], and [8] (Any subsequent use of the hybrid device to enable functionality would be *subsequent to the external PDK* (Notary PDK) *entering the proximity zone of the integrated RDC*.).

104. Giobbi-157 teaches that the PDK profiles store information including "the specific hardware, Notary, and site used at the time the profile data was created and stored to the PDK." MS-1005, FIG.2, ¶[0044]. During the initialization process a RDC must be used to communicate with the Notary PDK. MS-1005, ¶[0050]. A POSITA would have found obvious that during the initialization process, that the integrated RDC is ***sending the enablement signal from the integrated RDC*** (received from the Notary PDK) ***to the integrated PDK***. For example, during the initialization process the Notary PDK "administers [(enables)] the acquisition and storage of information in the PDK." MS-1005, ¶[0029]. During this process, the Notary PDK signs the PDK being initialized with the Notary's PDK ID number. MS-1005, ¶[0044]. Based on the discussed PDK/RDC architecture, a POSITA would have found obvious the use of an RDC (the integrated RDC) to retrieve the Notary PDK's ID through standard PDK/RDC communication methods discussed. In this example, the RDC then ***send[s] the enablement signal*** (at least some of which

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

includes the Notary PDK's ID) ***from the integrated RDC*** (communicating with the Notary PDK) ***to the integrated PDK*** that is being initialized. MS-1005, ¶[0044].

105. Alternatively, Giobbi-139 teaches "enabling/disabling" a device entirely, or that "access to the storage is enabled/disabled by interrupting the communications path, signaling to the hosting device that the storage is either 'ready' or 'busy,'" ("***sending the enablement signal***"). MS-1006, ¶¶[0087-0090]. Therefore, an external PDK can be used to protect digital storage (an integrated PDK's memory) within the hybrid device. For example, Giobbi-139 teaches that:

> As when utilized in PDK hard drives [devices that include an RDC], the PDK's Security features provide the same convenient, non-intrusive, wireless security mechanism for the above-defined devices. This security mechanism protects any data stored on such devices in the event they are ever stolen, left unattended, or even purposely "disabled' to prevent access to sensitive content (i.e. preventing minors from accessing adult files, websites, etc.). When the associated PDK-Key(s) is not present, these devices and their Storage means are locked and disabled. MS-1006, ¶[0090].

106. Giobbi-139, therefore, teaches the protection of data within the hybrid device (e.g., the profile data of the integrated PDK) from theft, or when left unattended, or if the user wishes to purposefully disable the integrated PDK, through use of an external PDK. MS-1006, ¶[0090]. Giobbi-139 also teaches that a component or device controlled by an RDC ("***the integrated RDC***") "will only

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

function when the associated PDK-Key 336 is within range," showing that individual components of a device (at least some portions of ***the integrated PDK***) can be controlled with an external PDK. MS-1006, ¶[0071]. For example, a POSITA would have understood that during an authentication process that relies on an external PDK (e.g., PDK-Key 336) to access components within a hybrid device, the integrated RDC of the hybrid device, upon successfully authenticating the external PDK, ***sends the enablement signal from the integrated RDC*** to one or more internal components of the hybrid device to enable access to those components. MS-1006, ¶¶[0071], [0090]. A POSITA would have understood that, in some implementations, the integrated PDK could be one of these internal components and, therefore, that, in this circumstance, the integrated RDC ***sends the enablement signal from the integrated RDC to the integrated PDK***.

[13.3] creating a second wireless link between the integrated PDK and an external RDC; and

Grounds 1A/IB

107. The "first wireless link" of claim 10 is between the integrated RDC and an external PDK. *See supra* [10.1].

108. Giobbi-157 teaches that RDCs automatically communicate with multiple, distinct PDKs that are within the proximity zone. MS-1005, ¶[0062]. Therefore, when ***the integrated PDK*** "comes within range of a Reader 108[("***external RDC***")], communication is automatically established[("***create[es] a***

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

second wireless link")] 402 between the RDC 304 [("***the external RDC***")] of the Reader 108 and the PDK 102 [("***the integrated PDK***")]." MS-1005, ¶[0059].

109. As Giobbi-157 repeatedly shows, communication between a PDK and an RDC is automatic within range. MS-1005, FIG. 4, ¶[0059]. In Giobbi-157's examples, the PDK and RDC ***creat[e] a second wireless link between the integrated PDK and an external RDC*** to begin the PDK/RDC communication and authentication process. MS-1005, ¶¶[0011]-[0012], [0026]-[0028], [0030], FIGS. 1-4.

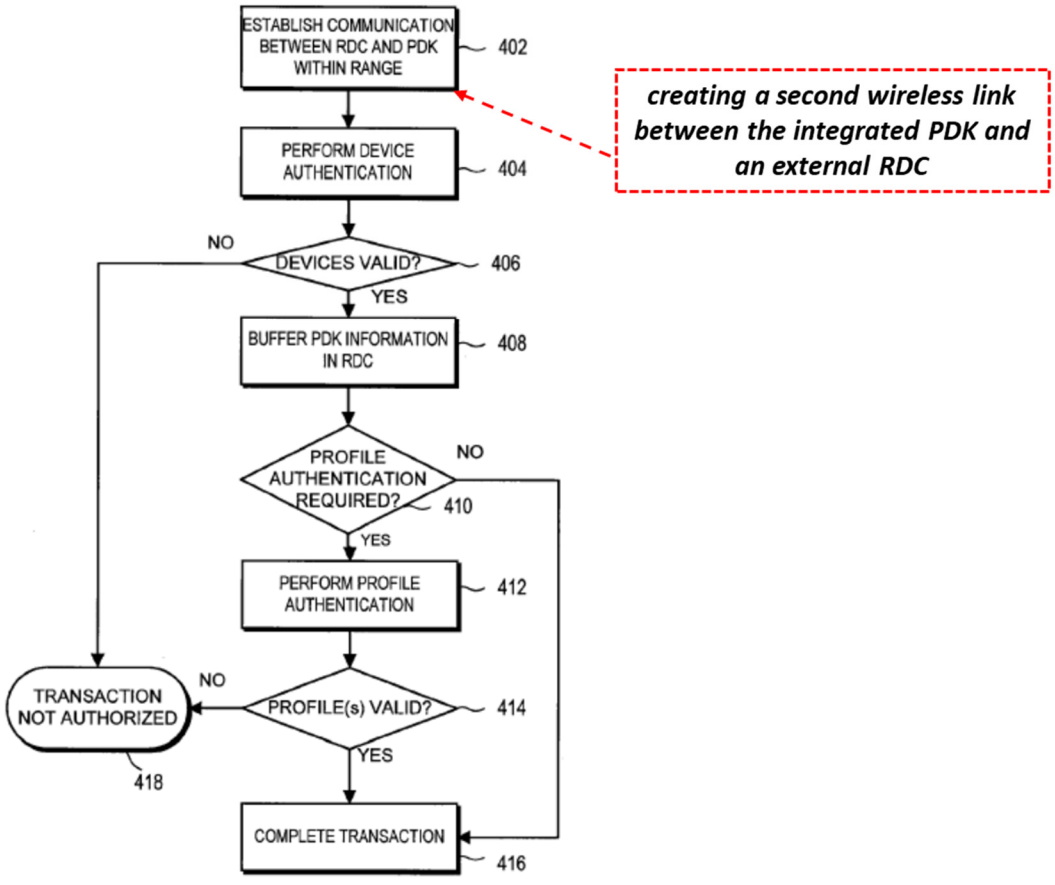


FIG. 4

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

MS-1005, FIG. 4

[13.4] sending the enablement signal from the integrated PDK to the external RDC using the second wireless link.

Grounds 1A/IB

110. *See supra* [10.4] (sending the enablement signal to . . . the device associated with an external RDC).

111. Giobbi-157 teaches that authentication of a PDK is used for "authorizing a transaction to be processed at the Reader 108 [(device containing an external RDC)]." MS-1005, ¶[0033], [0059], FIG. 3-4. Giobbi-139 teaches that a PDK can enable functions on a device or the device itself. MS-1006, ¶¶[0088-0090]. For example, Giobbi-139 teaches that the authentication process can enable the playing of music on a device:

> In a preferred embodiment, the device continues to play the digital content only while the physical key [(PDK)] is sufficiently close to the device to communicate . . . If the physical key [(PDK)] is moved out of range, the device is no longer enabled to decrypt and play the digital content. MS-1006, ¶[0037].

112. Thus as both Giobbi-157 and Giobbi-139 describe, the integrated PDK of the hybrid device can automatically establish a wireless link with an external RDC. MS-1005, ¶[0033], [0059], FIG. 3-4; MS-1006, ¶¶[0088-0090]. The hybrid device can then ***send[] the enablement signal from the integrated PDK to the external***

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

RDC using the second wireless link. MS-1005, ¶[0033], [0059], FIG. 3-4; MS-1006, ¶¶[0088-0090].

[14] The method of claim 11, wherein the integrated PDK modifies the enablement signal to produce a modified enablement signal, and the modified enablement signal is sent from the integrated PDK to the external RDC.

Grounds 1A/IB

113. Giobbi-157 first teaches that signals between a PDK and RDC can be unencrypted stating that "[g]enerally, initial communication between the Reader 108 and the PDK 102 is not encrypted in order to provide faster and more power efficient communication." MS-1005, ¶[0059]

114. Giobbi-157 then teaches that the data sent from a PDK to an RDC is encrypted prior to transmission. MS-1005, ¶¶[0037], [0050], claim 30. Giobbi-139 further states that broadcasted content can be modified where the "[t]he modification is that the broadcast content is transmitted in a copy protected format (such as the DVD standard known as Content Scramble System (CSS))." MS-1006, ¶[0055]. For example, the ***integrated PDK*** can encrypt data (***modifies the enablement signal to produce a modified enablement signal***) for transmission over a secure link (***and the modified enablement signal is sent from the integrated PDK to the external RDC***). MS-1005, ¶[0047]. Then the RDC "provides the wireless interface to the PDK 102. Generally, the RDC 304 wirelessly receives data from the PDK 102 in an

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

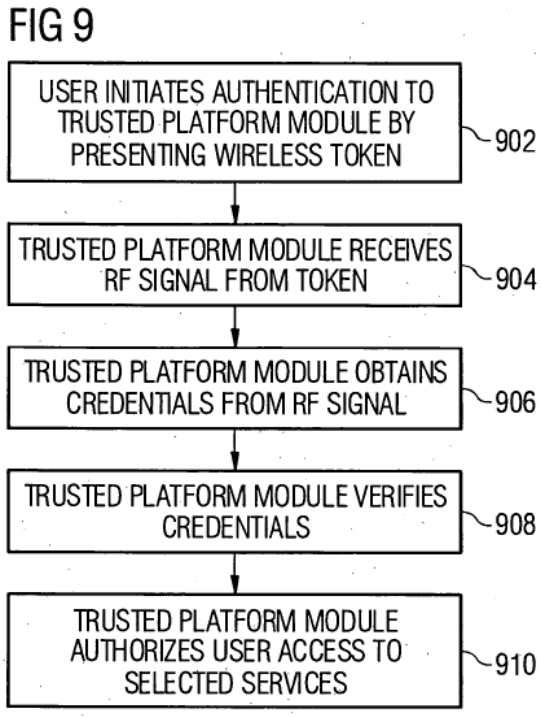
encrypted format and decodes the encrypted data for processing by the processor 306." MS-1005, ¶[0050].

VII. ANALYSIS OF BROADCOM

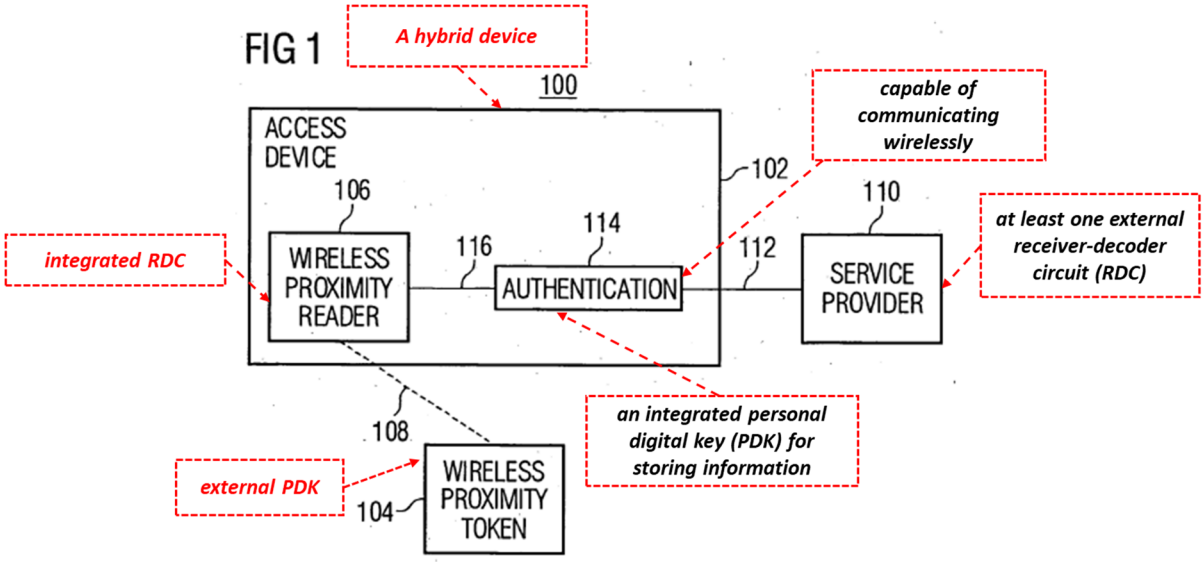
A. Overview of Broadcom

115. Broadcom discloses a system for secured access to a service based on a wireless device coming withing the proximity of a reader. MS-1008, Abstract; ¶¶[0009]-[0016]. Broadcom teaches that a user's credentials can be stored on an RFID token, and this token and the associated authentication credentials may be read by an RFID reader located in an Access Device. *Id*. The Access Device (including the RFID reader) can authenticate the RFID token and permit access to the secured service after authentication. *Id*. This system is illustrated below in Figure 1.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782



MS-1008, FIG. 9.



MS-1008, FIG. 1 (annotated).

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

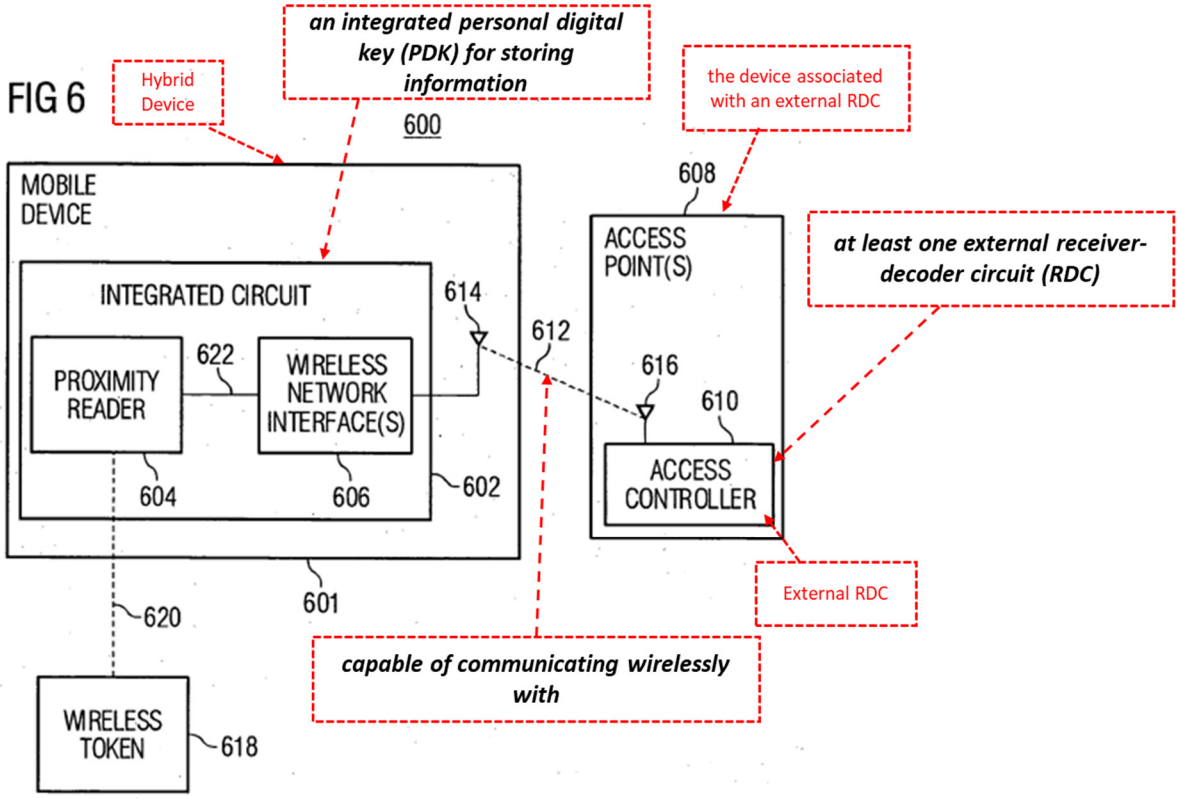
116. The authentication information is stored securely within memory that is "tamper resistant," and "is not exposed in the mobile device." MS-1008, ¶¶[0013], [0134], [0167], [0187]. The "authentication information" and "credentials" are secured in this memory. MS-1008, ¶¶[0013], [0134], [0167], [0187], [0192].

117. As shown in the figure, Access Device 102 requests access to a service provider 110 and "verif[ies] that the information sent from the token 104 includes a credential associated with an authorized user and or access device." MS-1008, ¶¶[0113]-[0119]. In some instances, "the user may be asked to input a password and/or provide a biometric (e.g., a fingerprint) to a biometric reader to further verify the authenticity of the user." MS-1008, ¶¶[0114]-[0115], [0181]. This input can be the presentation of a token to the reader. MS-1008, ¶¶[0130], [0181]. Example tokens include: "smart cards, credit cards, dongles, badges, biometric devices such as fingerprint readers, mobile devices such as cellular telephones, PDAs, etc." MS-1008, ¶¶[0130], [0181].

118. Additionally, Broadcom discloses enabling "computer functions to be securely executed" via this method. MS-1008, ¶¶[0177]-[0180], [0184]-[0186]. The authentication of the device and the "user may then be allowed to access the secured service." MS-1008, ¶[0010].

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

119. Broadcom discloses that the Access Device 102 can be a mobile phone which facilitates access to an access point for mobile communications, as illustrated below in FIG 6. MS-1008, ¶¶[0123]-[0124], [0191].



MS-1008, FIG. 6 (annotated).

B. Analysis

[10.pre] A method comprising:

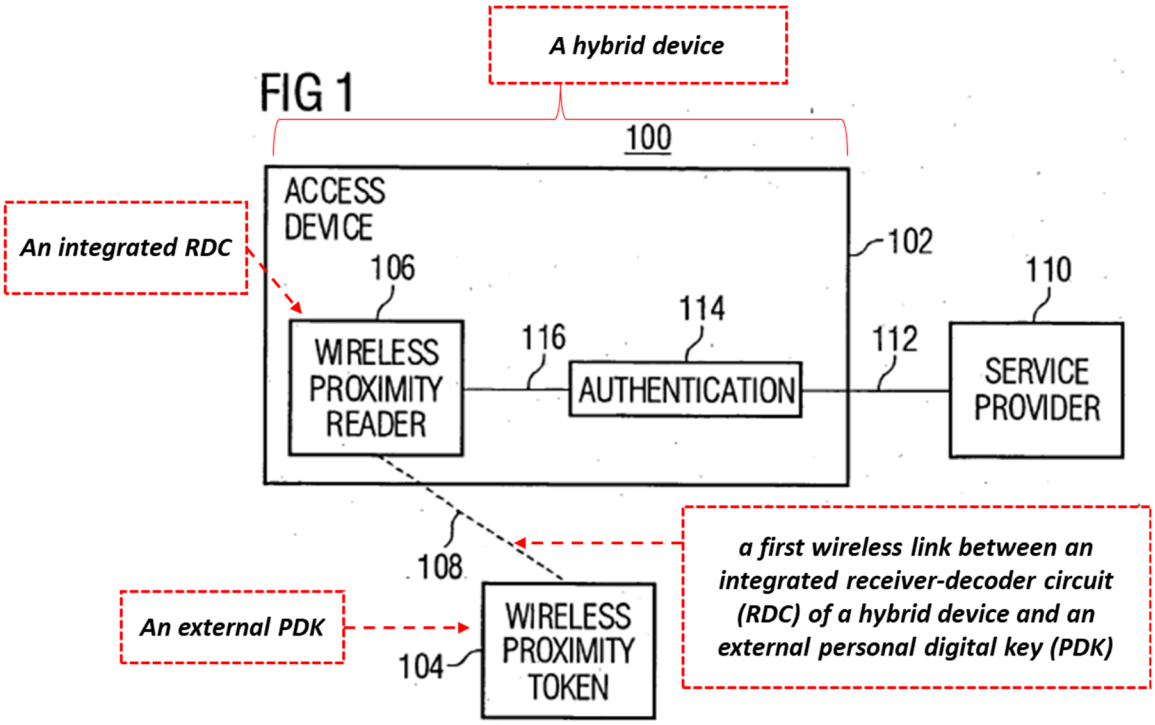
120. Broadcom discloses that its techniques can be embodied in a "method." MS-1008, ¶¶[0009]-[0010].

[10.1] creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external personal digital key (PDK), the hybrid device including an integrated PDK and the integrated RDC;

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

121. Broadcom discloses a "***hybrid device***," ("a device comprising an integrated, secure memory storing local, secured information and an integrated receiver-decoder circuit" or "a device comprising an integrated personal digital key (PDK) and an integrated receiver-decoder circuit"). MS-1008, ¶¶[0110]-[0119], FIGS. 1, 6; *see supra* §IV.A. Broadcom's "access device 102" reads credentials stored on a "wireless proximity token 104," ("an external PDK") using a "wireless proximity reader 106" ("an integrated reader-decoder circuit (RDC)"). MS-1008, ¶¶[0110]-[0119], FIGS. 1, 6. Broadcom also discloses that "the information provided by the token may be maintained within the access device 102 in a secure manner" using an "authentication component 114" (and an "integrated circuit 312" and "data memory 314" disclosed in FIG. 3) (an "integrated, secure memory storing local, secured information" and an "integrated personal digital key (PDK)"). MS-1008, ¶¶[0116]-[0118], [0135]-[0137], FIGS. 1, 3. Additionally, Broadcom's access device 102 can be a "mobile device," such as a "cellular phone." MS-1008, ¶¶[0125], [0130], [0162]-[0163], [0195], FIGS. 1, 3, 6. Accordingly, Broadcom renders obvious "a device comprising an integrated . . . (PDK) and an integrated . . . (RDC)" for the reasons discussed above. *See supra,* §§IV.A, VII.A. As shown below in FIGS. 1 and 3, Broadcom's cell phone includes an integrated PDK and an integrated RDC (a "***hybrid device***"). *Id*.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782



MS-1008, FIG. 1.

122. Broadcom, with its detailed FIG. 3 illustration and FIG. 6 illustration of a mobile device, also teaches "an operably connected collection of elements including an antenna and a transceiver for communicating with a RDC and a controller and memory for storing information particular to a user" as required by the above construction of a "***PDK***." MS-1008, FIGS. 3, 6; *see supra,* §IV.A. A POSITA would have recognized or found obvious that the "authentication component 114" would have included all of the features of a "PDK" (e.g., "an antenna … a transceiver … a controller and [a] memory …") because Broadcom discloses that the authentication component 114 performs functions that would have

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

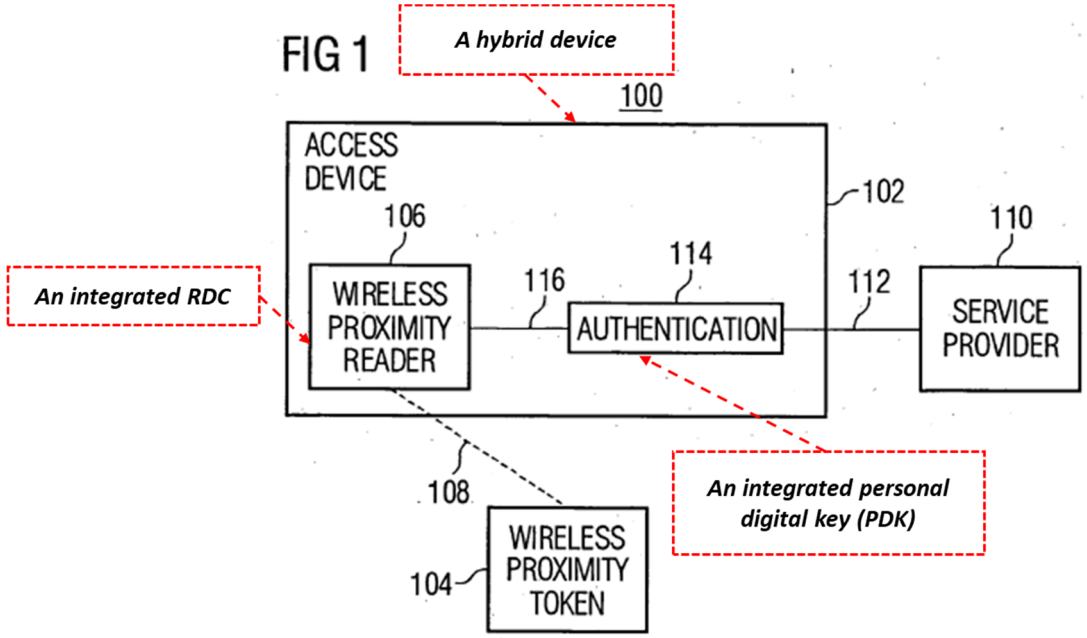
required these components. MS-1008, ¶¶[0116]-[0118] ("a cryptographically secured communication channel may be established between the authentication component 114 and the service provider 110," ("an antenna … a transceiver"), "the authentication component 114 may process (e.g., encrypt or sign) the information before sending it to the service provider 110" ("a controller"), and "authentication information may include information from the token" (a "memory for storing information particular to a user"). A POSITA would have recognized that the subsequent figures of Broadcom (e.g., FIG. 3) provide implementation details for the overview presented in FIG. 1. This is because the authentication component 114 is clearly expanded to show possible internal components in subsequent figures. Each figure builds on the complexity of the first, despite the fact that the numbering of components is not consistent across the figures.

123. Additionally, Broadcom discloses that its access device 102 includes a "wireless proximity reader 106" ("***an integrated reader-decoder circuit (RDC)***") to "receive signals 108" from a "wireless proximity token 104" that is "proximate to the access device 102." MS-1008, ¶¶[0110]-[0119], FIGS. 1, 6. Broadcom also discloses, as part of its detailed FIG. 3 view, an "RFID reader 306" ("***integrated RDC***") that is connected to a "data memory 314" via a "data bus 320." MS-1008, ¶¶[0133]-[0137], FIG. 3. Accordingly, Broadcom discloses "a component or collection of components, capable of wirelessly receiving data in an encrypted

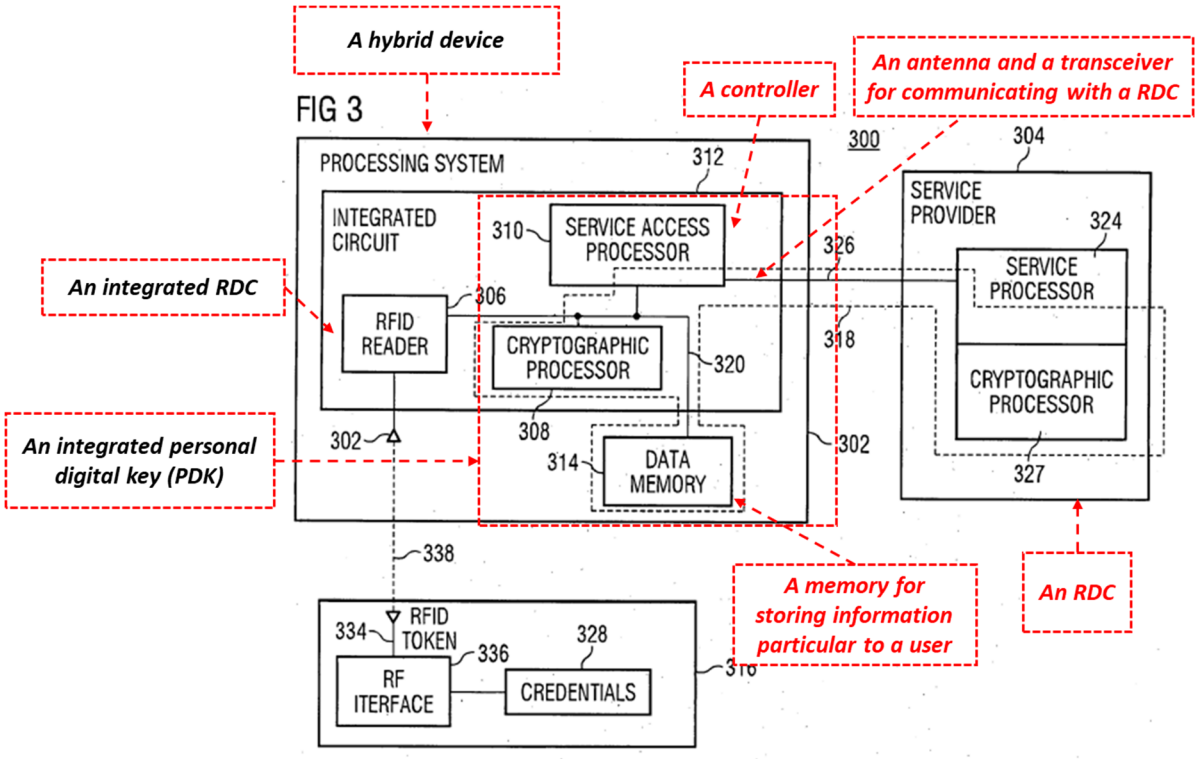
APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

format and decoding the encrypted data for processing" as required by the district court's construction for an "***integrated reader-decoder circuit (RDC)***." *See also* MS-1008, ¶¶[0158], [0184] *and supra*, §§IV.C. In more detail, Broadcom discloses that its reader wirelessly receives encrypted authentication information from the token and decodes the encrypted authentication information by extracting information, e.g., the user's credentials, from the encrypted authentication information for further processing by the authentication component to securely identify the specific token. *See also* MS-1008 ¶[0184], providing further detail of the processing of the token's signals by the reader, indicating that the reader "extracts any embedded information [from the signals] such as the user's credentials"; ¶[0158], providing further detail of the information in the signals wirelessly received by the reader, noting that the signals include "authentication information," such as "network authentication credentials," and further noting that "some or all of this authentication information may be encrypted"; FIG. 1, showing the reader providing its output to the authentication component 114 over line 116 for processing; ¶[0116], disclosing that the authentication component performs a "determination of whether the token 104 is proximate the access device 102 in a secure manner"; and ¶[0118], noting the function of the authentication component to "provide[] [a] cryptographically reliable authentication that the information is from a specific token that is proximate to the particular access device."

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

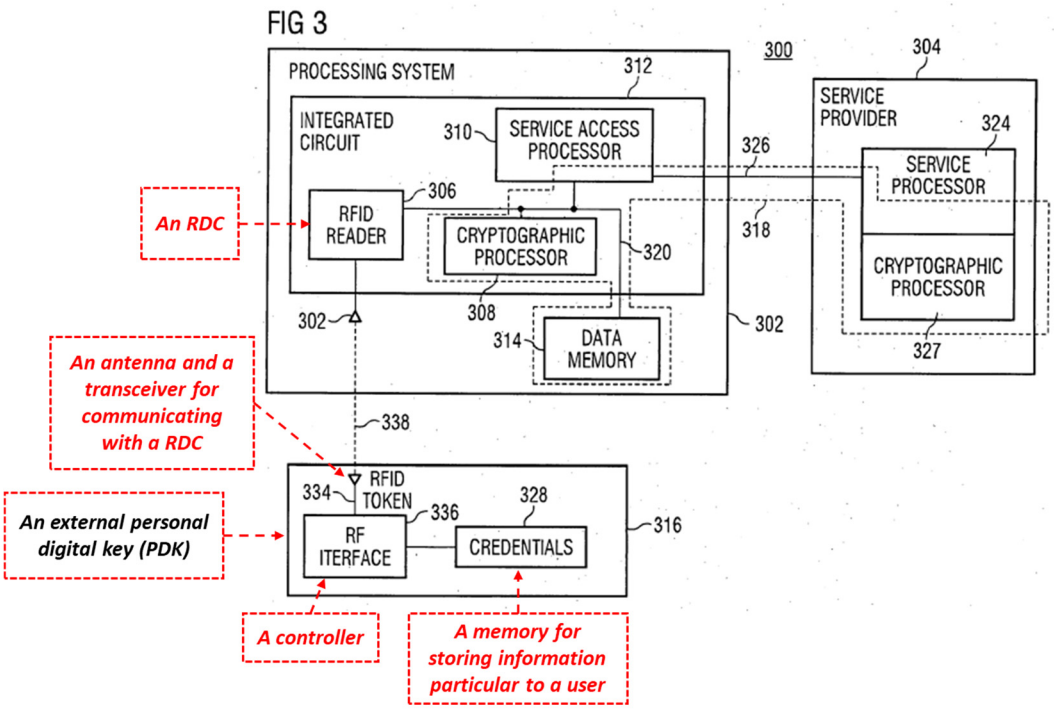


MS-1008, FIG. 1.

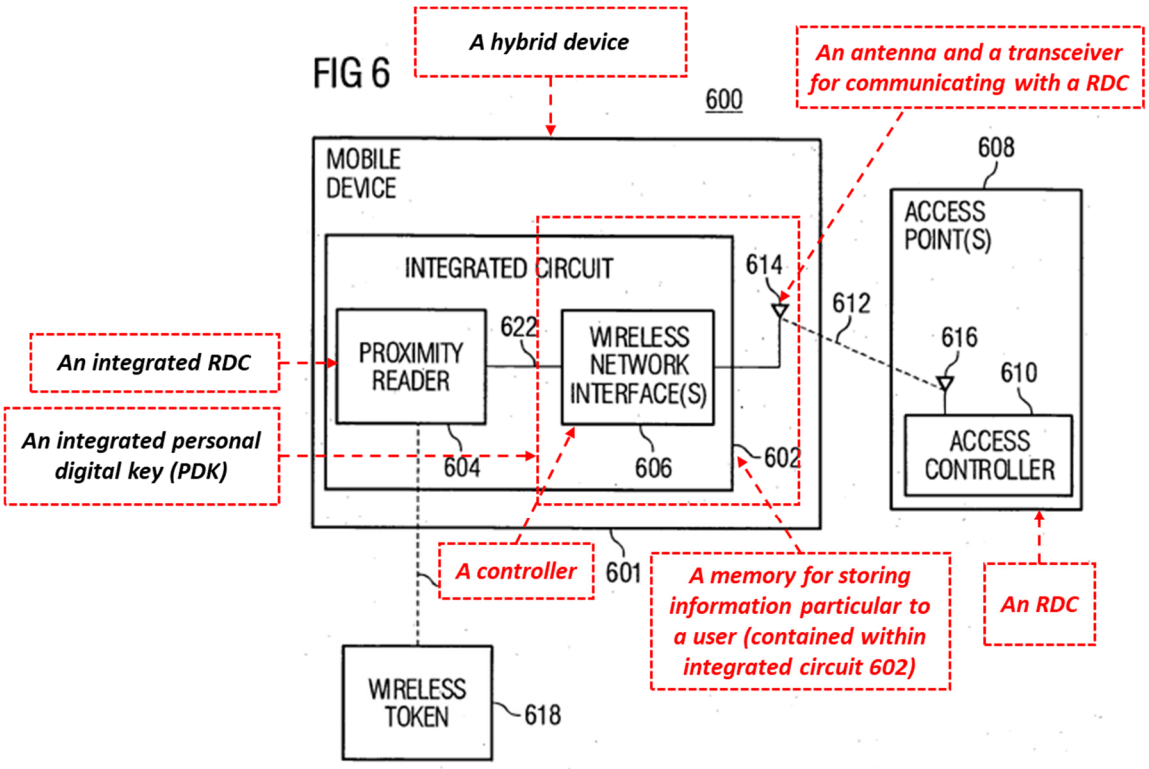


MS-1008, FIG. 3.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782



MS-1008, FIG. 3.



MS-1008, FIG. 6.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

124. Broadcom discloses that "the access device 102 may automatically request a predefined service once the user places the token 104 [(***"an external personal digital key (PDK)***")] proximate the access device 102" using "a wireless proximity reader 106 … configured to receive signals 108 (e.g., RF signals) from the wireless proximity token 104" (***"creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external personal digital key (PDK)***"). MS-1008, ¶¶[0111]-[0117]; *see supra* §VII.A, [1.1], [1.3]. As discussed above, the Broadcom's ***hybrid device includes*** both "***an integrated PDK***" and an "***integrated RDC***." MS-1008, ¶¶[0116]-[0119], [0135]-[0137], FIGS. 1, 3.

[10.2] receiving a first signal at the integrated RDC via the first wireless link from the external PDK;

125. As discussed above in [10.1], Broadcom's wireless proximity reader 106 is "configured to receive signals 108 (e.g., RF signals) ("***receiving a first signal, at the integrated RDC, via the first wireless link***") from the wireless proximity token 104" ("***from the external PDK***"). MS-1008, ¶[0111]; *see supra* [10.1]. For example, "[t]he proximity reader 501[("***the integrated RDC***")] may [] receive appropriate authentication information from the token 514 [("***from the external PDK***")]" MS-1008, ¶[0156].

[10.3] generating an enablement signal enabling one or more of an application, a function and a service on one or more of the hybrid device and a device associated with an external RDC; and

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

126. Broadcom discloses that "[a]ccess to secured services may be controlled based on the proximity of a wireless token." MS-1008, ¶[0057]. Once the token is within proximity, the access device 102 sends "authentication-related information [("***enablement signal***")] to the service provider 110 to indicate that the token 104 is proximate to the access device 102," which then "enable[s] access to the requested service (block 208)" ("***generating an enablement signal enabling one or more of an application, a function and a service on …one or more of the hybrid device and a device associated with an external RDC***"). MS-1008, ¶¶[0116]-[0119]. Specifically, the "term access may include, for example, acquiring, using, invoking, etc. Thus, data may be accessed by providing a copy of the data to the access device," from ***a device associated with an external RDC***. MS-1008, ¶[0122].

127. Alternatively, Broadcom discloses that the "service may enable an access device [("***hybrid device***")] to, for example, read or write data in a data memory, access encrypted data, use cryptographic keys, gain access to cryptographic material such as security associations and keys, access a web page, access a data network or access a processing application" ("***generating an enablement signal enabling one or more of an application, a function and a service on … the hybrid device***"). MS-1008, ¶[0120]. "[F]or example, invoking, interacting with or using the application or loading the application onto the access device" ("***on . . . the hybrid device***"). MS-1008, ¶[0122].

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

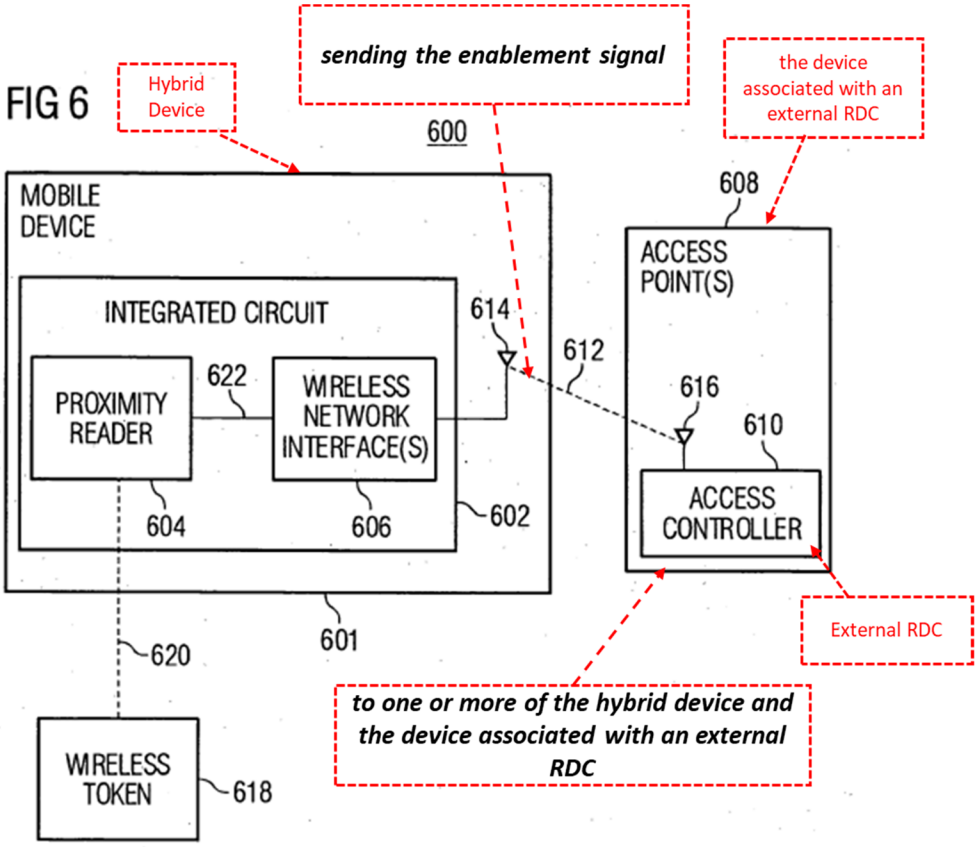
[10.4] sending the enablement signal to one or more of the hybrid device and the device associated with an external RDC.

128. As discussed above, Broadcom discloses that authentication is performed after a token 104 is proximate to the proximity reader 106 of the access device 102 and the service provider 110 ("***a device associated with an external RDC***") returns an authentication decision to the access device 102 ("***sending the enablement signal to … the hybrid device***"). MS-1008, ¶[0116]-[0119]; *see supra* [1.3], [14.1]-[14.3]. Recall that the service provider 110 "enable[s] access to the requested service." MS-1008, ¶[0119].

129. Additionally, Broadcom discloses an embodiment where the service provider 110 is replaced by a wireless "access point 608" which includes an "access controller 610." MS-1008, ¶¶[0163]-[0168], FIG. 6. In this embodiment, the user "use[s] the token 618 in a similar manner as discussed above" (e.g., as described in FIGS. 1 and 3) and "when a user moves the token 618 within relatively close proximity … to the reader 604" it "send[s] authentication information to one or more wireless network interface(s) 606" which wirelessly communicates with a network access point 608. MS-1008, ¶¶[0164]-[0165]. In this embodiment, access to the network for a "mobile device 601" ("***the one or more of the application, the function, and the service***") is enabled by "communicating with a respective access controller 610 [(***the device associated with an external RDC***")] in [the] access

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

point(s) 608 via RF signals 612 transmitted and received via one or more antennas 614 and 616" ("***sending the enablement signal***"). MS-1008, ¶[0165].



MS-1008, FIG. 6.

[11] The method of claim 10, wherein the hybrid device is a cell phone and the enablement signal is sent to the cell phone enabling one or more of a service, a feature and a functionality of the cell phone.

130. As described above in [10.3], one example access device is a "mobile device" and/or a "cellular phone" ("***the hybrid device is a cell phone***") and that "access to the wireless network may be provided when a user moves the token 618 within relatively close proximity … to the reader 604 [of mobile device 601]" ("***enabling one or more of a service, a feature and a functionality of the cell***

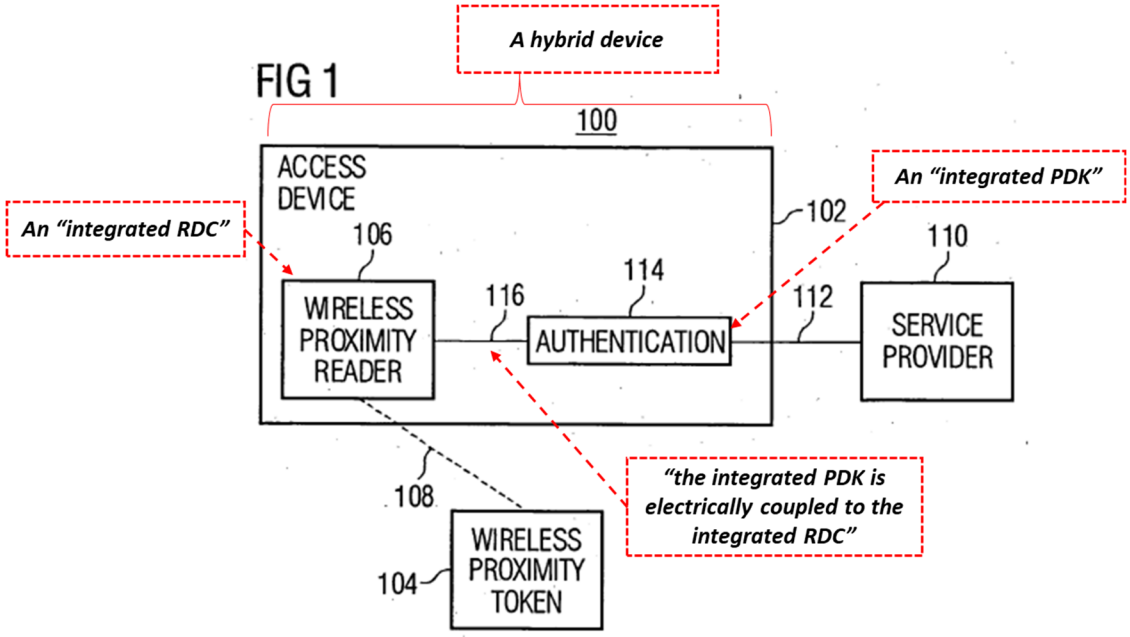
APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

phone"). MS-1008, ¶¶[0125], [0163]-[0168], FIG. 6; *see supra* [10.3]. Broadcom discloses that this access is provided by an "access controller 610 in one or more access point(s) 608 via RF signals 612 transmitted and received via one or more antennas 614 and 616" ("***the enablement signal is sent to the cell phone***"). MS-1008, ¶¶[0164]-[0165], FIG. 6.

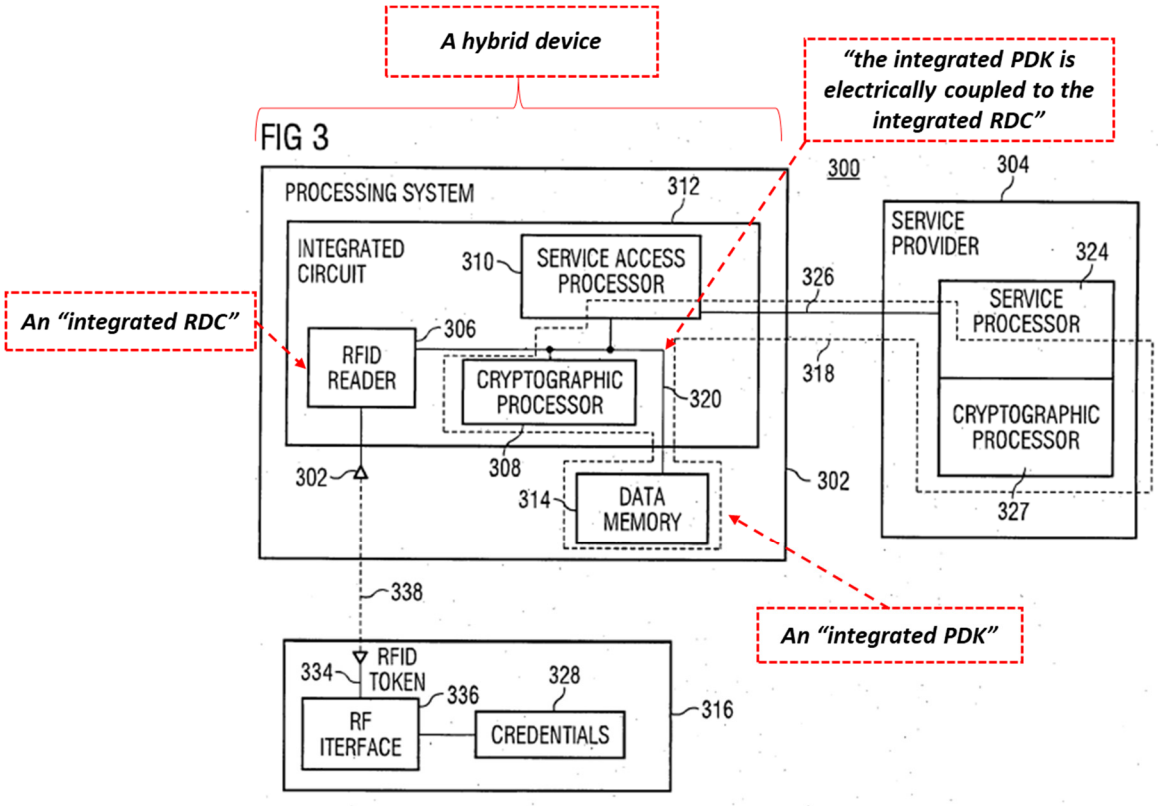
[13.1] The method of claim 10, wherein the integrated PDK is electrically coupled to the integrated RDC, and the method comprises:

131. Broadcom discloses that "information may only pass between the reader 106 and the authentication component 114 via a connection 116" ("***the integrated PDK is electrically coupled to the integrated RDC***"). MS-1005, ¶[0116]. Additionally, Broadcom discloses, as part of its detailed FIG. 3 view, an "RFID reader 306" that is connected to a "data memory 314" via a "data bus 320" ("***the integrated PDK is electrically coupled to the integrated RDC***"). MS-1008, ¶¶[0133]-[0137], FIG. 3; *see supra* [1.2].

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782



MS-1008, FIG. 1.



MS-1008, FIG. 3.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

[13.2] sending the enablement signal from the integrated RDC to the integrated PDK;

132. As discussed above, Broadcom's wireless proximity reader 106 ("***integrated RDC***") is "configured to receive signals 108 (e.g., RF signals) from the wireless proximity token 104" which include the "authentication information" ("***an enablement signal***"). MS-1008, ¶[0111]-[0118], [0148], [0156]-[0159], ; *see supra* [1.2]. Once received by the wireless proximity reader 106, the reader sends the information to the "authentication component 114" via a "cryptographically secured communication channel" such that the "determination of whether the token 104 is proximate the access device 102 is performed in a secure manner" ("***sending the enablement signal from the integrated RDC to the integrated PDK***"). MS-1008, ¶¶[0116]-[0117]; *see supra* [1.2].

[13.3] creating a second wireless link between the integrated PDK and an external RDC; and

133. Broadcom discloses that the authentication component 114 is also "in secure communication with the service provider 110" and that "a cryptographically secured communication channel may be established[("***creating***")] between the authentication component 114 and the service provider 110" ("***a second wireless link between the integrated PDK and an external RDC***"). MS-1008, ¶[0117].

[13.4] sending the enablement signal from the integrated PDK to the external RDC using the second wireless link.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

134. Broadcom discloses that the access device 102 (particularly the authentication component 114) "request[s] access to a service from the service provider 110 by sending a signal over a communication media 112" which includes the "authentication-related information" ("***sending the enablement signal from the integrated PDK to the external RDC using the second wireless link***"). MS-1008, ¶¶[0113]-[0119]. After the service provider 110 receives the signal, "the service provider 110 may then enable access to the requested service." MS-1008, ¶[0119].

[14] The method of claim 11, wherein the integrated PDK modifies the enablement signal to produce a modified enablement signal, and the modified enablement signal is sent from the integrated PDK to the external RDC.

135. In its FIG. 3 detailed view, Broadcom discloses a "cryptographic processor 308" that is part of the integrated circuit 312 that implements Broadcom's PDK. MS-1008, ¶¶[0137]-[0142], FIG. 3. This cryptographic processor 308 "perform[s] key exchange and encryption, decryption and/or authentication operations necessary to send and receive the encrypted information," particularly, "[authentication] information … received from an RFID token 316" ("***the integrated PDK modifies the enablement signal to produce a modified enablement signal***"). *Id*. Broadcom discloses that "[e]ncrypted [authentication] information [("***the modified enablement signal***")] also may be sent between the integrated circuit 312 and a cryptographic processor 322 and a service processor 324 in the service

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

provider 304 via a communication link 326" ("***the modified enablement signal is sent from the integrated PDK to the external RDC***"). MS-1008, ¶[0138], FIG. 3.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

ADDITIONAL REMARKS

136. 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.

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

Dated: 14 February 2024 By: 

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

APPENDIX A

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

B. Special Activities 43

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

EDUCATIONAL BACKGROUND

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

EMPLOYMENT HISTORY

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

CURRENT FIELDS OF INTEREST

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

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

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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 malcode through cellular infrastructure.

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

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

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

4. M.S. Students Supervised

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

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

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

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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 Scurity Challenges of Digital Financial Services. *IEEE S&P Magazine*, 15(5):85–89, 2017.

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

5. Bradley Reaves, Jasmine Bowers, Nolen Scaife, Adam Bates, Arnav Bharatiya, Patrick Traynor, and Kevin Butler. Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World. *ACM Transactions on Privacy and Seurity (TOPS)*, 2017.

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

7. Stephan Heuser, Bradley Reaves, Praveen Kumar Pendyala, Henry Carter, Alexandra Dmitrienko, William Enck, Negar Kiyavash, Ahmad-Reza Sadeghi, and Patrick Traynor. Phonion: Practical Protection of Metadata in Telephony Networks. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2017.

8. Bradley Reaves, Jasmine Bowers, Sigmond A. Gorski III, Olabode Anise, Rahul Bobhate, Raymond Cho, Hiranava Das, Sharique Hussain, Hamza Karachiwala, Nolen Scaife, Byron Wright, Kevin Butler, William Enck, and Patrick Traynor. *droid: Assessment and Evaluation of Android Application Analysis Tools. *ACM Computing Surveys (CSUR)*, 2016.

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

10. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Outsourcing Secure Two-Party Computation as a Black Box. *Journal of Security and Communication Networks (SCN)*, To Appear 2016.

11. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Secure Outsourced Garbled Circuit Evaluation for Mobile Devices. *Journal of Computer Security (JCS)*, 24(2):137–180, 2016.

12. Adam Bates, Kevin Butler, Micah Sherr, Clay Shields, Patrick Traynor, and Dan Wallach. Accountable Wiretapping -or- I Know They Can Hear You Now. *Journal of Computer Security (JCS)*, 23(2):167–195, 2015.

13. Henry Carter, Chaitrali Amrutkar, Italo Dacosta, and Patrick Traynor. For Your Phone Only: Custom Protocols for Efficient Secure Function Evaluation on Mobile Devices. *Journal of Security and Communication Networks (SCN)*, 7(7):1165–1176, 2014.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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%).

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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 Comunications 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 *Procedings 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%).

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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%).

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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 Sciafe, Henry Carter, and Patrick Traynor. OnionDNS: A Seizure-Resistant Top-level Domain. In *Proceedings of the IEEE Conference on Communications and Network Security (CNS)*, 2015. (Acceptance Rate: 28.1%).

39. Bradley Reaves, Nolen Scaife, Adam Bates, Patrick Traynor, and Kevin Butler. Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2015. (Acceptance Rate: 15.7%).

40. Bradley Reaves, Ethan Shernan, Adam Bates, Henry Carter, and Patrick Traynor. Boxed Out: Blocking Cellular Interconnect Bypass Fraud at the Network Edge. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2015. (Acceptance Rate: 15.7%).

41. David Dewey, Bradley Reaves, and Patrick Traynor. Uncovering Use-After-Free Conditions In Compiled Code. In *Proceedings of the International Conference on Availability, Reliability and Security (ARES)*, 2015. (Acceptance Rate: 22%).

42. Ethan Shernan, Henry Carter, Dave Tian, Patrick Traynor, and Kevin Butler. More Guidelines Than Rules: CSRF Vulnerabilities from Noncompliant OAuth 2.0 Implementations. In *Proceedings of the International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA)*, 2015. (Acceptance Rate: 22.7%).

43. Henry Carter, Charles Lever, and Patrick Traynor. Whitewash: Outsourcing Garbled Circuit Generation for Mobile Devices. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2014. (Acceptance Rate: 19.9%).

44. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Secure Outsourced Garbled Circuit Evaluation for Mobile Devices. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2013. (Acceptance Rate: 16.2%).

45. Chaitrali Amrutkar, Matti Hiltunen, Shobha Venkataraman, Kaustubh Joshi, Patrick Traynor, Trevor Jim, and Oliver Spatscheck. Why is My Smartphone Slow? On The Fly Diagnosis of Poor Performance on the Mobile Internet. In *Proceedings of The 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2013. (Acceptance Rate: 19.6%).

46. Saurabh Chakradeo, Brad Reaves, Patrick Traynor, and William Enck. MAST: Triage for Market-scale Mobile Malware Analysis. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2013. (Acceptance Rate: 15.0%)(Best Paper).

47. Charles Lever, Manos Antonakakis, Brad Reaves, Patrick Traynor, and Wenke Lee. The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2013. (Acceptance rate: 18.8%).

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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. PinDr0p: Using Single-Ended Audio Features to Determine Call Provenance. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2010. (Acceptance Rate: 17.2%).

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%).

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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%).

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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 Financal 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

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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, Franzi Roesner, Apu Kapadia, Eakta Jain.
Amount: *$7,500,000 for 5 years*
Awarded October 2022

2. **ROCKY: Reliable Obfuscated Communications Kit for everYone**
Sponsor: DARPA Resilient Anonymous Communication for Everyone (RACE) – Broad Agency Announcement
Investigator(s): Thomas Shrimpton (PI), Patrick Traynor, Kevin Butler, Vincent Bindschaedler, Nadia Heninger
Amount: *$1,600,000 over 4 years*
Awarded May 2019

3. **WiFiUS: Collaborative Research: SELIOT: Securing Lifecycle of Internet-of-Things**
Sponsor: NSF CNS WiFiUS
Investigator(s): Gene Tsudik (PI), Patrick Traynor
Amount: *$300,000 for 2 years*
Submitted December 2016

4. **Cloud-based Oblivious Spectrum Mapping and Allocation**
Sponsor: NSF CNS EARS
Investigator(s): John Shea (PI), Tan Wong, Patrick Traynor
Amount: *$532,952 for 2 years*
Submitted May 2016

5. **DURIP: Developing Research Capability in Cyber-Physical Systems at the University of Florida**
Sponsor: Small
Investigator(s): Kevin Butler (PI), Patrick Traynor, My Thai
Amount: *$200,000 for 2 years*
Submitted: June 2015

6. **Securing the New Converged Telephony Landscape**
Sponsor: NSF TWC: Small
Investigator(s): Mustaque Ahamad (PI) and Patrick Traynor
Amount: *$500,000 for 3 years*
Submitted: December 2012

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

7. **Facilitating Free and Open Access to Information on the Internet**
   Sponsor: NSF Trustworthy Computing
   Investigator(s): Nick Feamster (PI), Wenke Lee, Patrick Traynor, Hans Klein, Roger Dingledine, Michael Freedman and Edward W. Felten
   Amount: *$1,500,000 for 4 years*
   Awarded: June 2011

8. **Monitoring Free and Open Access to Information on the Internet**
   Sponsor: Google Focus Program
   Investigator(s): Nick Feamster (PI), Wenke Lee, Mustaque Ahamad, Patrick Traynor, Henry Owen, Ellen Zegura, Zvi Galil
   Amount: *$1,000,000 for 2 years*
   Awarded: November 2011

9. **Dynamic-attribute-based Disclosure of Health Information in Emergency Care Scenarios**
   Sponsor: Health Systems Institute (HSI) Seed Grant Program
   Investigator(s): Doug Blough (PI), Mustaque Ahamad, Patrick Traynor and Jim Jose
   Amount: *$50,000 over 1 year*
   Awarded: August 2009

10. **Federal Cyber Service Scholarships at Georgia Tech**
    Sponsor: NSF SFS Scholarships
    Investigator(s): Seymour Goodman (PI), Patrick Traynor
    Amount: *$1,250,682 over 5 years*
    Awarded: June 2009

11. **Security for IMS-Enabled Converged Applications**
    Sponsor: US Department of Defense
    Investigator(s): Mustaque Ahamad (PI), Patrick Traynor (PI), Michael Hunter, Russ Clark
    Amount: *$146,121 for 1 year*
    Awarded: August 2008

2. Pending

Removed for external version.

I. Research Honors and Awards

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

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

3. Xinyu Xing, College of Computing, Georgia Tech, Spring 2013.
   Advisor: Professor Wenke Lee.

4. Brad Reaves, College of Computing, Georgia Tech, Spring 2013.
   Advisor: Professor Patrick Traynor.

5. Chaz Lever, College of Computing, Georgia Tech, Spring 2013.
   Advisor: Professor Patrick Traynor.

6. Terry Nelms, College of Computing, Georgia Tech, Spring 2012.
   Advisor: Professors Mustaque Ahamad and Roberto Perdesci.

7. Saurabh Chakradeo, College of Computing, Georgia Tech, Spring 2012.
   Advisor: Professor Patrick Traynor.

8. Henry Carter, College of Computing, Georgia Tech, Spring 2012.
   Advisor: Professor Patrick Traynor.

9. David Dewey, College of Computing, Georgia Tech, Spring 2012.
   Advisor: Professor Jon Giffin.

10. Chaitrali Amrutkar, College of Computing, Georgia Tech, Fall 2011.
    Advisor: Professor Patrick Traynor.

11. Yacin Nadji, College of Computing, Georgia Tech, Fall 2011.
    Advisor: Professor Wenke Lee.

12. Yogesh Mundada, College of Computing, Georgia Tech, Fall 2011.
    Advisor: Professor Nick Feamster.

13. Hyojoon Kim, College of Computing, Georgia Tech, Fall 2011.
    Advisor: Professor Nick Feamster.

14. Ikpeme Erete, College of Computing, Georgia Tech, Spring 2011.
    Advisor: Professor Alex Orso.

15. Chaitrali Amrutkar, College of Computing, Georgia Tech, Spring 2011.
    Advisor: Professor Patrick Traynor.

16. Brendan Dolan-Gavitt, College of Computing, Georgia Tech, Spring 2011.
    Advisor: Professor Wenke Lee and Professor Jon Giffin.

17. Sam Burnett, College of Computing, Georgia Tech, Fall 2010.
    Advisor: Professor Nick Feamster.

18. Cong Shi, College of Computing, Georgia Tech, Fall 2010.
    Advisor: Professor Mostafa Ammar and Professor Ellen Zegura.

19. Partha Kanuparthy, College of Computing, Georgia Tech, Fall 2010.
    Advisor: Professor Constantine Dorvolis.

20. Long Lu, College of Computing, Georgia Tech, Spring 2010.
    Advisor: Professor Wenke Lee.

21. Virendra Kumar, College of Computing, Georgia Tech, Spring 2009.
    Advisor: Professor Alexandra Boldyreva.

22. Frank Park, College of Computing, Georgia Tech, Spring 2009.
    Advisor: Professor Patrick Traynor.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

4. Walter Nolen Scaife, Patrick G. Traynor and Christian Peeters, "Payment Card Overlay Skimmer Detection", United States Patent # 10,496,914, Filed October 2017, Issued December 2019. (See also # 10,936,928)

5. Patrick G. Traynor, David P. Arnold, Walter Nolen Scaife, Christian Peeters, and Camilo Valez Cuervo, "Detecting counterfeit magnetic stripe cards using encoding jitter", United States Patent # 10,803,261, Filed May 2017, Issued October 2020.

6. Patrick G. Traynor, Bradley Reaves, Logan Blue, Luis Vargas, Hadi Abdullah, and Thomas Shrimpton, "Identity and content authentication for phone calls", United States Patent # 10,764,043, Filed Apr 2017, Issued September 2020.

7. Walter Nolen Scaife, Henry Carter, Patrick G. Traynor and Kevin R. B. Butler. "Malware Detection Through User Data Transformation Monitoring", United States Patent # 10,685,114. Filed September 2015, Issued June 2020.

8. Vijay A. Balasubramaniyan, Mustaque Ahamad, Patrick G. Traynor. "Using Single-Ended Audio Features to Automatically Determine Voice Call Provenance", United States Patent, #9,037,113 June 2010, Issued May 2015. (See also #9,516,497 and #10,523,809)

9. Patrick G. Traynor, Byungsuk Kim and Farooq Anjum. "Secure Localization for 802.11 Networks with Fine Granularity", United States Patent, #8,107,400, Filed July 2008, Issued January 2012.

E. Editorial and Reviewer Work for Technical Journals and Publishers

Associate Editor:

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

Guest Editor:

Journals

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

Reviewer for:

Journals

- *ACM Transactions on Information and System Security (TISSEC)* 2008, 2009, 2010, 2011, 2012, 2013
- *IEEE Transactions on Dependable and Secure Computing (TDSC)* 2012, 2013
- *IEEE Security and Privacy Magazine (S&P)* 2010, 2011
- *Communications of the ACM (CACM)* 2010
- *Journal of Anesthesia & Analgesia* 2009
- *IEEE Transactions on Mobile Computing (TMC)* 2008, 2010, 2011, 2012, 2013
- *IEEE Transactions on Internet Technology (TOIT)* 2009, 2010
- *ACM Mobile Computing and Communications Review (MC2R)* 2008
- *IEEE/ACM Transactions on Networking (TON)* 2007, 2008
- *Journal of Pervasive and Mobile Computing (PMC)* 2009, 2010

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

- *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

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

- *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*.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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 Plantiff for Infringement (via Susman Godfrey LLP), Verdict: Infringement on 2 of 4 patents. *October 2012 - February 2015.*

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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, Sweeden.

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

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

14. Could this be the answer to the ransomware threat?, Consumer Affairs. Consumer Affairs - https://www.consumeraffairs.com/news/could-this-be-the-answer-to-the-ransomeware-threat-071116.html, July 2016.

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

16. Researchers Develop A Way To Stop Ransomware By Watching The Filesystem. Slashdot - https://yro.slashdot.org/story/16/07/08/2242244/researchers-develop-a-way-to-stop-ransomware-by-watching-the-filesystem, July 2016.

17. Mohul Ghosh. Trak.in - Digital Money Apps In India Are Unsafe and Unsecured – Researchers. http://trak.in/tags/business/2015/08/17/digital-money-apps-india-unsafe-unsecured/, August 2015.

18. Richard Handford. Mobile World Live - Survey finds security holes in mobile money apps. http://www.mobileworldlive.com/money/news-money/survey-finds-security-holes-in-mobile-money-apps/#.Vc27Y-QTmSQ.twitter, August 2015.

19. JENNIFER VALENTINO-DEVRIES. Wall Street Journal - Researchers Find Security Flaws in Developing-World Money Apps. http://blogs.wsj.com/digits/2015/08/11/researchers-find-security-flaws-in-developing-world-money-apps/, August 2015.

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

21. N. V. The Economist - The Threat in the Pocket. http://www.economist.com/blogs/babbage/2013/10/difference-engine-0?fsrc=scn/fb/wl/bl/thethreatinthepocket, October 2013.

22. Antone Gonsalves. ComputerWorld - Let's Dump Anti-Virus and Move On:. http://blogs.computerworld.com/mobile-security/22969/lets-dump-av-and-move, October 2013.

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

24. Kirsten Doyle. ITWeb - Android Threat Exaggerated, or is it? http://www.itweb.co.za/index.php?option=com_content&view=article&id=68055, October 2013.

25. Danielle Walker. SC Magazine - Mobile malware prevalence expands, but privacy-abusing apps should be top of mind. http://www.scmagazine.com/mobile-malware-prevalence-expands-but-privacy-abusing-apps-should-be-top-of-mind/article/300597/, June 2013.

26. Jim Burress. WABE NPR - Mobile Web Browsers Full of Security Risks, Tech Professor Finds. http://wabe.org/post/mobile-web-browsers-full-security-risks-tech-professor-finds, December 2012.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

27. Mark Huffman. Consumer Affairs - Georgia Tech: mobile browsers fail safety test. http://www.consumeraffairs.com/news/georgia-tech-mobile-browsers-fail-safety-test-120612.html, December 2012.

28. Matthew J. Schwartz. Information Week - Blame Screen Size: Mobile Browsers Flunk Security Tests. http://www.informationweek.com/security/mobile/blame-screen-size-mobile-browsers-flunk/240143999, December 2012.

29. Jon Gold. Network World - Ga. Tech researchers: Mobile Browsers need better HTTPS indicators. http://www.networkworld.com/news/2012/120512-mobile-browsers-264846.html, December 2012.

30. United Press International. Study: Most mobile Web browsers unsafe. http://www.upi.com/Science_News/Technology/2012/12/05/Study-Most-mobile-Web-browsers-unsafe/UPI-73431354743353/#ixzz2EGtQsuLd, December 2012.

31. Suzanne Choney. Mobile browser woes can fool even experts: report . http://www.nbcnews.com/technology/mobile-browser-woes-can-fool-even-experts-report-1C7451203, December 2012.

32. Meghan Kelly. VentureBeat - 3 hot security startups to watch. http://venturebeat.com/2012/02/27/3-security-startups-to-watch-at-the-2012-rsa-conference/, February 2012.

33. Jacob Goodwin. Government Security News - RSA 2012 – Pindrop Security can distinguish a fraudulent phone call from a real one. http://www.gsnmagazine.com/node/25721?c=communications, February 2012.

34. Matt Liebowitz. Phone hack logs keystrokes from nearby computers. MSNBC.com - http://www.msnbc.msn.com/id/44993238/ns/technology_and_science-security/#.TqU5MNSjPh4, October 2011.

35. Jacob Aron. iPhone keylogger can snoop on desktop typing. New Scientist - http://www.newscientist.com/article/dn21059-iphone-keylogger-can-snoop-on-desktop-typing.html, October 2011.

36. iPhone Keylogger Can Snoop on Desktop Typing. Slashdot - http://mobile.slashdot.org/story/11/10/18/2346222/iphone-keylogger-can-snoop-on-desktop-typing, October 2011.

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

38. Kevin McCaney. Bad vibrations: How smart phones could steal PC passwords. Government Computer News - http://gcn.com/articles/2011/10/18/smart-phone-sensors-steal-keystrokes.aspx, October 2011.

39. PhysOrg. Turning iPhone into spiPhone: Smartphones' accelerometer can track strokes on nearby keyboards. PhysOrg.com - http://www.physorg.com/news/2011-10-iphone-spiphone-smartphones-accelerometer-track.html, October 2011.

40. Brid-Aine Parnell. Securo-boffins call for 'self-aware' defensive technologies. The Register - http://www.theregister.co.uk/2011/09/14/self_aware_cyber_security_technologies_should_be_a_top_priority/, September 2011.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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

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

43. Science Daily. Voice Phishing: System to Trace Telephone Call Paths Across Multiple Networks Developed. http://www.sciencedaily.com/releases/2010/10/101005121820.htm, October 2010.

44. Brian Kalish. To Text or Not to Text During Emergencies. NextGov.com - http://www.nextgov.com/nextgov/ng_20100914_5986.php?oref=topnews, September 2010.

45. Ki Mae Heussner. 'Operation Chokehold': Fake Steve Jobs Rallies iPhone Users to Cripple AT&T Network. ABC News - http://abcnews.go.com/Technology/GadgetGuide/fake-steve-jobs-rallies- iphone-users-cripple-att/story?id=9355447, December 2009.

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

47. MacGregor Campbell. Botnets show their disruptive potential. New Scientist Magazine - http://www.newscientist.com/article/mg20427347.000-mobile-botnets-show-their-disruptive-potential.html, November 2009.

48. Angela Moscaritolo. Remote repair for infected phones in development. SC Magazine - http://www.scmagazineus.com/remote-repair-for-infected-phones-in- development/article/157504/, November 2009.

49. Bob Brown. iPhone worms, other smartphone malware in researchers' sights. Network World - http://www.networkworld.com/news/2009/111109-smartphone-security-georgia -tech.html?hpg1=bn, November 2009.

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

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

52. Ben Meyer. Georgia Tech to Lead Fight Against Cell Phone Hackers. NBC 11 Atlanta - http://www.11alive.com/news/local/story.aspx?storyid=132505&catid=3, July 2009.

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

54. Kelli B. Grant. Four Free Cellphone Apps to Help Manage Your Money. SmartMoney Magazine - http://www.smartmoney.com/Spending/Deals/4-Great-Free-Finance-Apps-for-Cellphones/, June 2009.

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

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782

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.

APPLE EXHIBIT 1044
APPLE v. PROXENSE
IPR2024-00782