IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	John J. Giobbi	
U.S. Patent No.:	8,352,730	Attorney Docket No.: 42342-0136IP1
Issue Date:	January 8, 2013	
Appl. Serial No.:	11/314,199	
Filing Date:	December 20, 2005	
Title:	BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION	

DECLARATION OF DR. PATRICK TRAYNOR

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

By: _____

Patrick G. Traynor, Ph.D.

MICROSOFT 1003

Table of Contents

I. QUALIFICATIONS AND BACKGROUND INFORMATION 3

II. OVERVIEW OF CONCLUSIONS FORMED 9

III. LEVEL OF ORDINARY SKILL IN THE ART 10

IV. LEGAL STANDARDS 11
- A. Terminology 11
- B. Legal Standards 11
  - 1. Anticipation 11
  - 2. Obviousness 12

V. RELEVANT CLAIM CONSTRUCTIONS 16

VI. THE ’730 PATENT 17
- A. Overview of the ’730 Patent 17
- B. Prosecution History of the ’730 Patent 20

VII. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES . 21
- A. Burger 21
- B. Robinson 45
- C. Combination of Burger and Robinson 49

VIII. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE ’730 CLAIMS UNPATENTABLE 52
- A. Ground 1: Claims 1, 2, 4-9, 11, 12, and 14-17 are obvious over Burger… 52
- B. Ground 2: Claims 3, 10, and 13 are obvious in view of Burger and Robinson 115

IX. CONCLUSION 117

I. QUALIFICATIONS AND BACKGROUND INFORMATION

1. I have been retained as an expert witness by Microsoft Corporation to provide my opinion regarding the validity of U.S. Patent No. 8,352,730 (hereinafter referred to as the "**'730 patent**." My qualifications for conducting my analysis and forming my conclusions are summarized below. My education and experience are described more fully in the attached curriculum vitae (APPENDIX A).

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

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

4. Prior to joining the University of Florida, I was an Associate Professor from March to August 2014 and an Assistant Professor of Computer Science from 2008

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

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

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

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

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

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

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

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

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

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

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

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

15. In writing this declaration, I have considered the following: my own knowledge and experience, including my work experience in the fields of computer science and computer graphics and imaging; my experience in teaching related subjects; and my experience in working with others involved in those

fields. In addition, I have analyzed various publications and materials, in addition to other materials I cite in my declaration.

16. I have reviewed the ’730 patent (MSC-1001), and relevant excerpts of the prosecution history (MSC-1002) of the ’730 patent. Among various textbooks, documents, and publications, I have also reviewed the following prior art references:

Prior Art Reference
US Patent Application Publication No. 2005/0050367 (“Burger” or MSC-1005)
US Patent Application Publication No. 2003/0177102 (“Robinson” or MSC-1006)
Institution Decision, Samsung Electronics America, Inc. v. Proxense, LLC, IPR2021-01444, Paper 11 (PTAB Feb. 28, 2022) (MSC-1007)
Merriam-Websters Dictionary, Definition of “transaction” (MSC-1008)
Google Pixel Serial Number Guide, HomeServe webpage, https://www.homeserve.com/en-us/customers/find-serial-number-device-type/google/ (MSC-1009)
US Patent No. 8,977,860 (“Barrus” or MSC-1010)
US Patent No. 7,681,050 (“Blom” or MSC-1011)

US Patent No. 10,755,300 ("Goodhart" or MSC-1012)
US Patent Application Publication No. 2009/0070219 ("D'Angelo" or MSC-1013)
US Patent No. 10,929,869 ("Rosenberg" or MSC-1014)
US Patent No. 8,200,980 ("Robinson 980" or MSC-1015)
Product Identification Codes, https://www.uc.edu/content/dam/uc/ce/docs/OLLI/Page%20Content/PRODUCT%20IDENTIFICATION%20CODES%20BAR%20QR.pdf, last visited April 12, 2024 (MSC-1020)
How to Find the Serial Number on TP-Link Devices, https://www.tp-link.com/us/support/faq/503/, last visited April 15, 2024 (MSC-1026)

17. Counsel (Fish & Richardson) has informed me that I should consider these materials through the lens of one of ordinary skill in the art related to the '730 patent at the time of the earliest possible priority date of the '730 patent, and I have done so during my review of these materials. I have been informed by Counsel to use the filing date (December 20, 2004) of the US provisional application No. 60/637,538, from which the '730 claims priority, as the "Priority Date" in my analysis below.

18. I have no financial interest in the outcome of this proceeding. I am being compensated for my work as an expert on an hourly basis. My compensation is not dependent on the outcome of these proceedings or the content of my opinions.

19. My opinions, as explained below, are based on my education, experience, and expertise in the fields relating to the '730 Patent. Unless otherwise stated, my testimony below refers to the knowledge of one of ordinary skill in the art as of the earliest possible priority date. Any figures that appear within this document have been prepared with the assistance of Counsel and reflect my understanding of the '730 Patent and the prior art discussed below.

II. OVERVIEW OF CONCLUSIONS FORMED

20. This 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 references listed above, I believe that:

- Claims 1, 2, 4-9, 11, 12, and 14-17 are obvious over Burger.
- Claims 3, 10, and 13 are obvious over Burger in combination with Robinson.

21. In support of these conclusions, I provide an overview of the references in Section VII and more detailed comments regarding the obviousness of claims 1-17 ("**the Challenged Claims**") of the '730 patent in Section VIII.

III. LEVEL OF ORDINARY SKILL IN THE ART

22. In my opinion, one of ordinary skill in the art relating to, and at the time of, the Priority Date would have been someone with (1) at least a bachelor's degree in computer science, computer engineering, electrical engineering, or a related field, and (2) at least two years of industry experience in wireless communications security. Additional advanced education could compensate for a deficiency in work experience, and *vice-versa*.

23. Based on my experiences, I have a good understanding of the capabilities of a POSITA. Indeed, I have taught, participated in organizations, and worked closely with many such persons over the course of my career. Based on my knowledge, skill, and experience, I have an understanding of the capabilities of a POSITA. For example, from my industry experience, I am familiar with what a POSITA would have known and found predictable in the art. From teaching and supervising my post-graduate students, I also have an understanding of the knowledge that a person with this academic experience possesses. Furthermore, I possess those capabilities myself.

IV. LEGAL STANDARDS

A. Terminology

24. 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 20, 2004 as the point in time for claim interpretation purposes.

B. Legal Standards

25. I have been informed by Counsel and understand that documents and materials that qualify as prior art can render a patent claim unpatentable as being anticipated or obvious.

26. I am informed by Counsel and understand that all prior art references are to be looked at from the viewpoint of a person of ordinary skill in the art at the time of the invention, and that this viewpoint prevents one from using his or her own insight or hindsight in deciding whether a claim is anticipated or rendered obvious.

1. Anticipation

27. I understand that patents or printed publications that qualify as prior art can be used to invalidate a patent claim as anticipated or as obvious.

28. I understand that, once the claims of a patent have been properly construed, the second step in determining anticipation of a patent claim requires a comparison of the properly construed claim language to the prior art on a limitation-by-limitation basis.

29. I understand that a prior art reference "anticipates" an asserted claim, and thus renders the claim invalid, if all limitations of the claim are disclosed in that prior art reference, either explicitly or inherently (i.e., necessarily present).

2. Obviousness

30. I understand that even if a patent is not anticipated, it is still invalid if the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a POSITA.

31. I have been informed by Counsel and understand that a claim is unpatentable for obviousness and that obviousness may be based upon a combination of references. I am informed by Counsel and understand that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. However, I am informed by Counsel and understand that a patent claim composed of several elements is not proved obvious

merely by demonstrating that each of its elements was, independently, known in the prior art.

32. I am informed by Counsel and understand that when a patented invention is a combination of known elements, a court determines whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue by considering the teachings of prior art references, the effects of demands known to people working in the field or present in the marketplace, and the background knowledge possessed by a person having ordinary skill in the art.

33. I am informed by Counsel and understand that a patent claim composed of several limitations is not proved obvious merely by demonstrating that each of its limitations was independently known in the prior art. I am informed by Counsel and understand that identifying a reason those elements would be combined can be important because inventions in many instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known. I am informed by Counsel and understand that it is improper to use hindsight in an obviousness analysis, and that a patent's claims should not be used as a "roadmap."

34. I am informed by Counsel and understand that an obviousness inquiry requires consideration of the following factors: (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.

35. I have been informed by Counsel and understand that an obviousness evaluation can be based on a single reference or a combination of multiple prior art references. I understand that the prior art references themselves may provide a suggestion, motivation, or reason to combine, but that the nexus linking two or more prior art references is sometimes simple common sense. I have been informed by Counsel and understand that obviousness analysis recognizes that market demand, rather than scientific literature, often drives innovation, and that a motivation to combine references may be supplied by the direction of the marketplace.

36. I have been informed by Counsel and understand that if a technique has been used to improve one device, and a person of ordinary skill at the time of invention would have recognized that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.

37. I have been informed by Counsel and understand that practical and common sense considerations should guide a proper obviousness analysis, because familiar

items may have obvious uses beyond their primary purposes. I have been informed by Counsel and understand that a person of ordinary skill looking to overcome a problem will often be able to fit together the teachings of multiple prior art references. I have been informed by Counsel and understand that obviousness analysis therefore takes into account the inferences and creative steps that a person of ordinary skill would have employed at the time of invention.

38. I have been informed by Counsel and understand that a proper obviousness analysis focuses on what was known or obvious to a person of ordinary skill at the time of invention, not just the patentee. Accordingly, I understand that any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.

39. I have been informed by Counsel and understand that a claim can be obvious in light of a single reference, without the need to combine references, if the elements of the claim that are not found explicitly or inherently in the reference can be supplied by the common sense of one of skill in the art.

40. I have been informed by Counsel and understand that there must be a relationship between any such secondary considerations and the invention, and that contemporaneous and independent invention by others is a secondary consideration supporting an obviousness determination.

41. In sum, my understanding is that prior art teachings are properly combined where one of ordinary skill having the understanding and knowledge reflected in the prior art and motivated by the general problem facing the inventor, would have been led to make the combination of elements recited in the claims. Under this analysis, the prior art references themselves, or any need or problem known in the field of endeavor at the time of the invention, can provide a reason for combining the elements of multiple prior art references in the claimed manner.

42. I have been informed by Counsel and understand that in an *inter partes* review, "the petitioner shall have the burden of proving a proposition of unpatentability," including a proposition of obviousness, "by a preponderance of the evidence." 35 U.S.C. §316(e).

V. RELEVANT CLAIM CONSTRUCTIONS

43. I was informed by Counsel that in a prior IPR proceeding (IPR2021-01444), the Board noted that:

1) "interpretation of 'tamper proof format' is not necessary to determine whether to institute an *inter partes* review";
2) "[t]he plain meaning of 'third-party trusted authority' suggests an entity or party separate from the principal parties to a transaction"; and
3) "no further interpretation of the 'access message' limitations is

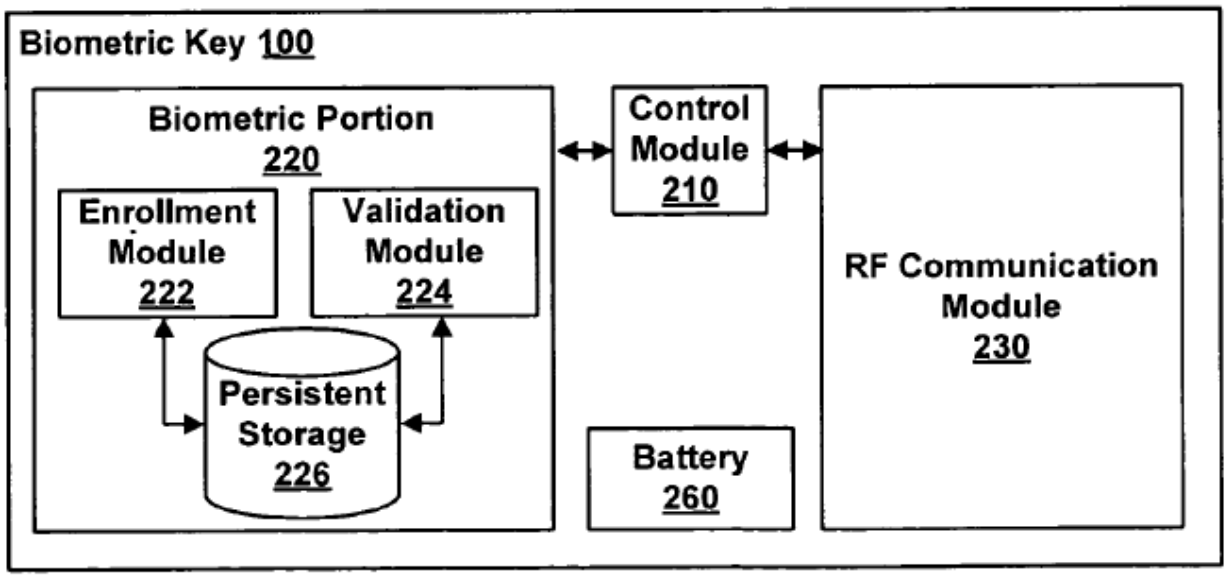
necessary." MSC-1007, 11-15.

44. I have not offered an opinion on these constructions but note that the prior art cited in my declaration renders the claims obvious in view of the above-noted constructions and/or their plain and ordinary meaning, which I have used to interpret the claims.

VI. THE '730 PATENT

A. Overview of the '730 Patent

45. The '730 Patent entitled "Biometric Personal Data Key (PDK) Authentication" is directed to systems and methods for performing "an authentication responsive to biometric verification of a user being authenticated." MSC-1001, 1:15-18, cover, Abstract, 2:60-67. In particular, the '730 patent discloses a biometric key 100, as shown in FIG. 2 below, that can be used to perform the biometric verification using a trusted key authority. MSC-1001, 3:47-5:2, 5:60-67.



MSC-1001, FIG. 2.

46. The '730 patent's FIG. 4 (reproduced below) is a flowchart "illustrating a method 400 for authenticating a biometrically verified user using a trusted key authority (e.g., authority 320). A biometric key (e.g., biometric key 100) is registered 410 with the trusted key authority" and "a user is enrolled 420 with the biometric key." MSC-1001, 5:60-67.

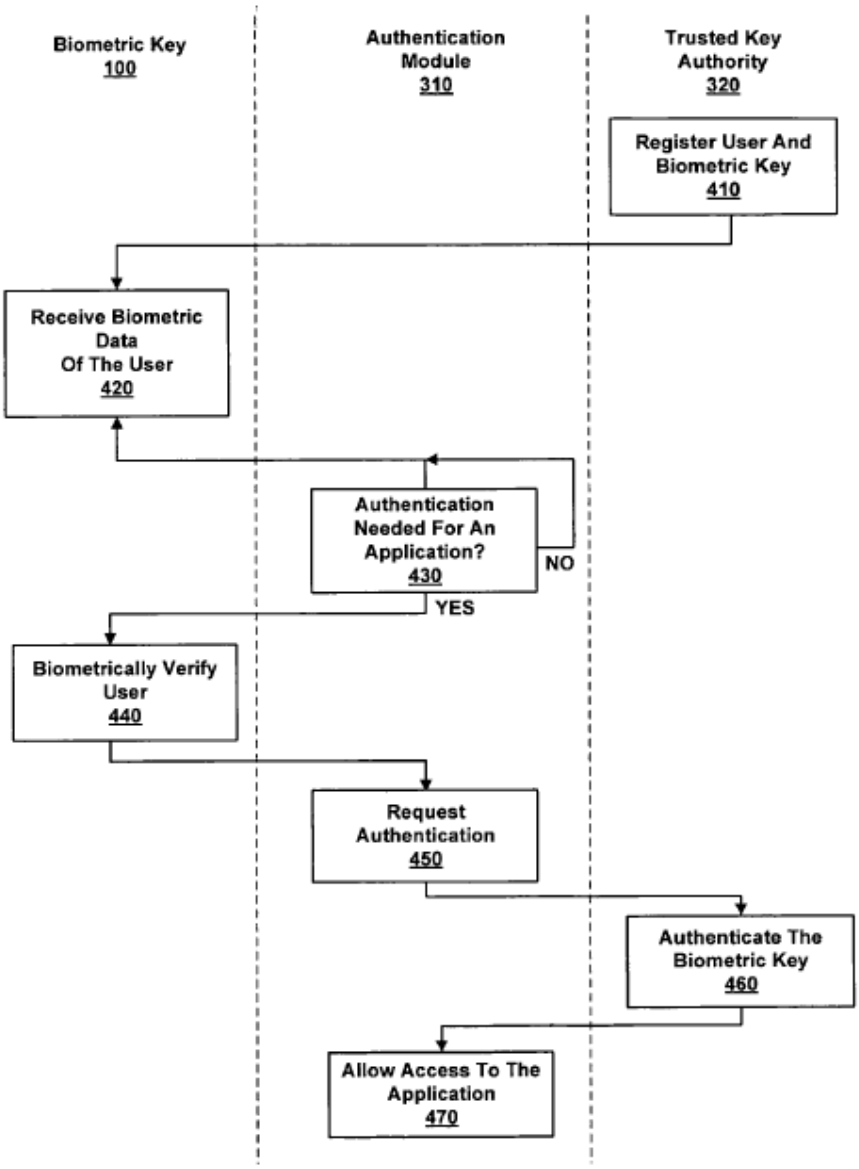


FIG. 4

MSC-1001, FIG. 4.

47. When authentication of the biometric key is needed ("[f]or example, [when] a user can be standing proximate to a slot machine in a casino which requires that a user be over the age of 21), "[t]he biometric key establishes communication with the authentication module using various techniques" and "performs the biometric verification of the user 440." MSC-1001, 6:1-25. "If the biometric verification of

the user is successful, the key provides its code over the secure communications channel." MSC-1001, 6:23-25. The biometric verification is successful when scanned biometric data of the user, e.g., fingerprint data, matches biometric data for the user stored on the biometric key 100. MSC-1001, FIG. 6, 6:65-7-9, 3:28-46.

48. The code of the key is the device ID of the key. MSC-1001, 5:65. The code sent by the biometric key 100 "is utilized to authenticate the biometric key itself." MSC-1001, 6:26-31, 7:10-23, FIG. 7.

B. Prosecution History of the '730 Patent

49. The '730 Patent issued from U.S. Patent Application No. 11/314,199 ("the '199 application"), which was filed on 12/20/2005. MS-1001, cover. I have reviewed the prosecution history of the '199 application. After numerous rounds of prosecution including three requests for continued examination, the '199 application was ultimately allowed. *See generally* MSC-1002. I have noted a few important details from the prosecution history below.

50. The Examiner allowed the claims by amending claim 1 (and the other independent claims similarly) to add "wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition" and "wherein the application is selected from a group consisting of a casino machine, a keyless

lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file" to the claims by virtue of an Examiner amendment attached to the notice of allowance dated August 31, 2012. MSC-1002, 31-43. However, as noted in this petition below, these features, corresponding to features [1.2] and [1.7], were well-known and would have been obvious to a POSITA.

VII. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES

A. Burger

51. Burger is related to a portable electronic authorization device, referred to as a Pocket Vault. MSC-1005, ¶[51]. The Pocket Vault is "used for producing, distributing, storing, and using the typical contents of a person's wallet, as well as the multiple, separate transaction authorization devices." MSC-1005, ¶[93]. Burger's system, shown below in FIG. 1, enables "individuals to replace nearly all of the paper and plastic contents of their wallets and all of their other transaction authorization implements with a single, hand-held portable electronic authorization device. The system may include the portable electronic authorization devices, removable morphing tokens or cards associated with such devices." MSC-1005, ¶[93]. Beneficially, "the system may eliminate virtually all of the distribution costs and security concerns associated with paper and plastic media." MSC-1005,

¶[93]. Burger's FIG. 1 (reproduced below) shows a system 100 in which the Pocket Vault can be used. MSC-1005, ¶[51].

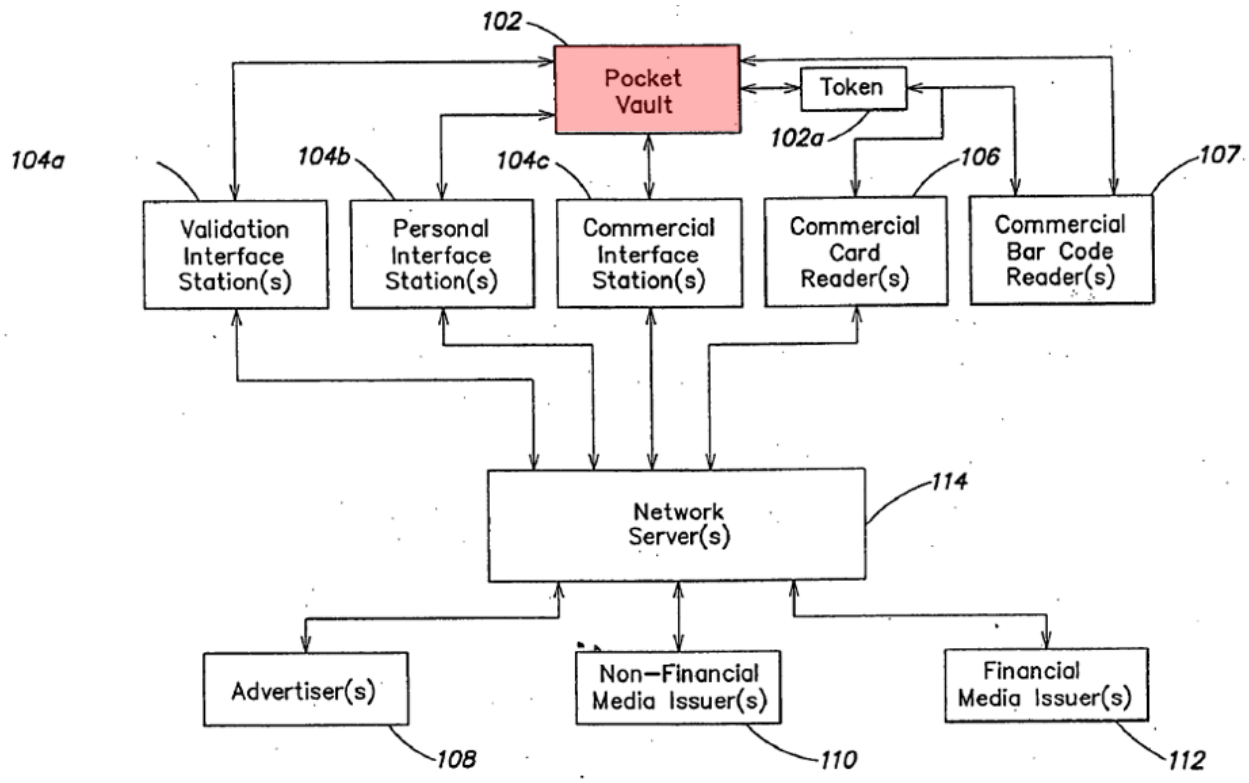


FIG. 1

MSC-1005, FIG. 1[1].

52. As shown in FIG. 1., Burger's system 100 includes the Pocket Vault 102, an associated token 102a, one or more network servers 114, several different types of interface stations 104a-c coupled to the network server(s) 114, one or more commercial card readers 106, one or more commercial bar code readers 107, and

[1] Annotations to figures in my declaration are marked up in color.

several computers 108, 110, and 112 operated by one or more advertisers, non-financial media issuers, and financial media issuers, respectively. MSC-1005, ¶¶[96]-[97]. The different components of the system 100 can be connected in a wired or wireless manner. MSC-1005, ¶¶[99]-[102]. The Pocket Vault 102 may communicate with the network server 114 directly in a wireless network or may communicate through the interface stations 104a-c. MSC-1005, ¶[101].

53. An example implementation of the Pocket Vault 102 is shown below in Burger's FIG. 2. Burger's Pocket Vault 102 "can include components similar to those used in modern personal digital assistants (PDAs) and palm top computers" such as "a controller 202, … a transceiver 204, a user input device 206, a docking interface 208, a read/write memory 210, a write-once memory 212, a power manager 214, an indicator 215, a display 216, a token port 218, and a fingerprint scanner 220, all coupled to the controller 202." MSC-1005, ¶[118]. Burger "is not limited to any particular type of memory. The memory 210 may, for example, comprise a suitable non-volatile SRAM. Similarly, any suitable memory device that permits a only [sic] single write operation to take place may be employed as the write-once memory 212." MSC-1005, ¶[127]. The Pocket Vault 102 may also include a hard-wired memory (not shown) to store device serial numbers and key operating system and encryption software components." MSC-1005, ¶[118]. A POSITA would have understood that device serial numbers are generally used to

identify a device, and, for a device such as the Pocket Vault, would have included a Pocket Vault ID (chip ID).

54. Memory 210 can include a high-security section used to "store value-based or value-linked media such as debit and credit cards and certain ID information such as driver's licenses, passports, building security passes, etc." MSC-1005, ¶[129].

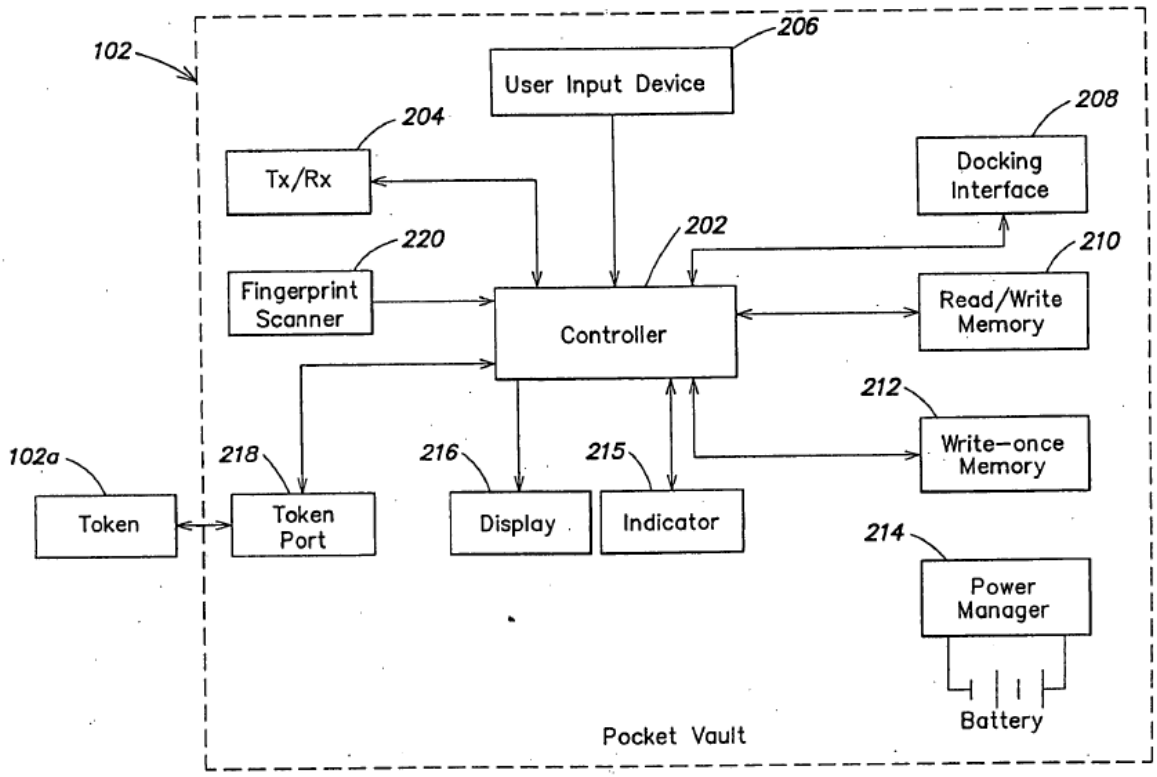


FIG. 2

MSC-1005, FIG. 2.

55. The controller 202 includes "a low-power multiprocessor or microcomputer having an on-board SRAM and/or flash memory." MSC-1005, ¶[122]. "The

controller 202 may include a software-programmable and encryption-protected or hard-wired unique chip ID. In one embodiment, this chip ID [(Pocket Vault ID)] is released from the Pocket Vault 102 only after the fingerprint scanner 220 … has successfully authenticated the identity of the holder." MSC-1005, ¶[122].

56. The Pocket Vault 102 includes a display 216 that can be used, e.g., to dynamically display branding and advertising messages. MSC-1005, ¶[110]. In addition, the display 216 can include a "touch screen or a separate user input device" to "effectively flip through the contents of the Pocket Vault 102 to locate and select a desired media (e.g., a credit card, driver's license, library card, frequent flier card, a particular RFID personality, etc.) much like a person can flip through the contents of his or her wallet to do the same." MSC-1005, ¶¶[109], [132], [133]. "By manipulating the user input device 206, a Pocket Vault holder may select one of a number of media stored in memory of the Pocket Vault 102 for display and/or use in connection with a transaction, and may otherwise control or provide input to software executing on the controller 202." MSC-1005, ¶[125].

57. The Pocket Vault 102 can also include or be coupled to a token 102a, which "may be used by the Pocket Vault holder to engage in a transaction." MSC-1005, ¶[103]. Token 102a can be released from the Pocket Vault 102 and can include a display device to display information such as credit card information and used in transactions with retailers. MSC-1005, ¶¶[103]-[104], [155]-[158]. For example,

"[w]hen used by a consumer, retailers may verify authenticity by matching the information displayed on the token 102a with that revealed in the swipe or other token reading process. Without a match, the token 102a may be rejected." MSC-1005, ¶[158].

58. Burger's Pocket Vault 102 also includes a fingerprint scanner 220. MSC-1005, FIG. 2. The fingerprint scanner 220 can, in some implementations, refer to "any device capable of accurately scanning a fingerprint of an individual for comparison with one or more fingerprint images stored in memory." MSC-1005, ¶[135]. "In addition to or in lieu of a fingerprint scanner, other bio-metric scanning devices may also be employed to verify the identity of the holder. For example, some embodiments may employ a charge coupled device (CCD) to serve as an iris or retina scanner, an optical sensor, and/or a voiceprint." MSC-1005, ¶[135].

59. When a user is interested in using the device, the user's biometric feature (e.g., fingerprint scan, retina scan, etc.) is used to authenticate the user. MSC-1005, ¶[112]. "In one illustrative embodiment, authentication information used to validate the holder's identity (e.g., the stored fingerprint and/or PIN code) is stored within the to-be-accessed device," the Pocket Vault, "and the validation is performed in its entirety on-board the same device, such that the user-specific authentication information never leaves the device in which it is stored. Thus,

using this technique, the likelihood that such information will be intercepted by unauthorized third parties may be reduced significantly." MSC-1005, ¶[112]. Burger explains that "great care may be taken to ensure that only authorized individuals are permitted to validate Pocket Vaults 102 by having their authentication information (e.g., their fingerprint data or PIN codes) stored therein. Therefore, after it has been confirmed that the holder's authentication information has been properly stored in the Pocket Vault 102, a trust relationship may be established between the network server 114 and the Pocket Vault 102. This relationship may involve, for example, the registration of a unique encrypted chip ID of the Pocket Vault 102 with the network server 114 through a secure Internet connection, the distribution of a digital certificate (e.g., a PKI certificate) to the Pocket Vault 102, and the grant of authority to the Pocket Vault 102 to permanently store the Pocket Vault holder's authentication information." MSC-1005, ¶[114]. "Because of the creation of the above-described trust relationships, each Pocket Vault 102 and each interface station 104 may communicate securely with the network server 114." MSC-1005, ¶[116].

60. Burger's network server(s) 114 can "serve as: (1) a repository of information for the network, (2) the entity that controls access to the stored information by the other network devices, and (3) a service provider for financial and non-financial media issuers, advertisers, as well as Pocket Vault holders." MSC-1005, ¶¶[98],

[117], FIG. 1. In one example shown in FIG. 4 (reproduced below), the network server 114 may include a database 406 that stores "a real-time record of critical reference data along with transaction histories, back-up files, and security audit trail information for key events. Examples of specific items that may be stored in the database 406 include: a list of current Pocket Vault holders and appropriate contact information for each; records regarding the versions of software loaded onto each Pocket Vault 102, … a list of currently authorized or registered Pocket Vaults 102, identified by chip ID and linked to the holder list; a list of currently authorized or registered tokens 102a, identified by chip ID and linked to the holder list; … authorized media data received from media issuers that has not yet been downloaded to individual Pocket Vaults 102; backup data sets for individual Pocket Vault holders." MSC-1005, ¶[146], FIG. 4.

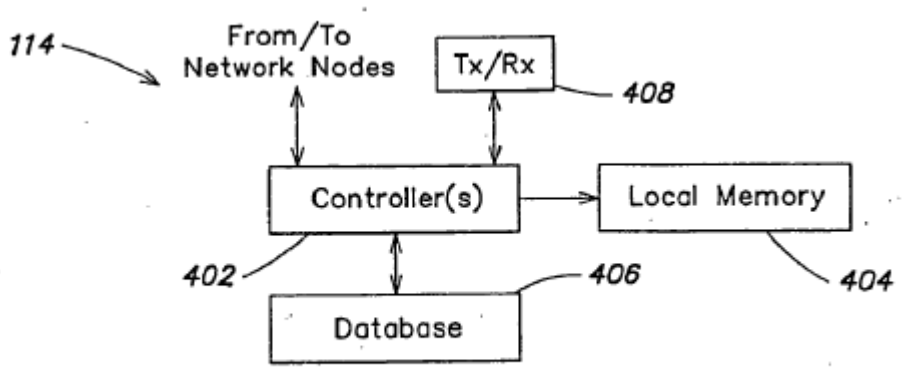


FIG. 4

MSC-1005, FIG. 4.

61. Another example of an implementation of a network server 114 is shown in FIG. 27, which depicts "a block diagram illustrating several additional features that may optionally be added to a network system such as that shown in FIG. 1 so as to enhance the functionality of the network." MSC-1005, ¶¶[0077], [0531]. "The network server 114 may include one or more controllers 402 and a database 406, as described above in connection with FIG. 4. In addition, the network server 114 may include a communication protocol layer 2716, which provides low-level communication functions to server communications software." MSC-1005, ¶[0540]. "Overall, the networking arrangement illustrated in FIG. 27 allows the Pocket Vault 102 to access the network server 114." MSC-1005, ¶[0542].

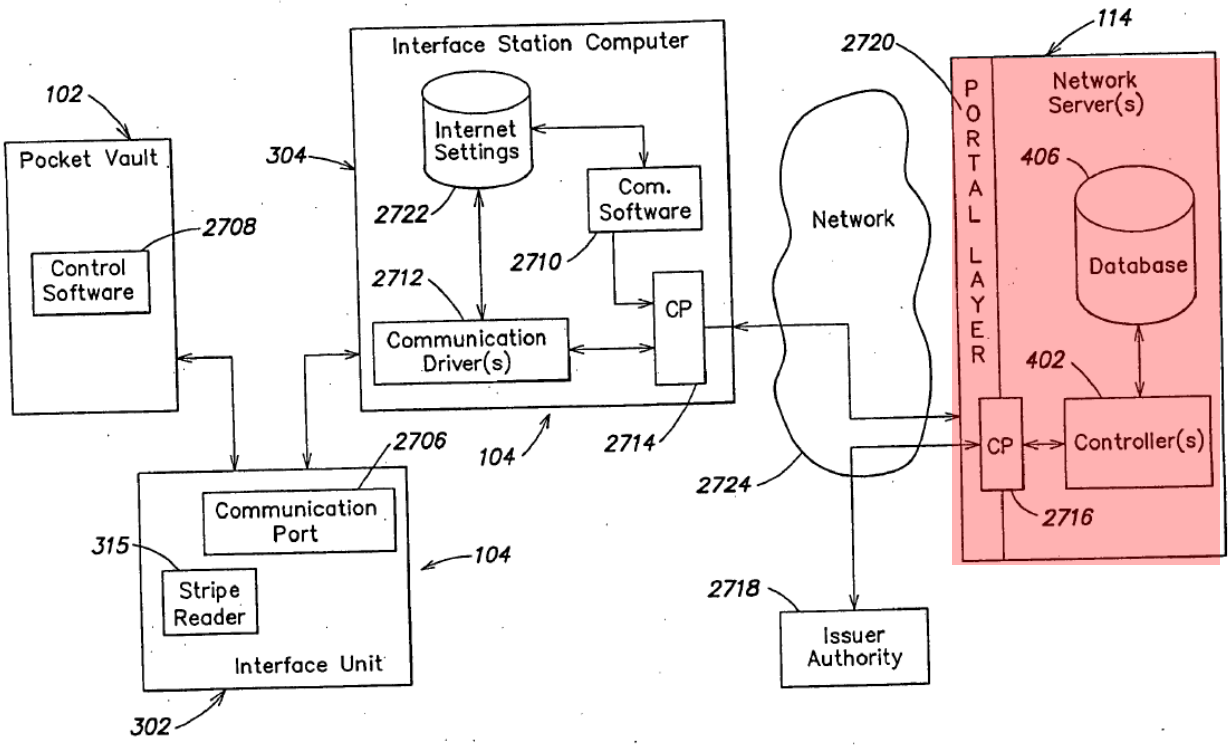
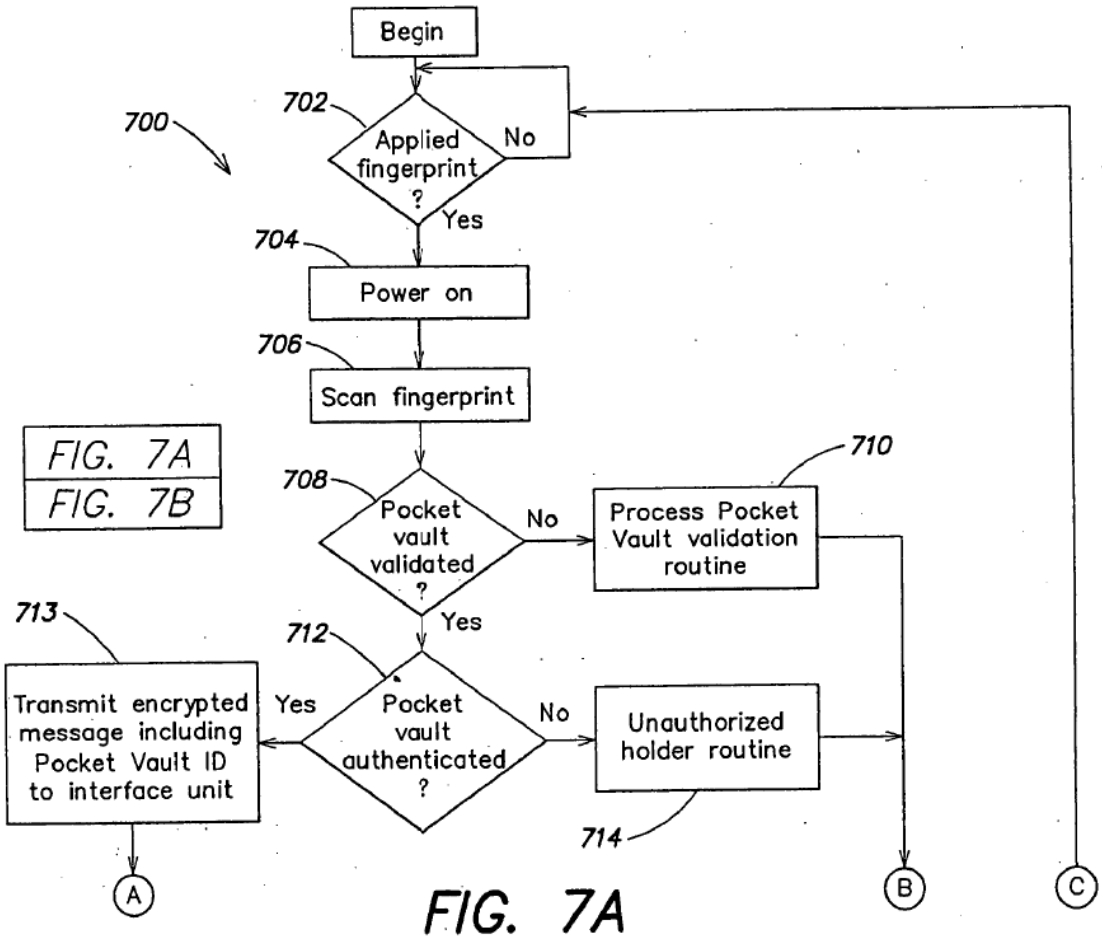


FIG. 27

MSC-1005, FIG. 27.

62. An example method of using Burger's Pocket Vault 102 to perform user and device authentication is shown in Burgers' FIG. 7A below. As shown in FIG. 7A, when a user applies the user's fingerprint to the fingerprint scanner 220, the power manager 214 powers on the Pocket Vault 102. MSC-1005, ¶¶[178]-[181]. "[T]he fingerprint scanner 220 [then] scans the applied fingerprint of the Pocket Vault holder" and determines whether the Pocket Vault 102 has been validated (step 708). MSC-1005, ¶¶[181]-[182]. Burger explains that "[i]n one embodiment, the Pocket Vault 102 is not validated until: (1) a user's fingerprints have been stored in the fingerprint memory (e.g., the write-once memory 212 of FIG. 2), and (2) the Pocket Vault 102 has received and stored encrypted validation information (e.g., a PKI certificate) from the network server 114." MSC-1005, ¶¶[182].



MSC-1005, FIG. 7A.

63. "When, at the step 708, it is determined that the Pocket Vault 102 has already been validated," at step 712 "it is determined whether Pocket Vault 102 has been authenticated, e.g., whether the fingerprint scanned at the step 706 matches one of the fingerprints stored in the fingerprint memory 212." MSC-1005, ¶¶[183]-[184], [209]-[210]. After "it is determined that the Pocket Vault 102 has been properly authenticated," "an encrypted message including the unique Pocket

Vault chip ID is transmitted to the pocket vault interface unit 302" or network server 114 at step 713. MSC-1005, ¶¶[185]-[186], [101], [114]-[116].

64. Burger then teaches that, in some embodiments, a check is performed to ensure that components used to interface the Pocket Vault 102 with the other components in the network 100 (either wirelessly or directly) are in place and operating correctly, and subsequently, a Pocket Vault holder is granted access to the contents of his or her Pocket Vault 102. MSC-1005, ¶[187].

65. In some embodiments, after the unique Pocket Vault chip ID is transmitted and a token 102a (e.g., Chameleon Card) is determined to be on-board the Pocket Vault 102, an "AUTHORIZED HOLDER" routine (step 722) is performed, as shown in FIGS. 7B, 10A, (reproduced below) and 11. MSC-1005, ¶¶[189]-[195]. In the "AUTHORIZED HOLDER" routine, advertisements sent from an advertiser 108 to the network server 104 are provided to the Pocket Vault 102 for display. MSC-1005, ¶¶[236]-[238], FIG. 10A. In addition, a user can make selections to enter a wireless transaction. MSC-1005, ¶¶[257]-[262], FIGS. 10A, 11.

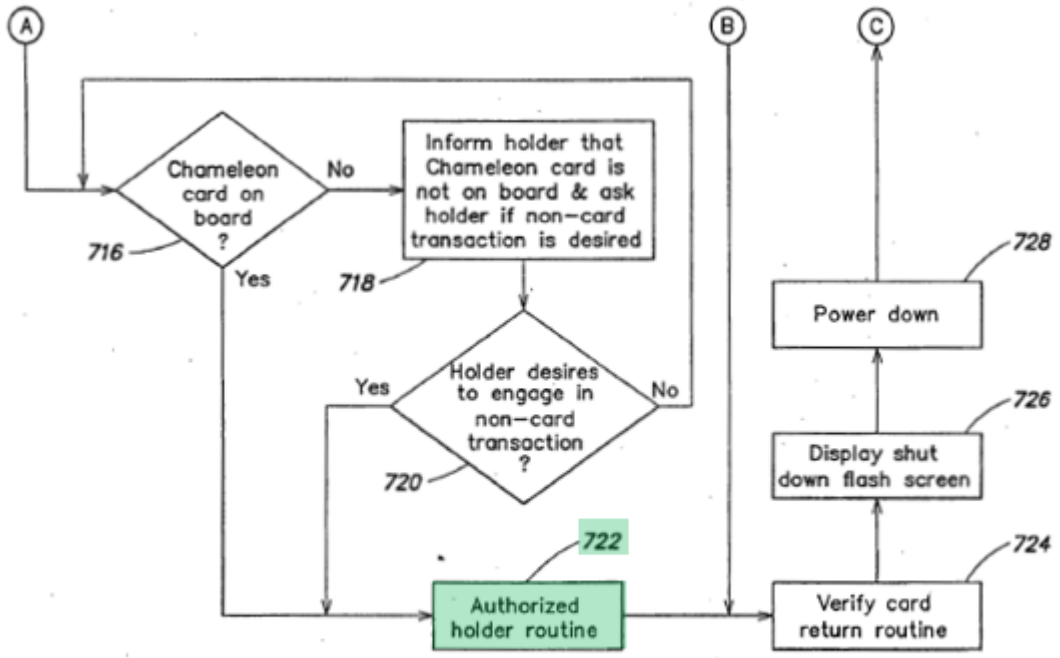


FIG. 7B

MSC-1005, FIG. 7B.

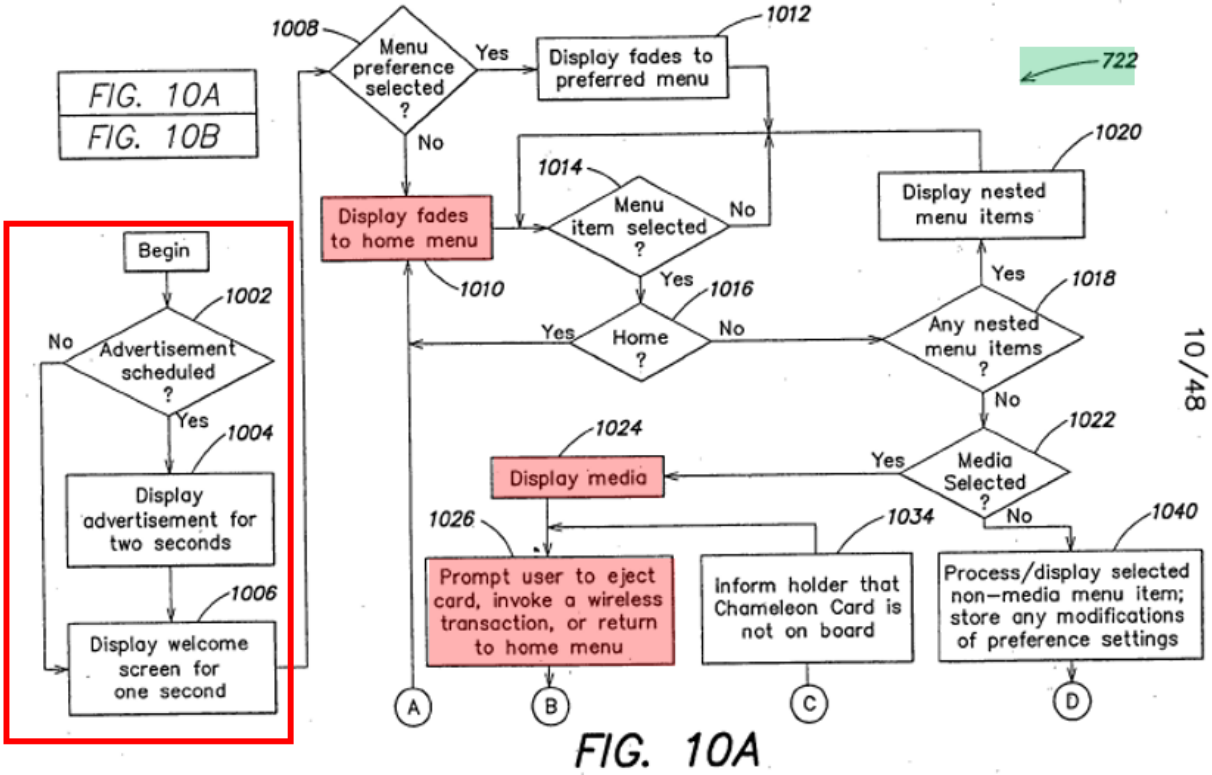


FIG. 10A

MSC-1005, FIG. 10A.

66. Burger's Pocket Vault 102 can be used to execute a transaction. MSC-1005, FIGS. 19, 24, 25. As noted above, the Pocket Vault can be used as a "wallet replacement" and can be used in a transaction. MSC-1005, ¶[93]. For example, when a request to authorize a transaction has been made, Burger's network server 114 implements the operations depicted in FIGS. 24 and 25 (reproduced below). MSC-1005, FIG. 19, ¶[0474].

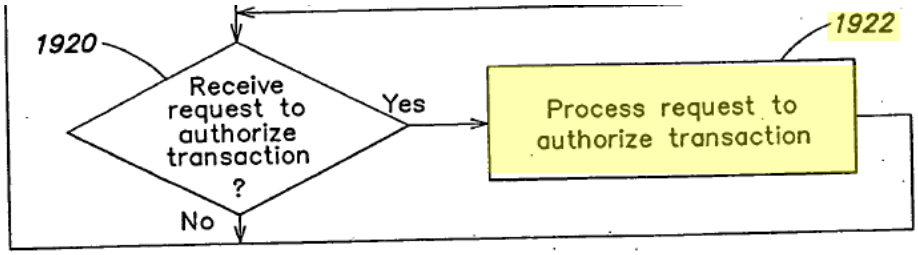


FIG. 19

MSC-1005, FIG. 19.

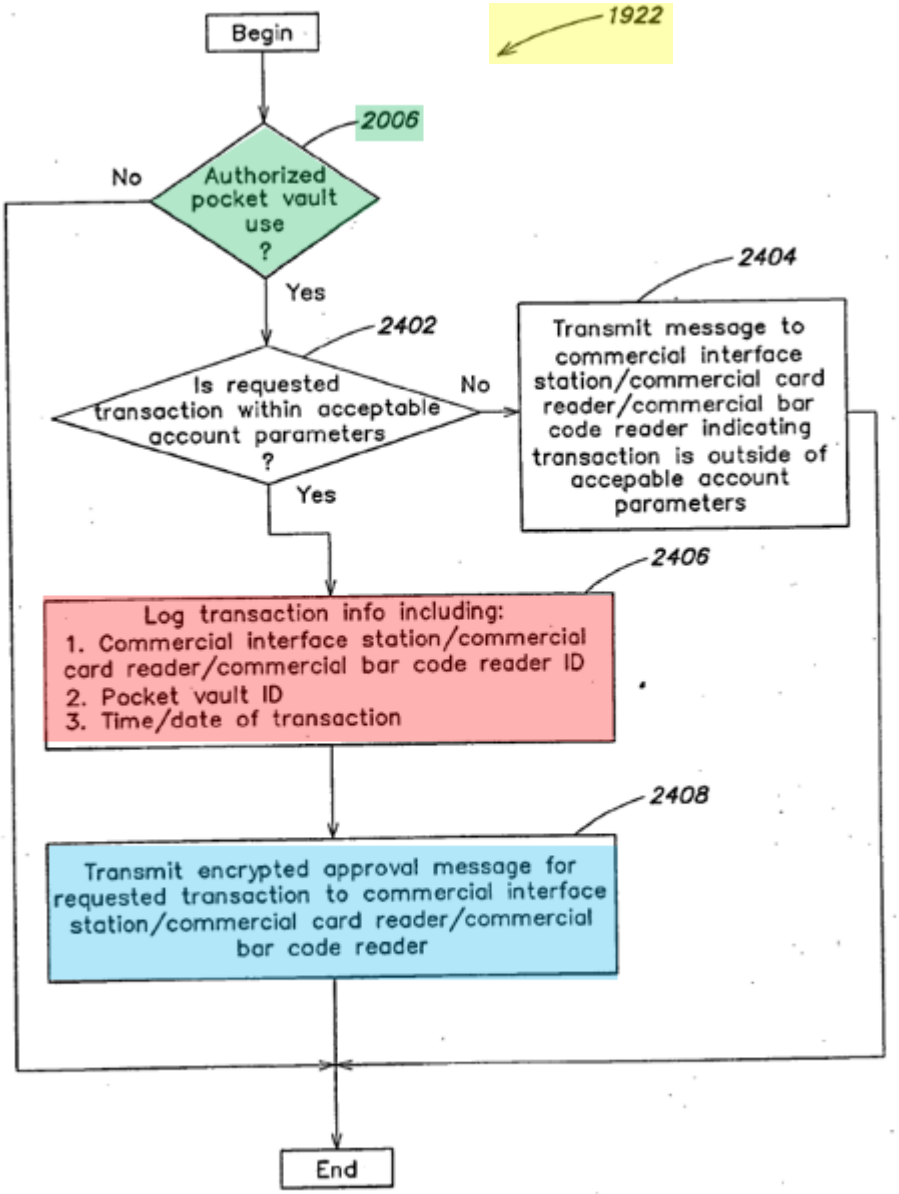
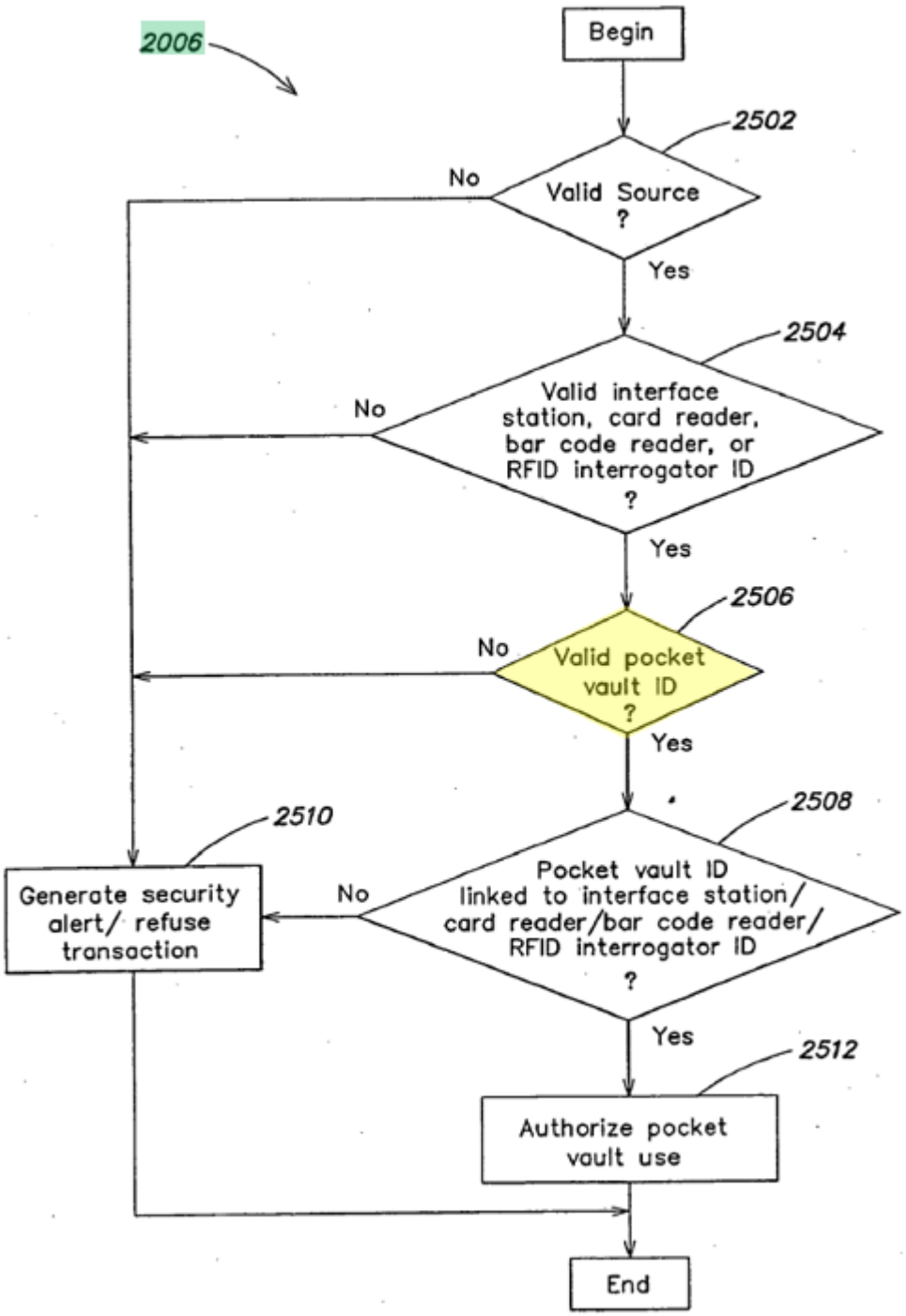


FIG. 24

MSC-1005, FIG. 24.



MSC-1005, FIG. 25.

67. For example, in response to the request to authorize a transaction, the network server 114 determines whether the Pocket Vault 102 is authorized. MSC-

1005, FIGS. 24, 25; ¶¶[0511]-[513]. To determine whether the Pocket Vault 102 is authorized, it is determined (1) whether the point of sale terminal or other entity with which a transaction is being attempted is connected to a valid source, and (2) whether the ID of the interface station, card reader, barcode reader or RFID interrogator is valid, and is properly linked to the source to which is connected. MSC-1005, FIG. 25; ¶¶[0520]-[523]. If the network server 114 determines that there is a valid source and the ID is valid, the network server 114 proceeds to determine whether the Pocket Vault ID is valid, and upon, doing so, determines that the Pocket Vault 102 is authorized. MSC-1005, FIG. 25; ¶¶[0524]-[529], [182].

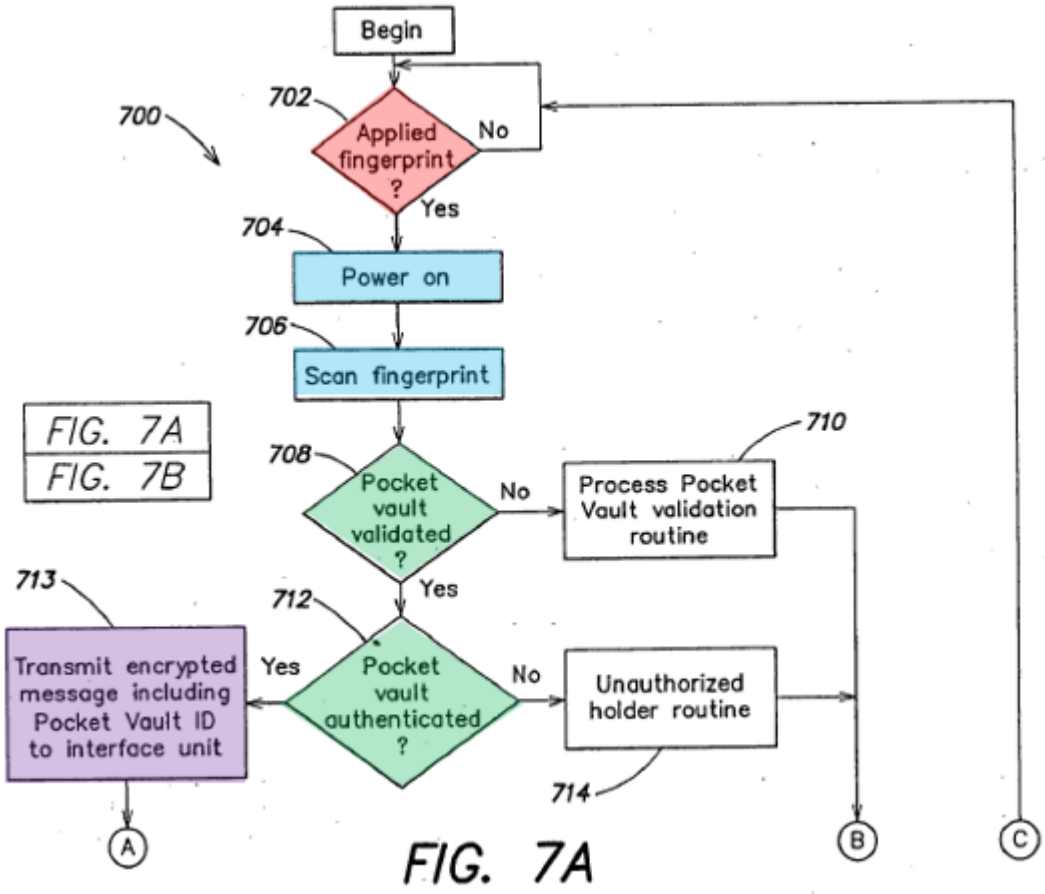
68. Once the Pocket Vault 102 use is authorized, "it is determined whether the requested transaction is within acceptable account parameters." MSC-1005, FIG. 24; ¶[0514]. "When … it is determined that the requested transaction is within acceptable account parameters, information regarding the transaction is logged into the database 406 of the network server 114 (FIG. 4). As shown [in FIG. 24], the logged information may include the identification of the entity with which the transaction took place, the Pocket Vault ID (if available), and the time and date of the transaction." MSC-1005, FIG. 24; ¶¶[0511]-[513]. "[A]n encrypted approval message is transmitted to the entity with which the transaction is being attempted

(e.g., a commercial interface station 104C, a card reader 106, or a barcode reader 107)." MSC-1005, FIG. 24; ¶[0518].

Example Use Case

69. To better illustrate how Burger's system would have been used, I describe an example use case of one implementation of Burger's system based on the teachings of Burger. Citations indicating support for the described details are also provided.

70. When a user is interested in using the Pocket Vault 102 for a transaction (e.g., when the user is at a grocery store or retail store), the user places the user's finger on the Pocket Vault scanner (*see* red annotated diamond in FIG. 7A below). MSC-1005, FIG. 7A, ¶¶[320], [158], [95]. The Pocket Vault activates and then obtains a biometric scan (e.g., fingerprint or retina scan) (*see* blue annotated rectangles in FIG. 7A below) of the user and checks to see if a matching record is stored in the Pocket Vault memory (*see* green annotated diamonds in FIG. 7A below). MSC-1005, FIG. 7A. In response to determining that the scanned biometric data matches the stored biometric data, the Pocket Vault transmits its Pocket Vault ID to the network server 114 (*see* purple annotated rectangle in FIG. 7A below). MSC-1005, FIG. 7A. A check is then performed to ensure that the components used to interface the Pocket Vault 102 with the other components in the network 100 (either wirelessly or directly) are in place and operating correctly. MSC-1005, FIGS. 7A, 7B, ¶[187].



MSC-1005, FIG. 7A.

71. Next, the Pocket Vault holder determines that the Pocket Vault includes a token 102a (also referred to as Chameleon Card), an Authorized Holder Routine (step 722) is performed (*see* yellow annotations in FIG. 7B below) in which a welcome screen and ads are displayed. A user can select, through a displayed menu, a desire for executing a transaction using the Pocket Vault (*see* red annotations in FIG. 10A below). *See e.g.,* MSC-1005, step 722 in FIG. 7B, step 1026 in FIG. 10A; steps 1920, 1922 in FIG. 19; ¶¶[320], [189], [158], [95], [96], [125], [236]-[238], [155]-[158].

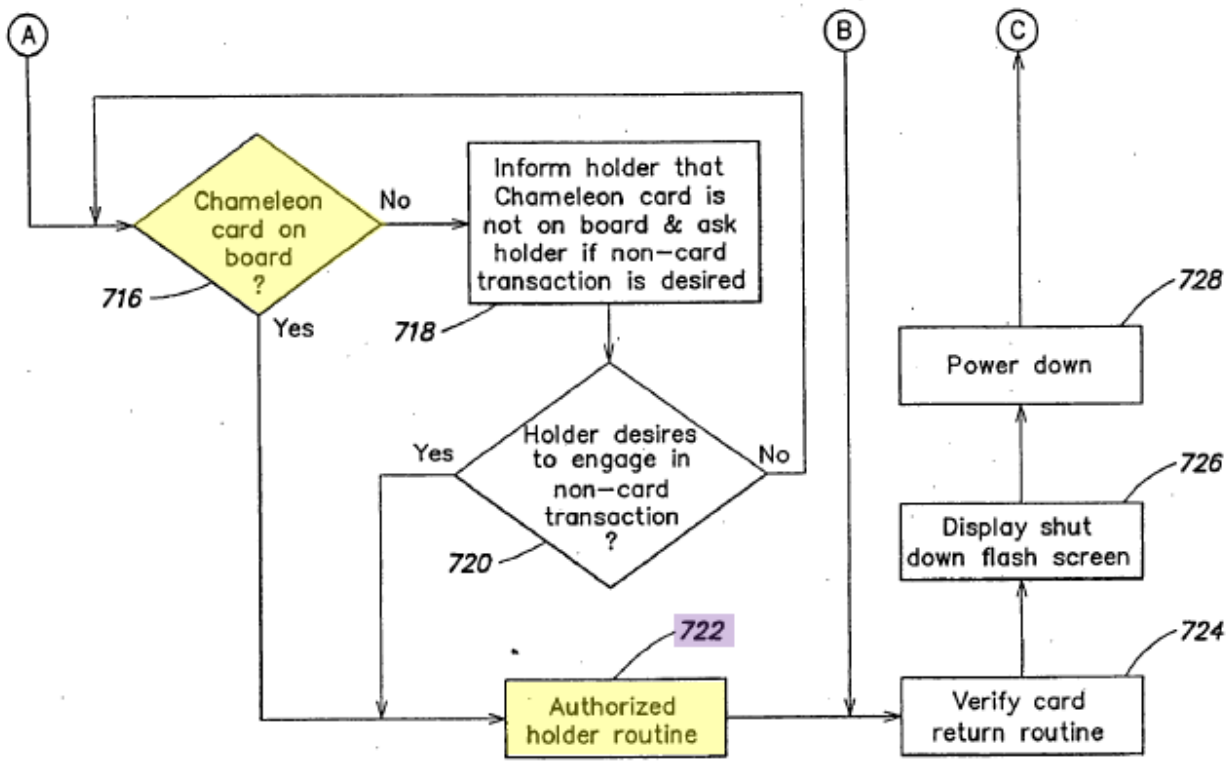


FIG. 7B

MSC-1005, FIG. 7B.

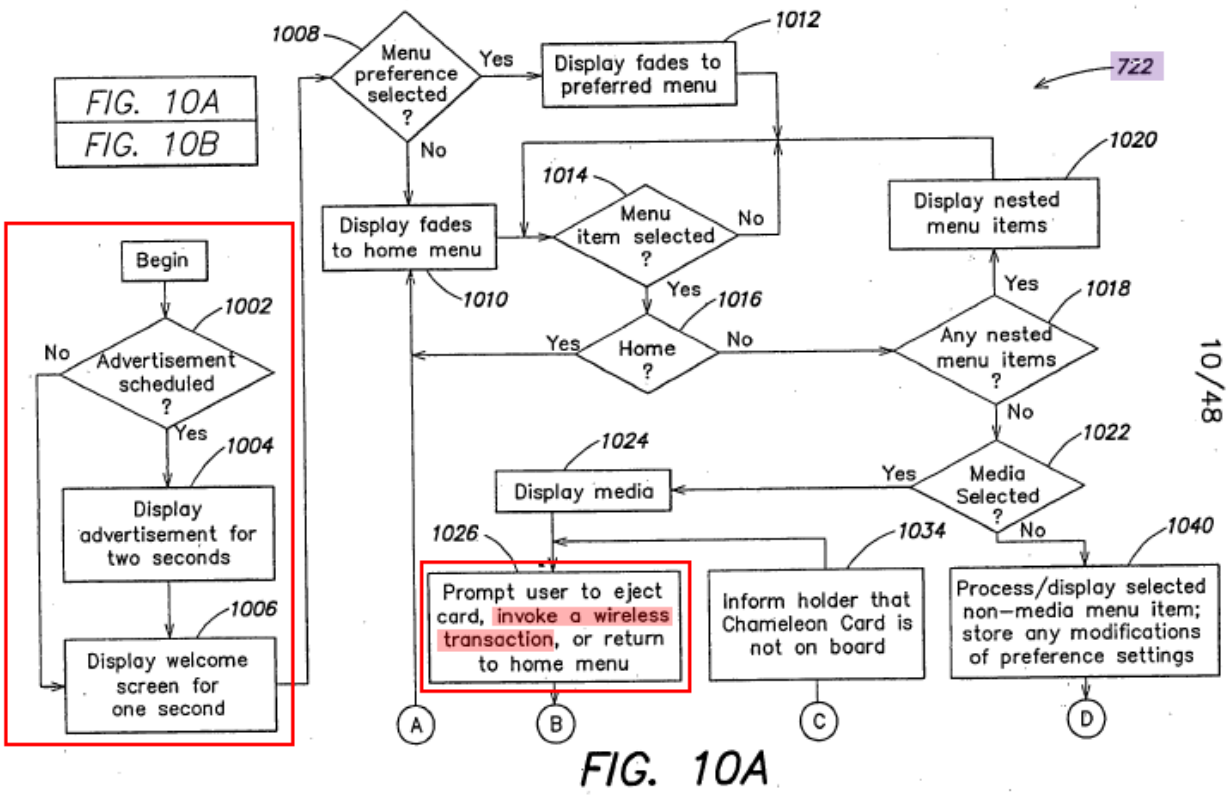


FIG. 10A

MSC-1005, FIG. 10A (displaying the steps performed in the Authorized Holder Routine 722 of FIG. 7B).

72. The network server 114 then determines whether the Pocket Vault is authorized to be used, e.g., by checking whether the transmitted Pocket Vault ID matches a stored ID in the network server 114, and then transmits an approval message for the transaction. MSC-1005, FIGS. 19 (steps 1920, 1922), 24 (steps 2006, 2406, 2408), 25 (Steps 2506), ¶¶[0511]-[529], [182].

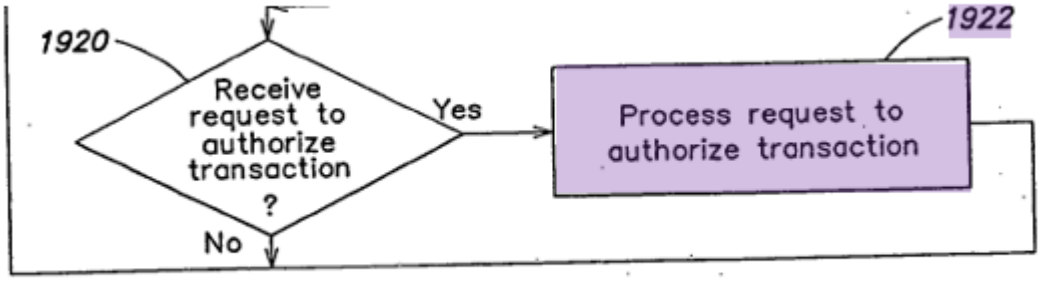


FIG. 19

MSC-1005, FIG. 19 (bottom portion of FIG. 19).

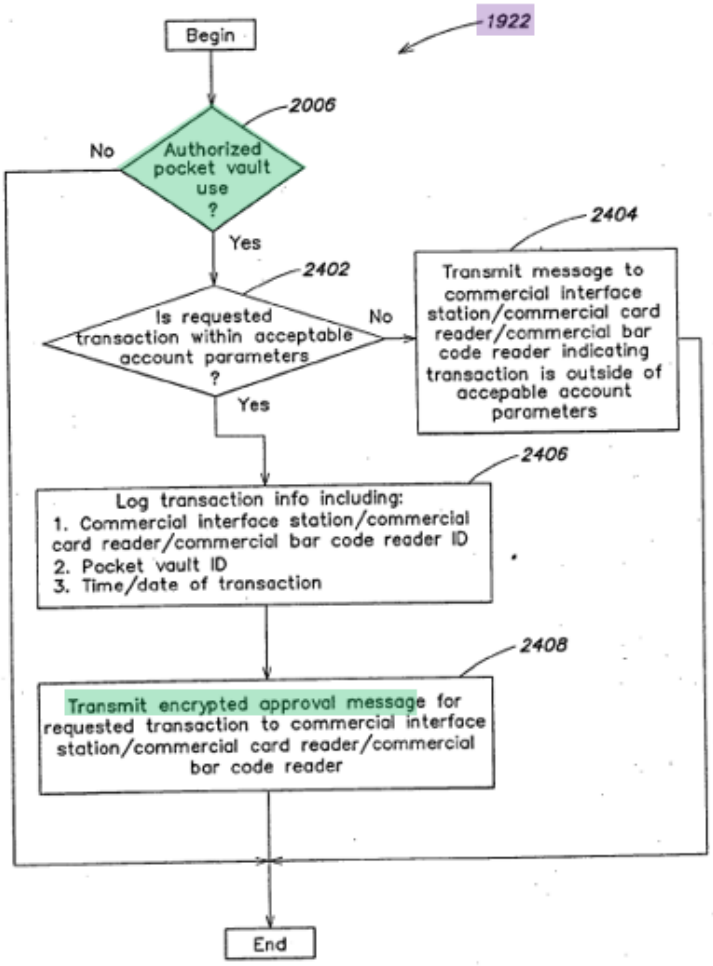


FIG. 24

MSC-1005, FIG. 24 (displaying) the steps performed in the step(s) of processing a request to authorize a transaction of FIG. 19.

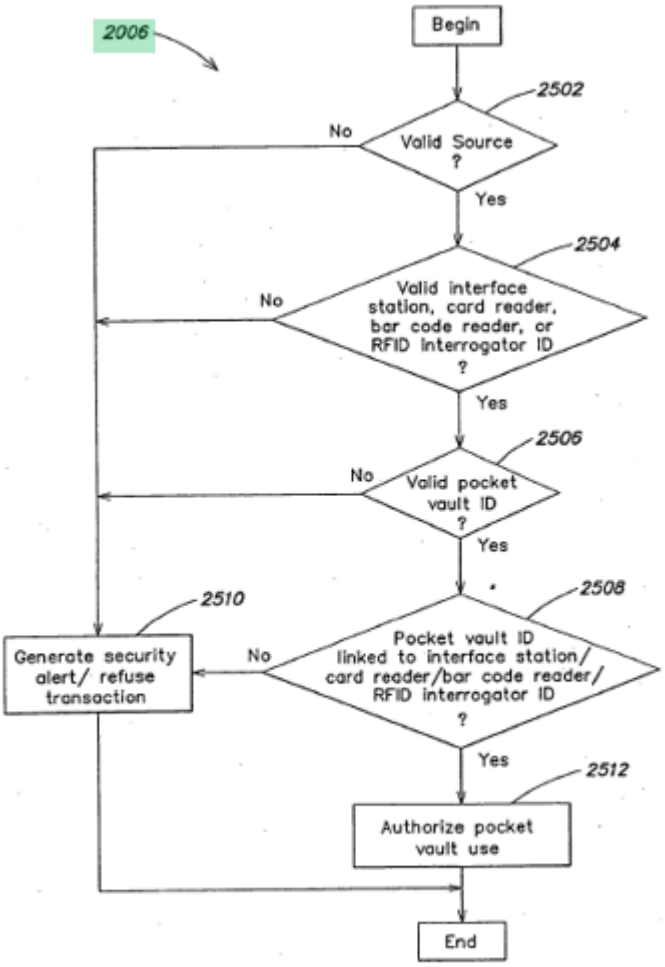


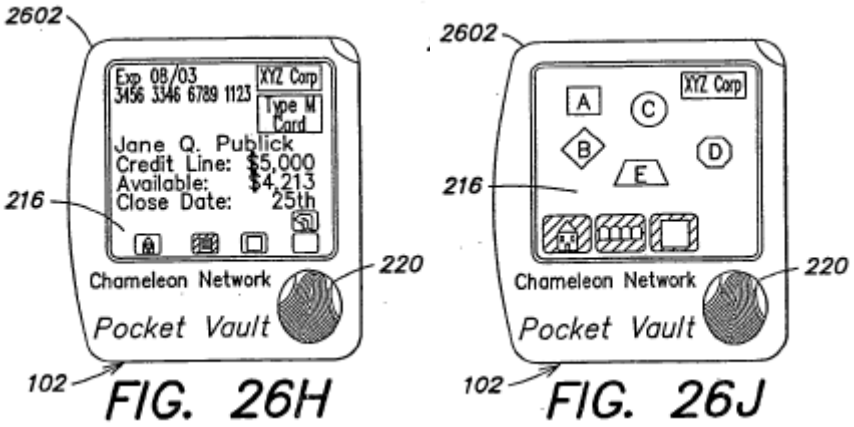
FIG. 25

MSC-1005, FIG. 25 (displaying the steps performed in the operation 2006 of authorizing use of a Pocket Vault in FIG. 24).

73. For instance, "[i]n the example of FIG. 26H, the preferred menu immediately shows the holder's preferred credit card as the selected menu item. Should the holder opt to use this media to engage in a transaction, the holder can simply choose the media directly. Alternatively, the holder may opt to access the HOME menu or other menu items by selecting appropriate icons displayed on the

screen. In the example of FIG. 26J, the preferred menu immediately shows, perhaps, a selected group of the holder's most frequently used menu items." MSC-1005, ¶[242]. A retailer may verify authenticity by matching the information displayed on the token 102a (or Pocket Vault 102) with that revealed in a swipe or other token reading process." MSC-1005, ¶[158].

74. In the above-described manner, a user or Pocket Vault holder would be able to securely use the Pocket Vault to execute a transaction, such as a financial transaction with a retailer.



MSC-1005, FIG. 26H, 26J.

B. Robinson

75. Robinson relates to "a reliable system and method that conducts age verification of individuals for access to age-restricted areas, goods, and services" and for use in "verification [of] *an age-restricted transaction with the use of a biometric read* (such as a fingerprint) and a system ID (SID) number entry." MSC-1006, ¶¶[0009]-[0010]. "[I]individuals trying to verify their own age" are

referred to as "presenters" in Robinson. MSC-1006, ¶[0010]. Robinson explains that:

> *To register in the system*, an individual presents at least one biometric sample, identity-verifying information, and *age-verifying information*. The biometric sample may be, for example and without limitation, a fingerprint, a retinal scan, a face geometric scan, or a voice print. The identity-verifying information may be, for example and without limitation, a name, a home address, a telephone number, or a government ID number and state of issue. *The age-verifying information may be, for example and without limitation, age, date of birth, or a driver's license scan. The individual also registers with the system a system identification number (SID)* that is used in conjunction with their biometric scan for age verification.
>
> An individual who has already registered in the system may verify their age at any participating POV by entering the individual's SID and biometric sample. This information is sent to a database where it is used to find the individual's age verifying record. Once the age verifying record is found, the individual's age is evaluated to determine whether or not it is at or above the level pre-set for the particular verification. If the individual's age is at or above the pre-set level, the individual's age is verified, and the individual is granted access. This access may be used for (but is not limited to) purchasing age-restricted goods, accessing age-restricted areas, or purchasing age-restricted services.

MSC-1006, ¶¶[0014]-[0015].

76. To implement the age-verification method, Robinson discloses a system that includes a verifier database 124 that contains age verification records or a central database 102 that stores data related to presenters and authorized points of verification (POVs). MSC-1006, ¶¶[0026]-[0027], [0030], FIG. 1. "Age verifying records hold presenter age verifying and identity verifying information, such as a presenter's age, date of birth, government ID number and state of issue, home address, or a telephone number; at least one biometric template; and *at least one ID number (SID)* that identifies the presenter within the system." MSC-1006, ¶[0028]. "The SID is a number used to help identify registered individuals in the invention's system. … The SID may be a unique number (a number with no chance of being honestly duplicated, e.g. social security number), reasonably unique number (a number with a statistically small chance of being duplicated, e.g. phone number), or a non-unique number (a number with a large chance of being duplicated)." MSC-1006, ¶[0043].

77. Presenters who want to participate in age-verification can pre-enroll with the age-verification system. MSC-1006, ¶¶[0032], [0034]. Pre-enrollment records can be stored in the verifier database 124 and/or the central database 102. MSC-1006, ¶[0032]. The enrollment process can include a check with other databases, such as a state or government database, to obtain presenter information such as driver's license data or employment data. MSC-1006, ¶¶[0034], [0040].

78. The age verification can be conducted by "verifier devices connected to a verifier database 124, such as a register 130 or presenter service computer 126" or devices such as kiosks, vending machines, PCs, or a wireless device attached to a biological identification device (BID). MSC-1006, ¶¶[0035], [0030]. Robinson's FIG. 3 depicts one example method for performing age verification. As shown in FIG. 3, "[t]he presenter enters their SID and their biometric sample (herein referred to as the "transaction biometric') and transaction information, which is then sent to the verifier database 304 where the presenter's age is verified. MSC-1006, ¶¶[0054]-[0057], FIG. 3. After the presenter's age has been verified (or declined), the verifier device outputs the verification result, e.g., through a digital display or printed receipt. MSC-1006, ¶¶[0057]-[0058], [0048], FIG. 3. Robinson's "verification [method] allows the system to track verifier behavior within the system, so that if a particular verifier falls under suspicion of fraudulent verification activity, each enrollment that verifier has confirmed may be evaluated." MSC-1006, ¶[0048].

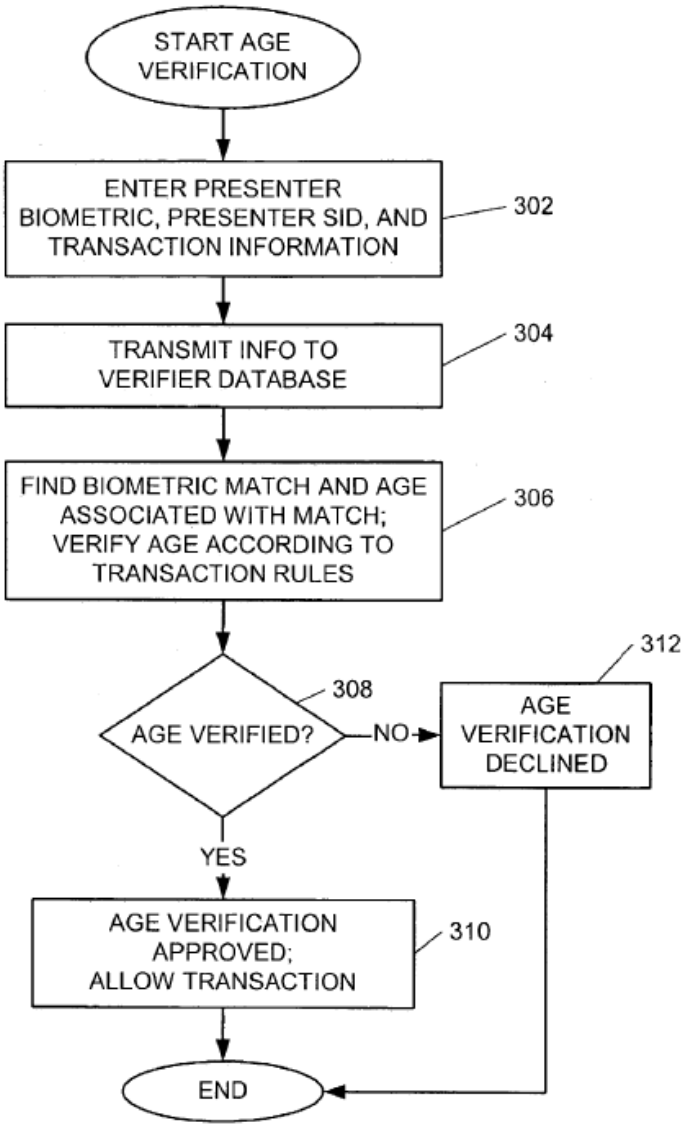


FIG. 3

MSC-1006, FIG. 3.

C. Combination of Burger and Robinson

79. Burger discloses a device and user authentication system that uses user biometric data, like fingerprint or retina scan, for various applications and transactions. MSC-1005, FIG. 7. Robinson explains that "both the employee and

merchant" of a business selling an age-restricted item, "may suffer monetary penalties and/or the merchant may even have their license to sell age-restricted goods revoked as a result of their employee's careless behavior." MSC-1006, ¶[0005]. Accordingly, it would have been obvious to a POSITA to incorporate the age verification method of Robinson in Burger so that Burger's system can be used by businesses interested in conducting transactions that require age-verification. Examples of such transactions include, e.g., buying alcohol or tobacco products, obtaining a driver's license or passport at a government office, entering or playing certain games at a casino, or being shown an advertisement for alcohol, tobacco, or gambling.

80. Combining the teachings of Burger and Robinson would have simply involved combining prior art elements according to known methods to yield predictable results and/or applying a known technique to a known device ready for improvement to yield predictable results. In particular, a POSITA would have understood that Robinson's age-verification method would have been implemented in Burger's system by allowing a user to present age-verifying information along with biometric sample and identity-verifying information, and *age-verifying information* when enrolling a user into an age-verification program. The age-verification information would have been stored in the database 406 of Burger's network server 114, which includes the verifier database described in Robinson.

When a user is involved in a transaction that requires age verification, the user enters the user's SID and biometric sample at a verifier device (e.g., a device used by the retailer). MSC-1006, ¶¶[0054]-[0057], FIG. 3. The verifier device sends the entered information to the network server, which verifies the user's age. MSC-1006, ¶¶[0054]-[0057], FIG. 3. If the user's age is authenticated, a confirmation message is then output by the verifier device. MSC-1006, ¶¶[0057]-[0058], [0048], FIG. 3.

81. The above-described combination would have been predictable and had a reasonable expectation of success because it merely involves combining known elements in a manner that would have been easily implemented and obvious to a POSITA. For instance, it would have been well-within the capabilities of a POSITA to receive user age-verification information at a verifier device, implement a database in a network server that stores age-verification information, send age-verification information from the verifier device to the network server, and perform age-verification by comparing the age-verification information provided by the verifier device to information stored in the network server. The combination would also have been predictable and obvious because, as described by Robinson, businesses selling age-restricted items could be penalized or have their licenses revoked if they did not verify a user's age. MSC-1006, ¶[0005]. Thus, a POSITA would have been motivated to combine the teachings of Burger

and Robinson in the above-noted matter to provide a simple solution to perform age-verification when selling age-restricted goods.

VIII. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '730 CLAIMS UNPATENTABLE

A. Ground 1: Claims 1, 2, 4-9, 11, 12, and 14-17 are obvious over Burger

(i) ***Claim 1***

[1.pre] A method for verifying a user during authentication of an integrated device, comprising the steps of:

82. Burger teaches systems, methods, and apparatus directed to "***verifying a user during authentication of an integrated device***." MSC-1005, ¶[0010]. As explained below in [1.1]-[1.7], Burger discloses verifying a Pocket Vault holder ("***user***") during authentication of a Pocket Vault 102 ("***integrated device***"). The Pocket Vault 102 can then be used in transactions involving financial and/or non-financial media. MSC-1005, ¶¶[0002], [0127]-[0128].

83. Burger's Pocket Vault 102, shown below in FIG. 2, is an integrated device at least because it integrates a plurality of components including a fingerprint scanner 220, display 216, memories 210, 212, and token 102a/token port 218. MSC-1005, ¶¶[0118], [0134]. "Because the device may incorporate many different media that are commonly stored in a person's wallet or elsewhere, possibly including both financial and non-financial media," the device may also be referred to as a multi-

purpose "point-of-transaction" device. MSC-1005, ¶[0094]. The Pocket Vault 102 is self-contained with a set of authentication security features to ensure privacy. MSC-1005, ¶[0095].

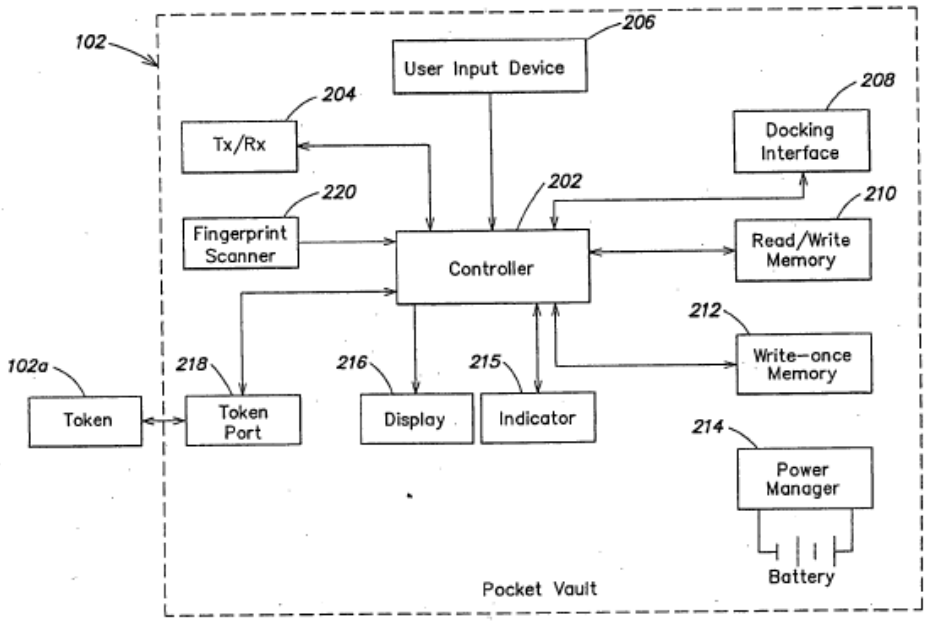


FIG. 2

MSC-1005, FIG. 2.

[1.1] persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered;

84. Like the 730 patent, Burger recognizes the importance of storing biometric data on the same device that authenticates a user's biometric scan. MSC-1005, ¶[112] ("the validation is performed in its entirety on-board the same device, such that the user-specific authentication information never leaves the device in which it

is stored"), ¶[114]. Burger's Pocket Vault 102 includes a write-once memory 212 or any suitable memory device that permits only a single write operation to take place ("***a storage element on the integrated device that is unable to be subsequently altered***"). MSC-1005, ¶¶[127], [182], FIG. 2 (reproduced below).

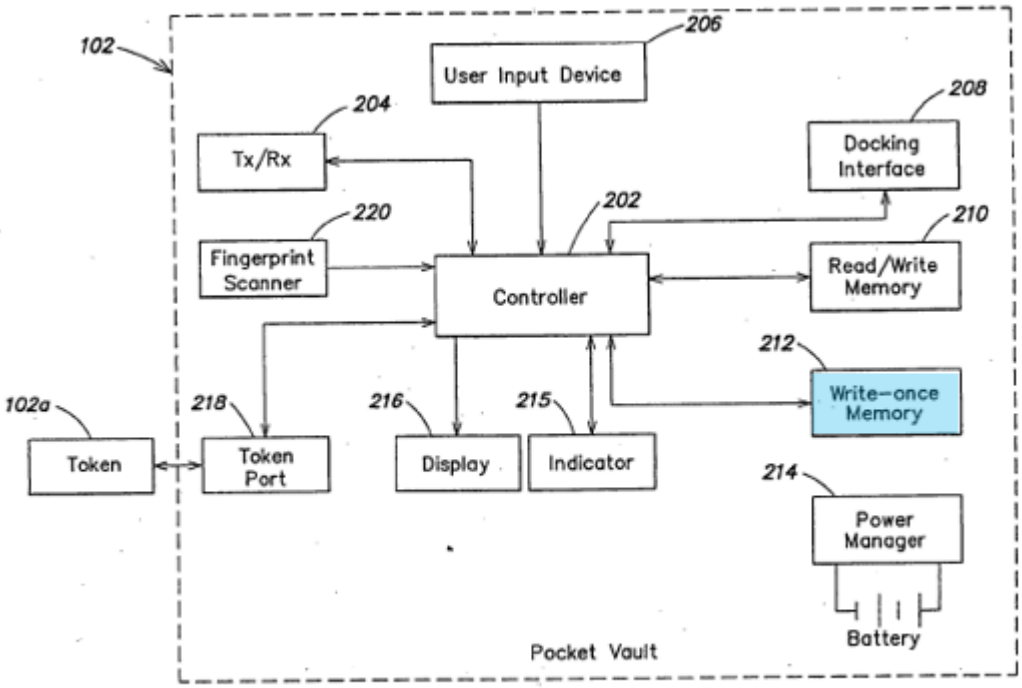


FIG. 2

MSC-1005, FIG. 2.

85. The Pocket Vault 102 stores authentication information, such as user fingerprints ("***biometric data of the user***"), device serial numbers such as a Pocket Vault ID (chip ID), and encryption/decryption information ("***a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value***"). MSC-1005, ¶¶[0112], [114],

[118], [122], [127], [129]. Indeed, Burger teaches that the network server 114 provides the PKI certificate to the Pocket Vault 102 and grants the Pocket Vault 102 authority to permanently store authentication information (***"persistently storing biometric data …"***). MSC-1005, ¶¶[114], [182].

86. In particular, a POSITA would have understood that a device serial number is typically unique to the device and would have, therefore, been often used as a device ID to advantageously distinguish that particular device from other devices. For example, device serial numbers in mobile devices can be referred to as International Mobile Equipment Identity (IMEI) and can be 14 or 15 digits long identification numbers of the mobile device. MSC-1009, 3. A well-known graphic example of a serial number identifying a wireless adapter is also shown below and includes various alphanumeric characters to identify the wireless adapter.

MSC-1026, 2.

87. Based on the well-known use of device serial numbers in the form of multiple alphanumeric characters to identify a device, a POSITA would have understood that Burger's Pocket Vault ID number renders obvious "***a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device.***" The '730 patent suggests that a device ID code can be both the "plurality of codes" and "other data values." MSC-1001, 7:24-31. Consistent with the description in the '730 patent, Burger's Pocket Vault ID thus satisfies "***a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device.***" Alternatively, it was also known and would have been obvious to a POSITA that a device serial number (Pocket Vault ID) includes different parts such that one part of the device ID code, which includes two or more alphanumeric code data, corresponds to the "plurality of codes" and

another portion of the device ID code, which may also include two or more alphanumeric code data, corresponds to the "other data values." Neither the claims nor the specification impose any restriction as to the individual contents of the "***plurality of codes***" or the "***other data values.***"

88. It was also known and would have been obvious to a POSITA that a device serial number includes different parts that respectively provide different type of information about the device. For instance, MSC-1020 describes various types of product serial numbers and provides several examples in which a device serial number includes different parts, such as a manufacture code and a product code. MSC-1020, 4, 17, 18. In the context of Burger, it would have been obvious to a POSITA that a device serial number would include manufacturer and product codes of the Pocket Vault.

89. Burger also discloses that encryption and decryption may be employed when transferring information and that encryption software resides in the hard-wired memory. MSC-1005, ¶¶[118], [551]-[552], [154]. Various encryption techniques including "asymmetric-key encryption types, such as public key encryption or private key encryption, may be used." MSC-1005, ¶[552]. Thus, it would have been obvious to a POSITA that Burger also discloses "***persistently storing …a secret decryption value.***" For example, asymmetric encryption, also known as public-key encryption, is a process that uses a pair of related keys (one public key

and one private key) to encrypt and decrypt a message and protect it from unauthorized access or use. A public key, such as PKI certificate, is a cryptographic key that can be used by any person to encrypt a message so that it can only be decrypted by the intended recipient with their private key. A private key, also known as a secret key, is only maintained by the key's initiator and can be used to decrypt a message. Thus, it would have been obvious to a POSITA that to use "asymmetric-key encryption types, such as public key encryption or private key encryption," Burger's system would have included a private key ("***secret decryption value***"). Moreover, because such a private key should not be accessible to anyone other than the holder of the private key or modified without the holder's consent, keeping the private key secure is important to prevent unauthorized parties from improperly using or modifying the private key. Accordingly, it would have been obvious to a POSITA that the private key would be stored in a secure location where it cannot be tampered with ("***a secret decryption value in a tamper proof format***").

90. It would have been obvious to a POSITA that a "write-once memory" 212 or a memory device that permits only a single write operation to take place stores data in "***a tamper proof format***," because the stored data in the memory is tamper resistant. For instance, Barrus (US Patent No. 8,977,860) explains that a write-once memory can be used to store data in a tamper-proof format. MSC-1010,

10:56-63 ("physical tamper proof device is a write once memory"), 6:25-29. Another reference, Blom, explains that "there are several different techniques which can be used to confidentiality and integrity protect data in a processor system" including using a "[o]ne-time write-only memory" that "is usually used to store data which does not need to be secret but which should be impossible to change." MSC-1011, 1:12-28. Burger's write-once memory 212 is similar to the 730 patent's description of tamper-proof, which states that "[t]amper-proofing increases reliability of authentication because it does not allow any changes to biometric data (i.e., allows reads of stored data, but not writes to store new data or modify existing data)." MSC-1001, 4:29-43.

91. While Burger explicitly discloses storing a user's biometric data, like fingerprints, in the write-once memory 212, and storing other data such as the Pocket Vault holder's private key (encryption/decryption information) and device serial numbers in a hard-wired memory that is not shown, it would have been obvious for all this information to be persistently stored "***in a tamper proof format [in] a storage element on the integrated device that is unable to be subsequently altered***." For instance, it would have been obvious that the hard-wired memory is also implemented as a protected, write-once memory so that sensitive information such as device serial number and encryption/decryption information is not tampered with and is kept secure. Moreover, a POSITA would have understood or

recognized that information, such as the user's biometric data, device ID, and private key, is unique and is typically not subject to change. For instance, a user's fingerprint does not change, and a unique Pocket Vault ID would not typically be modified to another number (otherwise there could be multiple devices with the same number). As such, it would have been obvious to a POSITA to persistently store this data (e.g., user's biometric data, device ID number, and private key) in the tamper proof memory in at least some implementations of the Burger system because of the sensitivity of this information and the fact that this information is typically meant to be unchangeable after it is written once.

[1.2] wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

92. Burger discloses that that various types of biometric scans and data can be used to perform the authentication including, e.g., a fingerprint scan, retina scan, a speech pattern analysis ("***wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition***"). MSC-1005, ¶¶[0112], [0135]. Although the example implementation used subsequently in the mapping of Burger to the 730 claims describes an example of fingerprint scanning, Burger's disclosure makes obvious that user authentication could include various

suitable authentication techniques in place of fingerprint scanning, such as, e.g., retina scanning, voice recognition, hand geometry. MSC-1005, ¶¶[0112], [0135].

[1.3] responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan,

93. As depicted below in Burger's FIGS. 7A and 2, Burger discloses that a user can activate the Pocket Vault by applying a finger on the fingerprint scanner 220 or perform "a physical action, e.g., the activation of a hardware switch." MSC-1005, ¶¶[0178]-[0180]. In response to this activation, the Pocket Vault 102 is powered up and "the fingerprint scanner 220 scan[s] the applied fingerprint of the Pocket Vault holder." MSC-1005, ¶[0181]. The application of the finger or physical action corresponds to "***a request for a biometric verification of the user***" because it is performed "with each attempted use of any of these devices" and because a biometric scan, such as a fingerprint scan or retina scan, is a known part of the process enabling such use. The Pocket Vault 102 or the controller 202 in the Pocket Vault 102 receives biometric scan data ("***receiving scan data from a biometric scan***"), e.g., from the fingerprint scanner 220 or retina scanner. MSC-1005, ¶¶[135], [0182], [0112].

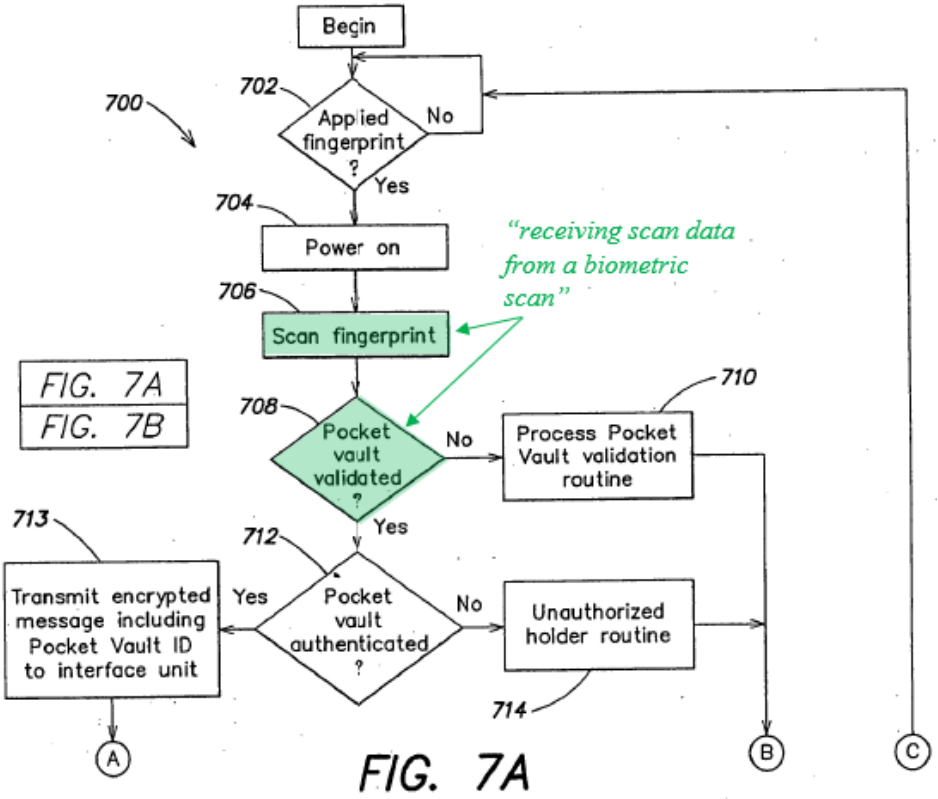


FIG. 7A

MSC-1005, FIG. 7A.

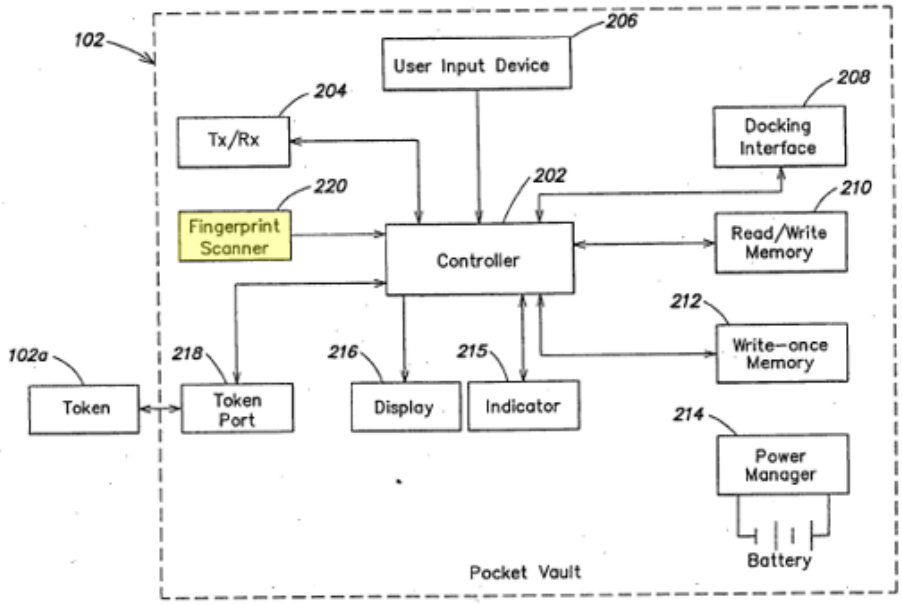


FIG. 2

MSC-1005, FIG. 2.

94. As noted below, although the example of Burger's mapping to the 730 claims is of fingerprint scanning, Burger's disclosure makes obvious that user authentication could include various suitable authentication techniques in place of fingerprint scanning, such as, e.g., retina scanning, voice recognition, hand geometry. MSC-1005, ¶¶[0112], [0135].

[1.4] comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

95. After receiving the scan data from the biometric scan, the user's scanned data (e.g., fingerprints) are compared to biometric data (e.g., fingerprints) stored in the write-once memory 212 to determine if the scanned data matches the user's stored biometric data ("***comparing the scan data to the biometric data to determine whether the scan data matches the biometric data***"). MSC-1005, ¶¶[0182]-[0184], FIGS. 7A, 2.

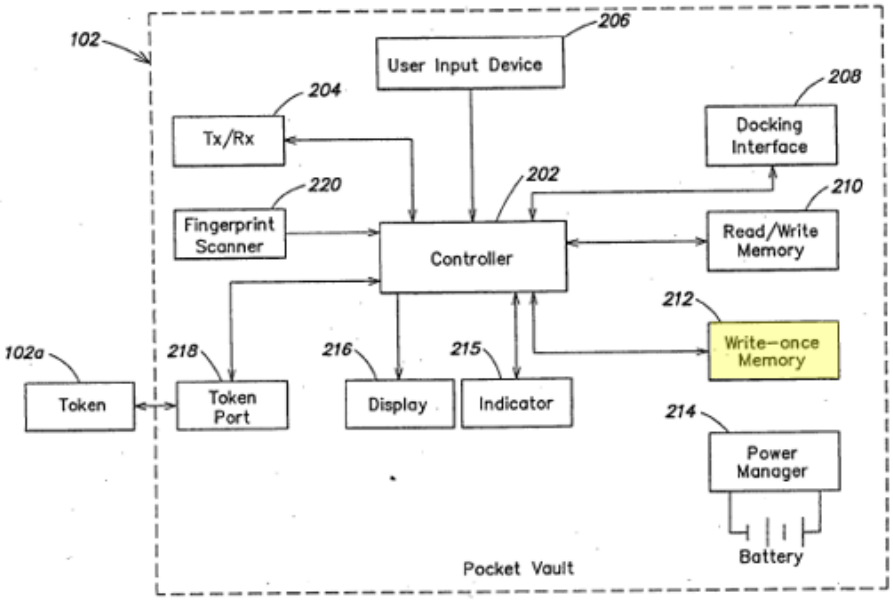


FIG. 2

MSC-1005, FIG. 2.

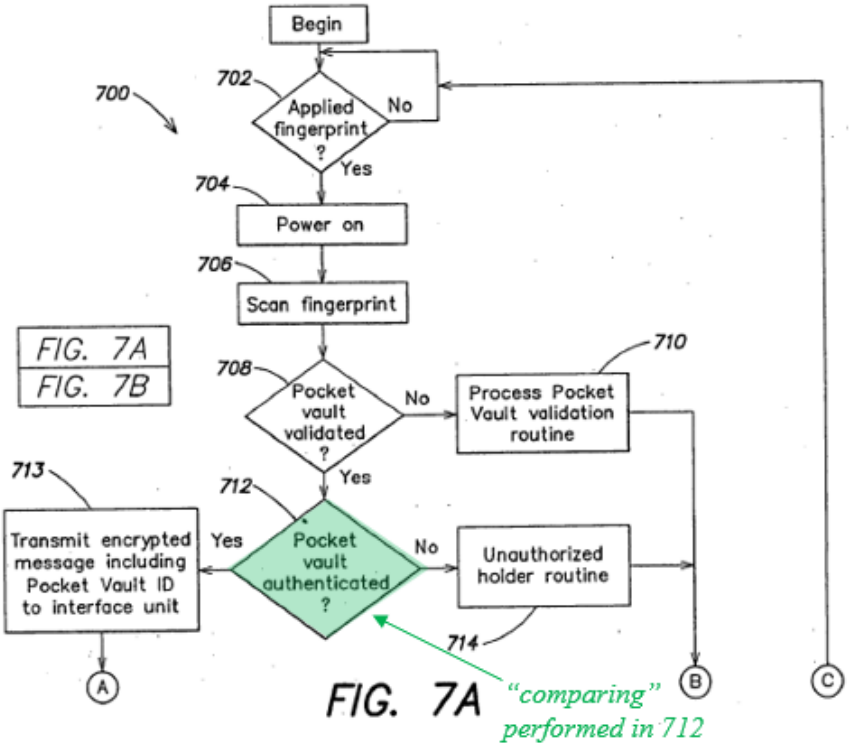
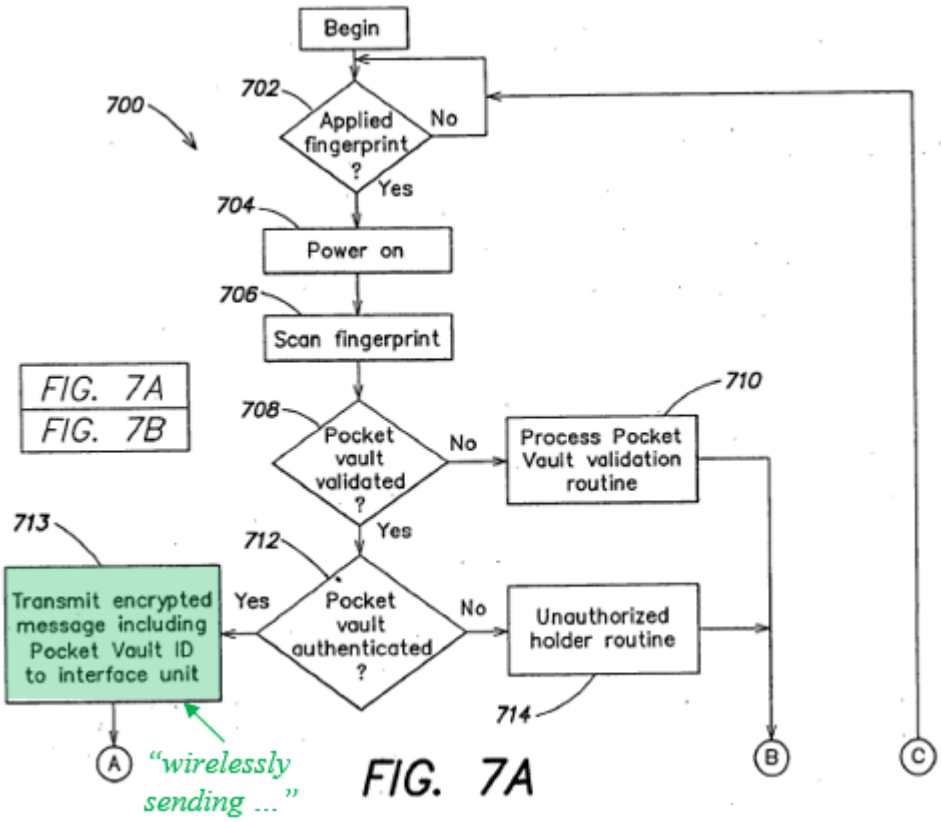


FIG. 7A

MSC-1005, FIG. 7A.

[1.5] responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices,

96. As shown in FIG. 7A, at step 712 "it is determined whether Pocket Vault 102 has been authenticated, e.g., whether the fingerprint scanned at the step 706 matches one of the fingerprints stored in the fingerprint memory 212." MSC-1005, ¶¶[183]-[184], [209]-[210]. And "***responsive to a determination that the scan data matches the biometric data***" (step 712), the Pocket Vault 102 wirelessly sends (step 713) an encrypted message including the unique Pocket Vault chip ID ("***wirelessly sending one or more codes from the plurality of codes and the other data values … wherein the one or more codes and other data values includes the device ID code***"). MSC-1005, ¶¶[0186], [114], [122], [146], FIG. 7A.



MSC-1005, FIG. 7A.

97. In related disclosure, Burger teaches that authentication information, such as the encrypted message including the unique Pocket Vault chip ID, are transmitted to the network server 114. MSC-1005, ¶¶[0113]-[0114]. A POSITA would have understood that the encrypted message would have also included other codes and data values such as header information, destination information, or encrypted data or information that are typically included in encrypted messages.

98. Communication between the various network elements, e.g., between the Pocket Vault 102, interface stations 104a-c, and network server 114 can be wireless, and the Pocket Vault 102 can communicate directly with the network

server 114. MSC-1005, ¶¶[0099]-[0101], [0097], [0123], FIG. 1 (reproduced below).

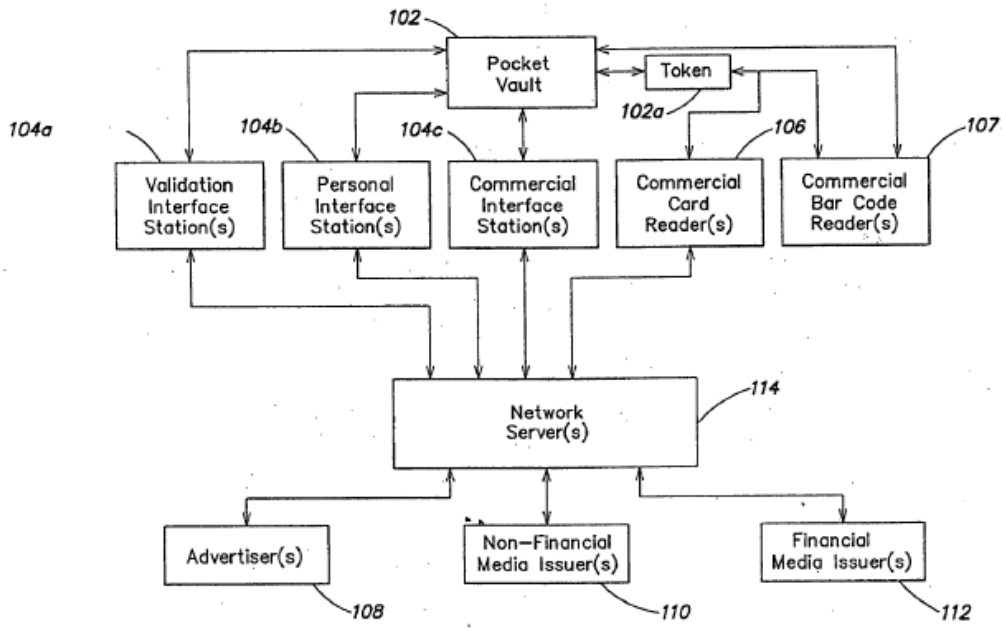


FIG. 1

MSC-1005, FIG. 1.

99. In Burger's system depicted above, the parties involved in a transaction (consistent with the Use Case above in §VII.A) involve a Pocket Vault (first party) user who wants to buy from a retailer, as noted in the table below.

Second party	**Third party**	**Agent that is a third-party trusted authority**
Retailer	Party/company operating the	The network server 114, as a

	network server 114	whole, or, in some cases, a portion (a controller 402 and database 406) of the network server 114. The "agent" may also refer to the entity operating the network server.

100. It would also have been obvious to a POSITA that Burger's disclosure is not limited to the above-noted parties and transaction, and that Burger contemplates several possible transactions between different parties, as noted in the table below. In each example below, the first party is the Pocket Vault holder (user).

Transaction	**Second party**	**Third party**	**Agent that is a third-party trusted authority**
Obtaining payment information or authorization for charging a credit	Financial media issuer 112 (e.g., bank or credit card company)	Party/company operating the network server 114	The network server 114, as a whole, or, in some cases, a portion (a controller 402 and

card or bank account			database 406) of the network server 114. The agent may also refer to the entity operating the network server.
Obtaining authorization to enter a secure building or facility	Non-financial media issuer 110 (e.g., hotel card key issuer, library, building management for company)		
Obtaining advertisement content or related information	Advertiser(s) 108		

101. MSC-1005, ¶¶[94], [98], [103]-[104], [111], [117], [128]-[129], [155]-[158], [237]-[240], [255], [324]-[328], [0511]-[513], [679].

"[A]gent that is a Third-Party Trusted Authority"

102. In an earlier IPR proceeding, the Board construed "'third-party trusted authority' as a trusted authority that is an entity separate from the parties to a

transaction." IPR2021-01444, Paper 11 at 15. Consistent with this description, Burger discloses "***an agent that is a third-party trusted authority***" in several different ways, as I explain below.

103. Specifically, in Burger, the network server 114 includes a controller 402 and database 406**.** MSC-1005, ¶¶[146], [0531]-[0543], FIG. 27. The database 406 stores a list of current Pocket Vault holders, a list of currently authorized or registered Pocket Vaults 102, identified by chip ID and linked to the holder list; a list of currently authorized or registered tokens 102 a, identified by chip ID and linked to the holder list ("***possessing a list of device ID codes uniquely identifying legitimate integrated devices").*** MSC-1005, ¶[146], FIG. 4 (reproduced below). Burger explains that "*a trust relationship* may be established between the network server 114 and the Pocket Vault 102. This relationship may involve, for example, the registration of a unique encrypted chip ID of the Pocket Vault 102 with the network server 114 through a secure Internet connection, the distribution of a digital certificate (e.g., a PKI certificate) to the Pocket Vault 102, and the grant of authority to the Pocket Vault 102 to permanently store the Pocket Vault holder's authentication information." MSC-1005, ¶[114]. "Because of the creation of the above-described *trust relationships*, each Pocket Vault 102 and each interface station 104 may *communicate securely with the network server 114*, as well as with

any other networked devices or sites that *require a high level of trust*." MSC-1005, ¶[116].

104. Accordingly, it would have been obvious to a POSITA that the controller 402 and database 406 of the network server 114 (or the network server 114 as a whole) can operate as "an agent that is a third-party trusted authority" under several different example implementations. For example, the controller 402 and database 406 of the network server 114 may operate as "***an agent that is a third-party trusted authority***" in a transaction between the Pocket Vault holder/user and a retailer, as noted above in the Use Case. MSC-1005, FIG. 19, ¶[0474]; FIGS. 24, 25; ¶¶[0511]-[513], [320], [158], [95]. It would also have been obvious to a POSITA that the company or entity owning the network server 114 can be the "***agent***" because the network server 114 or components thereof effectively operate on behalf of the company.

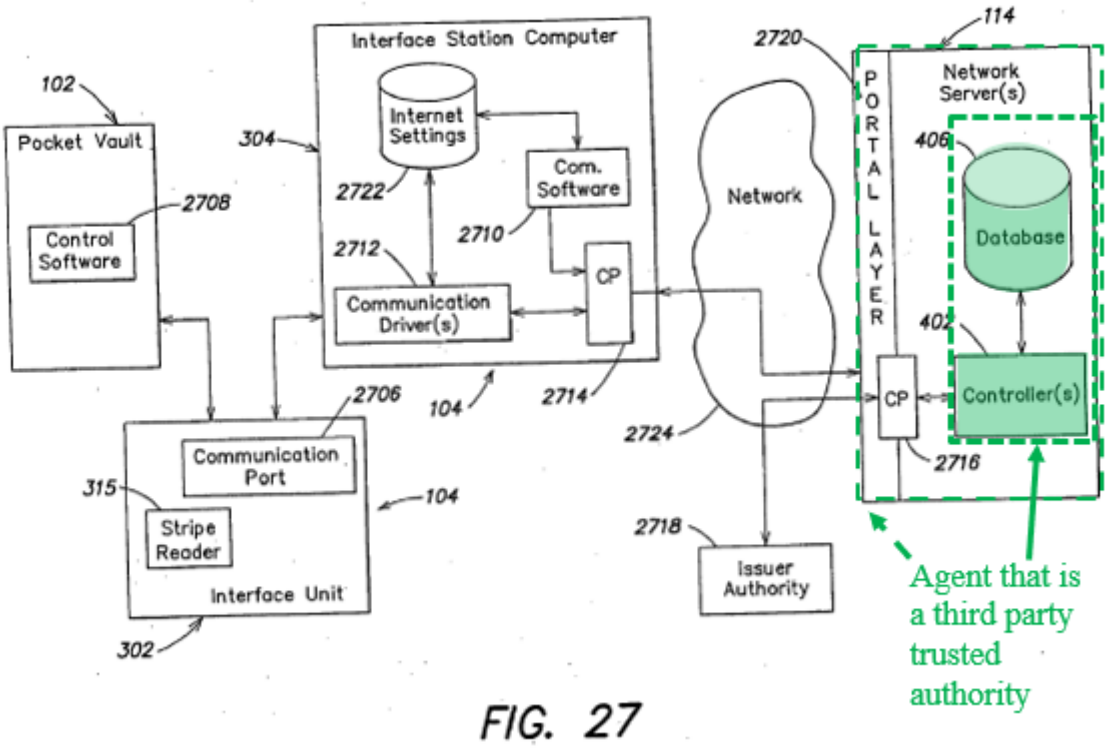


FIG. 27

MSC-1005, FIG. 27.

105. In another example, the controller 402 and database 406 of the network server 114 (or the network server 114 as a whole) may be "***an agent that is a third-party trusted authority***" when there is a transaction between a Pocket Vault holder/user and an entity such as the advertiser 108. For instance, an advertiser may send information to the network server 114, which is then forwarded onto a Pocket Vault 102 for display upon successful authentication of the user and Pocket Vault ID. MSC-1005, ¶¶[0117], [0146], [237] ("The advertiser 108 (FIG. 1) may, for example, have made arrangements with the company operating the network server 114 to have certain advertising information uploaded to Pocket Vaults 102

when particular Pocket Vault holders interface their Pocket Vaults 102 with their personal interface stations 104b"), [541], FIG. 1 (reproduced below).

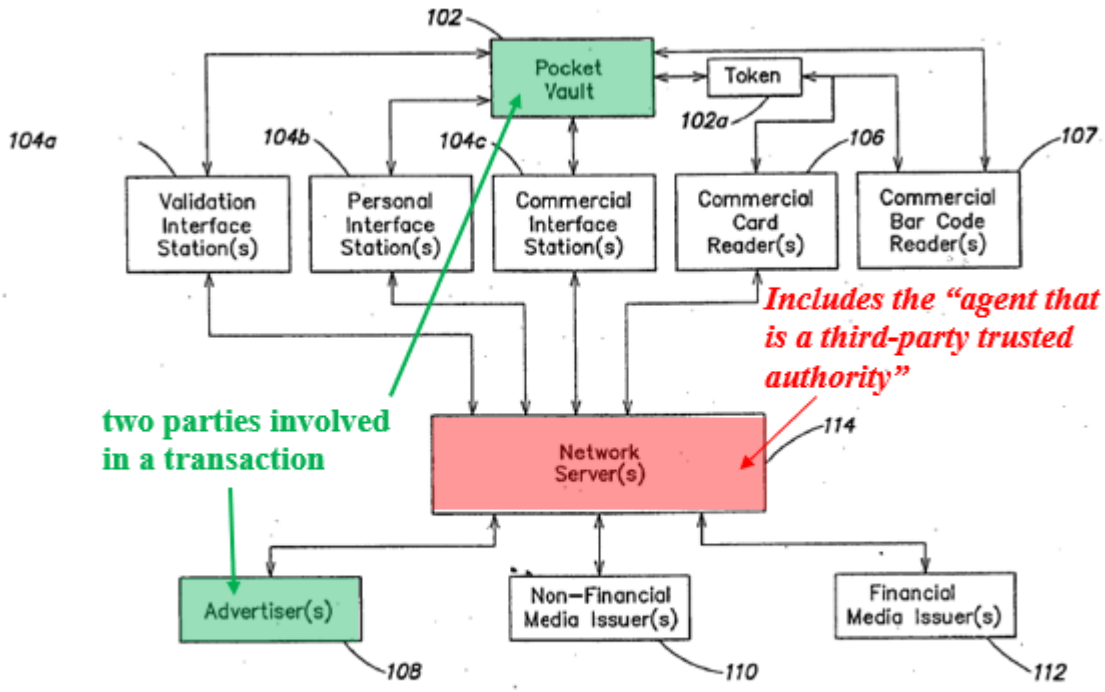
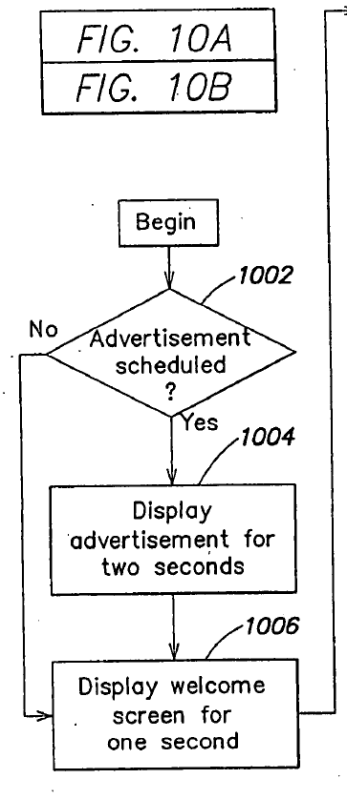


FIG. 1

MSC-1005, FIG. 1.

106. For example, in some embodiments, after the unique Pocket Vault chip ID is transmitted and a token 102a (e.g., Chameleon Card) is determined to be on-board the Pocket Vault 102, an "AUTHORIZED HOLDER" routine is performed, as shown in FIGS. 10 and 11. MSC-1005, ¶¶[189]-[195]. As part of the "AUTHORIZED HOLDER" routine, advertisements sent from an advertiser 108 to the network server 104 are provided to the Pocket Vault 102 for display. MSC-1005, ¶¶[236]-[238], FIG. 10 (reproduced below).



MSC-1005, FIG. 10 (portion of).

107. According to the Merriam-Websters Dictionary, a "transaction" is "a communicative action or activity involving two parties or things that reciprocally affect or influence each other" or "an act, process, or instance of transacting." MSC-1008, 1252. In the Use Case example described above in §VII.A and consistent with Burger's disclosure, the controller 402 and database 406 of the network server 114 (or the network server 114 as a whole) serve as "***an agent that is a third-party trusted authority***" because there is a transaction involving the display of advertisement content and potential subsequent selection of the

advertisement by a user, which is a communicative action or activity involving two parties or things that reciprocally affect or influence each other. For instance, the display of advertisement information impacts the user by conveying information to the user regarding the advertisement. The advertiser 108 also gets publicity, market exposure, and, if the user selects an advertisement, the advertiser can collect information on how useful or impactful the advertisement is. MSC-1012, 2:7-60, FIGS. 4, 8; MSC-1013, Abstract; MSC-1014, 1:19-3:21; MSC-1005, ¶¶ [0117], [0147], [0038]. In this transaction between the user/Pocket Vault holder of the Pocket Vault 102 and the advertiser 108, the controller 402 and database 406 of the network server 114 (or the network server 114 as a whole) are "***an agent that is a third-party trusted authority***" as they have a secure and trusted connection with at least the Pocket Vault 102 and operate as an intermediary device that facilitates information exchange between the advertiser 108 and the Pocket Vault 102.

108. Moreover, using the controller 402 and database 406 of the network server 114 as a third-party server or agent, would not have been something new and was known in the art. Indeed, in a transaction involving two parties, it would have been obvious to utilize a trusted third-party agent to execute one or more parts of the transaction. Doing so would remove potential bias or unfairness if authentication were to be conducted by either of the parties. As an example of this well-known practice, Robinson 980 (MSC-1015) teaches a system in which a

third-party database 106 (similar to Burger's 406 in network server 114) can be used as a third-party source to verify user-presented information. MSC-1015, 4:43-47.

[1.6] responsive to authentication of the one or more codes and the other data values by the agent, receiving an access message from the agent allowing the user access to an application,

109. As described in the example use case above in §VII.A, after the controller 402 and database 406 of the network server 114 authenticate the Pocket Vault ID ("***responsive to authentication of the one or more codes and the other data values by the agent***"), the user is granted access to the Pocket Vault 102 and can then select a transaction from a displayed menu. MSC-1005, step 722 in FIG. 7B (reproduced below); step 1026 in FIG. 10A (reproduced below); steps 1920, 1922 in FIG. 19 (reproduced below); ¶¶[320], [189], [95]-[96], [125], [236]-[238], [155]-[158]. Ultimately, the Pocket Vault 102 or token 102a coupled to the Pocket Vault 102 displays a credit card information to be used by a retailer. MSC-1005, ¶¶[0320], [0158], [0095]. Burger teaches that the token 102a coupled to Pocket Vault 102 "may be used by the Pocket Vault holder to engage in a transaction." MSC-1005, ¶[103]. A display in the token 102a can "be configured to display information that is typically embossed or printed on such cards." MSC-1005, ¶¶[0155]-[0158].

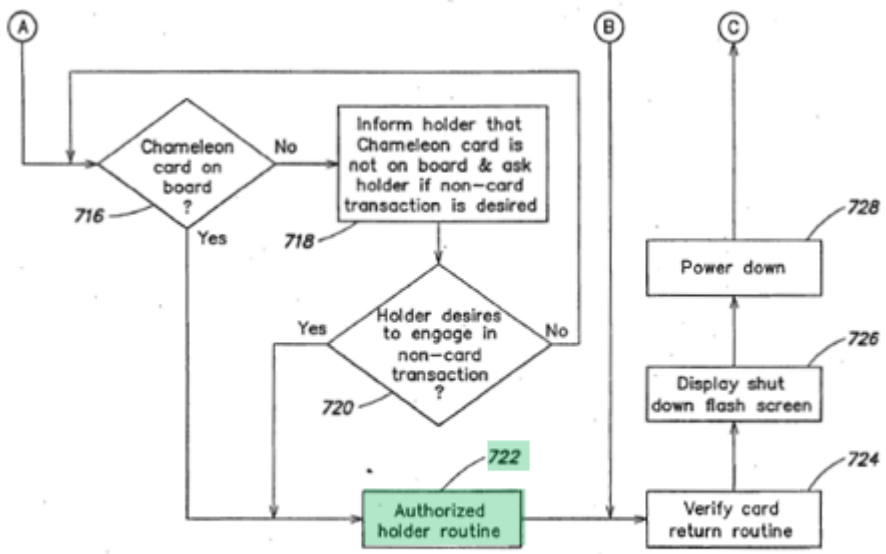


FIG. 7B

MSC-1005, FIG. 7B.

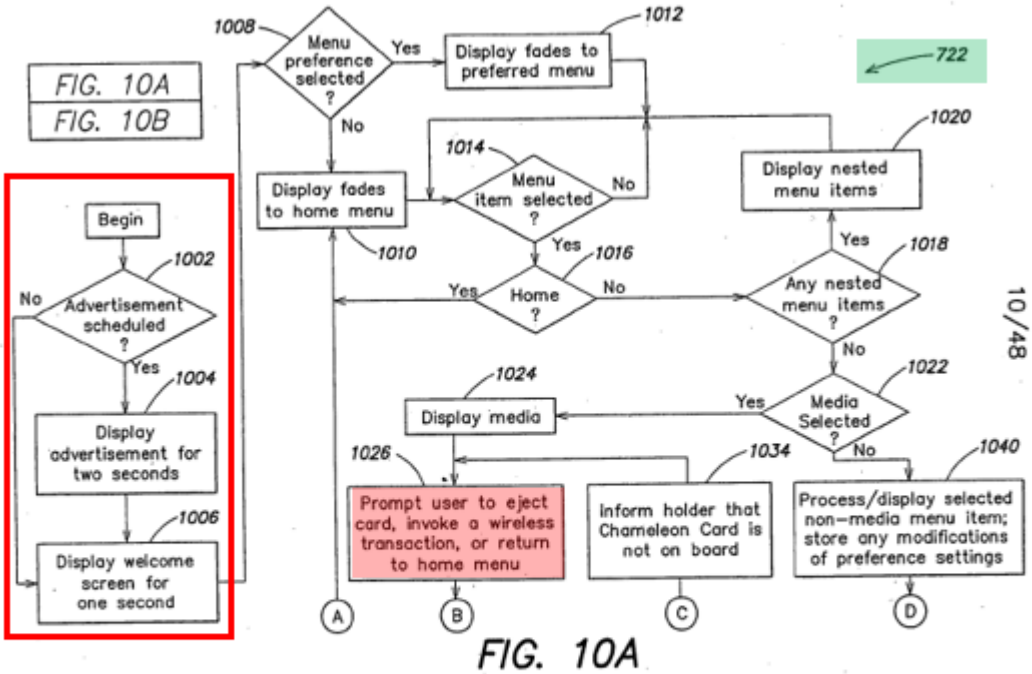


FIG. 10A

As part of the Authorized Holder Routine 722 in FIG. 7B, an advertisement is displayed and subsequently a user can select a wireless transaction to be conducted.

MSC-1005, FIG. 10A.

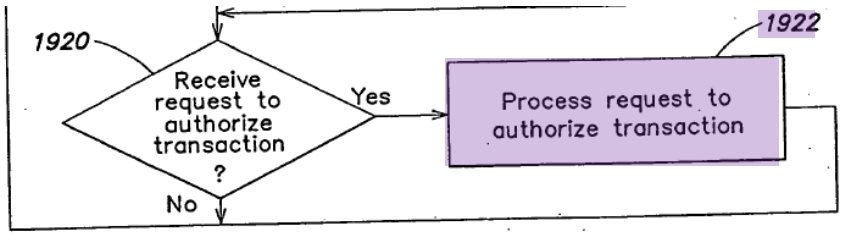


FIG. 19

When a request to conduct a transaction is received, the request is processed as shown in step 1922 in FIGS. 19, 24, and 25.

MSC-1005, FIG. 19.

110. It would have been obvious that the Pocket Vault 102 would have received an access message from the controller 402 of the network server 114 ("***receiving an access message from the agent***") to "***allow[ ] the user access to an application***" after the controller 402 and database 406 of the network server 114 authenticated the Pocket Vault ID that was sent to the network server 114 ("***responsive to authentication of the one or more codes and the other data values by the agent***") so that the Pocket Vault grants access to a user and displays sensitive information (e.g., credit or debit card info) for conducting a transaction.

111. For the mapping of "***application***," please see the remarks below for feature [1.7].

112. As noted above, the controller 402 of the network server 114 also transmits an encrypted approval message in operation 2408 after the Pocket Vault 102 is authorized by confirming that the Pocket Vault ID is valid (step 2006 in FIG. 24 (reproduced below); step 2506 in FIG. 25 (reproduced below)). MSC-1005, ¶¶[517]-[527], [182]-[186]. Because this encrypted approval message ("***access message***") is received by the Pocket Vault 102 in response to the Pocket Vault ID being successfully authenticated by the network server 114, Burger also discloses "***responsive to authentication of the one or more codes and the other data values by the agent, receiving an access message from the agent allowing the user access to an application***" in this additional way. Although operation 2408 indicates that the encrypted approval message is transmitted to an interface station (e.g., 104c, 106, 107), Burger also discloses that, in some cases, the communications may be directly between the Pocket Vault 102 and the network server 114, and thus, it would have been obvious that the encrypted approval message could be sent to the Pocket Vault 102 in addition to or instead of being sent to the interface stations. MSC-1005, ¶[101]. This may particularly be the case when all that is desired is for a credit or debit card to be displayed by the Pocket Vault 102 or token 102a coupled to the Pocket Vault 102.

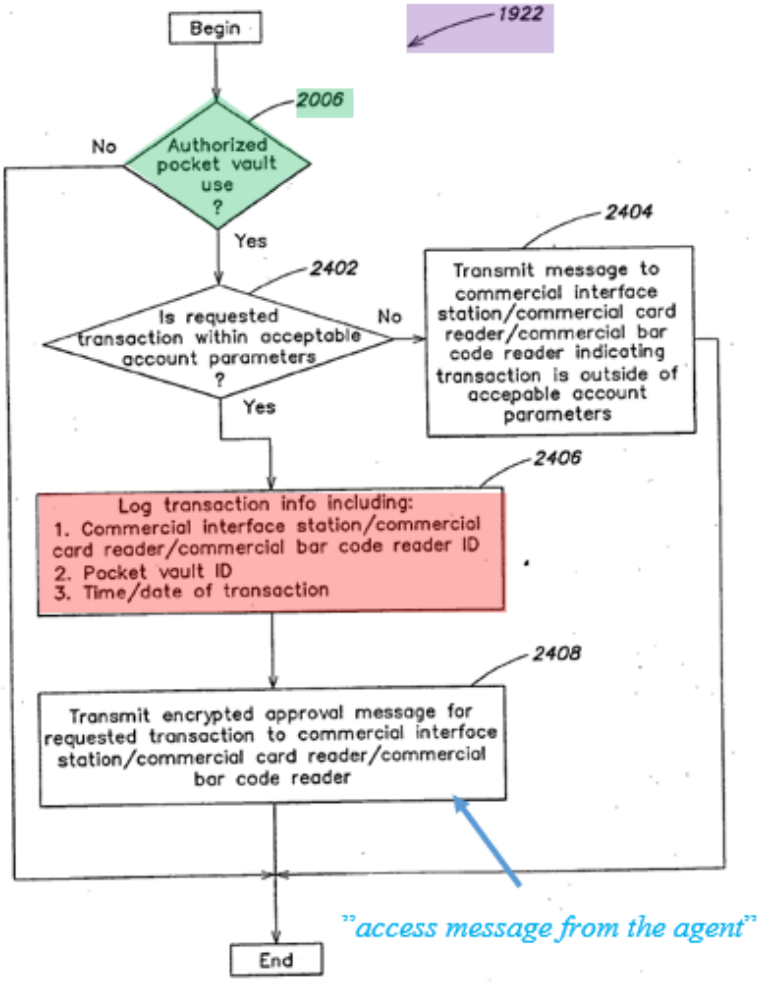
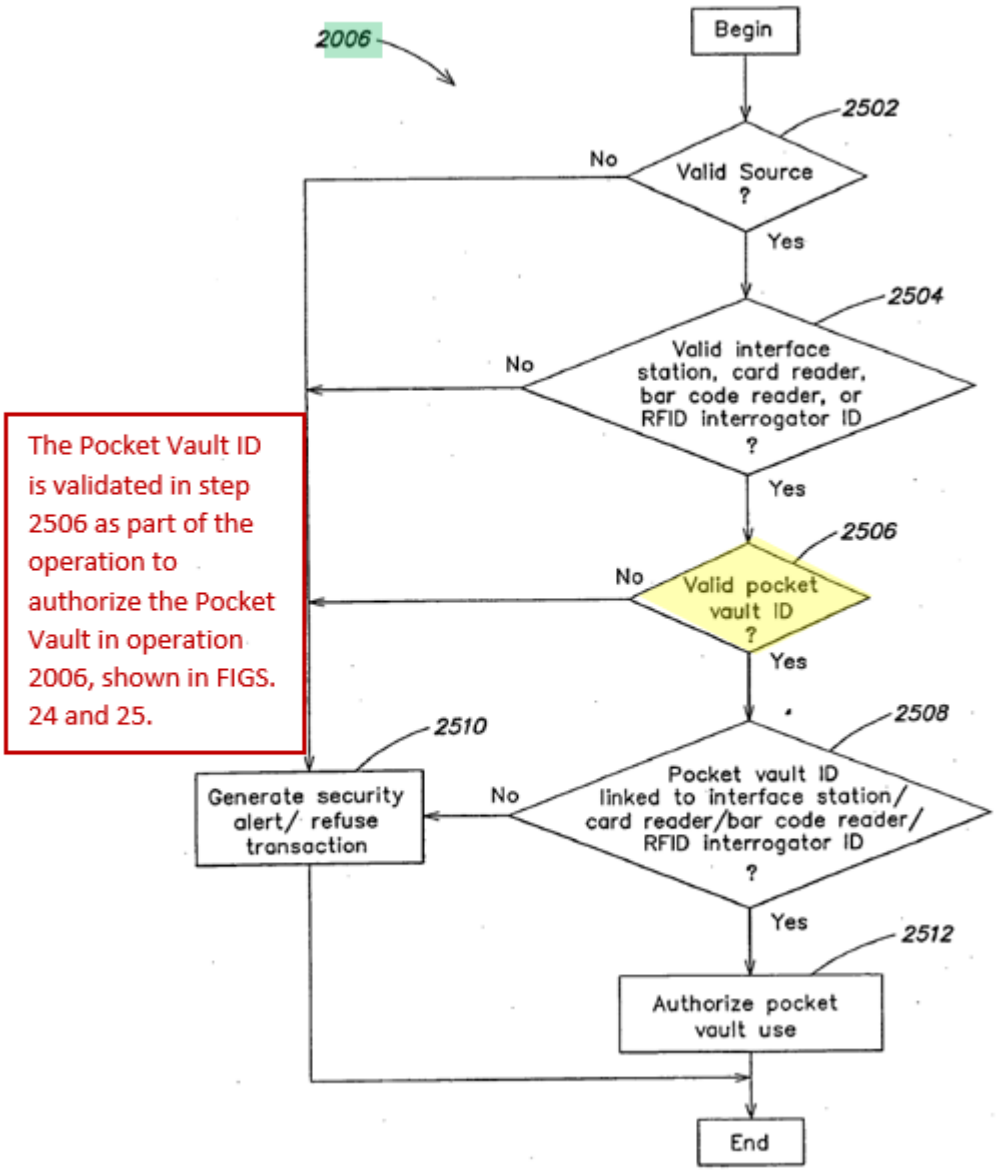


FIG. 24

MSC-1005, FIG. 24.



MSC-1005, FIG. 25.

113. Under another example implementation of the authorized holder routine 722 in Burger, an advertising message based on an advertisement received from the network server 114 and a welcome screen are displayed in response to authentication of the Pocket Vault. MSC-1005, ¶¶[0194], [0236]-[237], FIG. 7B, 10A (reproduced below). The user can then access ***an application***, such a file or

software for an advertisement, or a website (link) thereto. MSC-1005, ¶[0242], FIGS. 26H-26K, 14. Again, it would have been obvious that for the Pocket Vault to be allowed to display the advertisements and home menu, the Pocket Vault 102 would have received an access message from the network server 114 ("***receiving an access message from the agent***") to "***allow[ ] the user access to an application***" after and conditioned on the network server 114 successfully authenticating the Pocket Vault ID that was sent to the network server 114 ("***responsive to authentication of the one or more codes and the other data values by the agent***").

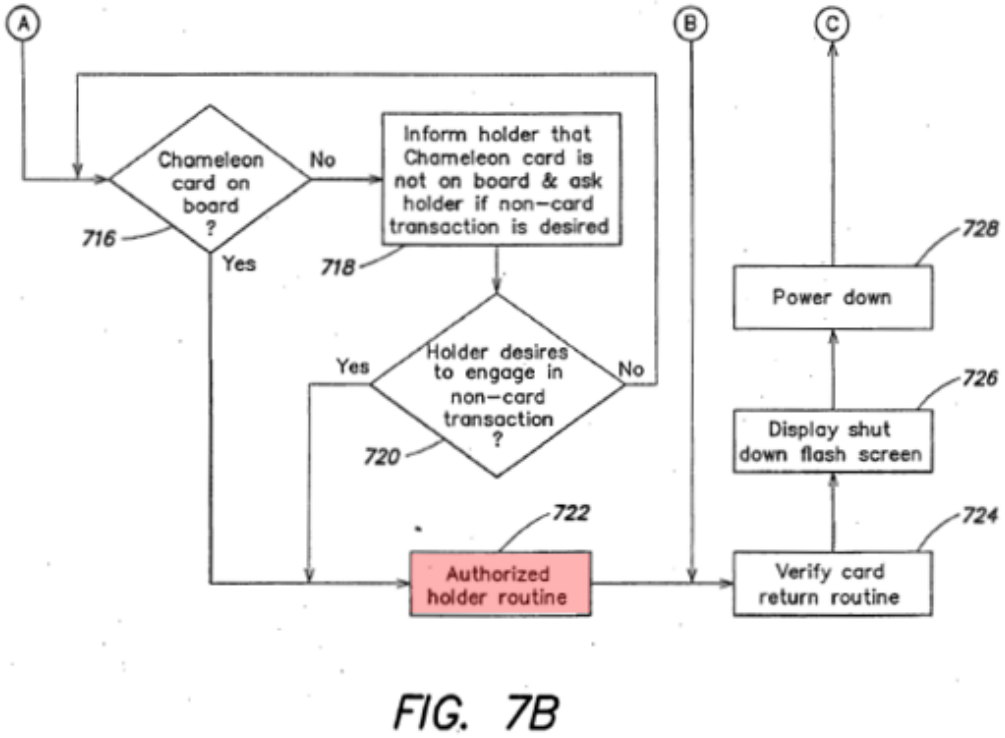


FIG. 7B

MSC-1005, FIG. 7B.

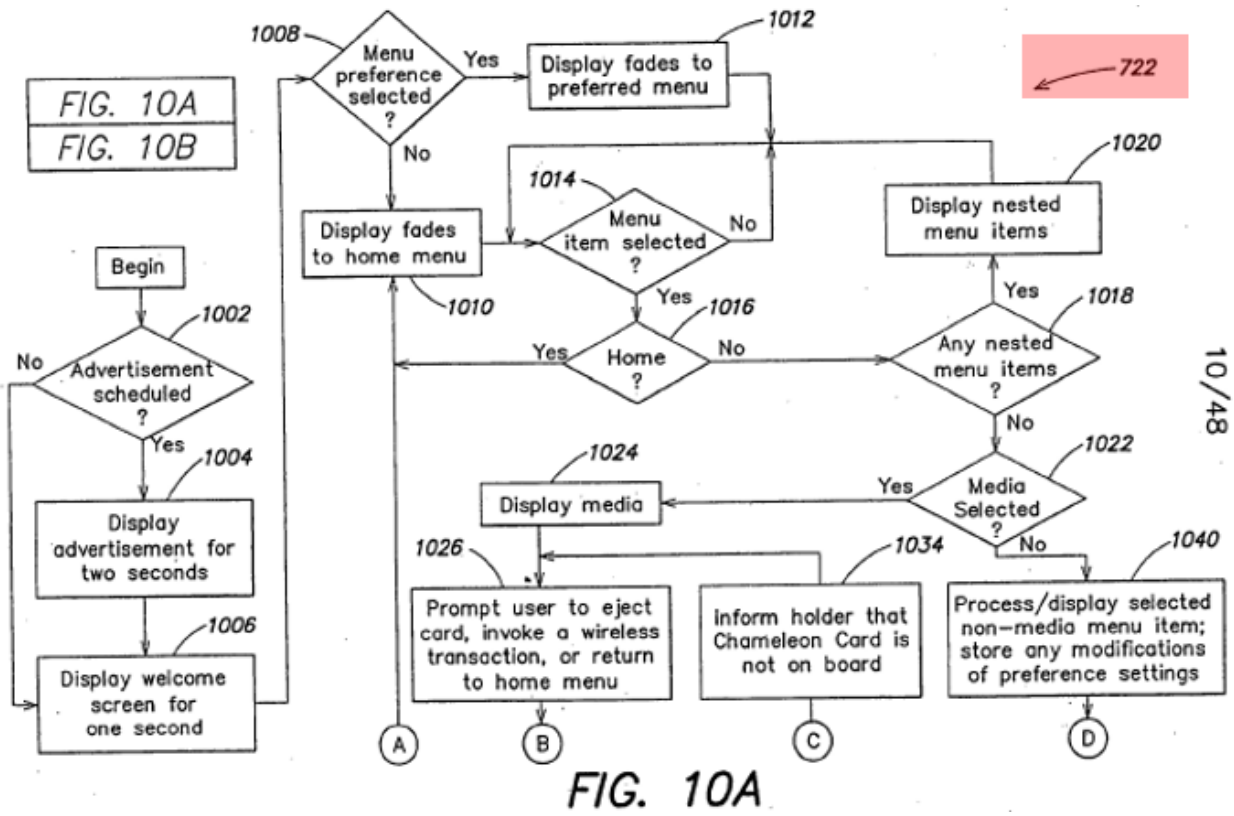
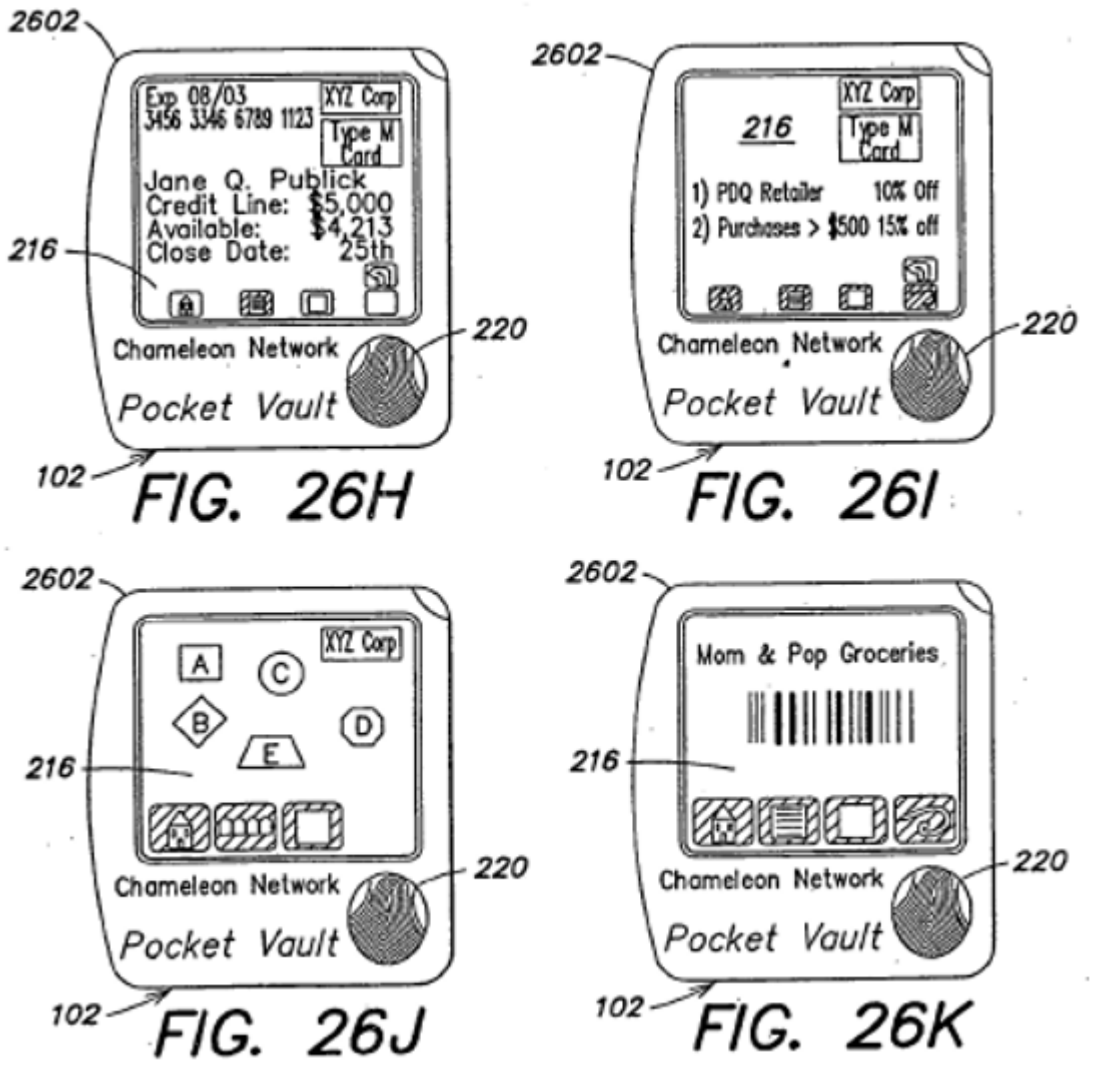


FIG. 10A

MSC-1005, FIG. 10A.



MSC-1005, FIGS. 26H-26K.

[1.7] wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

114. As explained in [1.6] and noted in the table below, Burger's Pocket Vault can be used in different scenarios and implementations, each of which demonstrate that Burger renders obvious [1.6] and [1.7]. *See* citations in [1.6] (MSC-1005, step 722 in FIG. 7B, step 1026 in FIG. 10A; steps 1920, 1922 in FIG. 19; ¶¶[320],

[189], [95]-[96], [125], [236]-[238], [155]-[158], [517]-[527], [182]-[186], [101], [0242], FIGS. 26H-26K, 14), ¶[250]. A POSITA would have understood that a user would only be allowed access to the computer software or file ("***application***") for displaying the above-noted content after the network server 114 sends a message back to the Pocket Vault 102 indicating that the Pocket Vault 102 has been authenticated by the network server 114.

"application"	**Implementation in Burger (after the Pocket Vault 102 has been authenticated by the network server 114)**
File or computer software (when a user is involved in a financial transaction with a retailer or credit card company)	A file or computer software that stores credit card information is accessed and data therein is displayed. A specific software (e.g., credit card specific user interface) is accessed to display credit card information.
File, computer software, or website (in a non-financial transaction)	A file or computer software containing advertising data is accessed and data therein is displayed. A particular website is accessed and displayed to display advertisement data.
Keyless lock	A room key (showing the hotel logo) is downloaded and displayed, and the Pocket Vault

	can be used to unlock the guest's hotel room. ¶¶ [679]-[680]; *see generally* [94] [102] [128] [129] (re "building security" or "building access cards")

115. Thus, Burger's "***application***" "***is selected from a group consisting of***" "***a computer software,***" "***a file,***" "***keyless lock***," or "***web site***." A POSITA would have understood that a user would only be allowed access to the computer software, file, keyless lock, or web site ("***application***") for displaying the above-noted content after the network server 114 sends a message back to the Pocket Vault 102 indicating that the Pocket Vault 102 has been authenticated by the network server 114.

(ii) ***<u>Claim 2</u>***

[2] The method of claim 1, wherein the one or more codes and the other data values are transmitted to the agent over a network.

116. As noted above in [1.5], Burger discloses that an encrypted message including the Pocket Vault ID ("***the one or more codes and the other data values***") is wirelessly transmitted to the controller 402 and/or database 406 of the network server 114 ("***agent***"). MSC-1005, ¶¶[0186], [114], [122], [146], FIG. 7A.

117. The transmission can be made over any one of various suitable networks, such as network 2724 in FIG. 27. For example, as disclosed in Burger's ¶[0099],

"[a]ny of a number of techniques may be used to interconnect the various elements of the network system 100, and *the invention is not limited to any particular networking technique*. In one illustrative embodiment, for example, *the network server 114 is coupled to the other elements in the network system 100 via the Internet or similar packet-switched communication system. Alternatively, dedicated or selectively established (e.g., using a dial-up modem) communication channels or time slots* thereof may be employed between the respective devices. *The connections between most of the network devices may be* either hardwired (including fiber optic connections) or *wireless (e.g., infrared (IR) or radio frequency (RF) links)*." Accordingly, it would have been obvious to a POSITA that Burger teaches "***wherein the one or more codes and the other data values are transmitted to the agent over a network***."

(iii) <u>Claim 4</u>

[4] The method of claim 1, wherein the one or more codes and the other data values indicate that the biometric verification was successful.

118. As shown above in FIG. 7A and noted above with respect to [1.3] and [1.4], the Pocket Vault ID is transmitted after the Pocket Vault holder's scanned biometric data matches stored biometric data. MSC-1005, ¶¶[135], [178]-[0184].

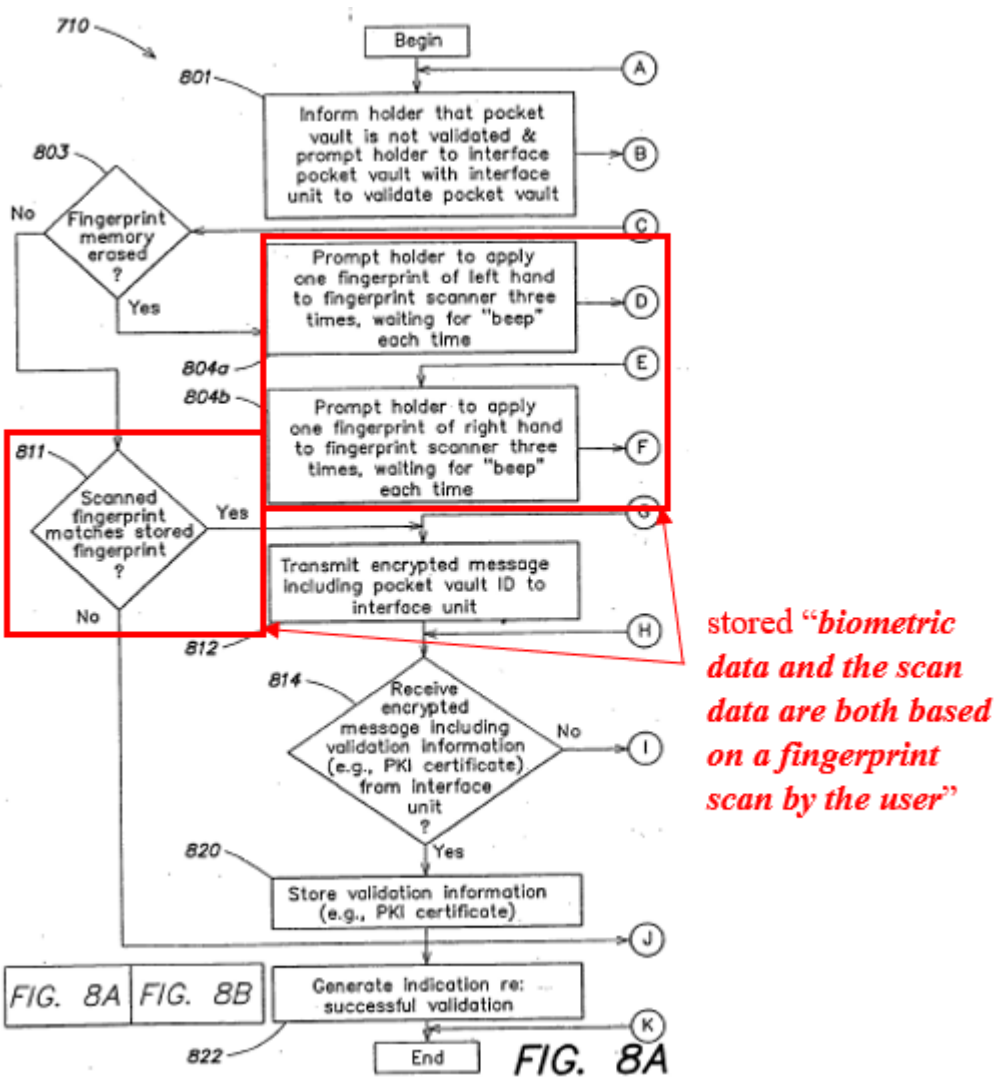
119. Burger also discloses, in several embodiments, that the chip ID or Pocket Vault ID is released from the Pocket Vault 102 only after the fingerprint scanner

220 (discussed below) has successfully authenticated the identity of the holder. MSC-1005, ¶[0122], [0349], [0358]. In some cases, "the Pocket Vault 102 may be adapted to not release any personal or secure information, even encrypted, until the holder presents satisfactory verification of his or her identity, such as, for example, presenting the holder's fingerprint to the fingerprint scanner 220." MSC-1005, ¶[0553]. Accordingly, it would have been obvious to a POSITA that the transmission of "***the one or more codes and the other data values***" to the network server 114 in a message would have been an indication "***that the biometric verification was successful***" because this transmission was only possible if the biometric verification was successful. Thus, the inclusion of "***the one or more codes and the other data values***" in a message to the network server 114 would have in and of itself indicated "***that the biometric verification was successful***."

(iv) ***<u>Claim 5</u>***

[5] The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.

120. As explained above in [1.3], [1.4], and [4], in some implementations, Burger discloses comparing scanned fingerprint data ("***scan data***") of a user with stored fingerprint data ("***biometric data***") previously stored. *See also* MSC-1005, FIGS. 8A (reproduced below), 8B (step 808b), ¶¶[0199]-[0209]. Thus, "***the biometric data and the scan data are both based on a fingerprint scan by the user.***"



MSC-1005, FIG. 8A.

(v) ***Claim 6***

[6] The method of claim 1, further comprising: establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication.

121. Burger discloses that after the Pocket Vault Holder's biometric scanned data has been validated, "a trust relationship may be established between the network

server 114 and the Pocket Vault 102" and that "***a secure Internet connection***" is established to facilitate the registration of the Pocket Vault 102 (FIG. 7A, Step 710), which is done prior to the Pocket Vault ID being sent for authentication (FIG. 7A, Step 713). MSC-1005, ¶[114]. Accordingly, Burger renders obvious "***establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication***."

(vi) ***<u>Claim 7</u>***

[7.1] The method of claim 1, further comprising: receiving a request for the one or more codes and the other data values without a request for biometric verification; and

122. When a request to register a new Pocket Vault holder is received, the operations 1904 (FIG. 19) shown in Burger's FIG. 20 below are performed by the network server 114. MSC-1005, FIGS. 19, 20, ¶¶[0462]-[0464], [0476]. In particular, after a request is received to register a new Pocket Vault holder, "the network server 114 requests the interface station computer 304 to transfer the information regarding the proposed new holder to the network server 114." MSC-1005, ¶¶[0476]-[0477]. After the requisite encrypted holder registration information is received through an interface station computer 304 and the network server 114 determines that the Pocket Vault is authorized for use, "all of the relevant information regarding the new Pocket Vault registration is logged into the

database 406 of the network server 114." MSC-1005, ¶¶[0476]-[0481]. The registration information "may include, for example, the interface station operator ID, the interface unit ID, the Pocket Vault ID, and all of the relevant information relating to the new Pocket Vault holder." MSC-1005, ¶[0481].

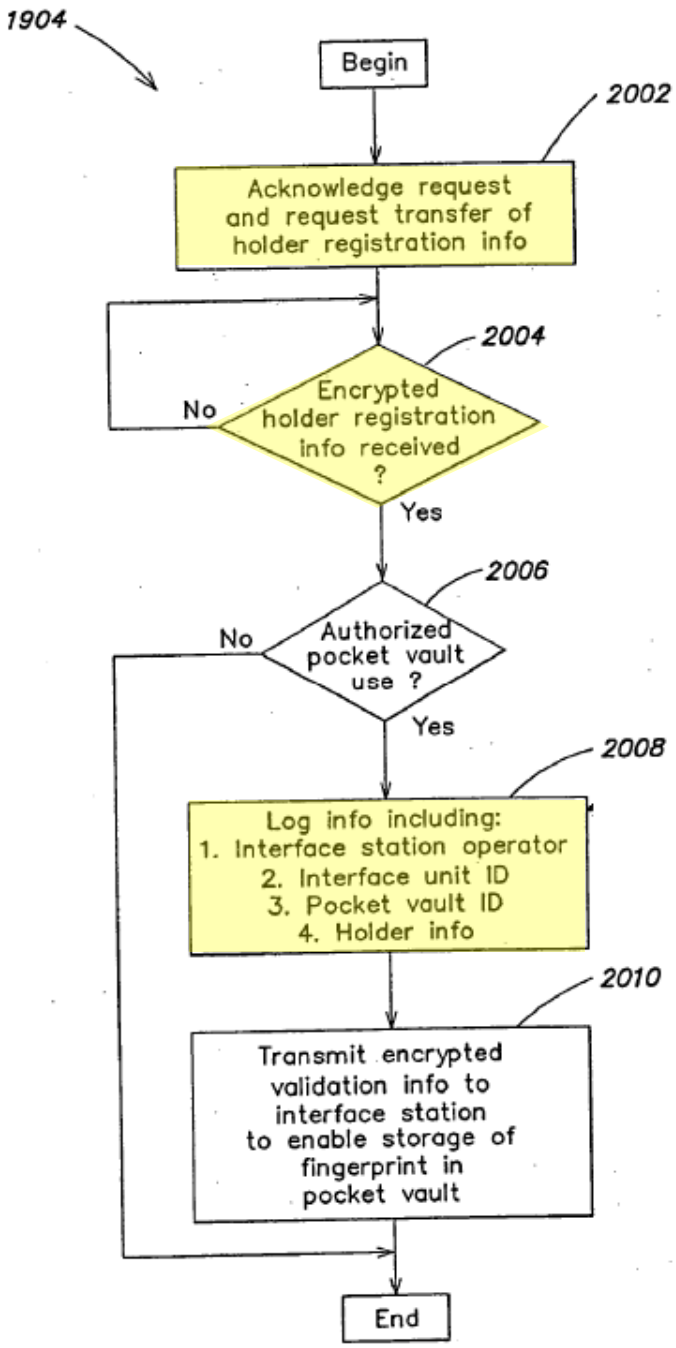


FIG. 20

MSC-1005, FIG. 20.

123. Although some of the communications described in FIG. 20 are described as being performed by an interface station, Burger also discloses that "in some

embodiments wherein appropriate networking capabilities are provided, each Pocket Vault 102 may communicate directly with the network server 114, without the interface stations 104a-c facilitating communication therebetween." MSC-1005, ¶¶[0101], [0562], [0573], [0585]. Thus, in such embodiments, it would have been obvious to a POSITA that the network server 114 would have communicated directly with the Pocket Vault 102 to obtain the registration information for a new Pocket Vault holder.

124. In this example of registering a new Pocket Vault holder, no request for biometric verification is made. However, the Pocket Vault 102 still receives a request ("***a request for the one or more codes and the other data values"***) for pocket holder registration information including "the Pocket Vault ID, and all of the relevant information relating to the new Pocket Vault holder." MSC-1005, ¶[0481]. Accordingly, Burger renders obvious "***receiving a request for the one or more codes and the other data values without a request for biometric verification***."[2]

---

[2] Recall from [1.1] above that Burger's Pocket Vault ID in the transmitted encrypted message satisfies "the plurality of codes and the other data values."

[7.2] responsive to receiving the request for the one or more codes and the other data values without a request for biometric verification, sending the one or more codes and the other data values without requesting the scan data.

125. As explained above in [7.1], in response to receiving the request for registration information ("***responsive to receiving the request***"), the Pocket Vault 102 sends all the Pocket Vault registration information, including the Pocket Vault ID, to the network server 114 to be logged into the database 406 of the network server 114 without requesting or performing any biometric scan ("***sending the one or more codes and the other data values without requesting the scan data***"). MSC-1005, ¶¶[0476]-[0481]. Accordingly, Burger also renders obvious "***responsive to receiving the request for the one or more codes and the other data values without a request for biometric verification, sending the one or more codes and the other data values without requesting the scan data***."

(vii) <u>Claim 8</u>

[8.pre] An integrated device for verifying a user during authentication of the integrated device, comprising:

126. Burger's Pocket Vault 102 is an "***integrated device***," as explained in [1pre]. *See* [1.pre]; MSC-1005, ¶¶[0002], [0010], [0127]-[0128], [0118], [0134], [0094]-[0095].

[8.1] a memory stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered;

127. [8.1]'s "memory" corresponds to [1.1]'s "storage element," which is rendered obvious for the reasons noted above in [1.1]. *See* [1.1]; MSC-1005, ¶¶[0112], [0114], [0118], [0122], [0127], [0129], [0154], [0182], [0551]-[0552], FIG. 2.

[8.2] wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

128. *See* [1.2]; MSC-1005, ¶¶[0112], [0135].

[8.3] a verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and the other data values includes the device ID code; and

129. *See* [1.3]-[1.5]; MSC-1005, ¶¶[0112]-[0114], [0122], [0135], [0146], [0178]-[0184], [0186], FIGS. 7A, 2.

130. The fingerprint scanner 220 (or any biometric scanner used instead of the scanner 220), the controller 202, the transceiver 204, the display 216, and the indicator 215 are the "***verification unit***" that is "***in communication with the memory***" and performs the recited operations. MSC-1005, ¶¶[0122], FIG. 2 (reproduced below). Because the scanner 220 obtains stored copies of biometric

data from the memory to perform the comparison with scanned biometric data, it would have been obvious to a POSITA that the scanner 220 would be "***in communication with the memory***." Moreover, the controller 202 is coupled to the memory and transceiver 204 to send and receive any data from the Pocket Vault 102.

131. [1.3]-[1.5] explain how Burger renders obvious "receives scan data …" and the remaining features in [8.3].

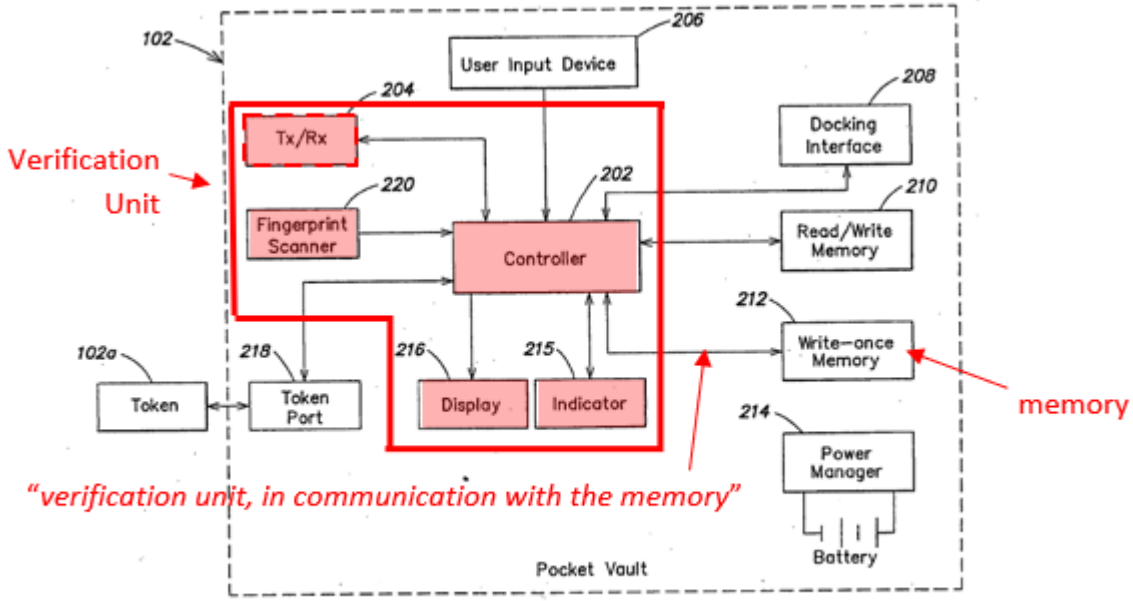


FIG. 2

MSC-1005, FIG. 2.

[8.4] responsive to the agent authenticating the one or more codes and the other data values, a radio frequency communicator, receives an access message from the agent allowing the user access to an application,

132. *See* [1.6]; MSC-1005, FIGS. 7A, 7B, 10A, 19, 26H-26K; ¶¶[0320], [0189], [0095]-[0096], [0101], [0125], [0236]-[0238], [0155]-[0158], [0103], [517]-[527], [182]-[186], [0194].

133. The "one or more antennas" of the transceiver 204 (alternatively the transceiver 204 itself) are the "***radio frequency communicator***" as the antennas perform the transmitting and receiving of data using RF signals for the Pocket Vault 102. MSC-1005, ¶[0123].

134. Note that claim 8 does not require that the "***radio frequency communicator***" is separate from the "***verification unit***," thus mapping the transceiver 204 to the "***radio frequency communicator***" within the "***verification unit***" is consistent with the claims.

135. To the extent, the "***radio frequency communicator***" is understood to not be part of the "***verification unit***," the antennas of the transceiver correspond to the "***radio frequency communicator***" and the fingerprint scanner 220 (or any biometric scanner used instead of the scanner 220), the controller 202, and parts of the transceiver 204 other than the antennas are the "***verification unit.***"

[8.5] wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

136. *See* [1.7], [8.4]; MSC-1005, FIGS. 7A, 7B, 10A, 19, 26H-26K; ¶¶[0320], [0189], [0095]-[0096], [0101], [0125], [0236]-[0238], [0155]-[0158], [0103], [517]-[527], [182]-[186], [0194], [0250].

(viii) <u>Claim 9</u>

[9] The integrated device of claim 8, wherein the one or more codes and the other data values are transmitted to the agent over a network.

137. *See* [2]; MSC-1005, ¶¶[0099], [0186], [114], [122], [146], FIG. 7A.

(ix) <u>Claim 11</u>

[11] The integrated device of claim 8, wherein the verifier[3] comprises: an LED to be activated for requesting the biometric scan.

138. Burger discloses that output devices, such as LEDs and a display, can be used to provide information to a Pocket Vault holder and prompt user input

---

[3] There is a typo or an antecedent basis issue in this claim because claim 8 does not recite a "***verifier***." The "***verifier***" is likely referring to the "***verification unit***" of claim 8. For purposes of this IPR, petitioner treats the "verifier" to be the same as the "verification unit."

options. MSC-1005, ¶¶[0133], [0177]. An indicator 215 can be "any device capable of generating a perceptible indication to a holder." MSC-1005, ¶[0131], FIG. 2. For example, the indicator 215, can include a LED and beeper, to prompt the Pocket Vault holder to apply a fingerprint on the fingerprint scanner 220 and a "beep" is emitted after each fingerprint is applied. MSC-1005, ¶¶[0204], [0206], [0133]; *see also* ¶¶[0232], [0355], [0384], [0585], [0598]. Although the prompting of a user to scan the user's fingerprints is not part of the method shown in FIG. 7A, it would have been obvious to a POSITA that there are multiple ways of the Pocket Vault 102 obtaining a fingerprint scan. One of the methods to obtain a fingerprint scan is to wait for the user to apply the user's finger on the fingerprint scanner 220 (as shown in Burger's FIG. 7A), but another obvious and predictable option is for the Pocket Vault 102 to prompt the user to apply the user's fingerprint through the use of an Indicator 215 (that includes a LED). The prompting for additional fingerprint scans can also be made when one fingerprint scan has been completed but scans of additional fingerprints are still requested. MSC-1005, ¶[0204]. Accordingly and because the verification unit includes the indicator 215, it would have been obvious to a POSITA that Burger renders obvious ***"the verifier compris[ing]: an LED to be activated for requesting the biometric scan."***

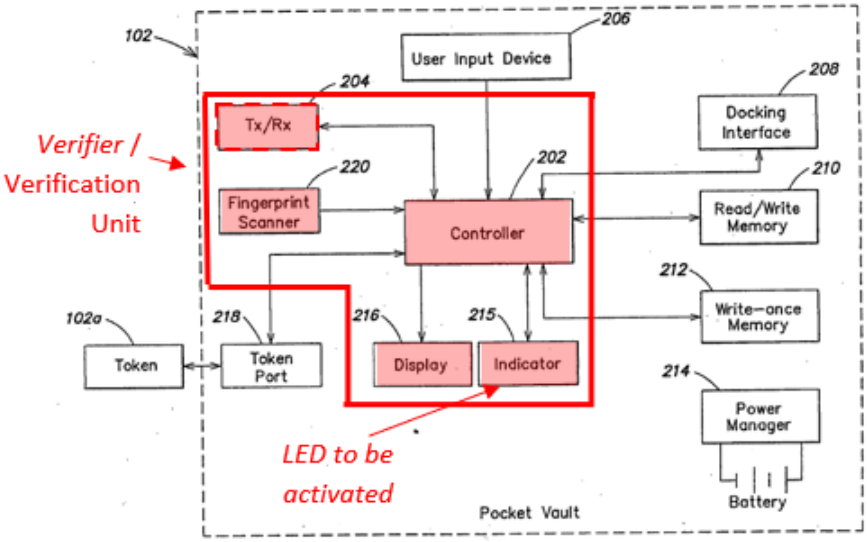


FIG. 2

MSC-1005, FIG. 2.

(x) ***Claim 12***

[12.pre] A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

139. For reasons similar to those noted above with respect to claim 1 and in particular [1.pre], Burger renders obvious a "***method for authenticating a verified user using a computer processor configured to execute method steps***," as recited in [12.pre]. MSC-1005, ¶¶[0002], [0010], [0127]-[0128], [0118], [0134], [0094]-[0095]. For example, Burger discloses a method of authenticating a verified Pocket Vault holder ("***user***") using a controller 402 ("***computer processor***") of the network server 114. MSC-1005, FIG. 4, ¶¶[0144]-[0145], [0540]. The network server 114 also includes a local memory 404 that has "instructions stored therein which, when executed by the controller 402, cause the controller 402 to implement

the routines described … in connection with FIGS. 19-25 and/or FIGS. 30-39." MSC-1005, ¶[145]. Although Burger does not explicitly describe the controller 402 as a computer processor, a POSITA would have understood that controller 402 is a computer processor that, as described in Burger, is configured to execute Instructions to Implement operations configured to be performed by the network sever 114, just like a computer processor would. MSC-1005, FIG. 4, ¶¶[0144]-[0145]. As noted below, the method including features [12.1]-[12.5] are rendered obvious by Burger.

[12.1] receiving one or more codes from a plurality of codes and other data values including a device ID code,

140. As explained above in [1.5], the network server 114 "***receiv[es] one or more codes from a plurality of codes and other data values including a device ID code***" from the Pocket Vault 102. MSC-1005, ¶¶[0112]-[0114], [0122], [0135], [0146], [0178]-[0184], [0186], FIGS. 7A, 2.

[12.2] wherein the plurality of codes and the other data values comprises the device ID code uniquely identifying the integrated device and a secret decryption value associated with a biometrically verified user, the device ID code being registered with an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices;

141. *See* [1.5], [1.1]; MSC-1005, ¶¶[0112]-[0114], [0118], [0122], [0127], [0129], [0135], [0146], [0154], [0178]-[0184], [0186], [0551]-[0552], FIGS. 7A, 2.

[12.3] requesting authentication of the one or more codes and the other data values by the agent, wherein the authentication determines whether the one or more codes and the other data values are legitimate;

142. *See* [1.5], [1.6]. As explained above in §VII.A, [1.5], and [1.6], Burger's network server 114 includes a database 406, controller(s) 402, local memory 404, and a communications protocol layer 2716. FIGS. 4, 27. Burger's database 406 stores "a list of current Pocket Vault holders … a list of currently authorized or registered Pocket Vaults 102, identified by chip ID and linked to the holder list; a list of currently authorized or registered tokens 102 a, identified by chip ID and linked to the holder list." MSC-1005, ¶[146]. The controller 402 executes instructions stored in memory 404 "to implement the routines described … in connection with FIGS. 19-25 and/or FIGS. 30-39." MSC-1005, ¶[145].

143. Turning to FIGS. 19, 24, and 25, as explained above in [1.5], it would have been obvious to a POSITA that the controller 402 and database 406 (collectively "***the agent***") authenticate the Pocket Vault ID or authorize the Pocket Vault 102 by confirming that the Pocket Vault ID is valid before sending the access message to the Pocket Vault. MSC-1005, FIGS. 19, 24, 25; ¶¶[517]-[527], [182]-[186]. To perform these steps, it would have been obvious to a POSITA that the stored instructions include instructions to "***request[ ] authentication of the one or more codes and the other data values by the agent***" [controller 402 and database 406], as recited in [12.3]. And because the Pocket Vault ID is part of "***the one or more***

codes and the other data values are legitimate," a POSITA would have understood that by authenticating the Pocket Vault ID, the network server 114 would determine "***whether the one or more codes and the other data values are legitimate."***

[12.4] receiving an access message from the agent; and

144. *See* [1.6].

[12.5] in response to a positive access message, allowing the biometrically verified user access to an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

145. *See* [1.6], [1.7].

(xi) ***<u>Claim 14</u>***

[14] The method of claim 12, further comprising: establishing a secure communications channel with a biometric key, wherein the one or more codes and the other data values associated with the biometrically verified user is received from the biometric key.

146. Claims 6 and 14 recite similar features. However, claim 6 recites that the secure communications channel is established "prior to sending the one or more codes and the other data values for authentication." *See* [6]. Claim 14 does not recite the "prior to" limitation but recites that the secure communications channel established "with a biometric key, wherein the one or more codes and the other data values associated with the biometrically verified user is received from the biometric key." As explained above in [1.5] and [6], Burger's network server 114

establishes a secure connection with the Pocket Vault 102 ("***biometric key***") and receives the Pocket Vault ID from the Pocket Vault 102 ("***wherein the one or more codes and the other data values associated with the biometrically verified user is received from the biometric key***.") *See* [6], [1.5]. MSC-1005, ¶¶[0097]-[0101], [0186], [113]-[114], [122]-[123], [146], FIGS. 1, FIG. 7A.

(xii) ***<u>Claim 15</u>***

[15.pre] A system, comprising:

147. *See* [1.pre]; MSC-1005, ¶¶[0002], [0010], [0127]-[0128], [0118], [0134], [0094]-[0095].

[15.1] a biometric key stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the biometric key and a secret decryption value in a tamper proof format written to a storage element on the biometric key that is unable to be subsequently altered, and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending, one or more codes from the plurality of codes and other data values wherein the one or more codes and the other data values include the device ID code and

148. *See* [1.1], [1.3]-[1.5]; MSC-1005, ¶¶[0112]-[0114], [0118], [0122], [0127], [0129], [0135], [0146], [0154], [0178]-[0184], [0186], [0551]-[0552], FIGS. 7A, 2.

[15.2] the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition; and

149. *See* [1.2]; MSC-1005, ¶¶[0112], [0135].

[15.3] an authentication unit receives the plurality of codes and the other data values and send the plurality of codes and the other data values to agent for

authentication to determine whether the one or more codes and the other data values are legitimate, wherein the agent is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, and

150. As explained above and shown in Burger's annotated FIG. 27 below, Burger discloses a communication protocol layer 2716 ("***authentication unit***") "which provides low-level communication functions to server communications software." MSC-1005, ¶[540]. As is obvious from Burger's FIG. 27 below, communications (e.g., device ID codes) between the network server 114's controller(s) 402 and database 406 (collectively "***agent***") and external elements (e.g., network 2724, Pocket Vault 102, or issuer authority 2718) all pass through the communication protocol layer 2716.

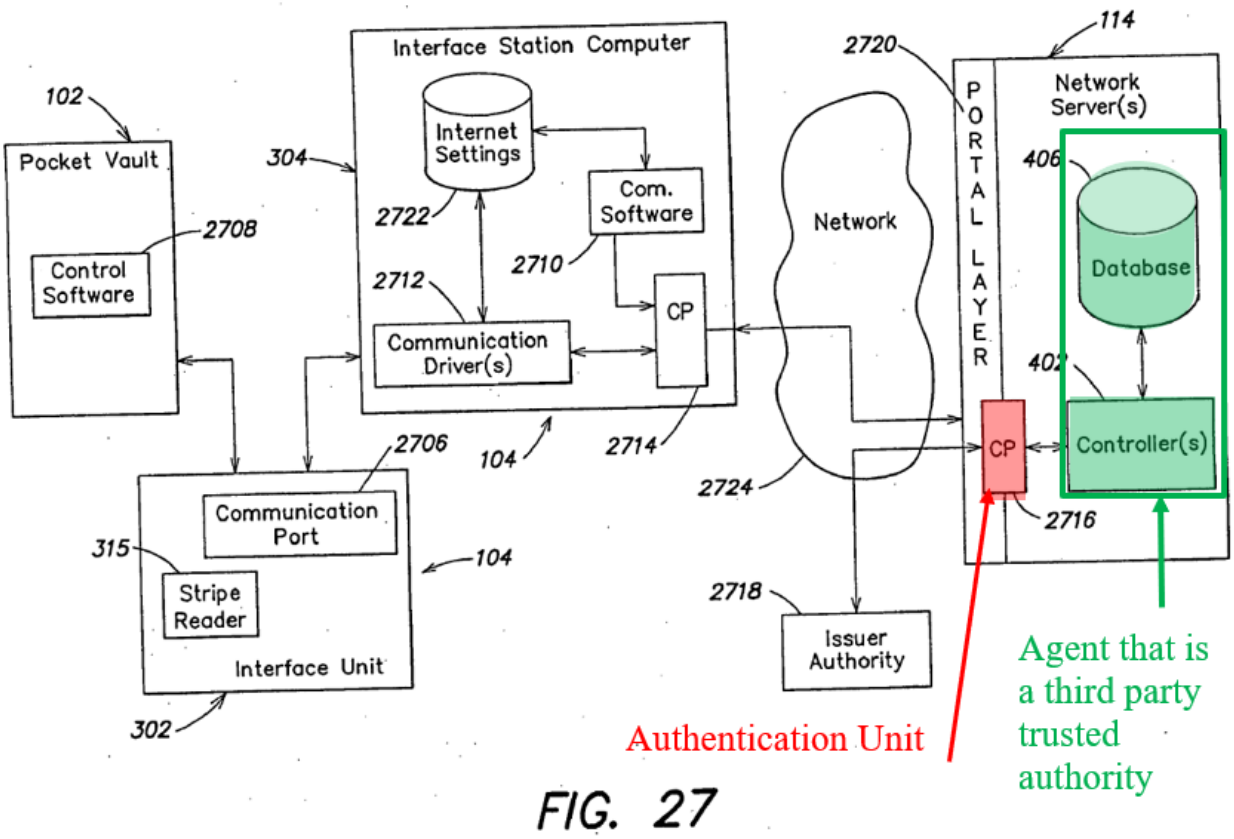


FIG. 27

MSC-1005, FIG. 27.

151. Accordingly, it would have been obvious to a POSITA that Burger renders obvious "***an authentication unit***[4] ***[that] receives the plurality of codes and the***

---

[4] Notably, the "authentication unit" recited in claim 15 is not recited as directly performing any type of "authentication." Rather, the extent of the "authentication" function ascribed to the recited "authentication unit" by the claim is merely that it receives and sends the plurality of codes and other data values to a third party "for authentication," i.e., the recited "agent" or "third-party trusted authority." Given

other data values and send the plurality of codes and the other data values to agent." For the reasons noted above in [1.5], Burger also renders obvious the remaining features of [15.3].

[15.4] responsive to the device ID code being authenticated, the authentication unit receiving an access message from the agent allowing the user to access an application,

152. *See* [1.6]; MSC-1005, FIGS. 7A, 7B, 10A, 19, 26H-26K; ¶¶[0320], [0189], [0095]-[0096], [0101], [0125], [0236]-[0238], [0155]-[0158], [0103], [517]-[527], [182]-[186], [0194]. In addition, because the network server 114 uses communication protocol layer 2716 for communications between its controller 402 and any other network element, it would have been obvious to a POSITA that when the network server 114 sends the access message to Pocket Vault 102, the communications protocol layer 2716 ("***authentication unit***") also "***receiv[es] an access message from the agent allowing the user to access an application***." *See* [1.6].

---

the breadth of this claim language, therefore, Burger's "communication protocol layer 2716," which similarly receives and sends such data to an entity "for authentication" (i.e., to controller(s) 402 and database 406), is an "authentication unit." Specifically, layer 2716 receives and sends this information "for authentication" by the controller(s) 402 and the database 406.

[15.5] wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

153. *See* [1.7], [8.4]; MSC-1005, FIGS. 7A, 7B, 10A, 19, 26H-26K; ¶¶[0320], [0189], [0095]-[0096], [0101], [0125], [0236]-[0238], [0155]-[0158], [0103], [517]-[527], [182]-[186], [0194], [0250].

(xiii) <u>Claim 16</u>

[16] The system of claim 15, wherein the biometric key receives an authentication request from the authentication unit, and in response, requests a biometric scan from the user to generate the scan data.

154. When a request to register a new Pocket Vault holder is received, the operations 1904 shown in Burger's FIG. 20 below are performed by the network server 114. MSC-1005, ¶¶[0464], [0476].

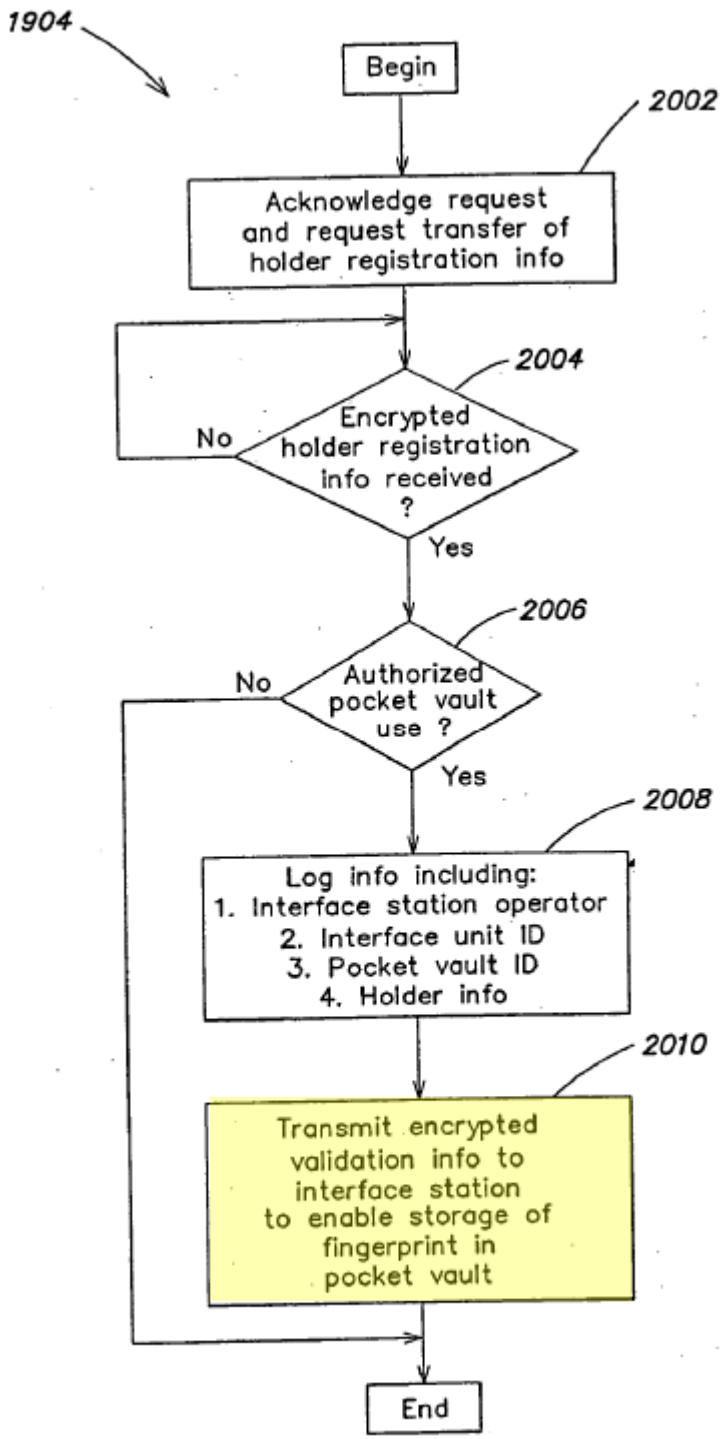


FIG. 20

MSC-1005, FIG. 20.

155. As shown in FIG. 20, after the requisite encrypted holder registration information is received through an interface station computer 304 or directly from the Pocket Vault and the network server 114 determines that the Pocket Vault is authorized for use, "all of the relevant information regarding the new Pocket Vault registration is logged into the database 406 of the network server 114." MSC-1005, ¶¶[0476]-[0481]. Next, in operation 2010, "the network server 114 transmits encrypted validation information to the interface station computer 304, which then may be passed on to the Pocket Vault interface unit 302, and then to the Pocket Vault 102, so as to enable the new holder's fingerprint to be stored in the memory of the Pocket Vault 102." MSC-1005, ¶[0482], FIG. 20.

156. In this example, the validation information sent from the communication protocol layer 2716[5] in the network server 114 to the Pocket Value 102 is the "***authentication request from the authentication unit***" that is received by the Pocket Vault 102 ("***biometric key***"), and, in response to receiving this information, the Pocket Vault 102 is enabled to ***request a biometric scan (e.g., fingerprints)***

---

[5] As shown in Burger's FIG. 27, it would have been obvious to a POSITA that the communication protocol layer 2716 ("***authentication unit***") sends and receives data between the pocket vault 102 and the network server 114.

from the user to generate and store scan data. MSC-1005, ¶[0482], FIG. 20. In this manner, Burger renders [16] obvious.

157. In another example, as part of a new Pocket Vault holder routine, shown below in FIG. 32, after a new holder's identity is verified (operation 3218) or a new holder account is created, instructions are sent to the Pocket Vault 102 "wherein the new holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 while the Pocket Vault 102 is interfaced with the interface unit 302. The user is further prompted to follow the directions on the Pocket Vault 102." MSC-1005, ¶¶[0575], [0585], FIG. 32.

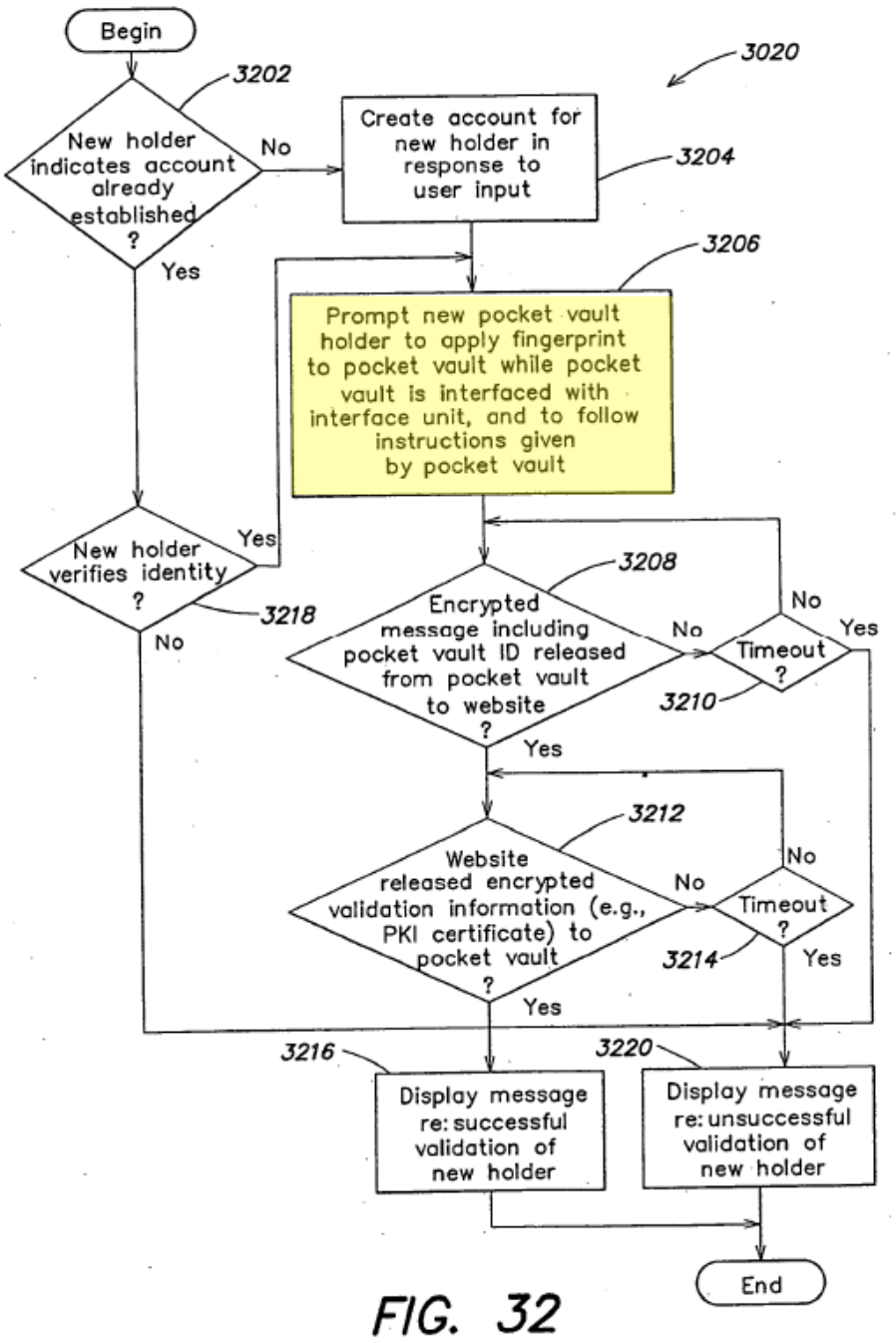


FIG. 32

MSC-1005, FIG. 32.

158. Although FIG. 32 is described as being performed by an interface station, "in some embodiments wherein appropriate networking capabilities are provided, each Pocket Vault 102 may communicate directly with the network server 114,

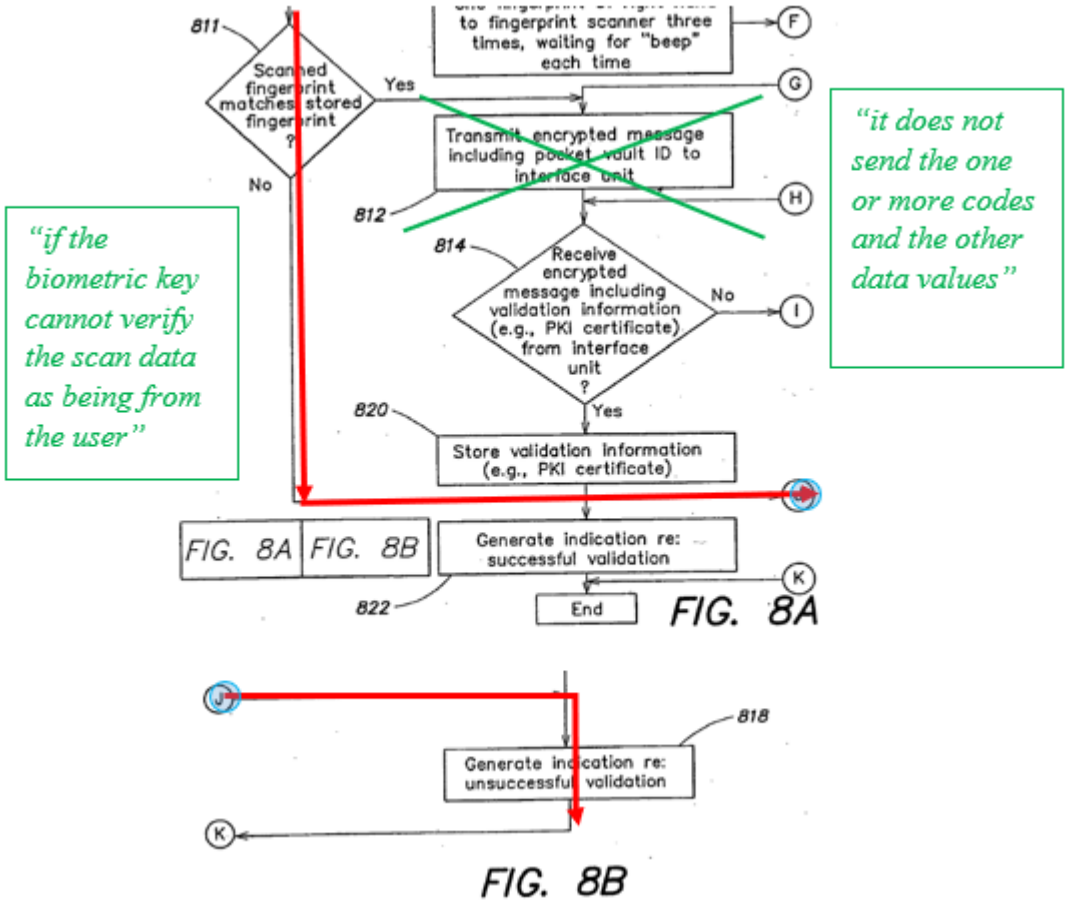
without the interface stations 104a-c facilitating communication therebetween." MSC-1005, ¶¶[0101], [0562], [0573], [0585]. Thus, in such embodiments, it would have been obvious to a POSITA that the communication protocol layer 2716 ("***authentication unit***") in the network server 114 would have communicated directly with the Pocket Vault 102 and sent a message ("***an authentication request***") to request the Pocket Vault 102 to prompt the new holder to apply the holder's fingerprints. In this additional way, Berger renders obvious "***wherein the biometric key receives an authentication request from the authentication unit, and in response, requests a biometric scan from the user to generate the scan data***," as recited in claim 16.

(xiv) <u>Claim 17</u>

[17] The system of claim 15, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the one or more codes and the other data values.

159. Burger teaches that when scanned fingerprints do not match stored fingerprints, an indication of unsuccessful validation is generated and no encrypted message including codes or other data values are sent. MSC-1005, FIGS. 7A, 8A, 8B, ¶[0211]. A marked-up example is shown below in FIG. 8B, in which Burger's system "***does not send the one or more codes and the other data values***" (steps

818, 820) "***if the biometric key cannot verify the scan data as being from the user***" (step 811).



MSC-1005, FIG. 8B.

B. Ground 2: Claims 3, 10, and 13 are obvious in view of Burger and Robinson

(i) ***Claim 3***

[3] The method of claim 1, further comprising: registering an age verification for the user in association with the device ID code.

160. As explained above in §VII.C, in the Burger-Robinson system, age-verification can be performed by receiving a user's information (including age information) at a verifier device, sending that information to the network server, verifying the user's age at the network server, and then outputting a result of the age verification. The Burger-Robinson combination renders [3] obvious in several ways.

161. First, a user registers with the system by presenting at least one biometric sample, identity-verifying information, and *age-verifying information*. MSC-1006, ¶¶[0014]-[0015]. This information is subsequently stored in the database 406 (verifier database) of network server 114. In this manner, Burger-Robinson renders obvious "***registering an age verification for the user***."

162. Second, when the age verification is performed, Robinson teaches that the results of the verifications are tracked. MSC-1006, ¶[0048]. That is, a result of the age verification is registered.

163. Robinson also teaches that age-verification records include "*at least one ID number (SID)* that identifies the presenter within the system." MSC-1006,

¶[0028]. Robinson explains that the "SID is a number used to help identify registered individuals in the invention's system. … The SID may be a unique number (a number with no chance of being honestly duplicated, e.g., social security number), reasonably unique number (a number with a statistically small chance of being duplicated, e.g., phone number), or a non-unique number (a number with a large chance of being duplicated)." MSC-1006, ¶[0043]. It would have been obvious to a POSITA that the user's Pocket Vault device ID is also a number "that can be used to identify registered individuals" and that the user's Pocket Vault device ID would be a device ID code. At least because the age verifying information registered for a presenter or user includes a SID and identity-verifying information such as the Pocket Vault device ID, Burger-Robinson renders obvious "***registering an age verification for the user in association with the device ID code***." MSC-1006, ¶¶[0014]-[0015].

(ii) ***<u>Claim 10</u>***

[10] The integrated device of claim 9, wherein an age verification is registered in association with the device ID code.

164. *See* [3].

(iii) ***Claim 13***

[13] The method of claim 12, further comprising: registering a date of birth or age with the agent.

165. Similar to the explanation above in [3], the Burger-Robinson combination registering age-verification information, such as a date of birth or age, with the database 406 ("***the agent***") in the network server 114. MSC-1006, ¶¶[0014]-[0015]. Accordingly, the Burger-Robinson combination renders [13] obvious.

IX. CONCLUSION

166. For all the reasons I have noted in the foregoing paragraphs, claims 1-17 of the '730 Patent are obvious in view of the references discussed above.

APPENDIX A

Patrick Gerard Traynor

Professor
Associate Chair for Research in CISE
John and Mary Lou Dasburgh Preeminent Chair in Engineering

Department of Computer & Information Science & Engineering (CISE)
University of Florida
E301 CSE Building, PO Box 116120
Gainesville, FL 32611 USA
traynor@cise.ufl.edu
http://www.cise.ufl.edu/∼traynor

Table of Contents

EDUCATIONAL BACKGROUND **4**

EMPLOYMENT HISTORY **4**

CURRENT FIELDS OF INTEREST **4**

I. TEACHING **6**
- A. Courses Taught . . . 6
- B. Continuing Education . . . 6
- C. Curriculum Development . . . 6
- D. Individual Student Guidance . . . 7
- E. Teaching Honors and Awards . . . 11

II. RESEARCH AND CREATIVE SCHOLARSHIP **12**
- A. Thesis . . . 12
- B. Published Journal Papers (Refereed) . . . 12
- C. Published Books and Parts of Books . . . 14
- D. Edited Proceedings . . . 14
- E. Conference Presentations . . . 14
  - E.1. Conference Presentations with Proceedings (Refereed) . . . 14
  - E.2. Conference Presentations with Proceedings (Non-Refereed) . . . 20
  - E.3. Conference Presentations without Proceedings . . . 20
- F. Other . . . 20
  - F.1. Submitted Journal Papers . . . 20
  - F.2. Refereed Research Reports . . . 20
  - F.3. Software . . . 20
  - F.4. Published Papers (Non-Refereed) . . . 21
  - F.5. Books in Preparation . . . 21
  - F.6. Workshops and External Courses . . . 21
- G. Research Proposals and Grants (Principal Investigator) . . . 22
- H. Research Proposals and Grants (Contributor) . . . 24
- I. Research Honors and Awards . . . 25

III. SERVICE **27**
- A. Professional Activities . . . 27
  - A.1. Memberships and Activities in Professional Societies . . . 27
  - A.2. Conference Committee Activities . . . 27
- B. On-Campus Committees . . . 28
  - B.1. University of Florida . . . 28
  - B.2. Georgia Tech . . . 29
- C. Special Assignments . . . 29
- D. Ph.D. Examining Committees . . . 29
- E. External Member of M.S. Examining Committee . . . 33
- F. Consulting and Advisory Appointments . . . 33
- G. Civic Activities . . . 33

IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION **34**
- A. Honors and Awards . . . 34
- B. Invited Conference Session Chairmanships . . . 34
- C. Professional Registration . . . 34
- D. Patents . . . 34
- E. Editorial and Reviewer Work for Technical Journals and Publishers . . . 35
- F. Expert Witness Services . . . 37

V. OTHER CONTRIBUTIONS **39**
- A. Seminar Presentations (Invited Papers and Talks at Meetings and Symposia) . . . 39

B. Special Activities 43

EDUCATIONAL BACKGROUND

Degree	Year	University	Field
Ph.D.	2008	Pennsylvania State University State College, PA *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.

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

I. TEACHING

A. Courses Taught

Semester/Year	Course Number & Title	Number of Students	Comments
Fall 2022	CNT 5410 Computer and Network Security	75	New Topics
Fall 2021	CNT 5410 Computer and Network Security	45	New Topics
Fall 2019	CNT 5410 Computer and Network Security	28	New Topics
Fall 2018	CIS 6930 Cellular and Mobile Network Security	16	New Course
Fall 2017	CNT 5410 Computer and Network Security	27	New Topics
Fall 2016	CNT 5410 Computer and Network Security	60	New Topics
Spring 2016	CNT 5410 Computer and Network Security	13	New Topics
Spring 2015	CNT 5410 Computer and Network Security	12	New Topics
Fall 2014	CNT 5410 Computer and Network Security	30	New Course
Spring 2014	CS 6262 Network Security	55	New Projects
Fall 2013	CS 3251 Computer Networks I	73	Expanded Syllabus
Spring 2013	CS 6262 Network Security	65	All New Projects
	CS 8001 Information Security Seminar	20	New Speakers
Fall 2012	CS 8803 Cellular & Mobile Network Security	17	New Topics
	CS 8001 Information Security Seminar	20	New Speakers
Spring 2011	CS 8001 Information Security Seminar	20	New Speakers
Fall 2011	CS 6262 Network Security	27	Expanded Syllabus
	CS 8001 Information Security Seminar	35	New Speakers
Spring 2011	CS 3251 Computer Networks I	61	Expanded Syllabus
	CS 8001 Information Security Seminar	20	New Speakers
Fall 2010	CS 8803/4803 Cellular & Mobile Network Security	16	New Course
	CS 8001 Information Security Seminar	31	New Speakers
Fall 2009	CS 6262 Network Security	55	Expanded Syllabus
Spring 2009	CS 3251 Computer Networks I	45	Expanded Syllabus
Fall 2008	CS 8003 Destructive Research	10	New Course

Guest lecturer for CS 4235 (Introduction to Information Security) and CS 8803 (e-Democracy) in Fall 2008.

Advised ECE 4811/CS 4802 (Vertically Integrated Project) with Ed Coyle

B. Continuing Education

None.

C. Curriculum Development

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

company to potential investors.

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

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

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

D. Individual Student Guidance

1. Research Scientists Supervised

None.

2. Ph.D. Students Graduated

Chaitrali Amrutkar Georgia Institute of Technology
Fall 2009–Fall 2013
Her research discovered vulnerabilities in mobile web browsers and developed techniques to detect malicious mobile web pages. Joined Oracle in Spring 2014.

Jasmine Bowers University of Florida
Fall 2015–Summer 2020
Her research focuses on mobile applications, and the development of tools for building secure systems. Now: Research Scientist, MITRE

Henry "Hank" Carter Georgia Institute of Technology
Fall 2010–Spring 2016
Developing techniques for secure function evaluation for privacy-preserving applications on constrained mobile devices. Now: Assistant Professor, Villanova University

Italo Dacosta Georgia Institute of Technology
Fall 2008–Summer 2012
Co-advised with Mustaque Ahamad. Research on scaling performance of SIP network components. Graduated Summer 2012, currently research scientist at EPFL.

David Dewey Georgia Institute of Technology
Fall 2011–Summer 2015
Investigated compiler techniques to remove software vulnerabilities from code. Now CTO of MailChimp.

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

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

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

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

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

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

2. Ph.D. Students Supervised

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

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

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

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

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

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

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

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

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

3. Ph.D. Students - Other

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

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

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

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

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

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

4. M.S. Students Supervised

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

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

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

Christopher Grayson Georgia Institute of Technology
Fall 2012–Fall 2013
Developed continuous authentication mechanisms using the multitude of sensors available on a mobile phone. Now at Bishop Fox Consulting (industry).

Young Seuk Kim Georgia Institute of Technology
Fall 2012–Fall 2013
Performed research that compared the security vulnerabilities found in the traditional and mobile web.

Daniel Komaromy Georgia Institute of Technology
Fall 2008–Summer 2009
Research on building a real-time streaming audio system using attribute-based crypto for broadcast encryption.

Nigel Lawrence Georgia Institute of Technology
Fall 2011–Spring 2012
Discovered hijacking attacks in SNMPv3, a widely used and thought to be secure network management protocol. Now at Solute (industry).

Philip Marquardt Georgia Institute of Technology
Fall 2009–Present
Research on developing an iPhone application to prevent individuals from being profiled by Shopper Loyalty Programs. First with MIT Lincoln Labs, now Raytheon

Rishikesh Naik Georgia Institute of Technology
Fall 2008–Spring 2010
Research on converting expensive cryptographic primitives (e.g., Secure Function Evaluation) into efficient applications for mobile phones. Now with Cisco Systems.

Ashish Nautiyal CISE
Fall 2015–Spring 2016
Research on connecting telephone calls to the larger authentication infrastructure.

Nilesh Nipane Georgia Institute of Technology
Fall 2008–Spring 2010
Research on creating provably anonymous networks on a base of secure function evaluation. Now with VMWare.

Walter "Nolen" Sciafe Georgia Institute of Technology
Spring 2012–Spring 2014
Developed the OnionDNS architecture, which prevents domain delisting attacks by leveraging a Tor hidden service. Joined Ph.D. program at UF.

Tyler Tucker University of Florida
Fall 2018–Spring 2021
Evaluating the security of Bluetooth radios.

5. M.S. Special Problems Students

Siddhant Deshmukh University of Florida
Fall 2016–Present
Developed tools for analysis of mobile digital financial services.

Chinmay Gangakhedkar Georgia Institute of Technology
Spring 2009
Research on multi-factor authentication using mobile phones.

Christopher Grayson Georgia Institute of Technology
Spring 2013
Research on continuous authentication using mobile phones.

Aarushi Karnany University of Florida
Fall 2016–Present
Developed tools for analysis of mobile digital financial services.

Rohit Matthews Georgia Institute of Technology
Spring 2011
Developed mobile phone-based tools for measuring performance and reachability throughout the Internet.

Ashwin Narasimhan Georgia Institute of Technology
Spring 2009
Research on developing efficient security mechanisms for the IMS cellular core.

Aamir Poonawalla Georgia Institute of Technology
Spring 2010
Helped develop a call provenance infrastructure, which included both networking and machine learning components.

Erin Reddick Georgia Institute of Technology
Fall 2008–Fall 2009
Research on IPTV security with GTRI.

Lalanthika Vasudevan Georgia Institute of Technology
Spring 2009
Research on developing efficient security mechanisms for the IMS cellular core.

6. Undergraduate Special Problems Students

Ethan Shernan Georgia Institute of Technology
Spring 2014
Developed an infrastructure for detecting billing bypass fraud attacks.

Young Seuk Kim Georgia Institute of Technology
Fall 2011–Spring 2012
Developed a mobile phone application for taking measurements of cellular networks.

Dane Van Dyck Georgia Institute of Technology
Summer 2009
Research on virtualization support for mobile phones.

E. Teaching Honors and Awards

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

II. RESEARCH AND CREATIVE SCHOLARSHIP

A. Thesis

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

B. Published Journal Papers (Refereed)

1. Cassidy Gibson, Vanessa Frost, Katie Platt, Washington Garcia, Luis Vargas, Sara Rampazzi, Vincent Bindschaedler, Patrick Traynor, and Kevin Butler. Analyzing the Monetization Ecosystem of Stalkerware. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2022.

2. Bradley Reaves, Luis Vargas, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, and Kevin Butler. Characterizing the Security of the SMS Ecosystem with Public Gateways. *ACM Transactions on Privacy and Security (TOPS)*, 22(1), 2018.

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

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

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

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

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

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

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

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

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

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

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

14. Chaitrali Amrutkar, Patrick Traynor, and Paul van Oorschot. An Empirical Evaluation of Security Indicators in Mobile Web Browsers. *IEEE Transactions on Mobile Computing (TMC)*, 14(5), 2015.

15. Andrew Harris, Seymour Goodman, and Patrick Traynor. Privacy and Security Concerns Associated with Mobile Money Applications in Africa. *Washington Journal of Law, Technology & Arts*, 8(3), 2013.

16. Italo Dacosta, Saurabh Chakradeo, Mustaque Ahamad, and Patrick Traynor. One-Time Cookies: Preventing Session Hijacking Attacks with Stateless Authentication Tokens. *ACM Transactions on Internet Technology (TOIT)*, 12(1), 2012.

17. Cong Shi, Xiapu Luo, Patrick Traynor, Mostafa Ammar, and Ellen Zegura. ARDEN: Anonymous netwoRking in Delay tolErant Networks. *Journal of Ad Hoc Networks*, 10(6):918–930, 2012.

18. Patrick Traynor. Characterizing the Security Implications of Third-Party EAS Over Cellular Text Messaging Services. *IEEE Transactions on Mobile Computing (TMC)*, 11(6):983–994, 2012.

19. Italo Dacosta, Vijay Balasubramaniyan, Mustaque Ahamad, and Patrick Traynor. Improving Authentication Performance of Distributed SIP Proxies. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 22(11):1804–1812, 2011.

20. Patrick Traynor, Chaitrali Amrutkar, Vikhyath Rao, Trent Jaeger, Patrick McDaniel, and Thomas La Porta. From Mobile Phones to Responsible Devices. *Journal of Security and Communication Networks (SCN)*, 4(6):719 – 726, 2011.

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

22. Patrick Traynor, Kevin Butler, William Enck, Kevin Borders, and Patrick McDaniel. malnets: Large-Scale Malicious Networks via Compromised Wireless Access Points. *Journal of Security and Communication Networks (SCN)*, 2(3):102–113, 2010.

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

24. Kevin Butler, Sunam Ryu, Patrick Traynor, and Patrick McDaniel. Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 20(12):1803–1815, 2009.

25. Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Mitigating Attacks On Open Functionality in SMS-Capable Cellular Networks. *IEEE/ACM Transactions on Networking (TON)*, 17(1), 2009.

26. Patrick Traynor, Michael Chien, Scott Weaver, Boniface Hicks, and Patrick McDaniel. Non-Invasive Methods for Host Certification. *ACM Transactions on Information and System Security (TISSEC)*, 2008.

27. Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. *Journal of Computer Security (JCS)*, 16(6):713–742, 2008.

28. Patrick Traynor, Raju Kumar, Heesook Choi, Sencun Zhu, Guohong Cao, and Thomas La Porta. Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks. *IEEE Transactions on Mobile Computing (TMC)*, 6(6), 2007.

C. Published Books and Parts of Books

1. Andrew Harris, Frank S. Park, Seymour Goodman, and Patrick Traynor. *Emerging Privacy and Security Concerns for Digital Wallet Deployment*. Privacy in America: Interdisciplinary Perspectives. Scarecrow Press, July 2011.

2. Kevin Butler, William Enck, Patrick Traynor, Jennifer Plasterr, and Patrick McDaniel. *Privacy Preserving Web-Based Email*. Algorithms, Architectures and Information Systems Security, Statistical Science and Interdisciplinary Research. World Scientific Computing, November 2008.

3. Patrick Traynor, Patrick McDaniel, and Thomas La Porta. *Security for Telecommunications Networks*. Number 978-0-387-72441-6 in Advances in Information Security Series. Springer, August 2008.

D. Edited Proceedings

None.

E. Conference Presentations

E.1. Conference Presentations with Proceedings (Refereed)

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

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

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

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

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

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

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

8. Christian Peeters, Christopher Patton, Imani N. Sherman, Daniel Olszewski, Thomas Shrimpton, and Patrick Traynor. SMS OTP Security (SOS): Hardening SMS-Based Two Factor Authentication. In *ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2022. (Acceptance rate: 18.2%).

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

10. Imani Sherman and Daniel Delgado and Juan Gilbert and Jaime Ruiz and Patrick Traynor. Characterizing User Comprehension in the STIR/SHAKEN Anti-Robocall Standard. In *Proceedings of the Annual Research Conference on 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%).

21. Lius Vargas, Logan Blue, Vanessa Frost, Christopher Patton, N. Scaife, K. Butler, and P. Traynor. Digital Healthcare-Associated Infection Analysis of a Major Multi-Campus Hospital System. In *Proceedings of the ISOC Network & Distributed Systems Security Symposium (NDSS)*, 2019. (Acceptance Rate: 17.1%).

22. Dominik Wermke, Nicolas Huaman, Yasemin Acar, Bradley Reaves, Patrick Traynor, and Sascha Fahl. A Large Scale Investigation of Obfuscation Use in Google Play. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2018. Acceptance Rate: 20.1%.

23. Nolen Scaife, Christian Peeters, and Patrick Traynor. Fear the Reaper: Characterization and Fast Detection of Card Skimmers. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2018. Acceptance Rate: 19.0%.

24. Dave (Jing) Tian, Grant Hernandez, Joseph Choi, Vanessa Frost, Christie Raules, Kevin Butler, Patrick Traynor, Hayawardh Vijayakumar, Lee Harrison, Amir Rahmati, and Mike Grace. ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2018. Acceptance Rate: 19.0%.

25. Logan Blue, Hadi Abdullah, Luis Vargas, and Patrick Traynor. 2MA: Verifying Voice Commands via Two Microphone Authentication. In *ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2018. (Acceptance Rate: 20.0%).

26. Nolen Scaife, Christian Peeters, Camilo Velez, Hanqing Zhao, Patrick Traynor, and David Arnold. The Cards Aren't Alright: Detecting Counterfeit Gift Cards Using Encoding Jitter. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2018. (Acceptance Rate: 10.4%).

27. Christian Peeters, Hadi Abdullah, Nolen Scaife, Jasmine Bowers, Patrick Traynor, Bradley Reaves, and Kevin Butler. Sonar: Detecting SS7 Redirection Attacks Via Call Audio-Based Distance Bounding. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2018. (Acceptance Rate: 10.4%).

28. Tyler Ward, Joseph Choi, Kevin Butler, John M. Shea, Patrick Traynor, and Tan Wong. Privacy Preserving Localization Using a Distributed Particle Filtering Protocol. In *IEEE MILCOM*, 2017. (Acceptance Rate: 56%).

29. Bradley Reaves and Logan Blue and Hadi Abdullah and Luis Vargas and Patrick Traynor and Thomas Shrimpton. AuthentiCall: Efficient Identity and Content Authentication for Phone Calls. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2017. (Acceptance Rate: 16.3%).

30. Jasmine Bowers and Bradley Reaves and Imani N. Sherman and Patrick Traynor and Kevin Butler. Regulators, Mount Up! Analysis of Privacy Policies for Mobile Money Applications. In *Proceedings of the USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2017. (Acceptance Rate: 26.5%).

31. Bradley Reaves, Logan Blue, and Patrick Traynor. AuthLoop: End-to-End Cryptographic Authentication for Telephony over Voice Channels. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2016. (Acceptance Rate: 15.5%).

32. Dave Tian, Nolen Scaife, Adam Bates, Kevin Butler, and Patrick Traynor. Making USB Great Again with USBFILTER. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2016. (Acceptance Rate: 15.5%).

33. Bradley Reaves, Dave Tian, Logan Blue, Patrick Traynor, and Kevin Butler. Detecting SMS Spam in the Age of Legitimate Bulk Messaging. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2016. (Acceptance Rate: 35.0%).

34. Nolen Scaife, Henry Carter, Patrick Traynor, and Kevin Butler. CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. In *IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2016. (Acceptance Rate: 17.6%).

35. Bradley Reaves, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, and Kevin Butler. Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2016. (Acceptance Rate: 13.0%).

36. Benjamin Mood, Debayan Gupta, Henry Carter, Kevin Butler, and Patrick Traynor. Frigate: A Validated, Extensible, and Efficient Compiler and Interpreter for Secure Computation. In *Proceedings of the IEEE European Symposium on Security and Privacy*, 2016. (Acceptance Rate: 17.3%).

37. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Outsourcing Secure Two-Party Computation as a Black Box. In *Proceedings of the International Conference on Cryptology and Network Security*, 2015. (Acceptance Rate: 52.9%).

38. Nolen 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%).

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%).

61. Italo Dacosta and Patrick Traynor. Proxychain: Developing a Robust and Efficient Authentication Infrastructure for Carrier-Scale VoIP Networks. In *Proceedings of the USENIX Annual Technical Conference (ATC)*, 2010. (Acceptance Rate: 17.0%).

62. Frank S. Park, Chinmay Gangakhedkar, and Patrick Traynor. Leveraging Cellular Infrastructure to Improve Fraud Prevention. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2009. (Acceptance Rate: 19.0%).

63. Patrick Traynor, Michael Lin, Machigar Ongtang, Vikyath Rao, Trent Jaeger, Thomas La Porta, and Patrick McDaniel. On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2009. (Acceptance Rate: 18.4%).

64. Brendan Dolan-Gavitt, Abhinav Srivastava, Patrick Traynor, and Jonathon Giffin. Robust Signatures for Kernel Data Structures. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2009. (Acceptance Rate: 18.4%).

65. Italo Dacosta, Vijay Balasubramaniyan, Mustaque Ahamad, and Patrick Traynor. Improving Authentication Performance of Distributed SIP Proxies. In *Proceedings of the Conference on Principles, Systems and Applications of IP Telecommunications (IPTComm)*, 2009. (Acceptance Rate: 43.3%).

66. Patrick Traynor, Kevin Butler, William Enck, and Patrick McDaniel. Realizing Massive-Scale Conditional Access Systems Through Attribute-Based Cryptosystems. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2008. (Acceptance Rate: 17.7%).

67. Patrick Traynor, Patrick McDaniel, and Thomas La Porta. On Attack Causality in Internet-Connected Cellular Networks. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2007. (Acceptance Rate: 12.3%).

68. Sunam Ryu, Kevin Butler, Patrick Traynor, and Patrick McDaniel. Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems. In *Proceedings of the IEEE International Symposium on Security in Networks and Distributed Systems (SSNDS)*, 2007. (Acceptance Rate: 40%).

69. Luke St. Clair, Lisa Johansen, William Enck, Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Trent Jaeger. Password Exhaustion: Predicting the End of Password Usefulness. In *Proceedings of the International Conference on Information Systems Security (ICISS)*, 2006. (Invited Paper).

70. Kevin Butler, William Enck, Jennifer Plasterr, Patrick Traynor, and P. McDaniel. Privacy-Preserving Web-Based Email. In *Proceedings of the International Conference on Information Systems Security (ICISS)*, December 2006. (Acceptance Rate: 30.4%).

71. Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters. Secure Attribute-Based Systems. In *Proceedings of the Thirteenth ACM Conference on Computer and Communications Security (CCS)*, November 2006. (Acceptance Rate: 14.8%).

72. Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks. In *Proceedings of the Twelfth Annual ACM International Conference on Mobile Computing and Networking (MobiCom)*, September 2006. (Acceptance Rate: 11.7%).

73. Patrick Traynor, Michael Chien, Scott Weaver, Boniface Hicks, and Patrick McDaniel. Non-Invasive Methods for Host Certification. In *Proceedings of the Second IEEE International Conference on Security and Privacy in Communication Networks (SecureComm)*, August 2006. (Acceptance Rate: 25.4%).

74. Patrick Traynor, JaeShung Shin, Barat Madan, Shashi Phoha, and Thomas La Porta. Efficient Group Mobility for Heterogeneous Sensor Networks. In *Proceedings of the IEEE Vehicular Technology Conference (VTC Fall)*, September 2006. (Acceptance Rate: 58%).

75. Patrick Traynor, Raju Kumar, Hussain Bin Saad, Guohong Cao, and Thomas La Porta. LIGER: Implementing Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks. In *Proceedings of the 4th ACM International Conference on Mobile Systems, Applications and Services (MobiSys)*, June 2006. (Acceptance Rate: 15.4%).

76. Patrick Traynor, Guohong Cao, and Thomas La Porta. The Effects of Probabilistic Key Management on Secure Routing in Sensor Networks. In *Proceedings of the 2006 IEEE Wireless Communications and Networking Conference (WCNC)*, April 2006. (Acceptance Rate: 38.8%).

77. Patrick Traynor, Heesook Choi, Guohong Cao, Sencun Zhu, and Thomas La Porta. Establishing Pair-Wise Keys In Heterogeneous Sensor Networks. In *Proceedings of the 25th Annual IEEE Conference on Computer Communications (INFOCOM)*, April 2006. (Acceptance Rate: 18%).

78. William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. In *Proceedings of the Twelfth ACM Conference on Computer and Communications Security (CCS)*, November 2005. (Acceptance Rate: 15%).

Removed for external version.

E.2. Conference Presentations with Proceedings (Non-Refereed)

None.

E.3. Conference Presentations without Proceedings

1. Patrick Traynor. Work in Progress Presentations: Fine-Grained Secure Localization for 802.11 Networks. 15th USENIX Security Symposium (SECURITY), August 2006.

2. Patrick Traynor. Work in Progress Presentations: Fundamental Limitations of Sensor Network Security. ACM/USENIX Fourth International Conference on Mobile Systems Applications and Services (MobiSys), June 2006. (Award: Most Entertaining WIP).

3. Patrick Traynor, Heesook Choi, Guohong Cao, and Thomas La Porta. Poster Session: Probabilistic Unbalanced Key Distribution and Its Effects on Distributed Sensor Networks. Workshop on Wireless Security (WiSe), October 2004.

F. Other

F.1. Submitted Journal Papers

None.

F.2. Refereed Research Reports

None.

F.3. Software

1. *GSM Air Interface Simulator:* Developed a full voice, data and SMS capable simulator for the wireless portion of a GSM network. Models communications down to the timeslot for highest possible accuracy. Used in the majority of our work on cellular security.

2. *Malicious Telephony Load Tester:* Built a system on top of the TM1 Telecom Database testing suite to allow for a comparison of malicious traffic of varying composition.

F.4. Published Papers (Non-Refereed)

1. Patrick Traynor. Characterizing the Limitations of Third-Party EAS Over Cellular Text Messaging Services. Technical report, 3G Americas Whitepaper, 2008.

2. Lisa Johansen, Kevin Butler, William Enck, Patrick Traynor, and Patrick McDaniel. Grains of SANs: Building Storage Area Networks from Memory Spots. Technical Report NAS-TR-0060-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, 2007.

F.5. Books in Preparation

None.

F.6. Workshops and External Courses

1. Luis Vargas, Patrick Emami, and Patrick Traynor. On the Detection of Disinformation Campaign Activity with Network Analysis. In *Proceedings of the 2020 ACM SIGSAC Cloud Computing Security Workshop*, CCSW '20, 2020.

2. Siddhant Deshmukh, Henry Carter, Grant Hernandez, Patrick Traynor, and Kevin Butler. Efficient and Secure Template Blinding for Biometric Authentication. In *IEEE Workshop on Security and Privacy in the Cloud (SPC)*, 2016.

3. Debayan Gupta, Benjamin Mood, Joan Feigenbaum, Kevin Butler, and Patrick Traynor. Using Intel Software Guard Extensions for Efficient Two-Party Secure Function Evaluation. In *Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC)*, 2016.

4. Chaitrali Amrutkar and Patrick Traynor. Rethinking Permissions for Mobile Web Apps: Barriers and the Road Ahead. In *Proceedings of the ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, 2012.

5. Nigel Lawrence and Patrick Traynor. Under New Management: Practical Attacks on SNMPv3. In *Proceedings of the USENIX Workshop on Offensive Technologies (WOOT)*, 2012.

6. Andrew Harris, Frank S. Park, Seymour Goodman, and Patrick Traynor. Emerging Privacy Concerns for Digital Wallet Deployment. In *Proceedings of the Workshop on Making Privacy in America*, 2009.

7. Patrick Traynor. Privacy and Security Concerns for Personal and Mobile Health Devices. In *Proceedings of the Workshop to Set A Research Agenda for Privacy and Security of Healthcare Technologies*, 2009.

8. Kevin Butler, William Enck, Harri Hursti, Stephen McLaughlin, Patrick Traynor, and Patrick McDaniel. Systemic Issues in the Hart InterCivic and Premier Voting System: Reflections Following Project EVEREST. In *Proceedings of the USENIX/ACCURATE Electronic Voting Technology (EVT) Workshop*, 2008.

G. Research Proposals and Grants (Principal Investigator)

1. Approved and Funded

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

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

3. **SaTC:CORE:Medium: Securing the Voice Processing Pipeline Against Adversarial Audio**
   Sponsor: NSF Secure and Trustworthy Cyberspace
   Investigator(s): Patrick Traynor (PI), Thomas Shrimpton, Vincent Bindschaedler
   Amount: *$1,199,999 over 4 years*
   Awarded: October 2019

4. **Artus Protocol STTR Phase II**
   Sponsor: Office of Naval Research
   Investigator(s): Patrick Traynor (PI), Kevin Butler
   Amount: *$800,000 over 4 years*
   Awarded: August 2019

5. **Evaluating the Security of QR Code-Based Payments**
   Sponsor: Discover Financial
   Investigator(s): Patrick Traynor (PI)
   Amount: *$50,000 over 1 year*
   Awarded: September 2018

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

9. **Evaluating and Improving Security in Emerging Branchless Banking Systems**
   Sponsor: NSF Secure and Trustworthy Cyberspace
   Investigator(s): Patrick Traynor (PI)
   Amount: *$500,000 over 3 years*
   Awarded July 2015

10. **Prevention and Detection of Disallowed Connections in Mobile and Pervasive Systems**
    Sponsor: CISE-ECE Harris Endowed Seed Fund Program
    Investigator(s): Patrick Traynor (PI), Renato Figueiredo (PI)
    Amount: *$40,000 over 1 year*
    Awarded December 2014

11. **Mobile Excursion Study Support**
    Sponsor: Hanscom AFB Electronic Systems Command Development Planning Division (ESC/XR)
    Investigator(s): Patrick Traynor (PI), Mustaque Ahamad, Jeff Evans, Chuck Bokath
    Amount: *$280,000 over 3 months*
    Awarded July 2012

12. **Characterizing the Security Limitations of Accessing the Mobile Web**
    Sponsor: NSF Secure and Trustworthy Cyberspace
    Investigator(s): Patrick Traynor (PI) and William Enck (NC State)
    Amount: *$334,000 over 3 years*
    Awarded July 2012

13. **Mitigating Attacks on Mobile Devices and Critical Cellular Infrastructure**
    Sponsor: US Department of Defense - Defense University Research Instrumentation Program (DURIP)
    Investigator(s): Patrick Traynor (PI), Jon Giffin, Mustaque Ahamad
    Amount: *$210,081 over 1 year*
    Awarded June 2011

14. **Characterizing and Implementing Efficient Primitives for Privacy-Preserving Computation**
    Sponsor: DARPA PROgramming Computation on EncryptEd Data (PROCEED) – Broad Agency Announcement
    Investigator(s): Patrick Traynor (PI) and Kevin Butler (UOregon)
    Amount: *$580,000 over 4 years*
    Awarded May 2011

15. **Security for Converged IMS Networks**
    Sponsor: US Department of Defense
    Investigator(s): Patrick Traynor (PI), Mustaque Ahamad and Russ Clark
    Amount: *$242,401 over 1 year*
    Awarded August 2010

16. **CAREER: Protecting User Data on Lost, Stolen and Damaged Mobile Phones**
    Sponsor: NSF Trustworthy Computing
    Investigator(s): Patrick Traynor (PI)
    Amount: *$400,000 over 5 years*
    Awarded: May 2010

17. **Provably Anonymous Networking Through Secure Function Evaluation**
    Sponsor: NSF Trustworthy Computing
    Investigator(s): Patrick Traynor (PI)
    Amount: *$200,000 over 2 years*
    Awarded: July 2009

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

2. Pending

Removed for external version.

H. Research Proposals and Grants (Contributor)

1. Approved and Funded

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

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

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

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

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

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

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

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

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

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

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

2. Pending

Removed for external version.

I. Research Honors and Awards

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

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

III. SERVICE

A. Professional Activities

A.1. Memberships and Activities in Professional Societies

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

A.2. Conference Committee Activities

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

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

B. On-Campus Committees

B.1. University of Florida

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

B.2. Georgia Tech

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

C. Special Assignments

None.

D. Ph.D. Examining Committees

Ph.D. Examining Committees

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

9. Manos Antonakakis, College of Computing, Georgia Tech, Summer 2012.
   Advisor: Professor Wenke Lee.

10. Junjie Zhang, College of Computing, Georgia Tech, Summer 2012.
    Advisor: Professor Wenke Lee.

11. Italo Dacosta, College of Computing, Georgia Tech, Summer 2012.
    Advisor: Professor Patrick Traynor.

12. Virendra Kumar, College of Computing, Georgia Tech, Summer 2012.
    Advisor: Professor Alexandra Boldyreva.

13. Anirudh Ramachandran, College of Computing, Georgia Tech, Summer 2011.
    Advisor: Professor Nick Feamster.

14. Vijay Balasubramaniyan, College of Computing, Georgia Tech, Summer 2011.
    Advisor: Professor Mustaque Ahamad.

15. Kapil Singh, College of Computing, Georgia Tech, Summer 2011.
    Advisor: Professor Wenke Lee.

16. Abhinav Srivastava, College of Computing, Georgia Tech, Summer 2011.
    Advisor: Professor Jon Giffin.

17. Adam O'Neill, College of Computing, Georgia Tech, Summer 2010.
    Advisor: Professor Alexandra Boldyreva.

18. David Cash, College of Computing, Georgia Tech, Fall 2009.
    Advisor: Professor Alexandra Boldyreva.

External Member of Ph.D. Research Committee

None.

External Member of Ph.D. Examining Committee

1. Shannon Eggers, Department of Materials Sciences and Engineering - Nuclear Engineering Program, University of Florida, Fall 2016.
   Advisor: Professor Kelly Jordan.

2. Ed Carlisle, Department of Electrical and Computer Engineering, University of Florida, Summer 2016.
   Advisor: Professor Alan George.

3. Claudio Marforio, Department of Computer Science, Swiss Federal Institute of Technology Zurich (ETH Zurich), Fall 2015.
   Advisor: Professor Srdjan Capkun.

4. Nils Ole Tippenhauer, Department of Computer Science, Swiss Federal Institute of Technology Zurich (ETH Zurich), Spring 2012.
   Advisor: Professor Srdjan Capkun.

5. Bongkyoung Kwon, School of Electrical and Computer Engineering, Georgia Tech, Summer 2009.
   Advisor: Professor John Copeland.

Ph.D. Thesis Proposal Committees

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

Ph.D. Qualifying Exam Committees—Georgia Tech

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

23. Italo Dacosta, College of Computing, Georgia Tech, Fall 2008.
    Advisor: Professor Mustaque Ahamad and Professor Patrick Traynor.

24. Adam O'Neill, College of Computing, Georgia Tech, Fall 2008.
    Advisor: Professor Alexandra Boldyreva.

E. External Member of M.S. Examining Committee

M.S. Thesis Defense Committees None.

F. Consulting and Advisory Appointments

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

G. Civic Activities

None.

IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION

A. Honors and Awards

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

B. Invited Conference Session Chairmanships

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

C. Professional Registration

None.

D. Patents

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

4. Walter Nolen Scaife, Patrick G. Traynor and Christian Peeters, "Payment Card Overlay Skimmer Detection", United States Patent # 10,496,914, Filed October 2017, Issued December 2019. (See also # 10,936,928)
5. Patrick G. Traynor, David P. Arnold, Walter Nolen Scaife, Christian Peeters, and Camilo Valez Cuervo, "Detecting counterfeit magnetic stripe cards using encoding jitter", United States Patent # 10,803,261, Filed May 2017, Issued October 2020.
6. Patrick G. Traynor, Bradley Reaves, Logan Blue, Luis Vargas, Hadi Abdullah, and Thomas Shrimpton, "Identity and content authentication for phone calls", United States Patent # 10,764,043, Filed Apr 2017, Issued September 2020.
7. Walter Nolen Scaife, Henry Carter, Patrick G. Traynor and Kevin R. B. Butler. "Malware Detection Through User Data Transformation Monitoring", United States Patent # 10,685,114. Filed September 2015, Issued June 2020.
8. Vijay A. Balasubramaniyan, Mustaque Ahamad, Patrick G. Traynor. "Using Single-Ended Audio Features to Automatically Determine Voice Call Provenance", United States Patent, #9,037,113 June 2010, Issued May 2015. (See also #9,516,497 and #10,523,809)
9. Patrick G. Traynor, Byungsuk Kim and Farooq Anjum. "Secure Localization for 802.11 Networks with Fine Granularity", United States Patent, #8,107,400, Filed July 2008, Issued January 2012.

E. Editorial and Reviewer Work for Technical Journals and Publishers

Associate Editor:

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

Guest Editor:

Journals

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

Reviewer for:

Journals

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

- *IEEE Transactions on Parallel and Distributed Systems (TPDS)* 2005, 2009, 2010
- *IEEE Transactions on Computers (TOC)* 2010
- *Journal of Security and Communication Networks (SCN)* 2008
- *IEEE Communications Letters (CL)* 2007, 2009
- *IEEE Transactions on Wireless Communications (TWC)* 2007
- *Pervasive and Mobile Computing (PMC)* 2007
- *IEEE Transactions on Software Engineering (TSE)* 2007, 2008
- *Journal of Wireless Networks (WiNet)* 2006, 2007, 2008, 2009
- *Journal of Wireless Communications and Mobile Computing* 2006
- *ACM Computing Surveys (ACMCS)* 2006
- *Information Processing Letters (IPL)* 2006
- *IEEE Transactions on Very Large Scale Integration Systems (TVLSIS)* 2006

Conferences and Workshops

- *ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2011
- *ACM Conference on Computer and Communications Security (CCS)*, 2008, 2011
- *IEEE Symposium on Security and Privacy (OAKLAND)* 2007, 2008
- *Computer Security Foundations (CSF)*, 2011
- *IFIP Conference on Data and Applications Security (DBSec)* 2008
- *Financial Cryptography (FC)* 2007, 2008
- *International Conference on VLSI Design (VLSI)* 2007
- *Annual Computer Security Applications Conference (ACSAC)* 2005, 2006, 2007
- *USENIX Workshop on Hot Topics in Security (HotSec)* 2007
- *International Conference on Information Systems Security (ICISS)* 2007
- *IEEE International Conference on Computer Engineering & Systems (ICCES)* 2007
- *International Workshop on Security (IWSec)* 2006, 2007
- *USENIX Security Symposium (SECURITY)* 2006, 2007
- *IEEE Sarnoff Symposium (SARNOFF)* 2007
- *International Conference on New Technologies, Mobility and Security (NTMS)* 2007
- *IEEE Infocom (INFOCOM)* 2007
- *Network and Distributed System Security Symposium (NDSS)* 2007
- *International Workshop on Storage Security and Survivability (IWSSS)* 2006
- *ACM Conference on Computer and Communications Security (CCS)* 2006

- *IEEE GLOBECOM (GLOBECOM)* 2006
- *International Conference on Mobile and Ubiquitous Systems: Networks and Services (MOBIQUITOUS)* 2006
- *IFIP Conference on Data and Applications Security (DBSec)* 2006
- *Emerging Trends in Information and Communications Security (ETRICS)* 2006
- *International Conference on Applied Cryptography and Network Security (ACNS)* 2006
- *ACM Symposium on Access Control Models and Technology (SACMAT)* 2006
- *IEEE Conference on Communication Systems Software & Middleware (COMSWARE)* 2006
- *International Conference on Cryptology in India (IndoCrypt)* 2005
- *IEEE Symposium on New Frontiers in Dynamic Spectrum Access (DySPAN)* 2005
- *European Symposium on Research in Computer Security (ESORICS)* 2005

F. Expert Witness Services

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

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

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

14. *William Grecia v. Apple Inc. et al:* Expert Consultant for the Defendant for Invalidity (via Kirkland & Ellis LLP). Verdict: Closed in initial pleadings, dismissed with prejudice. *July 2014 - August 2014.*

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

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

17. *Intellectual Ventures LLC vs. Check Point; et al.:* Expert Consultant for the Plantiff for Infringement (via Susman Godfrey LLP), Verdict: Infringement on 2 of 4 patents. *October 2012 - February 2015.*

V. OTHER CONTRIBUTIONS

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

1. Keynote: Well, It Worked on My Computer: Reproducibility, 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.

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

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

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

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

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

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

23. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. KAIST Information Security Seminar - Korean Advanced Institute of Science and Technology, June 2016. Daejeon, South Korea.

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

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

26. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Illinois Science of Security (SoS) Lablet Speaker Series - University of Illinois, Urbana-Champaign, April 2016. Urbana-Champaign, Illinois.

27. New Trends in Cybersecurity:Vulnerabilities in Branchless Banking Systems. United States Departments of State and Justice - Cybersecurity and Cybercrime Workshop for Lusophone Africa, September 2015. Maputo, Mozambique.

28. New Trends in Cybersecurity:Vulnerabilities in Branchless Banking Systems. United States Departments of State and Justice - ECCAS Cybersecurity and Cybercrime Workshop, August 2015. Kinshasa, Democratic Republic of Congo.

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

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

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

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

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

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

35. The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers. Invited Talk: Centre for Secure Information Technologies (CSIT) Queen's University, March 2013. Belfast, Northern Ireland.

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

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

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

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

40. Chasing Telephony Security: Where the Wild Things... Are? University of Washington Department of Electrical Engineering, Network Security Lab (NSL): Invited Talk, November 2012. Seattle, WA.

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

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

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

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

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

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

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

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

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

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

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

52. Privacy and Security Concerns for Personal and Mobile Health Devices. Invited Talk: Workshop to Set A Research Agenda for Privacy and Security of Healthcare Technologies, October 2009. Indianapolis, IN.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

B. Special Activities

Presentations to Lay Media

1. How technology can fight digital fakery. The Babbage Podcast/The Economist https://shows.acast.com/theeconomistbabbage/episodes/babbage-how-to-detect-a-deepfake, January 2023.
2. Deepfake audio has a tell and researchers can spot it. Ars Technica https://arstechnica.com/information-technology/2022/09/researchers-use-fluid-dynamics-to-spot-deepfake-voices/, September 2022.
3. This security tool could help stop the problem of ransomware in its tracks. TheJournal.ie https://www.thejournal.ie/ransomware-researchers-stop-2875032-Jul2016/, July 2016.
4. Researchers Unleash Ransomware Annihilation. BankInfoSecurity - http://www.bankinfosecurity.com/researchers-unleash-ransomware-annihilation-a-9255, July 2016.
5. CryptoDrop Stops Ransomware by Stopping its Encryption. Security Intelligence - https://securityintelligence.com/news/cryptodrop-stops-ransomware-by-stopping-its-encryption/?utm_source=tfeed&utm_medium=twitter, July 2016.
6. Ransomware 'stopped' by new software. BBC - http://www.bbc.com/news/technology-36772461, July 2016.
7. Researchers create effective anti-ransomware solution. Help Net Security - https://www.helpnetsecurity.com/2016/07/12/anti-ransomware-solution/, July 2016.
8. Florida U boffins think they've defeated all ransomware. http://www.theregister.co.uk/2016/07/12/ransomware_defeated/, July 2016.
9. This Anti-Ransomware Tool Could Save You Hundreds of Pounds. Huffington Post - http://www.huffingtonpost.co.uk/entry/anti-ransomware-tool-save-hundreds-pounds_uk_57838beee4b0935d4b4b30ba, July 2016.
10. Researchers develop method to stop 100% of ransomware before it encrypts all files. Myce - http://www.myce.com/news/researchers-develop-method-stop-100-ransomware-encrypts-files-79873/, July 2016.
11. Desarrollan una solución para detener el ransomware. ComputerHoy - http://computerhoy.com/noticias/software/desarrollan-solucion-detener-ransomware-47972, July 2016.
12. Why your antivirus software can't stop ransomware. Futurity - http://www.futurity.org/ransomware-computer-files-1198242-2/, July 2016.
13. CryptoDrop Gives Users Hope to Prevent Ransomware Infections in the Future. Softpedia - http://news.softpedia.com/news/cryptodrop-gives-users-hope-to-prevent-ransomware-infections-in-the-future-506187.shtml, July 2016.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

57. Dennis Carter. Questions abound as emergency alert flops Virginia Tech's text-message alert system failed when the sound of gunfire was heard on campus; officials scramble to understand why. eSchool News - http://www.eschoolnews.com/iphone/top-story/index.cfm?i=56122#_56122, November 2008.

58. Jessica Bauer. Study: Text alerts may fail in real emergency. Diamondback Online - http://media.www.diamondbackonline.com/media/storage/paper873/news/2008/10/14/News/Study.Text.Alerts.May.Fail.In.Real.Emergency-3485509.shtml, October 2008.

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

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

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

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

63. 3G Americas. 3G Americas Highlights New Research Report on Use of Cellular Text Messaging for Emergency Alert Services. 3G Americas http://www.3gamericas.org/English/news_room/DisplayPressRelease.cfm?id=3400&s=ENG, 2008.

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

65. Christopher Beam. How Do You Intercept a Text Message? Turn your cell phone into a spy gadget. Slate Magazine http://www.slate.com/id/2161402/, 2007.

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

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

68. John Schwartz. Text Hackers Could Jam Cellphones, a Paper Says. The New York Times http://www.nytimes.com/2005/10/05/technology/05phone.html?ex=1286164800&en=d917b9cd43dfaa31&ei=5090&partner=rssuserland&emc=rss, 2005.