

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Gregory G. Raleigh, et al.
U.S. Patent No.: 11,405,224 Attorney Docket No.: 39843-0163IP1
Issue Date: August 2, 2022
Appl. Serial No.: 16/993,012
Filing Date: August 13, 2020
Title: DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK
CAPACITY

DECLARATION OF DR. PATRICK TRAYNOR

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

QUALIFICATIONS AND BACKGROUND INFORMATION

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

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

3. I am currently a Professor in the Department of Computer and Information Science and Engineering (CISE) at the University of Florida. I was

hired under the “Rise to Preeminence” Hiring Campaign and serve as the Associate Chair for Research in my Department. I also hold the endowed position of the John and Mary Lou Dasburg Preeminent Chair in Engineering.

4. Prior to joining the University of Florida, I was an Associate Professor from March to August 2014 and an Assistant Professor of Computer Science from 2008 to March 2014 at the Georgia Institute of Technology. I have supervised many Ph.D., M.S., and undergraduate students during the course of my career.

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

6. I have received numerous awards for research and teaching, including being named a Kavli Fellow (2017), a Fellow of the Center for Financial Inclusion (2016), and a Research Fellow of the Alfred P. Sloan Foundation (2014). I also won the Lockheed Inspirational Young Faculty Award (2012), was awarded a National Science Foundation (NSF) CAREER Award (2010), and received the

Center for Enhancement of Teaching and Learning at Georgia Tech’s “Thanks for Being a Great Teacher” Award (2009, 2012, 2013).

7. I have published over 100 articles in top conferences and journals in the areas of information security, mobile systems, and networking. Many of my results are highly cited, and I have received multiple “Best Paper” Awards. I have also written a book entitled “Security for Telecommunications Networks”, which is used in wireless and cellular security courses at a number of top universities.

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

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

10. I was a co-Founder and Research Fellow for a private start-up, Pindrop Security, from 2012 to 2014. Pindrop provides anti-fraud and authentication solutions for Caller-ID spoofing attacks in enterprise call centers by creating and matching acoustic fingerprints. Pindrop Security currently employs

over 200 people, and their technology is based off of my research (US Patent 9,037,113 B2).

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

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

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

14. My curriculum vitae, included with this declaration as SAMSUNG-1003, includes a list of publications on which I am a named author. It contains

further details regarding my experience, education, publications, and other qualifications to render an expert opinion in connection with this proceeding.

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

16. U.S. Patent No 11,405,224 (SAMSUNG-1001), and its accompanying prosecution history (SAMSUNG-1002)

- U.S. Patent Publication No. 2008/0080458 A1 (“Cole”) (SAMSUNG-1005)
- U.S. Patent Publication No. 2009/0119773 A1 (“D’Amore”) (SAMSUNG-1006)
- U.S. Patent Publication No. 2006/0039354 A1 (“Rao”) (SAMSUNG-1007)
- U.S. Patent No. 5,987,611 (“Freund”) (SAMSUNG-1008)
- U.S. Patent Publication No. 2005/0037740 A1 (“Smith”) (SAMSUNG-1009)
- European Patent Publication No. 1 484 871 A1 (“Kelz”) (SAMSUNG-1010)
- U.S. Patent No. US 2008/0057894 A1 (“Aleksic”) (SAMSUNG-1011)
- U.S. Patent No. 7,924,730 B1 (“McAllister”) (SAMSUNG-1012)
- U.S. Patent No. 6,947,723 B1 (“Gurnani”) (SAMSUNG-1014)

LEGAL PRINCIPLES

Anticipation

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

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

Obviousness

19. I have been informed that a patent claim is invalid as "obvious" under 35 U.S.C. § 103 in light of one or more prior art references if it would have been

obvious to a POSITA, taking into account (1) the scope and content of the prior art, (2) the differences between the prior art and the claims, (3) the level of ordinary skill in the art, and (4) any so called “secondary considerations” of non-obviousness, which include: (i) “long felt need” for the claimed invention, (ii) commercial success attributable to the claimed invention, (iii) unexpected results of the claimed invention, and (iv) “copying” of the claimed invention by others. For purposes of my analysis above and because I know of no indication from the patent owner or others to the contrary, I have applied a date of January 28, 2009, as the date of invention in my obviousness analyses, although in many cases the same analysis would hold true even at an earlier time than January 28, 2009.

20. I have been informed that a claim can be obvious in light of a single prior art reference or multiple prior art references. To be obvious in light of a single prior art reference or multiple prior art references, there must be a reason to modify the single prior art reference, or combine two or more references, in order to achieve the claimed invention. This reason may come from a teaching, suggestion, or motivation to combine, or may come from the reference or references themselves, the knowledge or “common sense” of one skilled in the art, or from the nature of the problem to be solved, and may be explicit or implicit from the prior art as a whole. I have been informed that the combination of familiar elements according to known methods is likely to be obvious when it does

no more than yield predictable results. I also understand it is improper to rely on hindsight in making the obviousness determination.

OVERVIEW OF CONCLUSIONS FORMED

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

- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 1-11 and 16-17 of the '224 patent are obvious over Cole in view of D'Amore and Rao.
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 13-15 of the '224 patent are obvious over Cole in view of D'Amore, Rao, and Freund.
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claim 12 of the '224 patent is obvious over Cole in view of D'Amore, Rao, Aleksic.

BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE '224 PATENT

22. Based on the foregoing and upon my experience in this area, a person of ordinary skill in the art ("POSITA") relating to the subject matter of the '224 Patent as of January 28, 2009 would have had (1) at least a bachelor's degree in computer science, electrical engineering, or a related field, and (2) three to five years of experience with networking, power consumption of networked computing

devices, and/or wireless digital communications systems. Additional graduate education could substitute for professional experience, and *vice versa*. *Id.*

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

INTERPRETATIONS OF THE '224 PATENT CLAIMS AT ISSUE

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 January 28, 2009 as the point in time for claim interpretation purposes.

OVERVIEW OF THE '224 PATENT

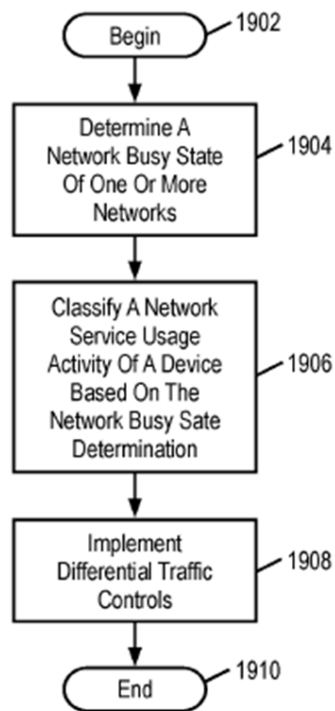
I. The '224 Patent

25. The '224 Patent is directed to “a Device Assisted Services (DAS) for protecting network capacity.” SAMSUNG-1001, Abstract. This includes “classifying” network activities “for differential network access control” with “priority levels” and determining respective “network service usage control polic[ies].” SAMSUNG-1001, Abstract, 77:23-49. The '224 Patent describes that these “priority levels” can be “based on one or more criteria/measures,” to include “network busy state, current access network, time based criteria, an associated service plan, and/or other criteria/measures.” SAMSUNG-1001, 77:23-49.

26. The '224 Patent describes “network capacity controlled service[s]” as being “selected for differential network service usage control for protecting network capacity.” SAMSUNG-1001, 14:17-36. Additionally, the '224 Patent explains that a “network capacity controlled services classification” includes “one or more network services associated with a network capacity controlled service/class priority setting for differential network service usage control for protecting network capacity.” SAMSUNG-1001, 14:17-36.

27. An example process for “implementing differential traffic controls” is shown below in FIG. 19 of the '224 Patent. SAMSUNG-1001; 72:34-67, 73:1-20. As illustrated below in step 1906, the process includes “classifying a network

service usage activity ... to facilitate differential network access control for protecting network capacity.” SAMSUNG-1001, 72:40-44. The process continues in step 1908 by “implementing differential traffic controls” which are “based on the service usage activity classification for protecting network capacity.” SAMSUNG-1001, 72:64-66.



A flowchart for
“device assisted
services (DAS) for
protecting network
capacity” according
to the ‘224 patent

SAMSUNG-1001, FIG. 19.¹

II. Prosecution History

28. The ‘224 Patent was allowed after one Office Action, in which only claim 1 was rejected under 35 U.S.C. § 102 as being anticipated by Morgensen

¹ Annotations to the figures throughout this Petition are shown in color.

(U.S. Patent Pub. No. 2004/0268351 A1). SAMSUNG-1002, 95-99. Following this Office Action, claim 1 was amended and claims 2-17 were added. SAMSUNG-1002, 87-94. Allowance was then received for all claims. SAMSUNG-1002, 27-33. During prosecution, the Examiner did not consider any of Cole, D'Amore, Rao, Freund, and Aleksic. These references render the Challenged Claims obvious, as discussed below.

ANALYSIS OF COLE, D'AMORE, AND RAO

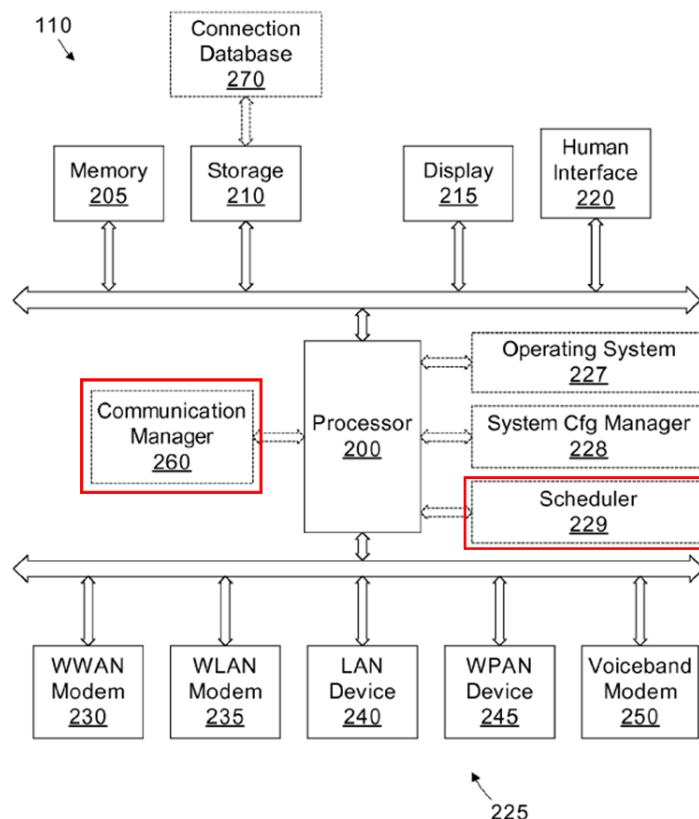
I. Overview of Cole²

29. Cole describes “[a] method for configuring a mobile device including a plurality of communication interfaces” including a “first communication interface” and multiple “second ... communication interfaces” that are “selected for establishing a second connection to a remote network.” SAMSUNG-1005, Abstract, ¶[0014]. Cole uses a “connection manager 260,”³ annotated below in Cole’s Figure 2, to select “communication interfaces” for connecting to remote

² Descriptions of the references and combinations in Section III are incorporated into each mapping that includes citations to these references. Emphasis is added to text using bold and/or italicized font unless otherwise indicated.

³ Cole also refers to the “connection manager 260” as the “communication manager 260.” SAMSUNG-1005, ¶[0088], FIG. 2.

networks (e.g., a wireless local area network (WLAN), a wireless wide area network (WWAN), and a wireless personal area network (WPAN)). SAMSUNG-1005, ¶¶[0015], [0003], [0031], [0035], [0036], FIGS. 1, 2. The connection manager can also “schedule various events” using a “scheduler” (also annotated) to “effectively use available bandwidth.” SAMSUNG-1005, ¶¶[0074], [0036], [0118], [0119]. This includes taking action when “monitored loads” exceed a “predetermined threshold.” SAMSUNG-1005, ¶[0075], [0077].



SAMSUNG-1005, FIG. 2.

30. Cole’s “connection manger” manages communication interfaces to “determine which connections should be active at any given time.” SAMSUNG-

1005, ¶[0036]. This determination includes monitoring various network connectivity metrics, such as, battery power, connection bandwidth, communication capabilities, connection availability, user preferences, application requirements, and mobile device resources. SAMSUNG-1005, ¶¶[0036], [0080]. For instance, in some cases, the connection manager may establish a connection with a communication interface based on application requirements. SAMSUNG-1005, ¶[0069]. To assist in evaluating communication interfaces, the connection manager “maintains data related to each of the communication interfaces,” to include “connection name, connection technology type, a location (LOC), a configuration flag (CFG), a bandwidth (BW), a connection time (CT), a user interaction required (UI) flag, a fast connect availability flag (FC), a power characteristics (PC), thermal characteristics (TC), a vendor name, a technical support contact (TSC) information, an ignore flag,” and more. SAMSUNG-1005, ¶[0037]. Cole describes that these above parameters may be “based on historical data ... user specified parameters, or static parameters,” and may also be “monitored” by the connection manager. SAMSUNG-1005, ¶[0038].

31. Cole describes that, when “the monitored load exceeds a predetermined threshold (e.g., 85% of capacity), the connection manager 260 may take one of several actions to manage the load.” SAMSUNG-1005, ¶[0075]. For example, Cole describes that applications can be “aborted,” “postpone[d],”

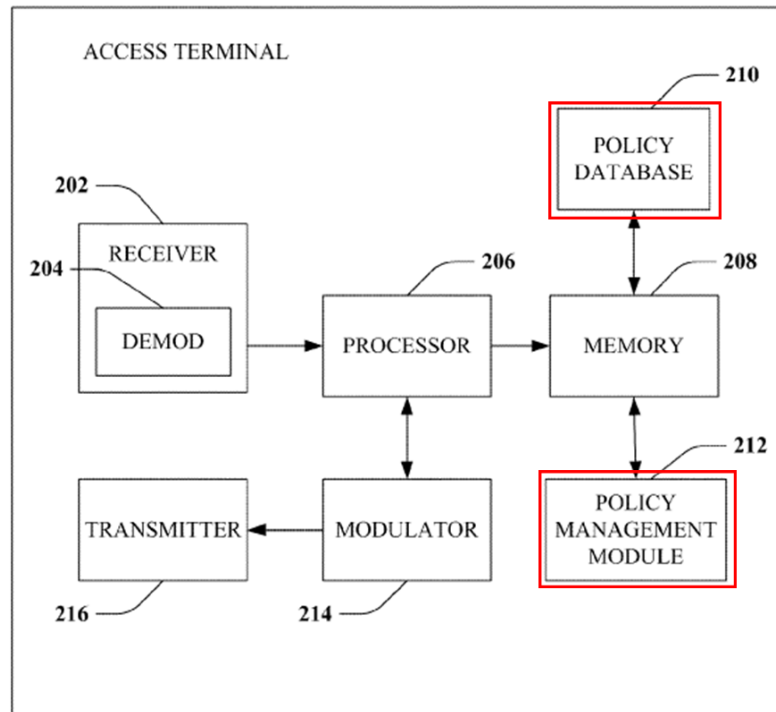
cancelled and rescheduled, and “block[ed].” SAMSUNG-1005, ¶[0080], ¶¶[0085]-[0090], ¶[0125]. Cole additionally describes that these above actions can be taken in response to mobile device states, including “power state.” SAMSUNG-1005, ¶¶[0090]-[0098]. “By monitoring the load on an active connection, the connection manager 260 tries to proactively prevent increased latency from an overloaded connection from impacting the performance of the running applications or the efficiency of the user.” SAMSUNG-1005, ¶[0075].

II. Overview of D’Amore

32. D’Amore describes “management and arbitration of dedicated mobile communication resources for mobile applications.” SAMSUNG-1006, Abstract. This management is accomplished through a “priority level that establishes an importance with respect to one or more other mobile applications and at least one mobile resource.” SAMSUNG-1006, Abstract. D’Amore explains that, “[if] competing applications attempt to access the mobile resource concurrently, access can be provided to an application having higher priority level” and that “control of a resource can be taken away from an application having lower priority in order to affect control of such resource for a higher priority application.” SAMSUNG-1006, Abstract.

33. D’Amore’s FIG. 2 (reproduced below) depicts an example of an access terminal, which is also referred to as a “mobile station, mobile, mobile

device, [or] cellular device.” SAMSUNG-1006, ¶¶[0049], [0019]. D’Amore’s access terminal includes a policy database 210 and a policy management module 212 (outlined in red in D’Amore’s FIG. 2 below). SAMSUNG-1006, ¶[0050].



SAMSUNG-1006, FIG. 2.

34. D’Amore’s policy database 210 “associates a privilege code or a priority level, or both, with at least one mobile application.” SAMSUNG-1006, ¶[0050]. This priority level “establishes a relative order of importance for the mobile application with respect to other mobile applications” for “managing and prioritizing access to network/device resources.” SAMSUNG-1006, ¶[0050].

35. D’Amore’s policy management module 212 can “approve or deny access to a mobile device resource and/or mobile network resource for a mobile

application” “based at least in part on a priority level or a privilege code associated with the mobile application.” SAMSUNG-1006, ¶[0050]. The policy management module 212 also includes “a configuration module” that allows “customization of privilege code or priority level information for one or more mobile applications” by a “user.” SAMSUNG-1006, ¶[0063].

III. Combination of Cole and D’Amore

36. It would have been obvious to a POSITA to combine the teachings of Cole and D’Amore such that D’Amore’s policies (e.g. policies stored in policy database 210, policy management module 212) would have been incorporated into the decision making of Cole’s connection manager. *See above Section I, II.* A POSITA would have combined Cole and D’Amore to further improve the management of applications in devices such as Cole’s mobile device.

37. D’Amore’s application level “priority policies” would add additional granularity to the decisions of Cole’s connection manager, such that the connection manager has a more accurate understanding of the activity/application priority when making deferral or rescheduling decisions. SAMSUNG-1005, ¶¶[0074]-[0097]; SAMSUNG-1006, ¶¶[0050], [0051]. Additionally, D’Amore’s “privilege codes” would have been used in the Cole mobile device to prevent unauthorized resource access, increasing user privacy protection and offering increased control

of sensitive mobile device information and resources. SAMSUNG-1006, ¶¶[0006], [0049]-[0051].

38. Incorporating D’Amore’s application level priorities would also allow conflict-resolution in the event Cole’s connection manager was faced with conflicting priorities, for example, determining which application should be afforded a rescheduled time slot during a time of limited connectivity. SAMSUNG-1005, ¶¶[0118]-[0127]; SAMSUNG-1006, ¶¶[0050], [0051]. Also, the increased ability to manage application priority and mobile device resources provided by D’Amore would have enabled Cole’s mobile device to host additional and more complex applications without fear of conflict. SAMSUNG-1006, ¶[0003]-[0004]. For example, the ability of D’Amore’s “service provider” to initially set priority levels for applications would enable greater provider control of mobile device resources across many such mobile devices, while simultaneously reducing requirements for user interaction to specify priorities for each one of many applications executing on their mobile device. SAMSUNG-1006, ¶¶[0050]-[0051], [0070]

39. As explained below in more detail, combining Cole and D’Amore would have been obvious at least because such a combination would have merely involved (1) combining prior art elements according to known methods to yield predictable results; and the (2) use of known technique to improve similar devices

in the same way. Indeed, Cole already describes utilizing certain policies to control the execution of applications and the combination of D'Amore's teachings would simply involve adding D'Amore's known policies to Cole's similar system, thus, for at least this reason, making the Cole-D'Amore combination predictable and foreseeable with a reasonable expectation of success. SAMSUNG-1005, ¶[0074]-[0075]. Moreover, because Cole's connection manager "proactively prevent[s] increased latency from an overloaded connection from impacting the performance of the running applications," a similar design objective to D'Amore, the use of D'Amore's policies in Cole would have improved a similar device in the same way. SAMSUNG-1005, ¶[0074]; SAMSUNG-1006, ¶[0032] ("systematically multiplex and distribute mobile device and/or network resources").

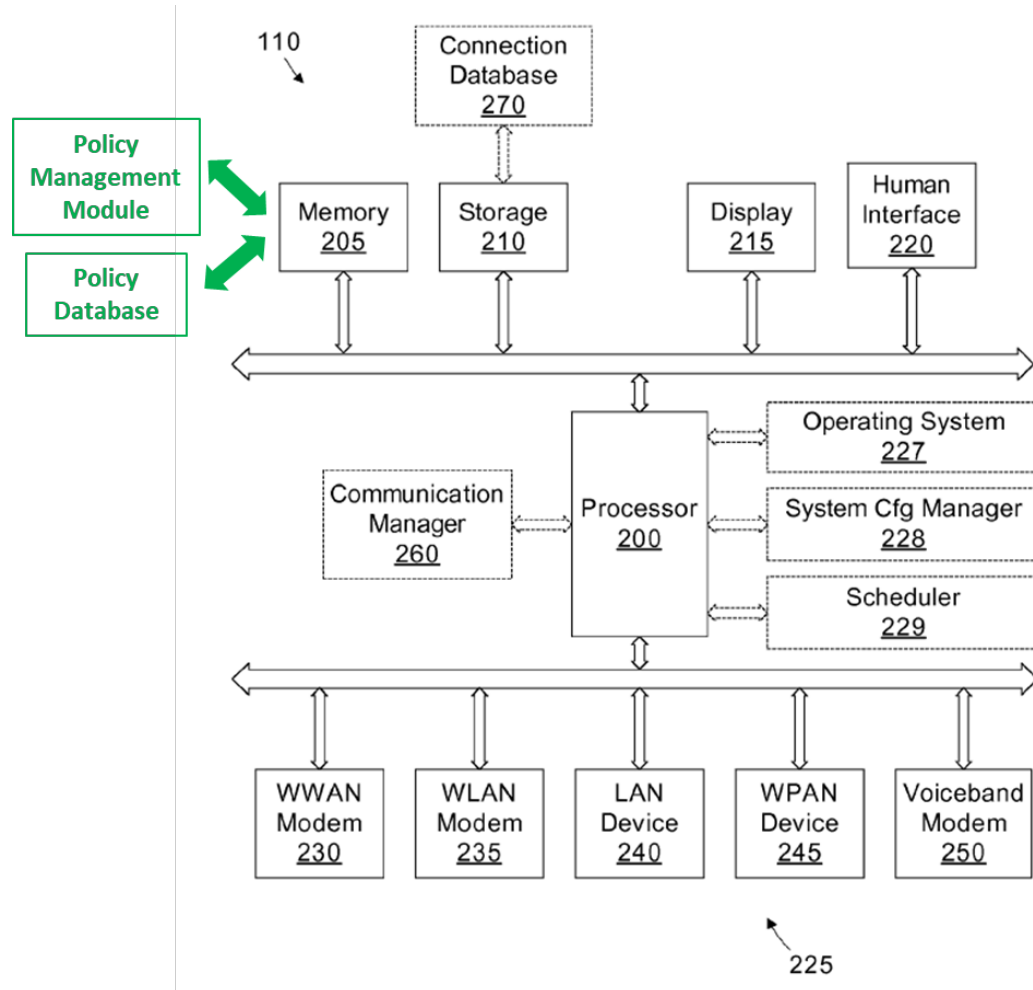
40. Incorporating D'Amore's policies (e.g. policies stored in policy database 210, policy management module 212) into Cole's communication manager would also have been predictable and foreseeable with a reasonable expectation of success because D'Amore's policies describe similar actions as those taken by Cole's connection manager in response to undesirable application activities. SAMSUNG-1005, ¶¶[0074]-[0097]; SAMSUNG-1006, ¶¶[0060]-[0061]. For example, D'Amore describes an "access termination module" that can "remove access to a system resource." SAMSUNG-1006, ¶[0060]. Similarly, Cole's connection manager "determines if one or more actions that are consuming

bandwidth should be postponed.” SAMSUNG-1005, ¶[0085], *see also* ¶¶[0074]-[0097]. A POSITA would have recognized or found obvious that the postponement of an action by Cole’s connection manager would also have involved removing access to device resources for an application, like in D’Amore. Indeed, to alleviate busy state issues the network resources allocated to deferred or rescheduled applications and activities would need to be recovered. SAMSUNG-1005, ¶[0085], ¶¶[0074]-[0097]. Additionally, both Cole and D’Amore implement their techniques in end-user devices (“mobile devices”). SAMSUNG-1005, ¶¶[0014]-[0015], SAMSUNG-1006, ¶¶[0007]-[0016]. Finally, the incorporation of D’Amore’s policies would have been nothing more than the implementation of software in a system already designed to execute similar program modules (for example, the “connection manager 260,” “scheduler 229,” and “and “policy management module 212”) and implement priority rules. SAMSUNG-1005, ¶¶[0033]-[0036], [0074]; SAMSUNG-1006, ¶¶[0032], [0049], [0052]. The decision to implement D’Amore’s policies in Cole would have been an obvious design choice as a POSITA would have naturally experimented with known policies within the capability of Cole’s processing capability, such as those described in D’Amore.

41. In the combined Cole-D’Amore system, illustrated below in Cole’s Figure 2, D’Amore’s policies (e.g. policies stored in policy database 210, policy

management module 212) would have been incorporated into Cole's memory 205, storage 210, and/or connection database 270), such that they could be referenced by the communication manager 260 when making deferral and rescheduling decisions. SAMSUNG-1005, ¶¶[0034]-[0036], ¶¶[0074]-[0097], FIG. 2; SAMSUNG-1006, ¶¶[0049]-[0060], FIG. 2. In the combined system, application activities would have been assigned a priority level or code based on their associated application (e.g., "classified"), as taught by D'Amore, and Cole's connection manager 260 would leverage this additional granularity when determining which application activities should be deferred. SAMSUNG-1005, ¶¶[0034]-[0036], ¶¶[0074]-[0097], FIG. 2; SAMSUNG-1006, ¶¶[0049]-[0060], FIG. 2. Moreover, Cole's scheduler evaluates many device states and parameters when scheduling application tasks. SAMSUNG-1005, ¶¶[0119]-[0126]. Therefore, D'Amore's priority policies would assist Cole's connection manager 260 in utilizing the scheduler to effectively schedule application tasks and improve the ability of the mobile device to use available network bandwidth (e.g., by reducing the number of high-priority tasks that are spuriously rescheduled, thus forcing the user to override the scheduler and execute the task). SAMSUNG-1005, ¶¶[0119]-[0126]; SAMSUNG-1006, ¶¶[0059]-[0061]. In doing so, the Cole-D'Amore device would improve network utilization efficiency by preferentially scheduling higher priority application activities during times of network availability (one of

the main objectives of Cole). SAMSUNG-1005, ¶¶[0006]-[0011], ¶¶[0074]-[0075].



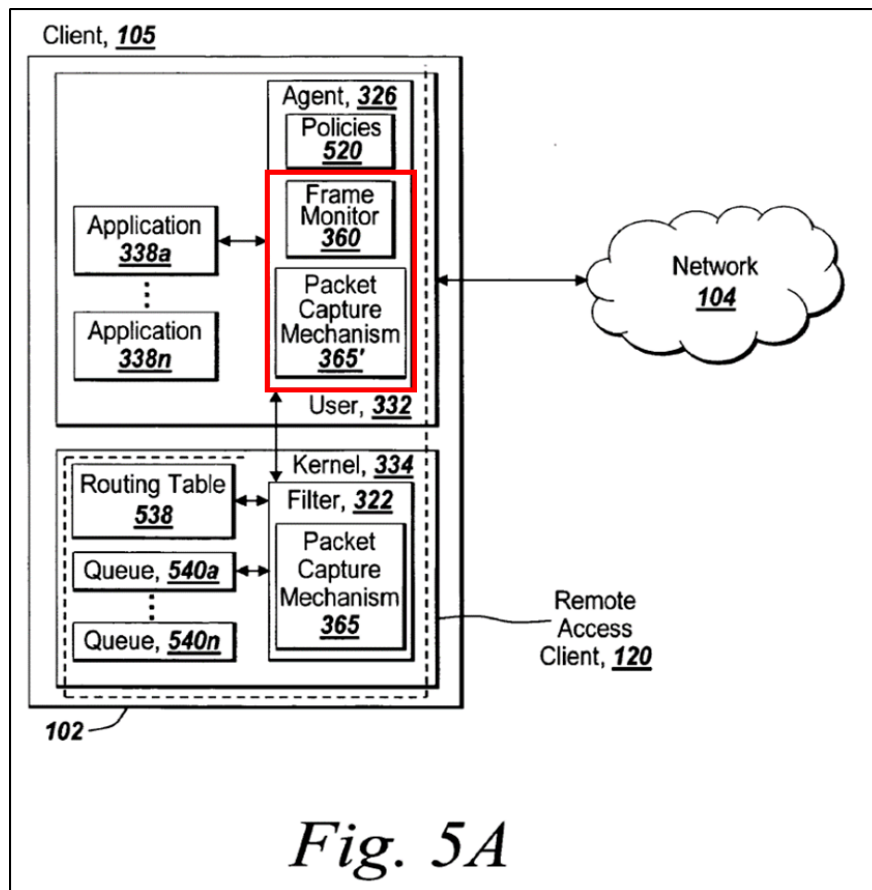
SAMSUNG-1006, FIG. 2.

IV. Overview of Rao

42. Rao discloses performing “intelligent and client centric prioritization of application network communications on a client based on the type and/or priority of an application.” SAMSUNG-1007, ¶[0179], FIG. 5A. Rao’s method can be used to prioritize “data communications” of some applications over others

(e.g., “real-time data communications” over data communications from “non-real-time data communication applications”), and can be used to “compliment Quality of Service (QOS) networks where network traffic prioritization occurs in intermediary network devices, such as switches and routers.” *Id.*, ¶[0184]. In order to effectuate this prioritization, Rao describes the use of a “packet capture mechanism” that “inspects” the network packets of applications and a “frame monitor” that “identifies an application ... that generated the packet.” SAMSUNG-1007, ¶¶[0109], [0158]-[0159], [0176], [0180], [0185], [0191], FIG. 5A.

43. As shown in Rao’s FIG. 5A below, Rao discloses that a “remote access client 105 of computing device 102 is connected to network 104” through one or more “LAN or WAN links” and/or “wireless connections.” SAMSUNG-1007, ¶[0179]. Further, “[t]he client 105 may execute one or more applications 338a-338n, which access the network 104 via the agent 326 and filter 322 of the remote access client 120.” SAMSUNG-1007, ¶[0179]. As examples, Rao’s applications can communicate with one or more servers on the network 104, such as “an application server providing email services such as Microsoft Exchange,” “a web or Internet server,” “a desktop sharing server,” or “a collaboration server.” SAMSUNG-1007, ¶[0090].



SAMSUNG-1007, FIG. 5A.

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

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

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

V. Combination of Cole-D’Amore and Rao

46. It would have been obvious to a POSITA to modify the Cole-D’Amore system based on the teachings of Rao such that Rao’s packet assessment and prioritization techniques (e.g., packet capture mechanism 365, frame monitor 360, and additional prioritization techniques) would have been incorporated in the Cole-D’Amore mobile device. SAMSUNG-1005, ¶¶[0074]-[0097], FIG. 2; SAMSUNG-1007, ¶¶[0158]-[0159], [0176], [0180], [0185], [0191], FIG. 5A. A

POSITA would have been motivated to update the Cole-D'Amore mobile device based on the teachings of Rao for the following reasons.

47. Incorporating the functionality of Rao's frame monitor 360 into the connection manager of Cole-D'Amore would beneficially provide Cole-D'Amore's system with an additional capability to identify application traffic at the packet level, allowing for inter-application classification of activities based on protocol. SAMSUNG-1007, ¶¶[0109], [0179]-[0184].

48. A POSITA would have recognized that Rao describes prioritization techniques (e.g., "whether an application is running in the foreground or the background") that would enhance the priority policies of the Cole-D'Amore device, allowing the connection manager to consider the impact (e.g., deferring an active browsing session or a call in progress) to the mobile device user. SAMSUNG-1006, ¶¶[0059]-[0061]; SAMSUNG-1007, ¶¶[0109], [0179]-[0184], FIG. 5A.

49. As explained below, combining Cole-D'Amore and Rao would have involved (1) combining prior art elements according to known methods to yield predictable results; and (2) using known technique to improve similar devices in the same way. Indeed, Cole describes policy decisions similar to Rao (the "actions" of the connection manager 260 to defer or reschedule activities) and the incorporation of the known prioritization methods of Rao into Cole would have yielded predictable results. SAMSUNG-1005, ¶¶[0074]-[0075]; SAMSUNG-1007,

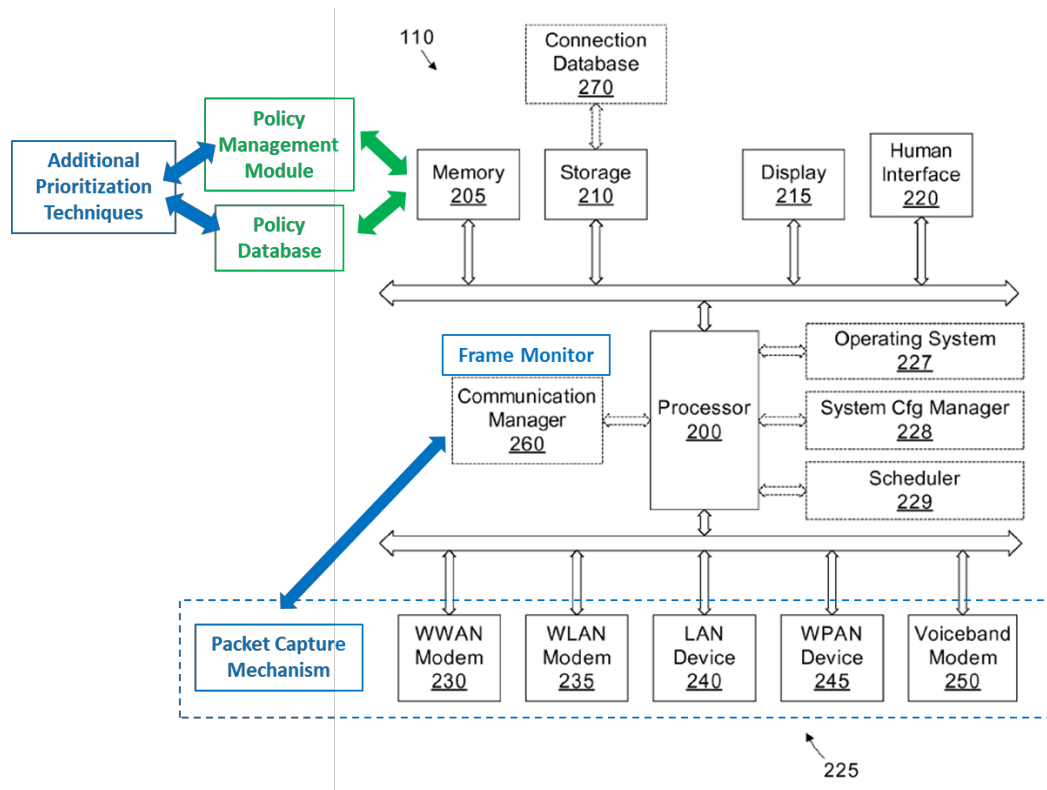
¶[0040] (“preventing” and “holding” activity traffic). Moreover, because Cole’s connection manager “proactively prevent[s] increased latency from an overloaded connection from impacting the performance of the running applications,” a similar design objective to Rao, the use of Rao’s prioritization techniques in Cole would have been improving a similar device in the same way. SAMSUNG-1005, ¶[0074]; SAMSUNG-1007, ¶[0179] (“prioritization of application network communications on a client based on the type and/or priority of an application”).

50. Incorporating Rao’s packet assessment and prioritization techniques (e.g., packet capture mechanism, frame monitor, and additional prioritization techniques) into the Cole-D’Amore device would have been predictable and foreseeable with a reasonable expectation of success because Rao also describes “optimizing ... communications” on mobile devices that “run one or more applications 338 that access a network” (“effectively use the available bandwidth”). SAMSUNG-1005, ¶¶[0074]-[0097], [0104]; SAMSUNG-1007, ¶¶[0075], [0088], [0133], [0179]-[0184]. Moreover, like Cole and D’Amore, Rao describes that its techniques can be implemented in end-user devices (“mobile telephones”). SAMSUNG-1005, ¶¶[0014]-[0015], SAMSUNG-1006, ¶¶[0007]-[0016]; SAMSUNG-1007, ¶[0130]. Additionally, the use of computer program modules to monitor and identify application packet flow on mobile devices was known as of the Critical Date. Kelz (a European patent application) provides corroboration and

describes a “controller module” that includes a “QoS packet processor,” which can “monitor the packet flow” of applications. SAMSUNG-1010, ¶[0036]. Additionally, the incorporation of Rao’s prioritization techniques would have been nothing more than the implementation of software in a system already designed to execute similar program modules. SAMSUNG-1005, ¶¶[0033]-[0036], [0074]; SAMSUNG-1007, ¶¶[0092] (a “software set-up”). The decision to implement Rao’s prioritization techniques in Cole would have been an obvious design decision as a POSITA would have naturally experimented with additional known policies within the capability of Cole’s processing capability, such as those described in Rao.”

51. In the combined system, illustrated below in Cole’s Figure 2, Rao’s packet capture mechanism and frame monitor would have been incorporated as program modules in the Cole-D’Amore device, such that they would monitor and identify data packets transmitted from the mobile device. SAMSUNG-1005, ¶¶[0034]-[0036], [0074]-[0097], FIG. 2; SAMSUNG-1006, ¶¶[0049]-[0060], FIG. 2; SAMSUNG-1007, ¶¶[0109], [0158]-[0159], [0176], [0180], [0185], [0191], FIG. 5A. In the combined Cole-D’Amore-Rao system, the packet capture mechanism and frame monitor would have aided the connection manager to classify and associate activities to applications, thus allowing the connection manager to reduce the impact of deferring and rescheduling activities on the mobile device and user.

Id. Additionally, Rao's prioritization techniques would have been used to further enhance the policy management module of the Cole-D'Amore device to allow the connection manager to make more effective prioritization decisions by monitoring additional application characteristics, for example, whether the application is running in the foreground or background. *Id.* In doing so, the Cole-D'Amore-Rao device would have been able to more effectively use available network connections by preferentially scheduling higher priority application tasks during times of network availability (one of the main objectives of Cole). SAMSUNG-1005, ¶¶[0006]-[0011], [0074]-[0075].



SAMSUNG-1005, FIG. 2 (modified based on CDR combination).

VI. Claims 1-11 and 16-17 are rendered obvious by Cole, D’Amore, and Rao

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

52. To the extent the preamble is limiting, the Cole-D’Amore-Rao combination (hereinafter referred to as “**CDR**”) renders [1.pre] obvious. For example, Cole’s communication system 100 includes “a mobile device 110 interfacing with a plurality of communication networks 120, such as a wireless wide area network (WWAN).” SAMSUNG-1005, ¶[0031], FIGS. 1, 2 (reproduced below).

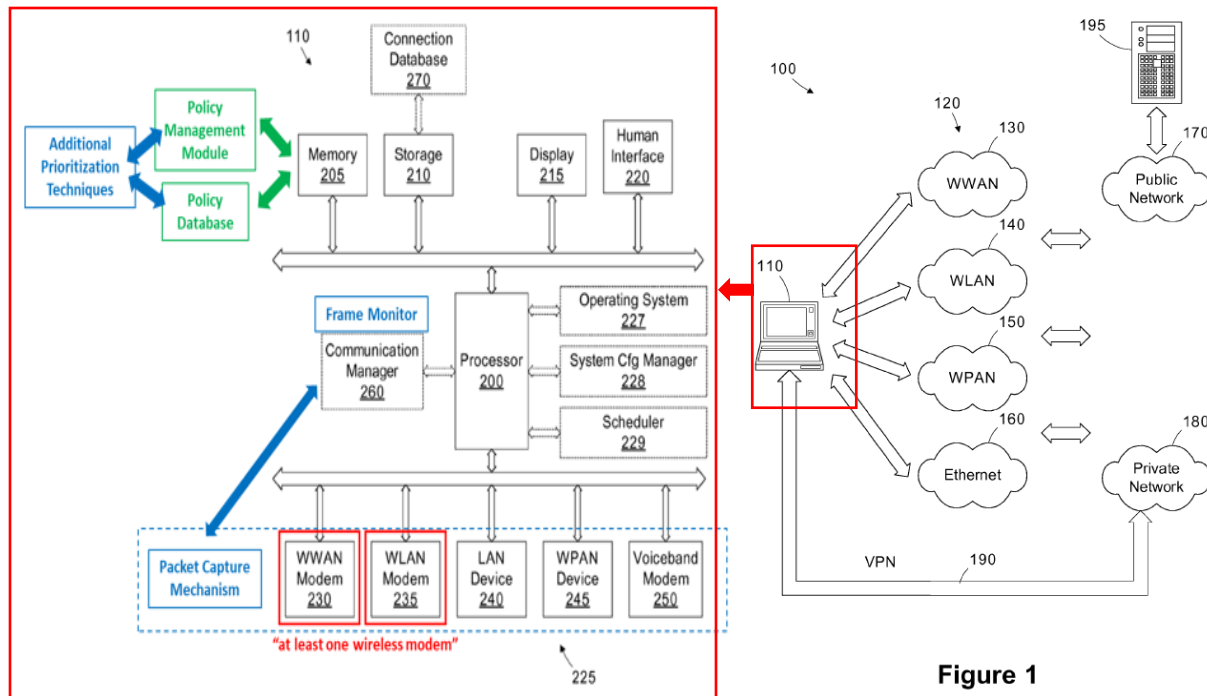


Figure 1

SAMSUNG-1005, FIG. 2 (left, modified based on CDR), FIG. 1 (right).

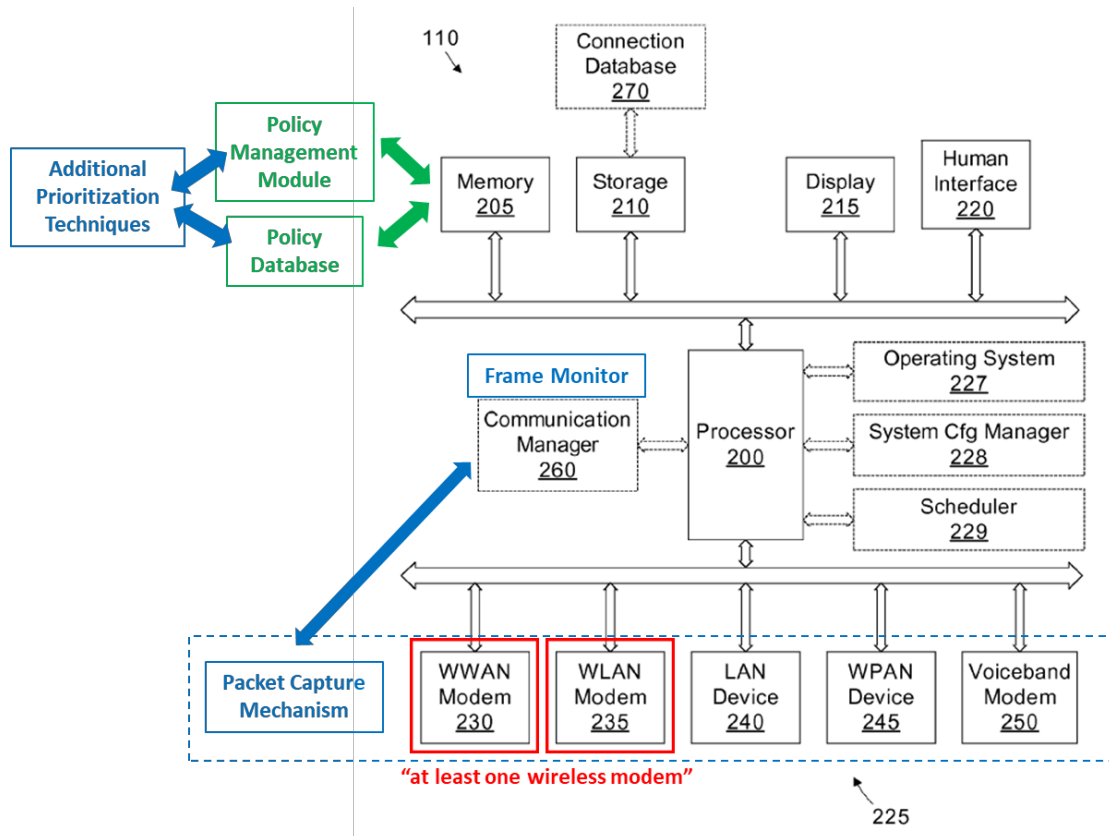
53. The “mobile device 110 may be ... a notebook computer, ... a personal data assistant (PDA), a mobile telephone, etc.” SAMSUNG-1005, ¶[0034]. Cole’s example implementations of the mobile device 110 are consistent with the examples of end-user devices described in the ’224 Patent, which include “smart phone devices, net book devices, tablet computing devices, and various other **wireless mobile computing devices**.” SAMSUNG-1001, 3:29-44.

54. It would have been known or obvious to a POSITA that Cole’s mobile device 110 is a “wireless end-user communication device” because Cole’s mobile device 110 can wirelessly communicate with other devices and can be used by an end-user. Indeed, Smith, a US patent application, corroborates this understanding and explains that an “end-user device,” can be “a **wireless telephone station**, a wired telephone station, a **personal digital assistant**, and a laptop computer.” SAMSUNG-1009, ¶[0007]. Thus, the references of Cole, D’Amore, and Rao each describe various examples of “*wireless end-user communications devices*.” SAMSUNG-1005, ¶¶[0014]-[0015], SAMSUNG-1006, ¶¶[0007]-[0016]; SAMSUNG-1007, ¶[0130].

55. As explained in more detail below, CDR also renders obvious the various features of the wireless end-user communications device claimed in the ’224 patent’s claims 1-11 and 16-17.

[1.1] at least one wireless modem;

56. As shown in Cole’s FIG. 2 below, Cole’s mobile device 110 includes “*at least one wireless modem*,” such as a WWAN modem and a WLAN modem. SAMSUNG-1005, ¶[0035]. Cole describes these modems as “communication interfaces 225.” *Id.*

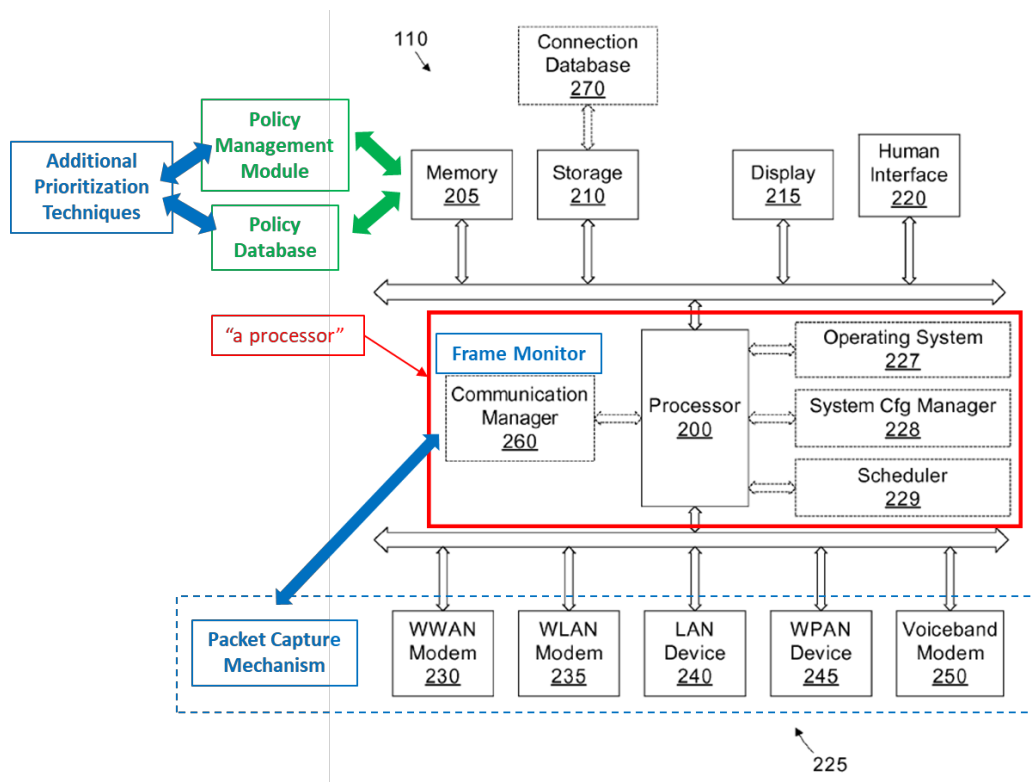


SAMSUNG-1005, FIG. 2 (modified based on CDR combination).

[1.2] a processor configured to:

57. As shown in Cole’s FIG. 2 below, Cole’s mobile device 110 includes a “*processor*.” SAMSUNG-1005, ¶[0015], ¶¶[0034]-[0036], FIG. 2. Cole’s “processor is coupled to the communication interfaces and operable to implement a connection manager.” SAMSUNG-1005, ¶[0015]. Additionally, Cole describes

that the processor executes “various software applications,” to include “user applications, an operating system 227, a system connection manager 228, a scheduler 229, device drivers, etc.” SAMSUNG-1005, ¶[0034]. Cole also describes its connection manager 260 as a “software application.” SAMSUNG-1005, ¶[0036]. Reproduced and annotated below is Cole’s FIG. 2, in which the red box labelled “a processor” includes several components whose operations are implemented by the processor. Thus, the red box represents, at least in part, a functional equivalent of the processor because the processor executes the operations that are described with respect to these components.



SAMSUNG-1005, FIG. 2 (modified based on CDR combination).

58. Moreover, a POSITA would have recognized or found obvious that because Cole's processor is configured to implement the connection manager and execute "various software applications," Cole's processor would have been "**configured to**" perform the features [1.3]-[1.7], as described in more detail below. SAMSUNG-1005, ¶[0015], ¶¶[0034]-[0036], [0153], FIG. 2. Indeed, Rao further corroborates the use of processors (e.g., a "processor" or "central processing unit") to execute various functions on computing devices. SAMSUNG-1007, ¶¶[0118]-[0122].

[1.3] for each given application of a plurality of applications on the wireless end-user device, monitor⁴ a network service usage activity of the wireless end-user communications device associated with the given application;

59. The '224 patent defines a "**network service usage activity**," as "any activity by the device that includes wireless network communication." SAMSUNG-1001, 12:58-60. Examples of network service usage activities include:

a voice connection (e.g., coded voice connection or voice over

⁴ The '224 patent describes "real-time traffic monitoring" of network service usage activities, for example, "at the packet level/layer, network stack application interface level/layer, and/or application level/layer." SAMSUNG-1001, 10:16-20.

IP (VOIP) connection), a device application or widget connection, a device OS function connection, an email text connection, an email download connection, a file download connection, a streaming media connection, a location service connection, a map services connection, a software update (e.g., application, operating system, and/or antimalware software update) or firmware update connection, a device backup connection, an RSS feed connection, a website connection, a connection to a server, a web browser connection, an Internet connection for a device based service activity, establishing a sync service account, a user data synchronization service, a device data synchronization service, a network connection flow or stream, a socket connection, a TCP connection, a destination/port assigned connection, an IP connection, a UDP connection, an HTTP or HTTPS connection, a TLS connection, an SSL connection, a VPN connection, a general network services connection (e.g., establishing a PPP session, authenticating to the network, obtaining an IP address, DNS service), and various other types of connections via wireless network communication. SAMSUNG-1001, 12:58-67, 13:1-21.

60. Similarly, Cole describes “voice-over-IP (VOIP) session[s],” “surfing a website,” “a file ... download,” “accessing [a] remote server,” and

“synchronizing files or email.” SAMSUNG-1005, ¶¶[0009], [0033], [0080], [0088]-[0089]. D’Amore and Rao also provide examples of network service usage activities, including “voice communication,” “e-mail,” “short message service (SMS),” “Internet webpage services,” “VoIP calls,” and a “TCP connection.” SAMSUNG-1006, ¶¶[0029]-[0032], [0068]; SAMSUNG-1007, ¶¶[0003]-[0005], [0024]-[0035].

61. Cole describes examples of “*a plurality of applications⁵ on the wireless end-user device*” that execute network service usage activities, such as “video,” “audio,” “VOIP,” web browsing, “photo files,” gaming applications (“game performance”), and “email.” SAMSUNG-1005, ¶¶[0009], [0088]-[0091], [0103]-[0105]. Indeed, these examples are consistent with the “applications” described in the ’224 Patent. SAMSUNG-1001, 16:37-56 (“streaming of video” and “browsing”). Finally, Cole also describes that the processor 200 executes “user applications.” SAMSUNG-1005, ¶[0034].

62. Cole’s connection manager 260 “*monitors the load on an active connection*” “to proactively prevent increased latency from an overloaded connection from impacting the performance of the running applications or the

⁵ Only two applications are needed to satisfy the claim feature of “*each given application of a plurality of applications.*”

efficiency of the user. In general, the connection manager 260 interfaces with the operating system 227 or other applications to schedule various events to effectively use the available bandwidth without negatively impacting performance.” SAMSUNG-1005, ¶[0074]. Specifically, Cole teaches that:

During operation of the mobile device 110, the connection manager *monitors the communication load being handled by the selected communication interfaces* and compares the monitored load to the bandwidth associated with the connection (e.g., based on historical performance or pre-set values) to determine periods of high load. *High load may result from one or more applications facilitating significant data transfers using the selected connection.* If the system load approaches the bandwidth limit for an extended period, performance of the mobile device 110 and the running applications may degrade. For example, if the connection is being used nearly to capacity and an additional application is executed that requires still more bandwidth, the connection may not be able to support the total load. As a result, the running applications may experience increased latency for data transfers. SAMSUNG-1005, ¶[0073].

63. Because Cole's connection manager can monitor the communication load from one or more applications (such as the applications described above) facilitating data transfers, Cole renders obvious [1.3]. ¶¶[0073]-[0075].

64. A POSITA would have recognized or found obvious that "data transfers" associated with network communication loads are examples of network service usage activities as the data transfers are facilitated by Cole's "communication interfaces," or "modems," which communicate this data over a wireless network, for example, a "WWAN" or "WLAN." ("wireless network communication"). SAMSUNG-1001, 12:58-60; SAMSUNG-1005, ¶¶[0014]-[0015], [0033]-[0037], [0073]-[0075]. Indeed, Cole provides examples of different network service usage activities, for example, a "file ... download" and a "synchronization," where the connection manager identifies the network service usage activities while "monitoring the load on an active connection" ("***monitor a network service usage activity of the wireless end-user communications device associated with the given application***"). SAMSUNG-1005, ¶¶[0074]-[0075], [0088]-[0089]. Other examples of applications in CDR that would contain "network service usage activities" include "video, chat, gaming, and virtual reality." SAMSUNG-1007, ¶[0133]. Some of these applications would even contain different types of "network service usage activities," communicated using

various protocols (e.g., a “gaming” application would have a control function transmitted via UDP and a chat function transmitted via TCP). *Id.*

65. Additionally, Rao describes a “packet capture mechanism” that “intercept[s] (*“monitors”*) ... network traffic ... such as **network packets associated with [an] application**” and a “frame monitor” that “identifies an application ... that generated the packet.” SAMSUNG-1007, ¶¶[0109], [0158]-[0159], [0176], [0180], [0185], [0191], FIG. 5A; §III.A.4. Rao also describes performing this process for “all outbound packets of the client” (*“each given application of a plurality of applications on the wireless end-user device”*). SAMSUNG-1005, ¶[0105]. Network packets are indicators of *“a network service usage activity ... associated with the given application”* because there would not be any network packet if there were no network service usage activity. For example, in the proceeding examples, network packets are transferred to effectuate some end result across the network (e.g., packets originating from a “gaming” chat service are transmitted to another user on the network in order to communicate across users). SAMSUNG-1007, ¶[0133]. Rao’s network traffic is described as including, for example, “real-time data,” for example, “RTP [Real Time Protocol] over UDP [User Datagram Protocol] via a TCP/IP [Transport Control Protocol/Internet Protocol] session” (all examples of “packet level” network traffic). SAMSUNG-1007, ¶¶[0153], [0184], [0198].

66. A POSITA would have recognized that the packet level monitoring of Rao would enhance the ability of CDR's connection manager to appropriately determine activity/application relationships, thus enabling the connection manager to make more effective classification decisions. *See above Section V.* For example, for an application that is associated with both "background" and "foreground" activities (e.g., a VoIP application that makes calls and also has recurring background updates), Rao's packet level monitoring would differentiate how the application was being used, for example, in the foreground (e.g., a call) or background (e.g., an update). Additionally, Rao's packet level monitoring would have also been used to determine that packets associated with a "file for download" are lossless (e.g., TCP/IP) and, therefore, could be deferred temporarily with less impact to the user. SAMSUNG-1005, ¶¶[0088]; SAMSUNG-1007, ¶¶[0082].

67. Moreover, a POSITA would have recognized or found obvious that the ability of the packet capture mechanism to determine the protocol associated with network packets would further enhance the ability of the CDR connection manager to effectively prioritize applications' network service usage activities, considering which protocols are "lossless" (e.g., TCP) and which are "lossy" (e.g., RTP over UDP). SAMSUNG-1007, ¶¶[0003], [0192]; *see above Section V.* For example, a POSITA would have recognized or found obvious that, when using the CDR device for an "interactive user session," such as "gaming," the connection

manager 260 would have responded to differences in transmission protocols, for example, prioritizing the transmission of application UDP packets (e.g., movement commands) over TCP packets (e.g., chat). SAMSUNG-1007, ¶[0140].

[1.4] classify, as a first classification for each given one of the network service usage activities, a classification based on the application associated with the given network service usage activity and that allows for a differential network access control, wherein the differential network access control comprises a set of service usage control policies applicable when a network service is available via the at least one wireless modem, including at least a first policy that allows the given network service usage activity to currently communicate data with a network destination via the at least one wireless modem, and a second policy that defers data communication associated with the given network service usage activity until a device state change occurs;

68. The '224 patent provides examples of “differential network service usage control” including “implementation of a network service usage activity policy (e.g., **block/allow**; traffic control techniques, such as throttle, **delay**, **priority queue**, **time window**, **suspend**, quarantine, kill, remove, and other well known traffic control techniques).” SAMSUNG-1001, 13:26-42. Additionally, the '224 patent describes “*differential network access control*” as “implementing different traffic controls for all or some of the network service usage activities (e.g., based on a network busy state or another criteria/measure)” (e.g., implementing differential network service usage controls). SAMSUNG-1001, 64:25-29.

69. The '224 patent also describes a “*service usage control policy*” as being “used for assisting in network access control of network service usage activities (e.g., deferring some or all of the network capacity demand from these

source activities).” SAMSUNG-1001, 12:20-23. Moreover, the ’224 patent describes that service usage control policies are used to “differentially control network services traffic based on a network busy state for an activity, a group of activities, or for a service class” (e.g., implementing differential network access control and/or differential network service usage control). *Id.*, 12:43-47.

70. Consistent with the examples and descriptions provided in the ’224 patent, as noted above, CDR renders obvious [1.4] for at least the reasons noted below. The mapping of the various features of [1.4] are discussed in detail below.

“classify, as a first classification for each given one of the network service usage activities, a classification based on the application associated with the given network service usage activity”

71. Cole describes that certain tasks, activities, and applications may be “**classified**” as background”. SAMSUNG-1005, ¶¶[0009], [0080], [0085]. This background classification is consistent with the ’224 patent, which describes that a network service usage activity can be “classified, associated with, and/or assigned to a background class ... to facilitate differential network service usage control to protect network capacity.” SAMSUNG-1001, 13:22-26; 64:21-25. A POSITA would have recognized or found obvious that a classification is made for “***each given one of the network service usage activities***” because to effectively manage network communications, each network service usage activity must be classified and managed. Not doing so would result in potentially overlooking a network

service usage activity that could damage or otherwise consume significant network resources. This is suggested by Cole, which describes that “some applications [and activities] require large amounts of bandwidth to operate efficiently.” SAMSUNG-1005, ¶[0008]. Indeed, Cole’s disclosure of its “communication load” including activities from “**one or more applications** facilitating significant data transfers” is consistent with the notion that the classification would have been performed “*for each given one of the network service usage activities.*” SAMSUNG-1005, ¶[0073]. Moreover, in differentiating “background” activities from non-background activities, the connection manager “*classifies*” all (“*each*”) of the activities in the communication load as those applications not classified as “background” would be assigned some other designation (e.g., “not background”). SAMSUNG-1005, ¶[0073]. Separately, Rao describes that the “packet capture mechanism” intercepts “any network traffic” (packets associated with “*each given one of the network service usage activities*”) transmitted by the end-user device. SAMSUNG-1007, ¶¶[0101], [0104], [0110].

72. Rao’s “frame monitor” also “identifies an application 338 that generated the packet” (“*a classification based on the application associated with the given network service usage activity*”). SAMSUNG-1007, ¶[0104], ¶¶[0108]-[0110]. Similarly, D’Amore describes a “system policy manager” (also referred to as the “policy management module”) that can “**delineate services** [(“*classify ... a*

*classification based on the application associated with the given network service usage activity”)] into clear priority and/or privilege levels and allow **policy decisions** to be described around such priority levels (“**service usage control policies**”).” SAMSUNG-1006, ¶¶[0036], [0050]-[0052].*

73. In CDR, the packet capture mechanism and frame monitor would classify activities, **based on their application**, to associate the activity and application with service usage control policies defined in the policy management module. *Id.*, SAMSUNG-1007, ¶¶[0104], [0108]-[0110]; *see below* §III.A.5, [1.5].

74. Additionally, the ability of the packet capture mechanism to determine an activity’s transmission protocol would have been used to further “classify” the “classification” of the network service usage activity (“classify ... a classification”). SAMSUNG-1007, ¶¶[0003], [0192]; *see above Section V*, [1.3]. For example, an activity assigned to a “not-a-background” “**classification**” (e.g., audio or video) would be further “**classified**” as a “lossy” activity if the associated transmission protocol is determined to be RTP over UDP. *Id.* By further classifying the activities in this way, the connection manager can evaluate additional relevant context that would be used to more effectively defer activities (e.g., activity UDP packets that are deferred are not able to be recovered). *Id.*

75. Other examples where “background” applications would be further “classified” include health monitoring and tracking applications which transmit

UDP data at specified intervals. The transmission behavior of these applications would be considered when deciding the priority of their traffic (e.g., if a transmission was previously made 30 seconds ago, a subsequent transmission may not be a priority).

“allows for a differential network access control, wherein the differential network access control comprises a set of service usage control policies applicable when a network service is available via the at least one wireless modem”

76. Cole describes that “certain background tasks” (“**network service usage activities**”) can be “postponed automatically” (“**allows for a differential network access control**”). SAMSUNG-1005, ¶[0085]. This action is consistent with the ’224 patent, which gives examples of differential network service usage control (the implementation of **differential network access control**) including actions to “delay” and/or “time window” a network service usage activity. SAMSUNG-1001, 13:26-42. Moreover, as described in [1.3] above, Cole “monitors” these activities prior to determining deferral is required. SAMSUNG-1005, ¶¶[0073]-[0075], [0085], [0088]-[0089]; *see above* [1.3]. The ’224 patent additionally describes “monitoring network service usage activity” as another example of differential network service usage control (“**allows for a differential network access control**”). SAMSUNG-1001, 13:26-42.

77. D’Amore and Rao provide additional examples of differential network access control consistent with the ’224 patent. SAMSUNG-1001, 13:26-42;

SAMSUNG-1006, ¶¶[0051]-[0052], [0056], [0060]; SAMSUNG-1007, ¶¶[0102], [0182]-[0195]. For example, D’Amore describes that the “policy management module” can “**approve or deny access** (*“differential network access control”* and *“a set of service usage control policies”*) to a **mobile device resource** and/or **mobile network resource** for a mobile application,” which is provided through a “communication interface” in the CDR device (*“applicable when a network service is available via the at least one wireless modem”*). SAMSUNG-1006, ¶[0051]; *see supra* [1.1]; *see infra* [1.5]. Approving or denying access is “based at least in part on a priority level or a privilege code **associated with the mobile application**” (the *“service usage control policy”* being associated with the *“network service usage activity,”* and based on the *“first classification [of the] network service usage activity,”* which is further *“based on the application.”*). SAMSUNG-1006, ¶[0051]; *see below* [1.5]. In CDR, Cole’s connection manager would also effectuate these examples of differential network access control. SAMSUNG-1006, ¶¶[0051]-[0052], [0056], [0060]; SAMSUNG-1007, ¶¶[0102], [0182]-[0195].

78. As described above, Cole’s connection manager “determines if one or more actions that are consuming bandwidth [and] should be postponed.” SAMSUNG-1005, ¶¶[0080], [0085]-[0086]. Additionally, Cole’s connection manager “may change the configuration of the communication functions in direct

response to the power state of the mobile device.” *Id.*, ¶[0090]. Indeed, Cole describes that “[if] the action can be postponed ... the connection manager 260 **cancels the action and schedules a deferred action**” (“*differential network access control*” and “*a set of service usage control policies*”). *Id.*, ¶[0086]. With respect to the set of service usage control policies (the “*service usage control policies*” comprise “*a set of service usage control policies applicable when a network service is available via the at least one wireless modem*”), CDR discloses various examples. For instance, Rao discloses that a communication can be prioritized when an application is running in the foreground (a “*first policy*”) and queued when running in the background and not a priority (a “*second policy*”). SAMSUNG-1007, ¶¶[0182]-[0183]. This same prioritization technique and set of policies are applicable when considering packet transmission protocol (e.g., UDP versus TCP). SAMSUNG-1007, ¶[0184]. In Cole, when “the monitored load exceeds a predetermined threshold ..., the connection manager 260 may take one of several actions to manage the load.” SAMSUNG-1005, ¶¶[0074], [0080], [0085]-[0086]. These actions, such as blocking, throttling, or withholding transmission, are reflective of different deferral policies (at least a “*second policy*”). SAMSUNG-1005, ¶[0125].

“a first policy that allows the given network service usage activity to currently communicate data with a network destination via the at least one wireless modem, and a second policy that defers data communication”

79. As a preliminary matter, CDR discloses this feature because CDR discloses various policies corresponding to this claimed feature as described above. A POSITA would have recognized or found obvious that the “determin[ation] if one or more actions that are consuming bandwidth,” made by the connection manager, would be “*at least*” a “*first policy that allows [communication]*” and a “*second policy that defers data communication*” because the communication manager defers or reschedules communication when bandwidth is a concern, and allows communication otherwise (“effectively use the available bandwidth”). SAMSUNG-1005, ¶¶[0074], [0080], [0085]-[0086]. The “determin[ation] performed by the connection manager 260 in this case would be with respect to various responses (at least a “*first*” and a “*second*” policy) that would be executed to either restrict or allow transmission. *Id.* Indeed, Cole describes that when “the monitored load exceeds a predetermined threshold ..., the connection manager 260 may take one of several actions to manage the load” (at least a “*second policy*”). *Id.* Moreover, the CDR system includes additional examples of a “*second policy that defers data communication*” such as blocking, throttling, or withholding transmission. SAMSUNG-1005, ¶[0125]; SAMSUNG-1007, ¶[0195]. Additionally, Rao’s prioritization techniques are also examples of a “*first*” and “*second*” policies in that communication is prioritized when an application is running in the foreground (a “*first policy*”) and queued when running in the

background and not a priority (a “*second policy*”). SAMSUNG-1007, ¶¶[0182]-[0183]. This same prioritization technique and set of policies are applicable when considering packet transmission protocol (e.g., UDP versus TCP). SAMSUNG-1007, ¶[0184].

80. Together, these two “*service usage control policies*” comprise “*a set of service usage control policies applicable when a network service is available via the at least one wireless modem.*” *Id.* Additionally, these “*service usage control policies*” can also be implemented by Cole’s connection manager in response to changes in device “power state.” *Id.*, ¶¶[0090]-[0100]. For example, Cole describes an example where an activity begins while a user is traveling on a WLAN. SAMSUNG-1005, ¶[0089] (“a scheduled synchronization starts while the user is traveling”). The connection manager 260 notices the battery consumption from the synchronization during the user’s travels and defers the activity (a “*second policy that defers data communication*”). *Id.* When the user later connects to a LAN, the connection manager 260 then reinitiates the synchronization (a “*first policy that allows [communication]*”). SAMSUNG-1005, ¶[0089].

“until a device state change occurs”

81. Cole describes that “**power state**” (a “*device state*”) can be used to “change the configuration of the communication functions.” SAMSUNG-1005,

¶¶[0087]-[0100]. The '224 patent acknowledges that a “change in device **power state**” is a “*device state change*.” SAMSUNG-1001, Claim 6. Cole describes that, once an activity is deferred, the connection manager “may reinitiate the action on its own by interfacing with the scheduler 229” (returning to a “*first policy that allows [communication]*”). SAMSUNG-1005, ¶[0087]. Determination to reinitiate the action (“*data communication associated with the given network service usage activity*”) can include “determining if **sufficient battery power** (“*a device state change*”) is present to complete the transaction.” *Id.* The operation of rescinding “*a second policy that defers data communication*” and restoring a “*first policy that allows [communication]*” in response to “*a device state change*” (e.g., a change in power state) is consistent with the examples described in Cole. *Id.*, ¶¶[0088]-[0092].

82. Moreover, a POSITA would have understood or found obvious that many other features described in Cole, D’Amore, and Rao associated with “*service usage control policies*” would be “*device states*” as these features are associated with a “state” of the mobile device. SAMSUNG-1005, ¶¶[0075]-[0100] (describing, among other things, channel “queue[s],” device “thermal conditions,” processor “performance,” device “quietness,” battery “alarms,” whether the device is “connected to an external power supply,” the “level of charge remaining, if operating on battery power,” and the “remaining time to fully charge the battery”);

SAMSUNG-1006, ¶¶[0031]-[0033] (describing, among other things, “arbitrat[ing] access to network and/or device resources”), SAMSUNG-1007, ¶[0182] (describing, among other things, “whether an application is running in the foreground or the background”). For example, the transition of an application from a background to a foreground state (“*a device state change*”) would have been used to rescind the “*second policy that defers data communication*” and implement the “*first policy that allows [communication]*.” SAMSUNG-1007, ¶[0182]. Additionally, the transition of a transmission protocol from one form to another, for example, a VoIP application concluding a voice call using UDP (“*a device state change*”) would also have been used in CDR to replace the “*second policy*” with the “*first*.” SAMSUNG-1007, ¶[0184]. Given that “*device state*” would have been interpreted broadly by a POSITA, there are many possible scenarios where a POSITA would have configured the CDR device to implement one or more service usage control policies in response to a “*change*” in one or more of these *device states*. *Id.* For example, given that CDR can execute “gaming” applications, a POSITA would have recognized or found obvious that “game performance” (e.g., processing power) would be optimized when network (e.g., bandwidth) and device conditions (e.g., battery power and temperature) allow. SAMSUNG-1005, ¶[0091]; SAMSUNG-1007, ¶[0133]. However, in response to a degradation in either network or device resources (e.g., a “*device state change*” of

a high busy state, or a battery alarm) the connection manager 260 would respond to best address the issue. *Id.*

[1.5] associate each given one of the network service usage activities with a service usage control policy dynamically selected from the set of service usage control policies, based on the first classification of the given network service usage activity and at least one device state; and

83. As an initial matter, the '224 patent provides examples where the word “dynamic” or “*dynamically*” is used to describe how its techniques are applied “based on” device states. SAMSUNG-1001, 77:50-53, 86:65-67, 87:1-9; 98:33-44, 99:3-14.

84. As discussed above with respect to feature [1.4], in CDR’s mobile device, the packet capture mechanism and frame monitor would classify network service usage activities, based on their application, and “*associate each given one of the network service usage activities with a service usage control policy*” defined in the policy management module. SAMSUNG-1007, ¶¶[0104], [0108]-[0110]; *see above Section V*, [1.4]. The CDR connection manager would then effectuate differential network access control according to the selected service usage control policy. SAMSUNG-1005, ¶¶[0073]-[0075], [0085], [0088]-[0089]; *see above Section V*, [1.4].

85. As described above, the CDR connection manager applies and rescinds service usage control policies in response to “device state changes” (“*dynamically*”). SAMSUNG-1005, ¶¶[0085]-[0100]; SAMSUNG-1006,

¶¶[0031]-[0033]; SAMSUNG-1007, ¶[0182]. This is consistent with the '224 patent, which describes *dynamical selection* based on device states. SAMSUNG-1001, 77:50-53, 86:65-67, 87:1-9; 98:33-44, 99:3-14. A POSITA would have recognized or found obvious that CDR's connection manager would have "*dynamically [selected]*" these service usage control policies "*based on*" both the network service usage activity "*classification*" and "*at least one device state*" consistent with the examples described in Cole, D'Amore, and Rao. SAMSUNG-1005, ¶¶[0088]-[0100], ¶¶[0119]-[0127], FIG. 6A, FIG. 6B, FIG. 7, FIG. 9; SAMSUNG-1006, ¶[0069], ¶[0087] (describing "*dynamic* priority").

86. For example, Cole describes:

In one example, the user is surfing a web site and selects a file for download [(a "*network service usage activity*")]. ... The user is in a public place and the lengthy transfer is conducted using the WWAN modem 230 (e.g., a 3G channel), which consumes significant battery power. The connection manager 260 identifies the **load on the WWAN modem 230** [("*at least one device state*")] and asks the user to **find a better connection** [("*a service usage control policy dynamically selected from the set of service usage control policies*" that defers communication)]. ... When the user returns home, **connects the mobile device 110 to a power source** [("*at least one*

device state”)], and the communication manager 260 connects **using the WLAN modem 235** (e.g., a Wi-Fi connection) [(also “*at least one device state*”)], the connection manager 260 reminds the user to **download the file** [(“*a service usage control policy dynamically selected from the set of service usage control policies*” that allows communication)]. The connection manager 260 may **provide the address for the file and even open the browser**, or the user may manually open the browser and use the browser history data to find the link to the file. SAMSUNG-1005, ¶[0088].

87. As described above, the “*classification*” of the network service usage activity would also be used by CDR’s connection manager in implementing policy decisions. SAMSUNG-1005, ¶¶[0009], [0080], [0085]; SAMSUNG-1006, ¶¶[0036], [0050]-[0052]; SAMSUNG-1007, ¶¶[0104], [0108]-[0110]; *see above Section V*, [1.3].

[1.6] manage network data access via the at least one wireless modem for each of the plurality of applications according to the dynamically selected service usage control policy for each given network service activity of that application; and

88. In the examples of differential network access control discussed above, the CDR connection manager defers communication in response to certain device states, and allows communication in others through a wireless modem (“*manage network data access via the at least one wireless modem*”). SAMSUNG-1005,

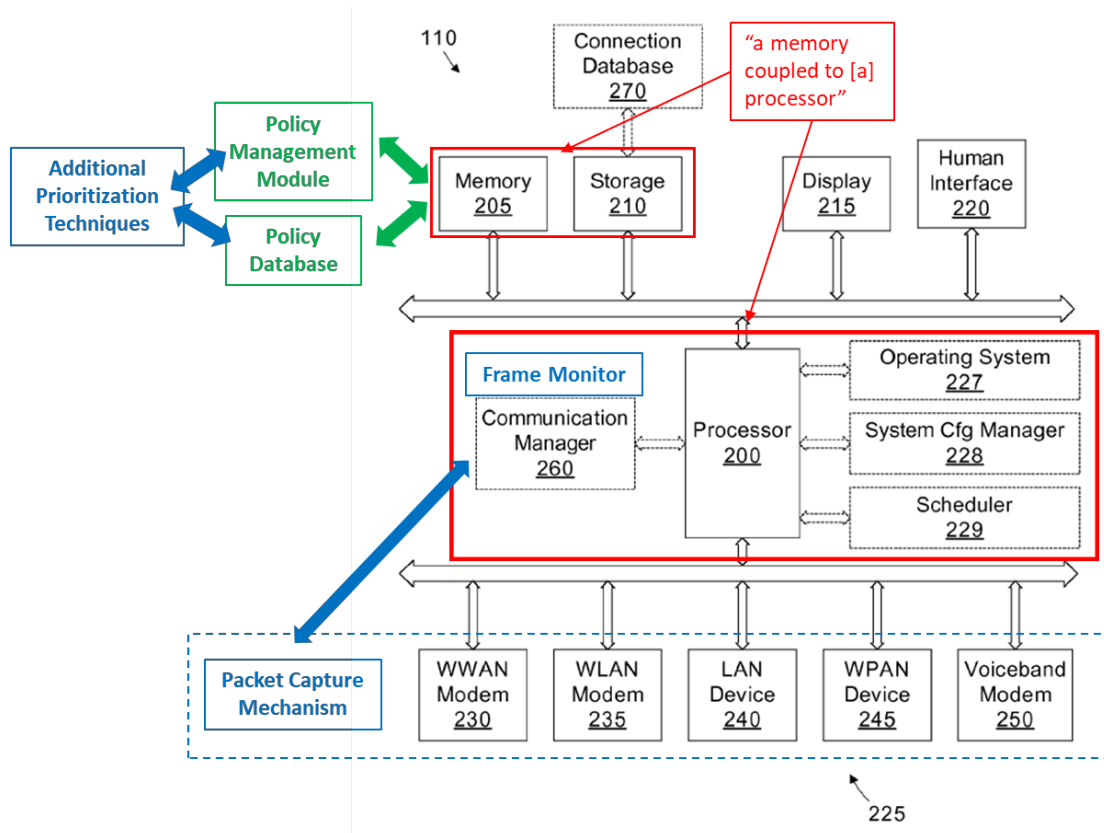
¶¶[0074]-[0100]; *see above* [1.1], [1.4], [1.5]. In this example, deferring communication is one example of managing network data access. Moreover, the CDR connection manager would have managed the access for “*each of the plurality of applications*” as the CDR mobile device monitors “*each given application of a plurality of applications.*” *See above* [1.3]. A POSITA would have recognized and found obvious that this “*network data access*” would be “*according to the dynamically selected service usage control policy*” as the CDR connection manager “*manage[s] network data access*” according to these policies. *See above* [1.4].

89. D’Amore also describes that the policy management module can control access to “device resources,” which in the CDR system includes “*at least one wireless modem.*” SAMSUNG-1006, ¶¶[0032]-[0033]. The CDR mobile device would thus be capable of “*manag[ing] network data access*” via the “*at least one wireless modem.*” SAMSUNG-1006, ¶¶[0032]-[0033].

[1.7] a memory coupled to the processor and configured to provide the processor with instructions.

90. Cole’s mobile device includes a “memory 205 and/or storage device 210 [that] typically store various software applications for execution by the processor 200, such as user applications, an operating system 227, a system connection manager 228, a scheduler 229, device drivers,” and connection manager 260. SAMSUNG-1005, ¶¶[0033]-[0036], FIG. 2. Accordingly, it would

have been obvious to a POSITA that CDR's memory is "*configured to provide the processor with instructions.*" As depicted in Cole's modified FIG. 2 below, the "*memory*" in CDR's mobile device is also "*coupled to the processor.*" SAMSUNG-1005, ¶[0033]-[0036].



SAMSUNG-1005, FIG. 2 (modified based on CDR combination).

[2] The wireless end-user communications device of claim 1, wherein the dynamically selected service usage control policy for a given network service usage activity is further selected based on an application behavior for the application associated with that network service usage activity.

91. Rao describes that “network packets may be further prioritized by **the characteristic of the application ... generating them.**” SAMSUNG-1007, ¶¶[0193]-[0195]. For example, Rao describes that its remote access client can “recognize **a high number of retransmits to a particular destination (“application behavior”)** and, in response, “throttle back or not communicate network packets” (a “*dynamically selected service usage control policy for [the] given network service usage activity*” that is “*further selected based on application behavior*”). SAMSUNG-1001, 103:6-33 (“frequent transmission”); SAMSUNG-1007, ¶[0195]; *see above* [1.4], [1.5]. Moreover, Rao describes additional “*application behaviors*” to include “a foreground application, the size of the network packet, or the time the network packet was intercepted.” *Id.*, ¶[0193].

92. A POSITA would have also considered “*application behavior*” to include other application characteristics described in CDR. For example, Cole describes that the connection manager can “[identify] load on the WWAN modem 230” caused by large activities such as a “file for download” that causes a “lengthy transfer” (an “*application behavior*”). SAMSUNG-1005, ¶[0088]. In response to identifying the lengthy transfer, the connection manager “asks the user to find a better connection,” and ultimately defers the activity until “the user returns home [and] the communication manager 260 connects using the WLAN modem” (all collectively a “*dynamically selected service usage control policy for a given*

network service usage activity... further selected based on an application behavior ... associated with that network service usage activity”). *Id.* Cole provides an additional example of the communication manager noticing specific application “*behavior.*” *Id.*, ¶[0089]. Additionally, Cole describes that the connection manager 260 “monitors the user's **connection behaviors** to identify patterns and attempt to automate ... configuration changes.” SAMSUNG-1005, ¶[0047].

93. Moreover, Rao’s ability to monitor packet-level traffic would have been used to monitor and respond to intra-**application behavior**. For example, Rao describes that its techniques can be used in “multimedia elements” such as “gaming.” SAMSUNG-1007, ¶[0140]. A POSITA would have recognized or found obvious that, when using the CDR device for an “interactive user session,” such as “gaming,” the connection manager 260 would have responded to intra-**application behaviors**, for example, prioritizing the transmission of application UDP packets (e.g., movement commands) over TCP packets (e.g., chat). SAMSUNG-1007, ¶[0140].

94. Other examples where packet-level traffic would be used to provide context to intra-**application behavior** include health monitoring and tracking applications which transmit UDP data at specified intervals. The transmission behavior of these applications would be considered when deciding the priority of

their traffic (e.g., if a transmission was previously made 30 seconds ago, a subsequent transmission may not be a priority).

[3] The wireless end-user communications device of claim 1, wherein the dynamically selected service usage control policy for a given network service usage activity is further selected based on whether the application associated with that network service usage activity is currently in the foreground of user interaction.

95. Rao describes “***foreground applications***” that are “in active use by the user (applications that are in the “***foreground of user interaction***”).” SAMSUNG-1007, ¶[0003]. Rao describes “prioritization based on whether an application is running in the ***foreground*** or the background” (a “***dynamically selected service usage control policy***”). *Id.*, ¶¶[0182], [0188]-[0189]; *see above* [1.4], [1.5]. As described above, Rao’s prioritization would be used to “***further***” consider the impact to the mobile device user, for example, “***whether the application associated with that network service usage activity is currently in the foreground of user interaction.***” *Id.*; *see above* Section V. A POSITA would have recognized or found obvious that the “foreground applications” of Rao would be “***associated with***” corresponding “***network service usage activities***” because Rao describes such activities, for example, “VoIP telephone calls,” “chat,” and “video.” *Id.*, ¶¶[0133]-[0135], [0140]-[0141], [0198], [0210].

[4] The wireless end-user communications device of claim 1, wherein the set of service usage control policies further comprises a third policy that blocks data communication associated with the given network service usage activity.

96. Cole describes that the connection manager can “**block**” updates (“*data communication associated with the network service usage activity*”) that do not meet “defined prerequisites.” SAMSUNG-1005, ¶[0125]. Moreover, Cole describes that additional conditions can require an activity to be blocked (“the task should be blocked unless the mobile device 110 is connected to external AC power”). SAMSUNG-1005, ¶[0119]. This “**third policy**” would have been in addition to the “**first**” and “**second**” policies described above as Cole’s consideration of power state conditions is in addition to its consideration of connectivity states. SAMSUNG-1005, ¶[0119]; *see supra* [1.4], [1.5]. For example, an activity scheduled with a required “connectivity state” may be later blocked due to a power state. *Id.* Moreover, a POSITA would have recognized or found obvious that blocking updates that do not meet defined prerequisites would be at least “**a third policy**” included in the “*set of service usage control policies*” as this mode of operation is substantially different than the operation of deferring activities described above in [1.4]. *Id.*; *see above* [1.4], [1.5].

97. In combining Cole with D’Amore, a POSITA would have also recognized that, when applications request access to a “mobile network resource” the “priority level” of the application can be used to “[deny] access to the resource” (“**block**” access). SAMSUNG-1006, ¶¶[0051]-[0052]. As described above, D’Amore’s “priority levels” are stored in a “policy database” (“**a third**

policy” included in the “*set of service usage control policies*”). *Id.*, ¶¶[0050]-[0051]; *see above* [1.4].

98. Moreover, the act of blocking data communication was well known in the art. Indeed, Freund, a US patent directed to “monitoring access to an open network,” describes a system that “is able to selectively **block** access, as dictated by the configurable rules.” SAMSUNG-1008, Abstract, 19:44-60.

[5] The wireless end-user communications device of claim 1, wherein the dynamically selected service usage control policy for a given network service usage activity is further selected based on a messaging layer behavior for the application associated with that network service usage activity.

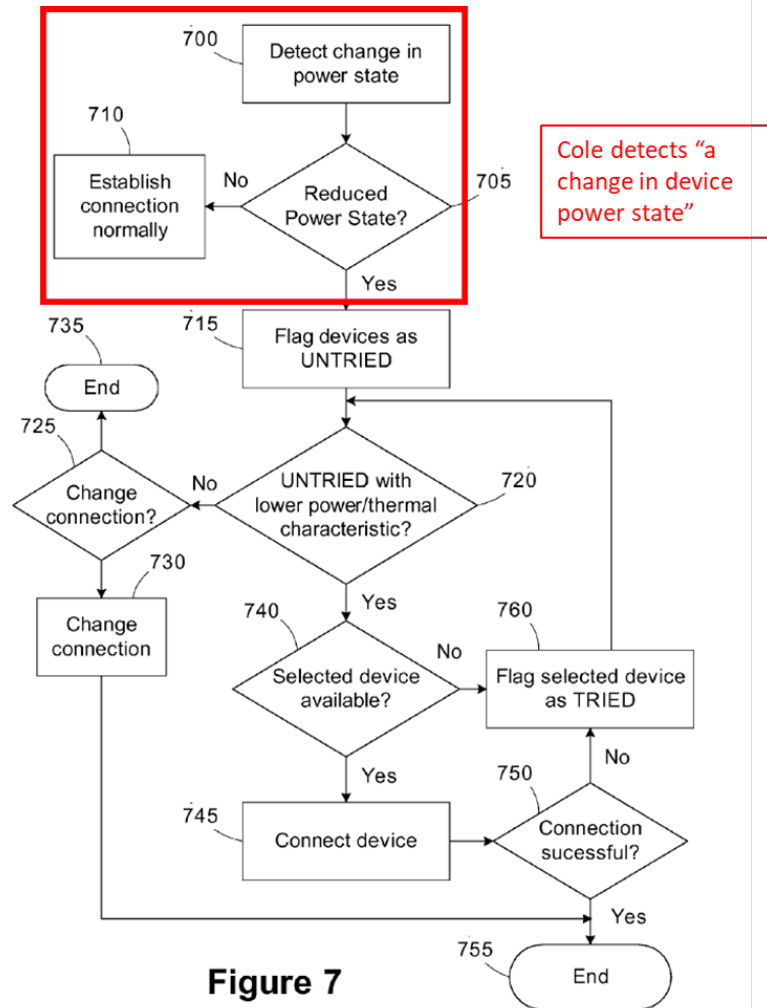
99. Rao describes a “packet capture mechanism” that can intercept “network packets” and perform various actions. SAMSUNG-1007, ¶[0104]. A POSITA would have recognized or found obvious that “network packets” (e.g., “RTP over UDP via a TCP/IP”) are transmitted using a “messaging layer” of the transmitting device. SAMSUNG-1007, ¶[0153], ¶[0184], ¶[0198]. Therefore, network packet transmissions are indicative of “**messaging layer behavior.**” *Id.* Indeed, this understanding in the art is reinforced by McAllister, a U.S. Patent that describes “TCP” and “UDP” as “[Open Systems Interconnection (OSI)] layer 4 protocols,” that form a “**message layer network (“[the] messaging layer”).**” SAMSUNG-1012, Cover, 1:61-67, 2:1-26; *see above* [1.4], [1.5].

100. As described in [2] above, the Cole-D’Amore-Rao end-user device selects service usage control policies in response to “**application behavior,**” which

includes the behavior of the application “*messaging layer.*” SAMSUNG-1005, ¶¶[0088]-[0089]; SAMSUNG-1007, ¶[0104], ¶¶[0193]-[0195]; *see above* [2].

[6] The wireless end-user communications device of claim 1, wherein for the second policy that defers data communication associated with the given network service usage activity until the device state change occurs, the device state change comprises a change in device power state.

101. Cole describes that the “connection manager 260 may **change the configuration of the communication functions** (rescinding “*the second policy that defers data communication associated with the given network service usage activity*”) in direct response to the **power state of the mobile device**” (“*a change in device power state*”). SAMSUNG-1005, ¶¶[0087]-[0098], FIG. 7; *see above* [1.4], [1.5]. For example, Cole describes that in reacting to device power state, “if the mode change is associated with an **increased power state (e.g., connection to AC power or change to high performance mode)**, (“*a change in device power state*”) the connection manager 260 establishes the connection normally using the ‘best’ connection technique.” SAMSUNG-1005, ¶[0098]. A POSITA would have recognized or found obvious that, in one example, this increased power state would result in allowing previously deferred “*data communication associated with the given network service usage activity*” because Cole provides an example of one such operation (“download the web file”). SAMSUNG-1005, ¶[0088]. Cole’s Figure 7 is reproduced and annotated below.



SAMSUNG-1005, FIG. 7.

102. Moreover, Cole describes that “the user may specify when scheduling a task, that the task **should be blocked unless the mobile device 110 is connected to external AC power**” and that the connection manager “may be configured to block ... updates unless the defined prerequisites are met (e.g., rich connectivity is available, **sufficient battery life is available**, the **battery is charged and the line power is provided**, etc.” *Id.*, ¶¶[0119], [0125].

[7] The wireless end-user communications device of claim 1, wherein for the second policy that defers data communication associated with the given network service usage activity until the device state change occurs, the device state change comprises a change from a modem power save state that is not triggered by the given network service usage activity.

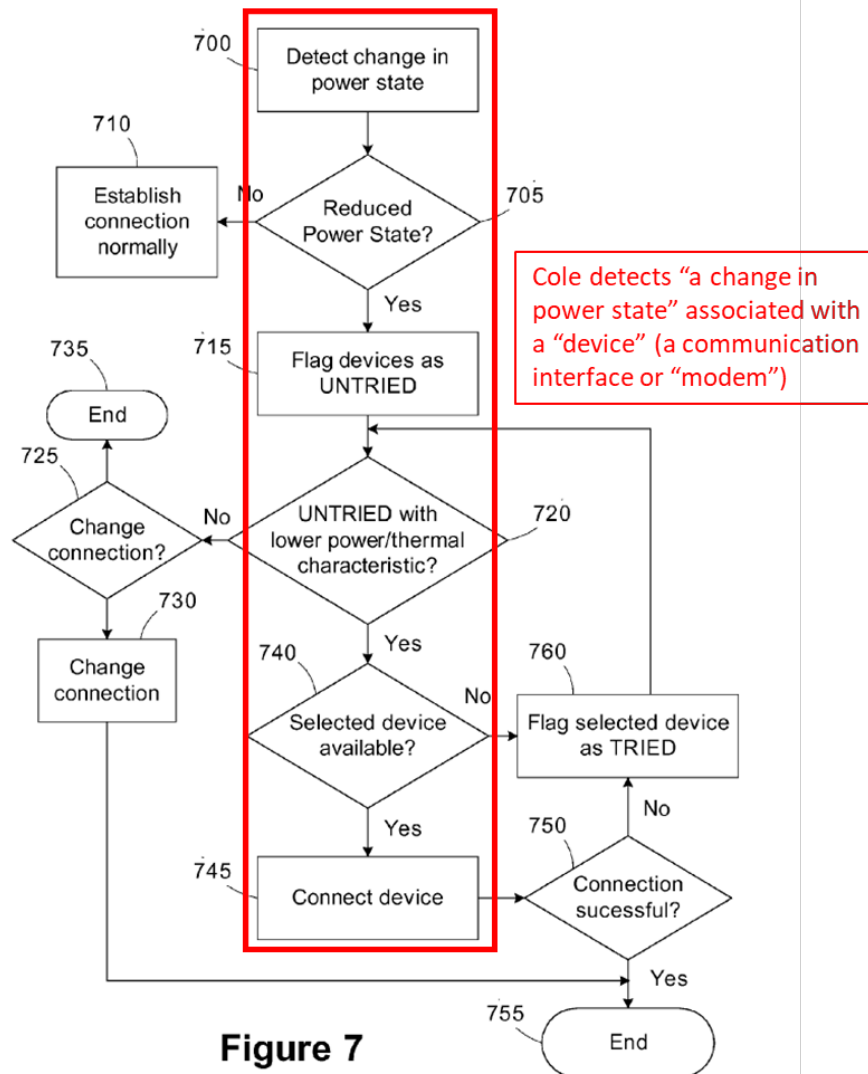
103. As an initial matter, the '224 Patent describes “power save state” in various contexts, an example of which is provided below. SAMSUNG-1001, 7:47-62.

Another example of device service activity behavior that can have an impact on network performance is the way the **device, device subsystem, and/or modem subsystem power cycling or transitions from one power save state to another**. ... If a device terminates the connection to the base station when **the modem subsystem (e.g., or some other portion of the device)** goes from **active connection state to a power save state**, then each time the device enters power save state and then exits power save state network resources are consumed, sometimes for time periods measured on the order of seconds or in extreme cases even minutes. *Id.*

104. Cole describes that end-user devices can “be placed into a particular system configuration to emphasize particular performance characteristics” to include “modes” that emphasize “battery life” (“***power save state***”). SAMSUNG-1005, ¶[0091].

105. Additionally, Cole describes that the “power state” of the mobile device can be used to “change the configuration of the communication functions.” SAMSUNG-1005, ¶[0090]. Cole also describes that “power ... characteristics” (“*power save state*”) can be determined for individual “communication interfaces (“*modem[s]*”).” *Id.*, ¶¶[0092]-[0097]. Cole describes that a “communication interface” can include a “*modem.*” *Id.*, ¶[0035].

106. A POSITA would have recognized or found obvious that a “*modem power save state*” rescinds a “*second policy that defers data communication associated with the given network service usage activity*” as the communication manger “includes the power state information in its evaluation of the appropriate communication interface.” SAMSUNG-1005, ¶¶[0092]-[0097]; *see above* [1.4], [1.5], [6]. Cole’s Figure 7 is reproduced and annotated below.



SAMSUNG-1005, FIG. 7.

107. Moreover, a POSITA would have recognized or found obvious that a device or modem power save state is “*triggered*” by activities other than “*the given network service usage activity*” as Cole describes many such cases where a change in power state is triggered independent of “*activities*” (e.g., whether the device is connected to an external power supply). SAMSUNG-1005, ¶[0090].

[8] The wireless end-user communications device of claim 1, wherein for the second policy that defers data communication associated with the given network service usage activity until the device state change occurs, the device state change comprises a change to a network connection state that is not triggered by the given network service usage activity.

108. Cole describes that tasks that are unsuitable for the WWAN can be deferred until another more suitable network is available (e.g., the WLAN) (“***the device state change comprises a change to a network connection state***”). SAMSUNG-1005, ¶[0088]; *see above* [2]. The connection manager connecting to the WLAN in this example “***is not triggered by the given network service usage activity,***” but rather when “the user returns home.” *Id.*

109. Cole also describes that, when the connection manager “detects a sustained high load on the current communication link over the active communication interface” it determines “if there is a device with **better connectivity** present in the group of untried devices (i.e., as determined by speed, latency, QoS)” (“***network connection state***”). SAMSUNG-1005, ¶[0083], FIG. 6A. Upon detecting an interface “with potentially better connectivity,” the connection manager “attempts to connect using the selected device.” *Id.* An overview of this process is presented in annotated Figure 6A below.

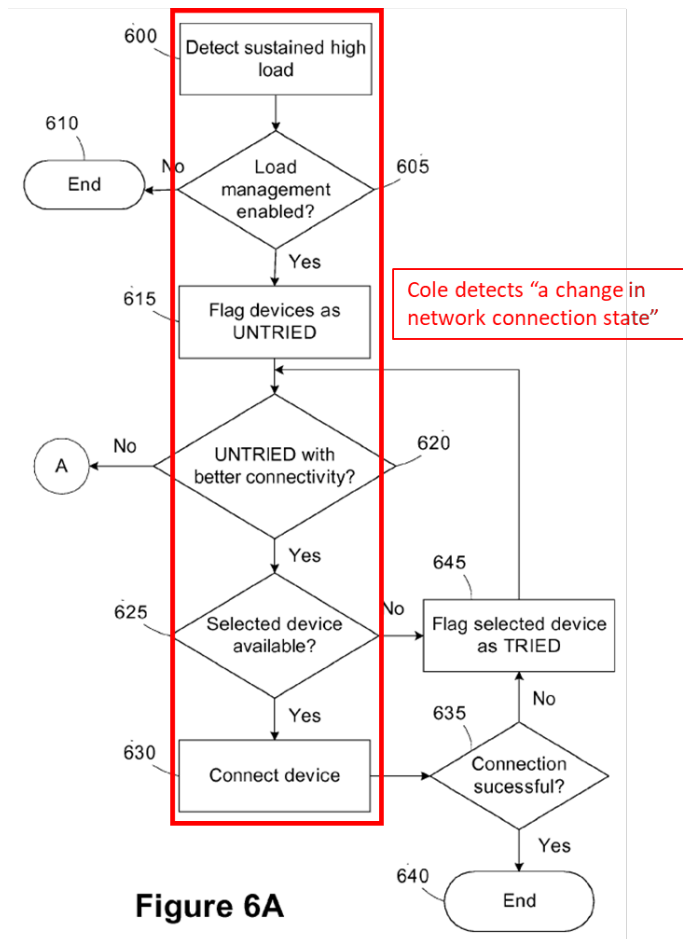


Figure 6A

SAMSUNG-1005, FIG. 6A.

110. A POSITA would have recognized or found obvious that because Cole’s connection manager selects communication interfaces “proactively,” that “*a change to a network connection state*” caused by selecting a more suitable communication interface would rescind a “*second policy that defers data communication associated with the given network service usage activity*” and thereby end deferral of data communication. SAMSUNG-1005, ¶¶[0074], [0083]-[0087], FIG. 6A; *see above* [1.4], [1.5]. Indeed, Cole describes that “[a]ctivities

may be triggered by changes in connectivity state” (“*a change to a network connection state*”). SAMSUNG-1005, ¶¶[0121]-[0122].

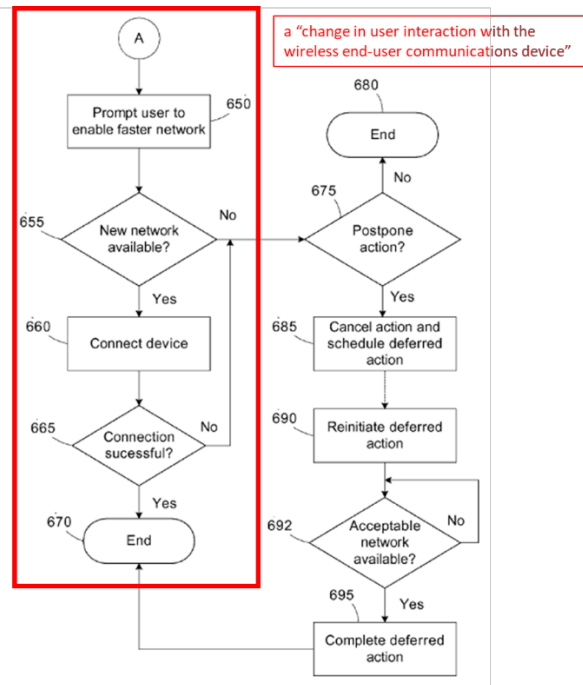
[9] The wireless end-user communications device of claim 1, wherein for the second policy that defers data communication associated with the given network service usage activity until the device state change occurs, the device state change comprises an aggregation of demand from multiple network service usage activity.

111. Recall from the mapping of claim 1 above that Cole discloses several “second polic[ies] that defer[] data communication associated with the given network service usage activity” through policy actions such as such as blocking, throttling, or withholding transmission. *See above* [1.4]; SAMSUNG-1005, ¶¶[0074], [0080], [0085]-[0086], [0125]. These second policies can be implemented “to emphasize particular performance characteristics,” e.g., battery life. SAMSUNG-1005, ¶[0091]. Relatedly, Rao describes policies and application activities in which “network packets intercepted ... may be stored in a queue” associated with an application (“*aggregation of demand from multiple network service usage activity*” for each of “*the given network service usage activit[ies]*”). SAMSUNG-1007, ¶[0184]-[0186], [0189]-[0194]. A POSITA would have understood that when packets from various applications are placed in a queue such a queue is one example of an aggregation of demand from multiple network service usage activities.

112. Relatedly, when these queues reach capacity due to queue capacity limits (“until the device state change occurs, the device state change comprises an aggregation of demand”), e.g., arising from an *“aggregation of demand,”* a POSITA would have understood that the deferral of packets by placing them in a queue would be stopped and the packets in the queue would have to be cleared (e.g., by transmitting them or clearing the queue). A POSITA would have recognized or found obvious that, particularly when the CDR device was placed in a mode to prolong battery life, the transmission of data from the queues of the CDR device would be based on the que size to prevent overly frequent transmission (rescinding the *“second policy”* in response to *“an aggregation of demand from multiple network service usage activity”*). SAMSUNG-1005, ¶¶[0091]; SAMSUNG-1007, ¶¶[0184]-[0186], [0189]-[0194]. For example, in order to reduce the power requirements of Cole’s “communication interfaces” (e.g., modems), a POSITA would have recognized that queuing activities and structuring their transmissions would lessen the load on the device’s communication interfaces, and thus, lower device battery consumption. SAMSUNG-1005, ¶¶[0092]-[0099]. Additionally, an *“aggregation of demand”* that exceeds the length of a que would require disposition (e.g., transmission during a scheduled time slot). SAMSUNG-1005, ¶¶[0119]-[0127]. Finally, an *“aggregation of demand”* would also drive a change to Rao’s que priority, rescinding *“the second policy.”* *Id.*

[10] The wireless end-user communications device of claim 1, wherein for the second policy that defers data communication associated with the given network service usage activity until the device state change occurs, the device state change comprises a change in user interaction with the wireless end-user communications device.

113. Cole describes that the “**user**” can “reinitiate [an] action” (a “**change in user interaction with the wireless end-user communications device**”) after deferral (a “**second policy that defers data communication associated with the given network service usage activity**”). SAMSUNG-1005, ¶[0087]. Additionally, Rao describes applications operating “in the foreground and currently in active use by the user” as having a higher priority than background applications. SAMSUNG-1007, ¶[0003]. In view of this, a POSITA would have recognized or found obvious that an application transitioning from a foreground to a background state (e.g., through “**user interaction**”) would have resulting in a change in application priority. *Id.* Cole also describes that the user may overrule the connection manager when making rescheduling decisions (“the user elects not to postpone”) (“**a change in user interaction**” that blocks a “**second policy that defers data communication with the wireless end-user communications device**”). *Id.*, ¶[0085]; *see above* [1.4], [1.5]. An example process where user interaction changes the operation of the end-user device is reproduced and annotated below.

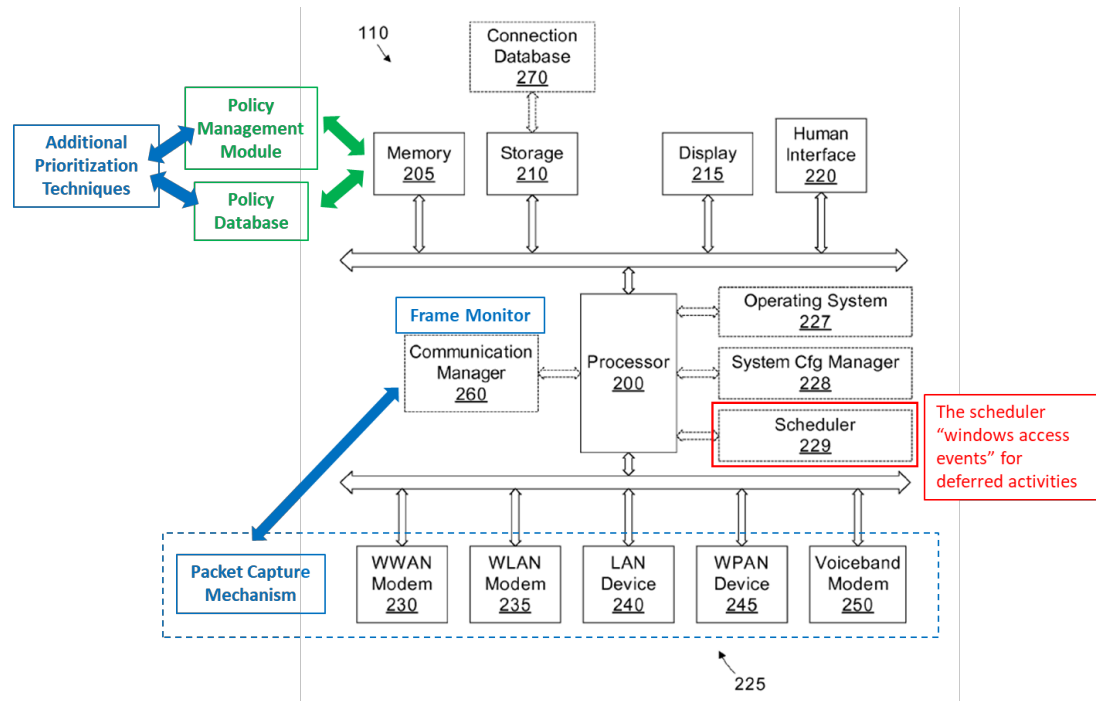


SAMSUNG-1005, FIG. 6B.

[11] The wireless end-user communications device of claim 1, wherein the dynamic selection of the service usage control policy is further based on a user preference setting for a given one of the applications.

114. D’Amore describes a “configuration module” that includes a “user input module” that allows a “user” to “to **modify priority level/privilege code** of one or more applications with respect to one or more system resources” (“*a user preference setting*”). SAMSUNG-1006, ¶¶[0063]-[0070]. D’Amore’s user input module is presented in the annotated Figure 4 below.

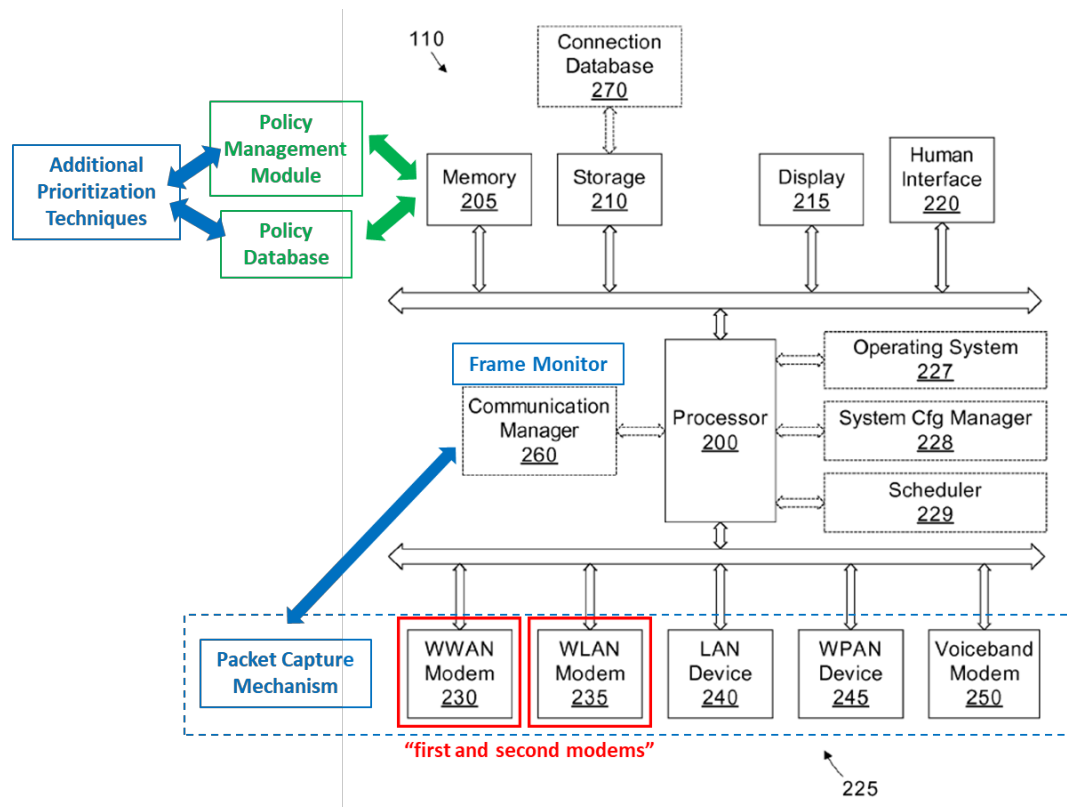
some later point in time. In some embodiments, the connection manager 260 may reinitiate the action on its own by interfacing with the scheduler 229.” SAMSUNG-1005, ¶[0087]. Cole’s scheduler is presented in the annotated FIG. 2 below.



SAMSUNG-1005, FIG. 2 (modified based on CDR combination).

[17] The wireless end-user communication device of claim 1, wherein the at least one wireless modem comprises first and second modems, and wherein the service usage control policy dynamically selected for at least one given one of the network service usage activities is further selected in dependence upon which of the first and second modems will supply network connectivity for that network service usage activity.

117. Cole describes that its “mobile devices” have a plurality of “modems,” to include a “WWAN modem” and a “WLAN modem” (“*first and second modems*”). SAMSUNG-1005, ¶[0035], FIG. 2.



SAMSUNG-1005, FIG. 2 (modified based on CDR combination).

118. Cole describes that tasks that are unsuitable for the WWAN can be deferred until another network is available (e.g., the WLAN). Indeed, Cole describes:

[A] user is in a public place and [a] **lengthy [file] transfer is conducted using the WWAN modem 230 (e.g., a 3G channel)**, which consumes significant battery power. The connection manager 260 identifies the load on the WWAN modem 230 and asks the user to find a better connection. A better connection is not available in the public setting, so the user opts to be reminded to download the web

file later. When the user returns home, connects the mobile device 110 to a power source, and **the communication manager 260 connects using the WLAN modem 235 (e.g., a Wi-Fi connection)**, the connection manager 260 reminds the user to download the file. The connection manager 260 may provide the address for the file and even open the browser, or the user may manually open the browser and use the browser history data to find the link to the file. SAMSUNG-1005, ¶[0088].

119. A POSITA would have recognized or found obvious that in Cole’s connection manager “*the service usage control policy [is] dynamically selected ... in dependence upon which of the first and second modems will supply network connectivity for that network service usage activity*” because the examples described in Cole take into consideration the communication interface that will be used for the network service usage activity. SAMSUNG-1005, ¶¶[0088]-[0089]; *see above* [1.4], [1.5].

ANALYSIS OF COLE, D’AMORE, RAO, AND FREUND

I. Overview of Freund

120. Freund discloses a “computing environment with methods for monitoring access to an open network, such as a WAN or the Internet. SAMSUNG-1008, Abstract. Freund’s computer environment includes a system

with one or more clients. SAMSUNG-1008, Abstract. Freund describes “[c]lient based monitoring and filtering of access” to include “[a]ccess rules which can be defined [to] specify criteria such as total time a user can be connected to the Internet ..., time a user can interactively use the Internet ..., a list of applications or application versions that a user can or cannot use in order to access the Internet, a list of URLs (or WAN addresses) that a user application can (or cannot) access, a list of protocols or protocol components ... that a user application can or cannot use, and rules to determine what events should be logged.” SAMSUNG-1008, Abstract. Freund’s system “can determine if a particular process in question should have access to the Internet and what kind of access ... is permissible for the given specific user.” *Id.*

II. Combination of Cole-D’Amore-Rao and Freund

121. It would have been obvious to a POSITA to combine CDR and the teachings of Freund such that Freund’s access rules would have been incorporated into the existing priority policies of CDR, to specify when internet access should be revoked for an application that exceeds an allowed usage limit. SAMSUNG-1005, ¶¶[0034]-[0036], ¶¶[0074]-[0097], FIG. 2; SAMSUNG-1006, ¶¶[0049]-[0060], FIG. 2; SAMSUNG-1007, ¶¶[0158]-[0159], ¶[0176], ¶[0180], ¶[0185], ¶[0191], FIG. 5A; SAMSUNG-1008, 4:5-19, 4:51-63, 10:44-58. A POSITA would have been motivated to combine the teachings of Freund into CDR because

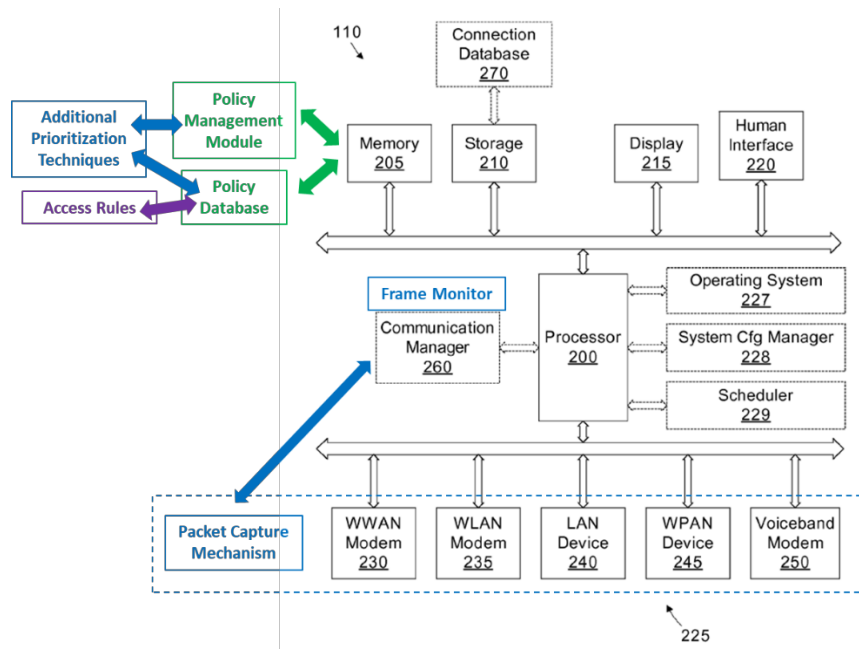
Cole describes that “operation of bandwidth intensive applications may significantly affect the user's service bill.” SAMSUNG-1005, ¶¶[0008], [0062], [0067], [0082]. A POSITA would have recognized or found obvious that the techniques of Freund would prevent an “intensive application” from consuming excessive network resources and creating a high “service bill.” *Id.*; SAMSUNG-1008, 4:5-19, 4:51-63, 10:44-58. Indeed, Gurnani, (a US Patent), corroborates “limiting service” in “mobile wireless communication subscribers” to “limit the customer’s ... financial exposure.” SAMSUNG-1014, 3:53-67, 4:1-45.

122. As explained below, combining CDR and Freund would have involved combining prior art elements according to known methods to yield predictable results. For example, Freund’s access limits would be incorporated as an additional condition to the CDR application priority policies, such that when an application reached its allowable usage limit, the connection manager would suspend or block execution until a later point in time. SAMSUNG-1005, ¶¶[0119]-[0125]; SAMSUNG-1006, ¶¶[0050]-[0051]; SAMSUNG-1008, 4:5-19, 4:51-63.

123. Incorporating Freund’s access rules into CDR’s priority policies would have been predictable and foreseeable with a reasonable expectation of success because Freund’s access rules are maintained in a “database” implemented in “memory” (much like the CDR “policy database”) and the resulting actions are

capable of being implanted by the CDR connection manager (e.g., “blocking access”). SAMSUNG-1005, ¶¶[0119]-[0125]; SAMSUNG-1006, ¶[0050]; SAMSUNG-1008, 4:5-29, 8:1-10. Moreover, like CDR, Freund describes that its techniques can be implemented in a “mobile computer.” SAMSUNG-1005, ¶¶[0014]-[0015], SAMSUNG-1006, ¶¶[0007]-[0016]; SAMSUNG-1007, ¶[0130]; SAMSUNG-1008, 5:14-16.

124. In an example of the combined system, illustrated below in Cole’s Figure 2, Freund’s access rules would have further enhanced the policy management module of the CDR mobile device to include revoking or deferring internet access for applications that exceed internet access limitations. SAMSUNG-1005, ¶¶[0034]-[0036], [0074]-[0097]; SAMSUNG-1008, 4:5-19, 4:51-63, 10:44-58. In doing so, the device in the CDR-Freund combination (hereinafter referred to as “**CDR-Freund**”) would have been able to more effectively use available network connections by revoking access for applications that consume more than an allowable amount of bandwidth or resources (one of the main objectives of Cole). SAMSUNG-1005, ¶¶[0006]-[0011].



SAMSUNG-1005, FIG. 2 (modified based on CDR-Freund combination).

III. Claims 13-15 are rendered obvious by Cole, D’Amore, Rao, and Freund

[13] The wireless end-user communications device of claim 1, wherein the processor is further configured to monitor network service usage behavior for each of the plurality of applications, and wherein the dynamic selection of the service usage control policy for a given network service usage activity is further based on a comparison of the monitored network service usage behavior for the application associated with the given network service usage activity to expected access limits for that application.

125. Freund, like CDR, describes that individual application “usage” can be “monitor[ed],” and further that describes “track[ing] Internet access on a per application basis” (“*monitor network service usage behavior for each of the plurality of applications*”). SAMSUNG-1008, 10:44-58; *see above* [2]. Freund’s “monitoring” includes “the total time applications access the Internet, and/or

monitoring the total time particular users/work stations access the Internet.” *Id.*, 10:5-15.

126. A POSITA would have recognized or found obvious that Freund’s “access rules” would be used by CDR-Freund’s connection manager to revoke or defer network access for activities and applications that exceed specified access limits (“*dynamic selection of [a] service usage control policy for a given network service usage activity*”). SAMSUNG-1005, ¶¶[0074]-[0097]; SAMSUNG-1008, 4:5-19; *see above* Section II, [1.4], [1.5].

127. Freund describes that “access rules” can be used to restrict or block network access upon reaching an access limit (“*further based on a comparison of the monitored network service usage behavior ... to expected access limits*”). SAMSUNG-1008, 4:5-19.

128. Moreover, a POSITA would have recognized or found obvious that because Cole’s processor is configured to implement the connection manager and execute “various software applications,” Cole’s processor would have been “*configured to*” perform the features of [13]-[14], as described above and below. SAMSUNG-1005, ¶¶[0015], [0034]-[0036], [0153], FIG. 2; *see above* [1.2], *below* [14].

129. As described above, the CDR-Freund device makes classification decisions on an activity/application basis, and would apply similar methodology in

implementing “access rules,” such that they are applied “*for each of the plurality of applications*” and with respect to “*expected access limits for that application.*” SAMSUNG-1008, 4:5-63; *see above* [1.3], [1.4], [1.5]. A POSITA would be motivated to implement “access rules” for “each” of the applications on the mobile device because, as previously noted, not doing so would result in potentially overlooking a network service usage activity or application that could damage or otherwise consume significant network resources. SAMSUNG-1005, ¶[0008].

[14] The wireless end-user communication device of claim 13, wherein the dynamic selection of the service usage control policy restricts network access due to the monitored network service usage behavior exceeding the expected access limits for the application associated with the given network service usage activity.

130. Freund describes various “remedial actions” (“*restricts network access*”) that can be performed due to an access rule being violated to include access being “terminated, redirected, [or] modified.” SAMSUNG-1008, 4:51-63; *see above* [13]. In the CDR-Freund device, the connection manager would implement these actions in response to an access rule violation (a “*dynamic selection of [a] service usage control policy*”). SAMSUNG-1005, ¶¶[0119]-[0125]; *see above* [1.4], [1.5].

131. As described above in [13], the CDR-Freund device makes classification decisions on an activity/application basis, and would apply similar methodology in implementing “access rules,” such that they are applied “*for each*

of the plurality of applications” and with respect to “expected access limits for that application.” SAMSUNG-1008, 4:5-63; see above [1.3], [1.4], [1.5].

[15] The wireless end-user communication device of claim 1, wherein the second policy limits an allowable duration of network access events for a given application.

132. As described in [13], Freund’s “access rules” can include “**permitted time limits**” a user can be connected to the Internet” (“*allowable duration of network access events*”). SAMSUNG-1008, 25:4-5; see above [13], [14]. As described above, Freund describes “track[ing] Internet access on a **per application basis**” (“*for a given application*”). SAMSUNG-1008, 10:5-15; see above [1.4], [1.5], [13].

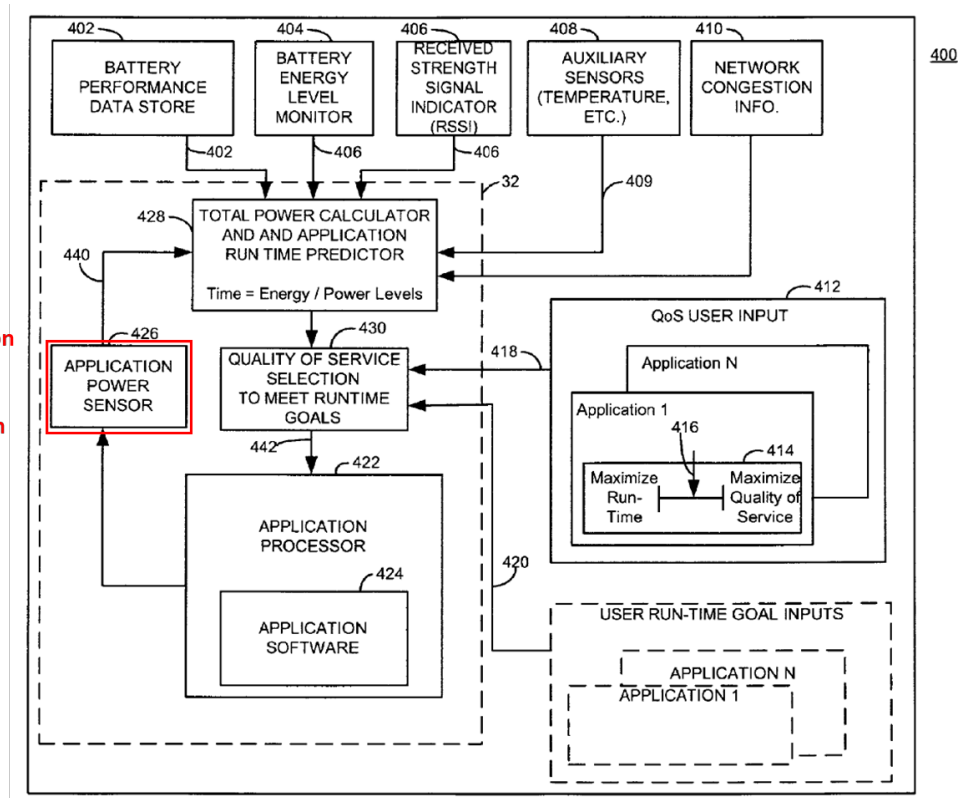
133. Moreover, as described above, the CDR-Freund device makes classification decisions on an activity/application basis, and would apply similar methodology in implementing “access rules,” such that they are applied for “*a given application.*” SAMSUNG-1008, 4:5-63; see above [1.3], [1.4], [1.5]. For instance, when evaluating a window of “connectivity state,” the CDR-Freund scheduler would be configured such that the connectivity window is an “*allowable duration of network access events*” as attempting to execute an activity with a longer estimated completion time would result in a failure. SAMSUNG-1005, ¶¶[0124]-[0127].

ANALYSIS OF COLE, D'AMORE, RAO, AND ALEKSIC

I. Overview of Aleksic

134. Aleksic describes “a controller that is responsive to a remaining power capacity of [a] battery” in a portable device. SAMSUNG-1011, Abstract. The controller “provides power for a higher priority feature at the expense of a lower priority functional processing capability feature.” *Id.* Aleksic describes that these “features” can be “software applications.” SAMSUNG-1011, ¶[0003], ¶[0028], ¶[0033], FIG. 10, FIG. 13. Aleksic’s controller includes an “application power sensor” that can “determine how much power is being consumed when executing [an] application.” SAMSUNG-1011, ¶¶[0035]-[0038].

Aleksic’s application power sensor measures power consumption on an “application level”



SAMSUNG-1011, FIG. 4.

II. Combination of Cole-D'Amore-Rao and Aleksic

135. It would have been obvious to a POSITA to combine CDR and the teachings of Aleksic such that Aleksic's application sensors would have enhanced the existing battery monitoring of Cole's connection manager, such that the connection manager could determine "how much power is being consumed when executing [an] application." SAMSUNG-1005, ¶¶[0034]-[0036], ¶¶[0074]-[0100], FIG. 2; SAMSUNG-1011, ¶¶[0035]-[0038], FIG. 4. A POSITA would have been motivated to combine the teachings of Aleksic into CDR because Aleksic's "application level power management system 400" would allow the CDR device to determine at the application level, "how much power is being consumed when executing [an] application" which would further enhance the ability of the connection manager to make deferral and rescheduling decisions based on "power state of the mobile device." SAMSUNG-1005, ¶¶[0088]-[0100]; SAMSUNG-1011, ¶¶[0035]-[0038]; *see above* [1.4], [1.5], [6]. Incorporating application level power consumption monitoring into the CDR device would also allow application power consumption behavior analysis that the connection manager would use to identify power-intensive applications and activities. *Id.*

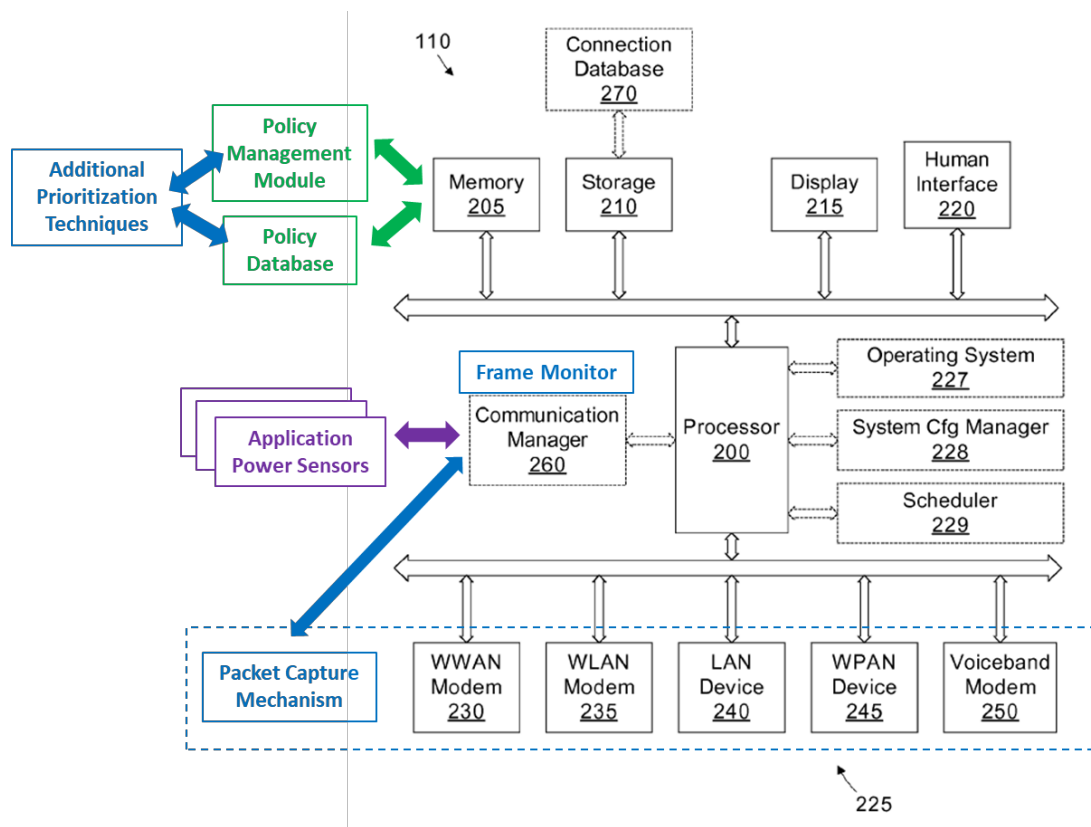
136. As explained below, combining CDR and Aleksic would have involved (1) combining prior art elements according to known methods to yield

predictable results; and (2) use of known technique to improve similar devices (methods, or products) in the same way.

137. Incorporating Aleksic's application power sensors as program modules into CDR's end-user device would have been predictable and foreseeable with a reasonable expectation of success because Cole describes that the operating system 227 "monitors and predicts battery life" and that the connection manager "interfaces with the operating system 227 to identify the current operating mode and power state." SAMSUNG-1005, ¶¶[0088]-[0100]; SAMSUNG-1011, SAMSUNG-1011, ¶¶[0035]-[0038], ¶[0041], FIG. 4, FIG. 5. Moreover, like Cole, D'Amore, and Rao, Aleksic describes that its techniques can be implemented in end-user devices (a "portable device"). SAMSUNG-1005, ¶¶[0014]-[0015], SAMSUNG-1006, ¶¶[0007]-[0016]; SAMSUNG-1007, ¶[0130]; SAMSUNG-1011, Abstract, ¶[0022].

138. In the combined system, illustrated below in Cole's Figure 2, Aleksic's application power sensors would have further enhanced the ability of the CDR connection manager to respond undesirable battery consumption associated with certain application activities, such that more accurate deferral and rescheduling decisions would be made regarding power consumption. SAMSUNG-1005, ¶¶[0034]-[0036], ¶¶[0074]-[0100], FIG. 2; SAMSUNG-1011, ¶¶[0035]-[0038], FIG. 4. For example, when starting a known power-intensive

application, the connection manager would be able to expediently identify, based on past monitoring of that application, that device power level did not support the application's activity, and as a result, recommend deferral or rescheduling. *Id.* In doing so, the Cole-D'Amore-Rao-Aleksic (hereinafter referred to as “**CDR-Aleksic**”) device would have been able to more effectively use device battery power (one of the purposes of Cole's connection manager) by identifying application activities that have excessive power consumption. SAMSUNG-1005, ¶¶[0090]-[0100].



SAMSUNG-1005, FIG. 2 (modified based on CDR-Aleksic combination).

III. Claim 12 is rendered obvious by Cole, D’Amore, Rao, and Aleksic

[12] The wireless end-user communications device of claim 1, wherein the processor is further configured to monitor power consumption for each of the plurality of applications, and wherein the dynamic selection of the service usage control policy for a given network service usage activity is further based on the monitored power consumption for the application associated with the given network service usage activity.

139. Aleksic describes an “**application level** power management system 400” that includes an “application power sensor” that can “**determine how much power is being consumed** when executing [an] application” (“*monitor power consumption for each of the plurality of applications*”). SAMSUNG-1011, ¶¶[0035]-[0038]. Aleksic describes monitoring this information for “controlling, at an application level [(“*each of the plurality of applications*”)], **operation of an application** ... based on a determined signal strength and battery capacity level.” *Id.*, ¶[0028]. In incorporating Aleksic into the CDR combination, the deferral and rescheduling decisions of the connection manager would be further enhanced by Aleksic’s “application level” measurement of power consumption (“*dynamic selection of the service usage control policy for a given network service usage activity*”). SAMSUNG-1005, ¶¶[0088]-[0100]; SAMSUNG-1011, ¶¶[0028], [0035]-[0038].

140. Indeed, Cole describes that the connection manager can identify and defer application activities that consume significant battery power (“the lengthy

transfer is conducted using the WWAN modem 230 (e.g., a 3G channel), **which consumes significant battery power**"). SAMSUNG-1005, ¶¶[0088]-[0100]. In implementing the CDR-Aleksic combination, application power sensors would assist the connection manager in making deferral decisions based on monitoring power consumption "at the application level" ("*dynamic selection of the service usage control policy ... based on the monitored power consumption for the application associated with the given network service usage activity*"). *Id.*; SAMSUNG-1011, ¶¶[0028], [0035]-[0038].

141. Moreover, a POSITA would have recognized or found obvious that because Cole's processor is configured to implement the connection manager and execute "various software applications," Cole's processor would have been "*configured to*" perform the features of [12], as described above. SAMSUNG-1005, ¶¶[0015], [0034]-[0036], [0153], FIG. 2; *see above* [1.2].

142. As described above, the CDR-Aleksic device makes classification decisions on an activity/application basis, and would apply similar methodology in "*monitor[ing] power consumption*" for "*each of [a] plurality of applications.*" SAMSUNG-1008, 4:5-63; *see above* [1.3], [1.4], [1.5].

ADDITIONAL REMARKS

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

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

Dated: 20 July 2023

By: 

APPENDIX A

Patrick Gerard Traynor

Professor

Associate Chair for Research in CISE

John and Mary Lou Dasburgh Preeminent Chair in Engineering

Department of Computer & Information Science & Engineering (CISE)

University of Florida

E301 CSE Building, PO Box 116120

Gainesville, FL 32611 USA

traynor@cise.ufl.edu

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

Table of Contents

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

B. Special Activities 43

EDUCATIONAL BACKGROUND

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

EMPLOYMENT HISTORY

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

CURRENT FIELDS OF INTEREST

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

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

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

I. TEACHING

A. Courses Taught

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

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

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

B. Continuing Education

None.

C. Curriculum Development

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

company to potential investors.

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

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

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

D. Individual Student Guidance

1. Research Scientists Supervised

None.

2. Ph.D. Students Graduated

Chaitrali Amrutkar Georgia Institute of Technology

Fall 2009–Fall 2013

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

Jasmine Bowers University of Florida

Fall 2015–Summer 2020

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

Henry “Hank” Carter Georgia Institute of Technology

Fall 2010–Spring 2016

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

Italo Dacosta Georgia Institute of Technology

Fall 2008–Summer 2012

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

David Dewey Georgia Institute of Technology

Fall 2011–Summer 2015

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

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

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

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

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

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

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

2. Ph.D. Students Supervised

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

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

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

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

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

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

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

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

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

3. Ph.D. Students - Other

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

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

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

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

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

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

4. M.S. Students Supervised

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

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

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

Christopher Grayson Georgia Institute of Technology

Fall 2012–Fall 2013

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

Young Seuk Kim Georgia Institute of Technology

Fall 2012–Fall 2013

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

Daniel Komaromy Georgia Institute of Technology

Fall 2008–Summer 2009

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

Nigel Lawrence Georgia Institute of Technology

Fall 2011–Spring 2012

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

Philip Marquardt Georgia Institute of Technology

Fall 2009–Present

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

Rishikesh Naik Georgia Institute of Technology

Fall 2008–Spring 2010

Research on converting expensive cryptographic primitives (e.g., Secure Function Evaluation) into efficient applications for mobile phones. Now with Cisco Systems.

Ashish Nautiyal CISE

Fall 2015–Spring 2016

Research on connecting telephone calls to the larger authentication infrastructure.

Nilesh Nipane Georgia Institute of Technology

Fall 2008–Spring 2010

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

Walter “Nolen” Sciafe Georgia Institute of Technology

Spring 2012–Spring 2014

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

Tyler Tucker University of Florida

Fall 2018–Spring 2021

Evaluating the security of Bluetooth radios.

5. M.S. Special Problems Students

Siddhant Deshmukh University of Florida

Fall 2016–Present

Developed tools for analysis of mobile digital financial services.

Chinmay Gangakhedkar Georgia Institute of Technology

Spring 2009

Research on multi-factor authentication using mobile phones.

Christopher Grayson Georgia Institute of Technology
Spring 2013

Research on continuous authentication using mobile phones.

Aarushi Karnany University of Florida
Fall 2016–Present

Developed tools for analysis of mobile digital financial services.

Rohit Matthews Georgia Institute of Technology
Spring 2011

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

Ashwin Narasimhan Georgia Institute of Technology
Spring 2009

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

Aamir Poonawalla Georgia Institute of Technology
Spring 2010

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

Erin Reddick Georgia Institute of Technology
Fall 2008–Fall 2009

Research on IPTV security with GTRI.

Lalanthika Vasudevan Georgia Institute of Technology
Spring 2009

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

6. Undergraduate Special Problems Students

Ethan Shernan Georgia Institute of Technology
Spring 2014

Developed an infrastructure for detecting billing bypass fraud attacks.

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

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

Dane Van Dyck Georgia Institute of Technology
Summer 2009

Research on virtualization support for mobile phones.

E. Teaching Honors and Awards

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

II. RESEARCH AND CREATIVE SCHOLARSHIP

A. Thesis

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

B. Published Journal Papers (Refereed)

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

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

C. Published Books and Parts of Books

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

D. Edited Proceedings

None.

E. Conference Presentations

E.1. Conference Presentations with Proceedings (Refereed)

1. Christian Peeters, Tyler Tucker, Anushri Jain, Kevin Butler, and Patrick Traynor. LeopardSeal: Detecting Call Interception via Audio Rogue Base Stations. In *Proceedings of the ACM International Conference on Mobile Systems, Applications and Services (MobiSys)*, 2023.
2. Tyler Tucker, Hunter Searle, Kevin Butler, and Patrick Traynor. Blue's Clues: Practical Discovery of Non-Discoverable Bluetooth Devices. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2023.
3. Hadi Abdullah, Aditya Karlekar, Saurabh Prasad, Muhammad Sajidur Rahman, Logan Blue, Luke Bauer, Vincent Bindschaedler, and Patrick Traynor. Attacks as Defenses: Designing Robust Audio CAPTCHAs Using Attacks on Automatic Speech Recognition Systems. In *Symposium on Network and Distributed System Security (NDSS)*, 2023.
4. Daniel Olszewski, Sandeep Sathyanarayana, Weidong Zhu, Kevin Butler, and Patrick Traynor. HallMonitor: A Framework for Identifying Network Policy Violations in Software. In *IEEE Conference on Communications and Network Security (CNS)*, 2022.
5. Hadi Abdullah, Aditya Karlekar, Vincent Bindschaedler, and Patrick Traynor. Demystifying Limited Adversarial Transferability in Automatic Speech Recognition Systems. In *Proceedings of the International Conference on Learning Representations (ICLR)*, 2022. (Acceptance rate: 32%).
6. Logan Blue, Kevin Warren, Hadi Abdullah, Cassidy Gibson, Luis Vargas, Jessica O'Dell, Kevin Butler, and Patrick Traynor. Who Are You (I Really Wanna Know)? Detecting Audio DeepFakes Through Vocal Tract Reconstruction. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2022. (Acceptance rate: 17.2%).
7. Grant Hernandez, Marius Muench, Dominik Maier, Alyssa Milburn, Shinjo Park, Tobias Scharnowski, Tyler Tucker, Patrick Traynor, and Kevin R. B. Butler. FirmWire: Transparent Dynamic Analysis for Cellular Baseband Firmware. In *Symposium on Network and Distributed System Security (NDSS)*, 2022. (Acceptance rate: 16.2%).
8. Christian Peeters, Christopher Patton, Imani N. Sherman, Daniel Olszewski, Thomas Shrimpton, and Patrick Traynor. SMS OTP Security (SOS): Hardening SMS-Based Two Factor Authentication. In *ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2022. (Acceptance rate: 18.2%).

9. Hadi Abdullah, Muhammad Sajidur Rahman, Christian Peeters, Cassidy Gibson, Washington Garcia, Vincent Bindschaedler, Thomas Shrimpton, and Patrick Traynor. Beyond L_p Clipping: Equalization based Psychoacoustic Attacks against ASRs. In *The Asian Conference on Machine Learning (ACML)*, 2021.
10. Imani Sherman and Daniel Delgado and Juan Gilbert and Jaime Ruiz and Patrick Traynor. Characterizing User Comprehension in the STIR/SHAKEN Anti-Robocall Standard. In *Proceedings of the Annual Research Conference on Communications Information and Internet Policy (TPRC 49)*, 2021.
11. Hadi Abdullah, Kevin Warren, Vincent Bindschaedler, Nicolas Papernot, and Patrick Traynor. The Faults in our ASRs: An Overview of Attacks against Automatic Speech Recognition and Speaker Identification Systems. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2021. (Acceptance rate: 12.1%).
12. Hadi Abdullah, Muhammad Sajidur Rahman, Washington Garcia, Logan Blue, Kevin Warren, Anurag Swarnim Yadav, Tom Shrimpton, and Patrick Traynor. Hear “No Evil”, See “Kenansville”: Efficient and Transferable Black-Box Attacks on Speech Recognition and Voice Identification Systems. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2021. (Acceptance rate: 12.1%).
13. Imani Sherman, Jasmine Bowers, Liz-Laure Laborde, Juan E. Gilbert, Jaime Ruiz, and Patrick Traynor. Truly Visual Caller ID? An Analysis of Anti-Robocall Applications and their Accessibility to Visually Impaired Users. In *IEEE International Symposium on Technology and Society (IEEE ISTAS)*, 2020.
14. Imani Sherman, Jasmine Bowers, Keith McNamara, Juan Gilbert, Jaime Ruiz, and Patrick Traynor. Are You Going to Answer That? Measuring User Responses to Anti-Robocall Application Indicators. In *Proceedings of the ISOC Network & Distributed Systems Security Symposium (NDSS)*, 2020. (Acceptance rate: 17.4%).
15. Joseph Choi, Dave Tian, Grant Hernandez, Christopher Patton, Benjamin Mood, Thomas Shrimpton, Patrick Traynor, and Kevin Butler. A Hybrid Approach to Secure Function Evaluation Using SGX. In *Proceedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS’19)*, 2019. (Acceptance Rate: 17.0% for full papers).
16. Vanessa Frost, Dave Tian, Christie Ruales, Patrick Traynor, and Kevin Butler. Examining DES-based Cipher Suite Support within the TLS Ecosystem. In *Proceedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS’19)*, 2019. (Acceptance Rate: 22.0% for all papers).
17. Dave Tian, Joseph Choi, Grant Hernandez, Patrick Traynor, and Kevin Butler. A Practical Intel SGX Setting for Linux Containers in the Cloud. In *Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY’19)*, 2019. (Acceptance rate: 23.5%).
18. Nolen Scaife, Jasmine Bowers, Christian Peeters, Grant Hernandez, Imani Sherman, Lisa Anthony, and Patrick Traynor. Kiss from a Rogue: Evaluating Detectability of Pay-at-the-Pump Card Skimmers. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2019. (Acceptance rate: 12.0%).
19. Jasmine Bowers, Imani Sherman, Kevin Butler, and Patrick Traynor. Characterizing Security and Privacy Practices in Emerging Digital Credit Applications. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2019. (Acceptance rate: 25.6%).
20. Hadi Abdullah, Washington Garcia, Christian Peeters, P. Traynor, K. Butler, and J. Wilson. Practical Hidden Voice Attacks against Speech and Speaker Recognition Systems. In *Proceedings of the ISOC Network & Distributed Systems Security Symposium (NDSS)*, 2019. (Acceptance Rate: 17.1%).

21. Lius Vargas, Logan Blue, Vanessa Frost, Christopher Patton, N. Scaife, K. Butler, and P. Traynor. Digital Healthcare-Associated Infection Analysis of a Major Multi-Campus Hospital System. In *Proceedings of the ISOC Network & Distributed Systems Security Symposium (NDSS)*, 2019. (Acceptance Rate: 17.1%).
22. Dominik Wermke, Nicolas Huaman, Yasemin Acar, Bradley Reaves, Patrick Traynor, and Sascha Fahl. A Large Scale Investigation of Obfuscation Use in Google Play. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2018. Acceptance Rate: 20.1%.
23. Nolen Scaife, Christian Peeters, and Patrick Traynor. Fear the Reaper: Characterization and Fast Detection of Card Skimmers. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2018. Acceptance Rate: 19.0%.
24. Dave (Jing) Tian, Grant Hernandez, Joseph Choi, Vanessa Frost, Christie Raules, Kevin Butler, Patrick Traynor, Hayawardh Vijayakumar, Lee Harrison, Amir Rahmati, and Mike Grace. AT-tention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2018. Acceptance Rate: 19.0%.
25. Logan Blue, Hadi Abdullah, Luis Vargas, and Patrick Traynor. 2MA: Verifying Voice Commands via Two Microphone Authentication. In *ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2018. (Acceptance Rate: 20.0%).
26. Nolen Scaife, Christian Peeters, Camilo Velez, Hanqing Zhao, Patrick Traynor, and David Arnold. The Cards Aren't Alright: Detecting Counterfeit Gift Cards Using Encoding Jitter. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2018. (Acceptance Rate: 10.4%).
27. Christian Peeters, Hadi Abdullah, Nolen Scaife, Jasmine Bowers, Patrick Traynor, Bradley Reaves, and Kevin Butler. Sonar: Detecting SS7 Redirection Attacks Via Call Audio-Based Distance Bounding. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2018. (Acceptance Rate: 10.4%).
28. Tyler Ward, Joseph Choi, Kevin Butler, John M. Shea, Patrick Traynor, and Tan Wong. Privacy Preserving Localization Using a Distributed Particle Filtering Protocol. In *IEEE MILCOM*, 2017. (Acceptance Rate: 56%).
29. Bradley Reaves and Logan Blue and Hadi Abdullah and Luis Vargas and Patrick Traynor and Thomas Shrimpton. AuthentiCall: Efficient Identity and Content Authentication for Phone Calls. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2017. (Acceptance Rate: 16.3%).
30. Jasmine Bowers and Bradley Reaves and Imani N. Sherman and Patrick Traynor and Kevin Butler. Regulators, Mount Up! Analysis of Privacy Policies for Mobile Money Applications. In *Proceedings of the USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2017. (Acceptance Rate: 26.5%).
31. Bradley Reaves, Logan Blue, and Patrick Traynor. AuthLoop: End-to-End Cryptographic Authentication for Telephony over Voice Channels. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2016. (Acceptance Rate: 15.5%).
32. Dave Tian, Nolen Scaife, Adam Bates, Kevin Butler, and Patrick Traynor. Making USB Great Again with USBFILTER. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2016. (Acceptance Rate: 15.5%).
33. Bradley Reaves, Dave Tian, Logan Blue, Patrick Traynor, and Kevin Butler. Detecting SMS Spam in the Age of Legitimate Bulk Messaging. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2016. (Acceptance Rate: 35.0%).

34. Nolen Scaife, Henry Carter, Patrick Traynor, and Kevin Butler. CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. In *IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2016. (Acceptance Rate: 17.6%).
35. Bradley Reaves, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, and Kevin Butler. Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2016. (Acceptance Rate: 13.0%).
36. Benjamin Mood, Debayan Gupta, Henry Carter, Kevin Butler, and Patrick Traynor. Frigate: A Validated, Extensible, and Efficient Compiler and Interpreter for Secure Computation. In *Proceedings of the IEEE European Symposium on Security and Privacy*, 2016. (Acceptance Rate: 17.3%).
37. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Outsourcing Secure Two-Party Computation as a Black Box. In *Proceedings of the International Conference on Cryptology and Network Security*, 2015. (Acceptance Rate: 52.9%).
38. Nolen Scaife, Henry Carter, and Patrick Traynor. OnionDNS: A Seizure-Resistant Top-level Domain. In *Proceedings of the IEEE Conference on Communications and Network Security (CNS)*, 2015. (Acceptance Rate: 28.1%).
39. Bradley Reaves, Nolen Scaife, Adam Bates, Patrick Traynor, and Kevin Butler. Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2015. (Acceptance Rate: 15.7%).
40. Bradley Reaves, Ethan Shernan, Adam Bates, Henry Carter, and Patrick Traynor. Boxed Out: Blocking Cellular Interconnect Bypass Fraud at the Network Edge. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2015. (Acceptance Rate: 15.7%).
41. David Dewey, Bradley Reaves, and Patrick Traynor. Uncovering Use-After-Free Conditions In Compiled Code. In *Proceedings of the International Conference on Availability, Reliability and Security (ARES)*, 2015. (Acceptance Rate: 22%).
42. Ethan Shernan, Henry Carter, Dave Tian, Patrick Traynor, and Kevin Butler. More Guidelines Than Rules: CSRF Vulnerabilities from Noncompliant OAuth 2.0 Implementations. In *Proceedings of the International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA)*, 2015. (Acceptance Rate: 22.7%).
43. Henry Carter, Charles Lever, and Patrick Traynor. Whitewash: Outsourcing Garbled Circuit Generation for Mobile Devices. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2014. (Acceptance Rate: 19.9%).
44. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Secure Outsourced Garbled Circuit Evaluation for Mobile Devices. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2013. (Acceptance Rate: 16.2%).
45. Chaitrali Amrutkar, Matti Hiltunen, Shobha Venkataraman, Kaustubh Joshi, Patrick Traynor, Trevor Jim, and Oliver Spatscheck. Why is My Smartphone Slow? On The Fly Diagnosis of Poor Performance on the Mobile Internet. In *Proceedings of The 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2013. (Acceptance Rate: 19.6%).
46. Saurabh Chakradeo, Brad Reaves, Patrick Traynor, and William Enck. MAST: Triage for Market-scale Mobile Malware Analysis. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2013. (Acceptance Rate: 15.0%)(Best Paper).
47. Charles Lever, Manos Antonakakis, Brad Reaves, Patrick Traynor, and Wenke Lee. The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2013. (Acceptance rate: 18.8%).

48. Chaitrali Amrutkar, Kapil Singh, Arunabh Verma, and Patrick Traynor. VulnerableMe: Measuring Systemic Weaknesses in Mobile Browser Security. In *Proceedings of the International Conference on Information Systems Security (ICISS)*, 2012. (Acceptance rate: 25%) (Best Paper - SAIC Student Paper Competition (GT)) (Finalist - CSAW AT&T Applied Security Research Best Paper Competition 2012).
49. Chaitrali Amrutkar, Patrick Traynor, and Paul van Oorschot. A Measurement Study of SSL Indicators on Mobile Browsers: Extended Life, or End of the Road? In *Proceedings of the Information Security Conference (ISC)*, 2012. (Acceptance rate: 32%) (Best Student Paper).
50. Italo Dacosta, Mustaque Ahamad, and Patrick Traynor. Trust No One Else: Detecting MITM Attacks Against SSL/TLS Without Third-Parties. In *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, 2012. (Acceptance Rate: 20.2%).
51. Adam Bates, Kevin Butler, Micah Sherr, Clay Shields, Patrick Traynor, and Dan Wallach. Accountable Wiretapping -or- I Know They Can Hear You Now. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2012. (Acceptance Rate: 17.8%).
52. Yacin Nadji, Jon Giffin, and Patrick Traynor. Automated Remote Repair for Mobile Malware. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2011. (Acceptance Rate: 18.5%).
53. Nilesh Nipane, Italo Dacosta, and Patrick Traynor. "Mix-In-Place" Anonymous Networking Using Secure Function Evaluation. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2011. (Acceptance Rate: 18.5%).
54. Philip Marquardt, Arunabh Verma, Henry Carter, and Patrick Traynor. (sp)iPhone: Decoding Vibrations From Nearby Keyboards Using Mobile Phone Accelerometers. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2011. (Acceptance Rate: 13.9%).
55. Philip Marquardt, David Dagon, and Patrick Traynor. Impeding Individual User Profiling in Shopper Loyalty Programs. In *Proceedings of the International Conference on Financial Cryptography and Data Security (FC)*, 2011. (Acceptance Rate: 35.1%).
56. David Dewey and Patrick Traynor. No Loitering: Exploiting Lingering Vulnerabilities in Default COM Objects. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2011. (Acceptance Rate: 20.1%).
57. Vijay Balasubramaniyan, Aamir Poonawalla, Mustaque Ahamad, Michael Hunter, and Patrick Traynor. PinDrOp: Using Single-Ended Audio Features to Determine Call Provenance. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2010. (Acceptance Rate: 17.2%).
58. Patrick Traynor, Joshua Schiffman, Thomas La Porta, Patrick McDaniel, Abhrajit Ghosh, and Farooq Anjum. Constructing Secure Localization Systems with Adjustable Granularity. In *IEEE Global Communications Conference (GLOBECOM)*, 2010. (Acceptance Rate: 35.6%).
59. Patrick Traynor. Characterizing the Security Implications of Third-Party EAS Over Cellular Text Messaging Services. In *Proceedings of the Second IEEE International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2010. (Acceptance Rate: 25.0%).
60. Kapil Singh, Samrit Sangal, Nehil Jain, Patrick Traynor, and Wenke Lee. Evaluating Bluetooth as a Medium for Botnet Command and Control. In *Proceedings of the International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA)*, 2010. (Acceptance Rate: 30.7%).

61. Italo Dacosta and Patrick Traynor. Proxychain: Developing a Robust and Efficient Authentication Infrastructure for Carrier-Scale VoIP Networks. In *Proceedings of the USENIX Annual Technical Conference (ATC)*, 2010. (Acceptance Rate: 17.0%).
62. Frank S. Park, Chinmay Gangakhedkar, and Patrick Traynor. Leveraging Cellular Infrastructure to Improve Fraud Prevention. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2009. (Acceptance Rate: 19.0%).
63. Patrick Traynor, Michael Lin, Machigar Ongtang, Vikyath Rao, Trent Jaeger, Thomas La Porta, and Patrick McDaniel. On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2009. (Acceptance Rate: 18.4%).
64. Brendan Dolan-Gavitt, Abhinav Srivastava, Patrick Traynor, and Jonathon Giffin. Robust Signatures for Kernel Data Structures. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2009. (Acceptance Rate: 18.4%).
65. Italo Dacosta, Vijay Balasubramaniyan, Mustaque Ahamad, and Patrick Traynor. Improving Authentication Performance of Distributed SIP Proxies. In *Proceedings of the Conference on Principles, Systems and Applications of IP Telecommunications (IPTComm)*, 2009. (Acceptance Rate: 43.3%).
66. Patrick Traynor, Kevin Butler, William Enck, and Patrick McDaniel. Realizing Massive-Scale Conditional Access Systems Through Attribute-Based Cryptosystems. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2008. (Acceptance Rate: 17.7%).
67. Patrick Traynor, Patrick McDaniel, and Thomas La Porta. On Attack Causality in Internet-Connected Cellular Networks. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2007. (Acceptance Rate: 12.3%).
68. Sunam Ryu, Kevin Butler, Patrick Traynor, and Patrick McDaniel. Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems. In *Proceedings of the IEEE International Symposium on Security in Networks and Distributed Systems (SSNDS)*, 2007. (Acceptance Rate: 40%).
69. Luke St. Clair, Lisa Johansen, William Enck, Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Trent Jaeger. Password Exhaustion: Predicting the End of Password Usefulness. In *Proceedings of the International Conference on Information Systems Security (ICISS)*, 2006. (Invited Paper).
70. Kevin Butler, William Enck, Jennifer Plasterr, Patrick Traynor, and P. McDaniel. Privacy-Preserving Web-Based Email. In *Proceedings of the International Conference on Information Systems Security (ICISS)*, December 2006. (Acceptance Rate: 30.4%).
71. Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters. Secure Attribute-Based Systems. In *Proceedings of the Thirteenth ACM Conference on Computer and Communications Security (CCS)*, November 2006. (Acceptance Rate: 14.8%).
72. Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks. In *Proceedings of the Twelfth Annual ACM International Conference on Mobile Computing and Networking (MobiCom)*, September 2006. (Acceptance Rate: 11.7%).
73. Patrick Traynor, Michael Chien, Scott Weaver, Boniface Hicks, and Patrick McDaniel. Non-Invasive Methods for Host Certification. In *Proceedings of the Second IEEE International Conference on Security and Privacy in Communication Networks (SecureComm)*, August 2006. (Acceptance Rate: 25.4%).

74. Patrick Traynor, JaeShung Shin, Barat Madan, Shashi Phoha, and Thomas La Porta. Efficient Group Mobility for Heterogeneous Sensor Networks. In *Proceedings of the IEEE Vehicular Technology Conference (VTC Fall)*, September 2006. (Acceptance Rate: 58%).
75. Patrick Traynor, Raju Kumar, Hussain Bin Saad, Guohong Cao, and Thomas La Porta. LIGER: Implementing Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks. In *Proceedings of the 4th ACM International Conference on Mobile Systems, Applications and Services (MobiSys)*, June 2006. (Acceptance Rate: 15.4%).
76. Patrick Traynor, Guohong Cao, and Thomas La Porta. The Effects of Probabilistic Key Management on Secure Routing in Sensor Networks. In *Proceedings of the 2006 IEEE Wireless Communications and Networking Conference (WCNC)*, April 2006. (Acceptance Rate: 38.8%).
77. Patrick Traynor, Heesook Choi, Guohong Cao, Sencun Zhu, and Thomas La Porta. Establishing Pair-Wise Keys In Heterogeneous Sensor Networks. In *Proceedings of the 25th Annual IEEE Conference on Computer Communications (INFOCOM)*, April 2006. (Acceptance Rate: 18%).
78. William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. In *Proceedings of the Twelfth ACM Conference on Computer and Communications Security (CCS)*, November 2005. (Acceptance Rate: 15%).

Removed for external version.

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

None.

E.3. Conference Presentations without Proceedings

1. Patrick Traynor. Work in Progress Presentations: Fine-Grained Secure Localization for 802.11 Networks. 15th USENIX Security Symposium (SECURITY), August 2006.
2. Patrick Traynor. Work in Progress Presentations: Fundamental Limitations of Sensor Network Security. ACM/USENIX Fourth International Conference on Mobile Systems Applications and Services (MobiSys), June 2006. (Award: Most Entertaining WIP).
3. Patrick Traynor, Heesook Choi, Guohong Cao, and Thomas La Porta. Poster Session: Probabilistic Unbalanced Key Distribution and Its Effects on Distributed Sensor Networks. Workshop on Wireless Security (WiSe), October 2004.

F. Other

F.1. Submitted Journal Papers

None.

F.2. Refereed Research Reports

None.

F.3. Software

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

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

F.4. Published Papers (Non-Refereed)

1. Patrick Traynor. Characterizing the Limitations of Third-Party EAS Over Cellular Text Messaging Services. Technical report, 3G Americas Whitepaper, 2008.
2. Lisa Johansen, Kevin Butler, William Enck, Patrick Traynor, and Patrick McDaniel. Grains of SANs: Building Storage Area Networks from Memory Spots. Technical Report NAS-TR-0060-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, 2007.

F.5. Books in Preparation

None.

F.6. Workshops and External Courses

1. Luis Vargas, Patrick Emami, and Patrick Traynor. On the Detection of Disinformation Campaign Activity with Network Analysis. In *Proceedings of the 2020 ACM SIGSAC Cloud Computing Security Workshop, CCSW '20*, 2020.
2. Siddhant Deshmukh, Henry Carter, Grant Hernandez, Patrick Traynor, and Kevin Butler. Efficient and Secure Template Blinding for Biometric Authentication. In *IEEE Workshop on Security and Privacy in the Cloud (SPC)*, 2016.
3. Debayan Gupta, Benjamin Mood, Joan Feigenbaum, Kevin Butler, and Patrick Traynor. Using Intel Software Guard Extensions for Efficient Two-Party Secure Function Evaluation. In *Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC)*, 2016.
4. Chaitrali Amrutkar and Patrick Traynor. Rethinking Permissions for Mobile Web Apps: Barriers and the Road Ahead. In *Proceedings of the ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, 2012.
5. Nigel Lawrence and Patrick Traynor. Under New Management: Practical Attacks on SNMPv3. In *Proceedings of the USENIX Workshop on Offensive Technologies (WOOT)*, 2012.
6. Andrew Harris, Frank S. Park, Seymour Goodman, and Patrick Traynor. Emerging Privacy Concerns for Digital Wallet Deployment. In *Proceedings of the Workshop on Making Privacy in America*, 2009.
7. Patrick Traynor. Privacy and Security Concerns for Personal and Mobile Health Devices. In *Proceedings of the Workshop to Set A Research Agenda for Privacy and Security of Healthcare Technologies*, 2009.
8. Kevin Butler, William Enck, Harri Hursti, Stephen McLaughlin, Patrick Traynor, and Patrick McDaniel. Systemic Issues in the Hart InterCivic and Premier Voting System: Reflections Following Project EVEREST. In *Proceedings of the USENIX/ACCURATE Electronic Voting Technology (EVT) Workshop*, 2008.

G. Research Proposals and Grants (Principal Investigator)

1. Approved and Funded

1. Testing Audio Deep Fake Detectors

Sponsor: Bank of America

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

Amount: \$274,000 over 2 years

Awarded: August 2021

2. Deploying Defenses for Cellular Networks Using the AWARE Testbed

Sponsor: Department of Homeland Security: CISA:

Investigator(s): Patrick Traynor (PI), Kevin Butler, Guofei Gu, Radu Stoleru, Walter Magnussen, P. R. Kumar

Amount: \$3,100,000 over 4 years

Awarded: October 2019

3. SaTC: CORE: Medium: Securing the Voice Processing Pipeline Against Adversarial Audio

Sponsor: NSF Secure and Trustworthy Cyberspace

Investigator(s): Patrick Traynor (PI), Thomas Shrimpton, Vincent Bindschaedler

Amount: \$1,199,999 over 4 years

Awarded: October 2019

4. Artus Protocol STTR Phase II

Sponsor: Office of Naval Research

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

Amount: \$800,000 over 4 years

Awarded: August 2019

5. Evaluating the Security of QR Code-Based Payments

Sponsor: Discover Financial

Investigator(s): Patrick Traynor (PI)

Amount: \$50,000 over 1 year

Awarded: September 2018

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

Sponsor: NSF Secure and Trustworthy Cyberspace

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

Amount: \$50,000 over 1 year

Awarded: September 2017

7. Designing Strong End-to-End Authentication Mechanisms for Modern Telephony Systems

Sponsor: NSF Secure and Trustworthy Cyberspace

Investigator(s): Patrick Traynor (PI)

Amount: \$500,000 over 3 years

Awarded: July 2016

8. Digital Healthcare-Associated Infection: Measurement, Defense and Prevention in a Modern Digital Healthcare Ecosystem

Sponsor: National Science Foundation

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

Amount: \$1,200,000 over 4 years

Awarded: June 2016

9. **Evaluating and Improving Security in Emerging Branchless Banking Systems**
Sponsor: NSF Secure and Trustworthy Cyberspace
Investigator(s): Patrick Traynor (PI)
Amount: \$500,000 over 3 years
Awarded July 2015
10. **Prevention and Detection of Disallowed Connections in Mobile and Pervasive Systems**
Sponsor: CISE-ECE Harris Endowed Seed Fund Program
Investigator(s): Patrick Traynor (PI), Renato Figueiredo (PI)
Amount: \$40,000 over 1 year
Awarded December 2014
11. **Mobile Excursion Study Support**
Sponsor: Hanscom AFB Electronic Systems Command Development Planning Division (ESC/XR)
Investigator(s): Patrick Traynor (PI), Mustaque Ahamad, Jeff Evans, Chuck Bokath
Amount: \$280,000 over 3 months
Awarded July 2012
12. **Characterizing the Security Limitations of Accessing the Mobile Web**
Sponsor: NSF Secure and Trustworthy Cyberspace
Investigator(s): Patrick Traynor (PI) and William Enck (NC State)
Amount: \$334,000 over 3 years
Awarded July 2012
13. **Mitigating Attacks on Mobile Devices and Critical Cellular Infrastructure**
Sponsor: US Department of Defense - Defense University Research Instrumentation Program (DURIP)
Investigator(s): Patrick Traynor (PI), Jon Giffin, Mustaque Ahamad
Amount: \$210,081 over 1 year
Awarded June 2011
14. **Characterizing and Implementing Efficient Primitives for Privacy-Preserving Computation**
Sponsor: DARPA PROgramming Computation on EncryptEd Data (PROCEED) – Broad Agency Announcement
Investigator(s): Patrick Traynor (PI) and Kevin Butler (UOregon)
Amount: \$580,000 over 4 years
Awarded May 2011
15. **Security for Converged IMS Networks**
Sponsor: US Department of Defense
Investigator(s): Patrick Traynor (PI), Mustaque Ahamad and Russ Clark
Amount: \$242,401 over 1 year
Awarded August 2010
16. **CAREER: Protecting User Data on Lost, Stolen and Damaged Mobile Phones**
Sponsor: NSF Trustworthy Computing
Investigator(s): Patrick Traynor (PI)
Amount: \$400,000 over 5 years
Awarded: May 2010
17. **Provably Anonymous Networking Through Secure Function Evaluation**
Sponsor: NSF Trustworthy Computing
Investigator(s): Patrick Traynor (PI)
Amount: \$200,000 over 2 years
Awarded: July 2009

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

2. Pending

Removed for external version.

H. Research Proposals and Grants (Contributor)

1. Approved and Funded

1. **SaTC: Frontier: Securing the Future of Computing for Marginalized and Vulnerable Populations**
Sponsor: NSF SaTC
Investigator(s): Kevin Butler (PI), Patrick Traynor, Tadayoshi Kohno, 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 Perdesi.
7. Saurabh Chakradeo, College of Computing, Georgia Tech, Spring 2012.
Advisor: Professor Patrick Traynor.
8. Henry Carter, College of Computing, Georgia Tech, Spring 2012.
Advisor: Professor Patrick Traynor.
9. David Dewey, College of Computing, Georgia Tech, Spring 2012.
Advisor: Professor Jon Giffin.
10. Chaitrali Amrutkar, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Patrick Traynor.
11. Yacin Nadji, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Wenke Lee.
12. Yogesh Mundada, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Nick Feamster.
13. Hyojoon Kim, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Nick Feamster.
14. Ikpeme Erete, College of Computing, Georgia Tech, Spring 2011.
Advisor: Professor Alex Orso.
15. Chaitrali Amrutkar, College of Computing, Georgia Tech, Spring 2011.
Advisor: Professor Patrick Traynor.
16. Brendan Dolan-Gavitt, College of Computing, Georgia Tech, Spring 2011.
Advisor: Professor Wenke Lee and Professor Jon Giffin.
17. Sam Burnett, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Nick Feamster.
18. Cong Shi, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Mostafa Ammar and Professor Ellen Zegura.
19. Partha Kanuparth, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Constantine Dorvolis.
20. Long Lu, College of Computing, Georgia Tech, Spring 2010.
Advisor: Professor Wenke Lee.
21. Virendra Kumar, College of Computing, Georgia Tech, Spring 2009.
Advisor: Professor Alexandra Boldyreva.
22. Frank Park, College of Computing, Georgia Tech, Spring 2009.
Advisor: Professor Patrick Traynor.

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

E. External Member of M.S. Examining Committee

M.S. Thesis Defense Committees None.

F. Consulting and Advisory Appointments

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

G. Civic Activities

None.

IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION

A. Honors and Awards

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

B. Invited Conference Session Chairmanships

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

C. Professional Registration

None.

D. Patents

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

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

E. Editorial and Reviewer Work for Technical Journals and Publishers

Associate Editor:

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

Guest Editor:

Journals

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

Reviewer for:

Journals

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

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

Conferences and Workshops

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

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

F. Expert Witness Services

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

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

V. OTHER CONTRIBUTIONS

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

1. Keynote: Well, It Worked on My Computer: Reproducibility, Tech Transfer, and Computer Security Research. National Science Foundation Secure and Trustworthy Cyberspace (SaTC) Vision 2.0 Workshop, March 2023. University of Texas at Dallas.
2. Humans vs The Computer Interfaces: Separating Deepfakes/Bots from People Using Psychoacoustics. UCLA Electrical and Computer Engineering Distinguished Seminar, February 2023. University of California, Los Angeles.
3. Keynote: Exploiting the Gaps Between Human and Machine Understanding of Audio: Frameworks, Attacks, and Defenses. ISCA Symposium on Security and Privacy in Speech Communication (SPSC), November 2021. Virtual.
4. The State of Voice Cloning Technology. Federal Trade Commission (FTC) Workshop on Voice Cloning Technologies, January 2020. Washington, DC.
5. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. North Carolina State University Department of Computer Science Colloquium, January 2020. Raleigh, NC.
6. Moving from research to practice: How to maximize the impact of SaTC projects. National Science Foundation Secure and Trustworthy Cyberspace (SaTC) PI Meeting, October 2019. Alexandria, VA.
7. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. Purdue University Computer Science Excellence Lecture Series, October 2019. West Lafayette, IN.
8. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. Bank of America - Colloquium Series, March 2019. Charlotte, NC.
9. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. CISPA – Helmholtz Center for Information Security, Saarland University, February 2019. Saarbrücken, Germany.
10. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. University of Maryland - Distinguished Colloquium, February 2019. College Park, MD.
11. Responsible Finance for the Digital Client. Foromic Conference, October 2018. Barranquilla, Colombia.
12. Panel: Authentication Challenges for New Interfaces, Devices, and Wireless Networks. ACM Conference on Security and Privacy in Wireless and Mobile Networks, June 2018. Stockholm, Sweden.
13. Sonar: Detecting SS7 Redirection Attacks Via Call Audio-Based Distance Bounding. CyberSecurity@KAIST Workshop - KAIST, June 2018. Daejeon, South Korea.
14. Why Caller-ID Spoofing Is So Easy (and Why End-To-End Solutions Are the Way Forward). IEEE Workshop on Technology and Consumer Protection (ConPro'18), May 2018. San Francisco, CA.
15. Panel: The Future of Cybersecurity. SEC Academic Conference - Auburn University, May 2018. Auburn, AL.
16. Sound Principles: Verifying Voice Commands in an IoT World. IoT Security Workshop - Aalto University, September 2017. Helsinki, Finland.

17. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Eurecom Institute, September 2017. Sophia Antipolis, France.
18. Panel: Infrastructure Stability. ITU-T Focus Group Digital Financial Services, December 2016. Geneva, Switzerland.
19. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. ETH Zurich, December 2016. Zurich, Switzerland.
20. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. University of Richmond, October 2016. Richmond, Virginia.
21. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Indiana University, September 2016. Bloomington, Indiana.
22. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Aalto University Computer Science Department Forum, August 2016. Helsinki, Finland.
23. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. KAIST Information Security Seminar - Korean Advanced Institute of Science and Technology, June 2016. Daejeon, South Korea.
24. Updated Mobile Money Vulnerability Report. International Telecommunications Union Digital Financial Services Working Group Workshop, May 2016. Washington, DC.
25. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. UF Eye Opener Discovery Breakfast - University of Florida, May 2016. Gainesville, FL.
26. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Illinois Science of Security (SoS) Lablet Speaker Series - University of Illinois, Urbana-Champaign, April 2016. Urbana-Champaign, Illinois.
27. New Trends in Cybersecurity: Vulnerabilities in Branchless Banking Systems. United States Departments of State and Justice - Cybersecurity and Cybercrime Workshop for Lusophone Africa, September 2015. Maputo, Mozambique.
28. New Trends in Cybersecurity: Vulnerabilities in Branchless Banking Systems. United States Departments of State and Justice - ECCAS Cybersecurity and Cybercrime Workshop, August 2015. Kinshasa, Democratic Republic of Congo.
29. Chasing Telephony Security: Where the Wild Things... Are? University of Florida - Department Colloquium, January 2014. Gainesville, FL.
30. Chasing Telephony Security: Where the Wild Things... Are? Verizon Wireless RNC/Data Center, October 2013. Alpharetta, GA.
31. Chasing Telephony Security: Where the Wild Things... Are? University of Waterloo - CrySP Speaker Series on Privacy, October 2013. Waterloo, ON, Canada.
32. Analyzing Malicious Traffic in Cellular Networks. GSM Association's (GSMA) Mobile Malware Community Workshop, July 2013. Mountain View, CA.
33. Threats to Mobile Devices. US Federal Trade Commission (FTC) Public Forum - Invited Speaker, June 2013. Washington, D.C.
34. Chasing Telephony Security: Where the Wild Things... Are? University of Wisconsin - Madison, Security Seminar, March 2013. Madison, WI.

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

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

B. Special Activities

Presentations to Lay Media

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

14. Could this be the answer to the ransomware threat?, Consumer Affairs. Consumer Affairs - <https://www.consumeraffairs.com/news/could-this-be-the-answer-to-the-ransomware-threat-071116.html>, July 2016.
15. Extortion extinction: Researchers develop a way to stop ransomware. Phys.org - <http://phys.org/news/2016-07-extortion-extinction-ransomware.html>, July 2016.
16. Researchers Develop A Way To Stop Ransomware By Watching The Filesystem. Slashdot - <https://yro.slashdot.org/story/16/07/08/2242244/researchers-develop-a-way-to-stop-ransomware-by-watching-the-filesystem>, July 2016.
17. Mohul Ghosh. Trak.in - Digital Money Apps In India Are Unsafe and Unsecured - Researchers. <http://trak.in/tags/business/2015/08/17/digital-money-apps-india-unsafe-unsecured/>, August 2015.
18. Richard Handford. Mobile World Live - Survey finds security holes in mobile money apps. <http://www.mobileworldlive.com/money/news-money/survey-finds-security-holes-in-mobile-money-apps/#.Vc27Y-QTmSQ.twitter>, August 2015.
19. JENNIFER VALENTINO-DEVRIES. Wall Street Journal - Researchers Find Security Flaws in Developing-World Money Apps. <http://blogs.wsj.com/digits/2015/08/11/researchers-find-security-flaws-in-developing-world-money-apps/>, August 2015.
20. Jonathon Cheng. Wall Street Journal - Samsung Phone Studied for Possible Security Gap. <http://online.wsj.com/news/articles/SB10001424052702304244904579276191788427198>, December 2013.
21. N. V. The Economist - The Threat in the Pocket. <http://www.economist.com/blogs/babbage/2013/10/difference-engine-0?fsrc=scn/fb/wl/bl/thethreatinthepocket>, October 2013.
22. Antone Gonsalves. ComputerWorld - Let's Dump Anti-Virus and Move On:. <http://blogs.computerworld.com/mobile-security/22969/lets-dump-av-and-move>, October 2013.
23. Mathew J. Schwartz. InformationWeek - Google: Don't Fear Android Malware. <http://www.informationweek.com/security/mobile/google-dont-fear-android-malware/240162399>, October 2013.
24. Kirsten Doyle. ITWeb - Android Threat Exaggerated, or is it? http://www.itweb.co.za/index.php?option=com_content&view=article&id=68055, October 2013.
25. Danielle Walker. SC Magazine - Mobile malware prevalence expands, but privacy-abusing apps should be top of mind. <http://www.scmagazine.com/mobile-malware-prevalence-expands-but-privacy-abusing-apps-should-be-top-of-mind/article/300597/>, June 2013.
26. Jim Burrell. WABE NPR - Mobile Web Browsers Full of Security Risks, Tech Professor Finds. <http://wabe.org/post/mobile-web-browsers-full-security-risks-tech-professor-finds>, December 2012.

27. Mark Huffman. Consumer Affairs - Georgia Tech: mobile browsers fail safety test. <http://www.consumeraffairs.com/news/georgia-tech-mobile-browsers-fail-safety-test-120612.html>, December 2012.
28. Matthew J. Schwartz. Information Week - Blame Screen Size: Mobile Browsers Flunk Security Tests. <http://www.informationweek.com/security/mobile/blame-screen-size-mobile-browsers-flunk/240143999>, December 2012.
29. Jon Gold. Network World - Ga. Tech researchers: Mobile Browsers need better HTTPS indicators. <http://www.networkworld.com/news/2012/120512-mobile-browsers-264846.html>, December 2012.
30. United Press International. Study: Most mobile Web browsers unsafe. http://www.upi.com/Science_News/Technology/2012/12/05/Study-Most-mobile-Web-browsers-unsafe/UPI-73431354743353/#ixzz2EGtQsuLd, December 2012.
31. Suzanne Choney. Mobile browser woes can fool even experts: report. <http://www.nbcnews.com/technology/mobile-browser-woes-can-fool-even-experts-report-1C7451203>, December 2012.
32. Meghan Kelly. VentureBeat - 3 hot security startups to watch. <http://venturebeat.com/2012/02/27/3-security-startups-to-watch-at-the-2012-rsa-conference/>, February 2012.
33. Jacob Goodwin. Government Security News - RSA 2012 – Pindrop Security can distinguish a fraudulent phone call from a real one. <http://www.gsnmagazine.com/node/25721?c=communications>, February 2012.
34. Matt Liebowitz. Phone hack logs keystrokes from nearby computers. MSNBC.com - http://www.msnbc.msn.com/id/44993238/ns/technology_and_science-security/#.TqU5MNSjPh4, October 2011.
35. Jacob Aron. iPhone keylogger can snoop on desktop typing. New Scientist - <http://www.newscientist.com/article/dn21059-iphone-keylogger-can-snoop-on-desktop-typing.html>, October 2011.
36. iPhone Keylogger Can Snoop on Desktop Typing. Slashdot - <http://mobile.slashdot.org/story/11/10/18/2346222/iphone-keylogger-can-snoop-on-desktop-typing>, October 2011.
37. Robert Lemos. Smart Phones Could Hear Your Password. Technology Review - <http://www.technologyreview.com/computing/38913/?p1=A2>, October 2011.
38. Kevin McCaney. Bad vibrations: How smart phones could steal PC passwords. Government Computer News - <http://gcn.com/articles/2011/10/18/smart-phone-sensors-steal-keystrokes.aspx>, October 2011.
39. PhysOrg. Turning iPhone into spiPhone: Smartphones' accelerometer can track strokes on nearby keyboards. PhysOrg.com - <http://www.physorg.com/news/2011-10-iphone-spiphone-smartphones-accelerometer-track.html>, October 2011.
40. Brid-Aine Parnell. Securo-boffins call for 'self-aware' defensive technologies. The Register - http://www.theregister.co.uk/2011/09/14/self_aware_cyber_security_technologies_should_be_a_top_priority/, September 2011.

41. Clay Dillow. 'PinDr0p' Tech Uses Unique Noise Fingerprints to Trace Calls. Popular Science - <http://www.popsci.com/technology/article/2010-10/pindr0p-tech-tags-phone-calls-unique-fingerprints-trace-call-paths-across-networks>, October 2010.
42. Lewis Page. Voice-routing call fingerprint system fights vishing. The Register - http://www.theregister.co.uk/2010/10/06/voice_fingerprints, October 2010.
43. Science Daily. Voice Phishing: System to Trace Telephone Call Paths Across Multiple Networks Developed. <http://www.sciencedaily.com/releases/2010/10/101005121820.htm>, October 2010.
44. Brian Kalish. To Text or Not to Text During Emergencies. NextGov.com - http://www.nextgov.com/nextgov/ng_20100914_5986.php?oref=topnews, September 2010.
45. Ki Mae Heussner. 'Operation Chokehold': Fake Steve Jobs Rallies iPhone Users to Cripple AT&T Network. ABC News - <http://abcnews.go.com/Technology/GadgetGuide/fake-steve-jobs-rallies-iphone-users-cripple-att/story?id=9355447>, December 2009.
46. Bob Brown. Researchers Set Their Sights on iPhones, Mobile Malware. PC World Magazine - http://www.pcworld.com/article/182005/iphone_worms_mobile_malware.html?tk=rss, November 2009.
47. MacGregor Campbell. Botnets show their disruptive potential. New Scientist Magazine - <http://www.newscientist.com/article/mg20427347.000-mobile-botnets-show-their-disruptive-potential.html>, November 2009.
48. Angela Moscaritolo. Remote repair for infected phones in development. SC Magazine - <http://www.scmagazineus.com/remote-repair-for-infected-phones-in-development/article/157504/>, November 2009.
49. Bob Brown. iPhone worms, other smartphone malware in researchers' sights. Network World - <http://www.networkworld.com/news/2009/111109-smartphone-security-georgia-tech.html?hpg1=bn>, November 2009.
50. Urvaksh Karkaria. GT researchers work to secure cellphones. Atlanta Business Chronicle - <http://atlanta.bizjournals.com/atlanta/blog/atlantech/2009/11/cellphone.html>, November 2009.
51. Making Carriers Shoulder Smartphone Security. http://mobile.slashdot.org/story/09/11/11/2318247/Making-Carriers-Shoulder-Smartphone-Security?art_pos=31, November 2009.
52. Ben Meyer. Georgia Tech to Lead Fight Against Cell Phone Hackers. NBC 11 Atlanta - <http://www.11alive.com/news/local/story.aspx?storyid=132505&catid=3>, July 2009.
53. Illena Armstrong. Safeguarding your mobile networks. SC Magazine - <http://www.scmagazineus.com/Safeguarding-your-mobile-networks/article/138289/>, June 2009.
54. Kelli B. Grant. Four Free Cellphone Apps to Help Manage Your Money. SmartMoney Magazine - <http://www.smartmoney.com/Spending/Deals/4-Great-Free-Finance-Apps-for-Cellphones/>, June 2009.
55. Amanda Hoffstrom. Technology's limitations in alerting campus danger. UWire Magazine - <http://www.uwire.com/Article.aspx?id=3738798>, February 2009.

56. Laura Sydell. Compromise Allows Obama To Keep BlackBerry. National Public Radio - <http://www.npr.org/templates/story/story.php?storyId=99790788>, January 2009.
57. Dennis Carter. Questions abound as emergency alert flops Virginia Tech's text-message alert system failed when the sound of gunfire was heard on campus; officials scramble to understand why. eSchool News - http://www.eschoolnews.com/iphone/top-story/index.cfm?i=56122#_56122, November 2008.
58. Jessica Bauer. Study: Text alerts may fail in real emergency. Diamondback Online - <http://media.www.diamondbackonline.com/media/storage/paper873/news/2008/10/14/News/Study.Text.Alerts.May.Fail.In.Real.Emergency-3485509.shtml>, October 2008.
59. Associated Press. Hackers Expected To Start Targeting Cell Phones. <http://cbs5.com/watercooler/Cell.Phones.Hackers.2.840909.html>, 2008.
60. Associated Press. College alert systems unreliable, study says. http://www.ajc.com/search/content/metro/stories/2008/09/25/college_campus_alerts.html, 2008.
61. Lee Shearer. Study: Campus alerts unreliable. Athens Banner Herald http://www.onlineathens.com/stories/092508/uga_336494829.shtml, 2008.
62. Bill Ray. 3G Americas warns against text warning systems. The Register - http://www.theregister.co.uk/2008/09/18/emergency_text/, 2008.
63. 3G Americas. 3G Americas Highlights New Research Report on Use of Cellular Text Messaging for Emergency Alert Services. 3G Americas http://www.3gamericas.org/English/news_room/DisplayPressRelease.cfm?id=3400&s=ENG, 2008.
64. Evan Koblentz. Web Exclusive: From Messaging to Management Duty. Wireless Week - <http://www.wirelessweek.com/Messaging-to-Management-Duty.aspx>, 2008.
65. Christopher Beam. How Do You Intercept a Text Message? Turn your cell phone into a spy gadget. Slate Magazine <http://www.slate.com/id/2161402/>, 2007.
66. Jamming Cellphones with Text Messages. Slashdot <http://it.slashdot.org/it/05/10/05/1839217.shtml?tid=215&tid=172>, 2005.
67. Cell phone networks at risk? CNN http://money.cnn.com/2005/10/05/technology/hacker_cellphones/, 2005.
68. John Schwartz. Text Hackers Could Jam Cellphones, a Paper Says. The New York Times <http://www.nytimes.com/2005/10/05/technology/05phone.html?ex=1286164800&en=d917b9cd43dfaa31&ei=5090&partner=rssuserland&emc=rss>, 2005.