

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Gregory G. Raleigh Attorney Docket No.:39843-0179IP1
U.S. Patent No.: 8,588,110
Issue Date: November 19, 2013
Appl. Serial No.: 13/615,217
Filing Date: September 13, 2012
Title: VERIFIABLE DEVICE ASSISTED SERVICE USAGE BILLING
WITH INTEGRATED ACCOUNTING, MEDIATION
ACCOUNTING, AND MULTI-ACCOUNT

DECLARATION OF DR. PATRICK MCDANIEL

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

Date: August 27, 2024

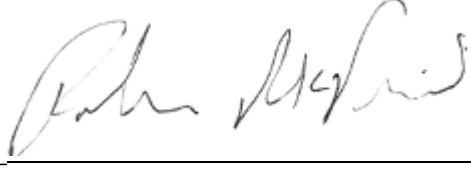
By: 
Patrick McDaniel, Ph.D.

Table of Contents

I.	ASSIGNMENT.....	4
II.	QUALIFICATIONS AND BACKGROUND INFORMATION.....	4
III.	OVERVIEW OF CONCLUSIONS FORMED	15
IV.	LEVEL OF ORDINARY SKILL IN THE ART	16
V.	LEGAL STANDARDS	17
	A. Terminology.....	17
	B. Legal Standards.....	18
	1. Anticipation	18
	2. Obviousness	19
VI.	RELEVANT CLAIM CONSTRUCTIONS	23
	Overview	23
	Means-plus-function elements (claim 26)	24
VII.	TECHNOLOGY OVERVIEW.....	33
	A. Mobile Devices	34
	1. Mobile Technology	34
	2. Billing Plans	38
	B. Policy-based Management.....	40
	C. Network Bandwidth Management.....	55
	D. Bandwidth Management Policy.....	57
VIII.	THE ‘110 PATENT	63
	A. Overview of the ‘110 Patent.....	63
	B. Prosecution History of the ‘110 Patent.....	63
IX.	OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES ..	63
	A. Jobs	63
	B. Jones	71
	C. Rao	74
	D. Jobs-Rao-Jones Combination	78
	Jobs-Jones	78
	Jobs-Jones-Rao	83
	E. Bocking	92
	F. Jobs-Jones-Rao-Bocking Combination	93
	G. Cunningham.....	95
	H. Jobs-Jones-Rao-Cunningham Combination	96
	I. Padmanabhan	98
	J. Jobs-Jones-Rao-Padmanabhan Combination	99

K.	Ibrahim.....	101
L.	Jobs-Jones-Rao-Ibrahim Combination	104
M.	Jobs-Jones-Rao-Bocking-Cunningham Combination	106
X.	MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '110 CLAIMS UNPATENTABLE	108
A.	Ground 1A: Jobs in view of Jones and Rao renders claims 1-16, 19, 21, 23-24, and 27-30 obvious	108
B.	Ground 1B: Jobs in view of Jones, Rao and Bocking renders claims 17, 18, and 24 obvious	161
C.	Ground 1C: Jobs in view of Jones, Rao, and Cunningham renders claim 20 obvious	166
	Ground 1D: Jobs in view of Jones, Rao, and Padmanabhan renders claim 22 obvious	170
D.	Ground 1E: Jobs in view of Jones, Rao, and Ibrahim renders claim 25 obvious	174
E.	Ground 2: Jobs in view of Jones, Rao, Bocking, and Cunningham renders claim 26 obvious	178
F.	CONCLUSION.....	190

I. ASSIGNMENT

1. I have been retained on behalf of Samsung Electronics Co., Ltd. (“Samsung”) to offer technical opinions related to 8,588,110 (“the ’110 patent”) (SAMSUNG-1001). I understand that Samsung is requesting that the Patent Trial and Appeal Board (“PTAB” or “Board”) to institute an *inter partes* review (“IPR”) proceeding of the ’110 patent.
2. I have been asked to provide my independent analysis of the ’110 patent based on the prior art publications cited in this declaration.
3. I am not and never have been, an employee of Samsung. I received no compensation for this declaration beyond my normal hourly compensation based on my time actually spent analyzing the ’110 patent, the prior art publications cited below, and issues related thereto, and I will not receive any added compensation based on the outcome of any IPR or other proceeding involving the ’110 patent.

II. QUALIFICATIONS AND BACKGROUND INFORMATION

4. I am over the age of 18 and am competent to write this declaration. I have personal knowledge, or have developed knowledge of these technologies based upon education, training, or experience, of the matters set forth herein.

5. My qualifications are summarized here and explained in more detail in my curriculum vitae, which is attached as Appendix A to this report.

Appendix A also includes a list of my publications and the cases in which I have testified at deposition, hearing, or trial within the past four years.

6. I earned a Ph.D. in Computer Science from the Computer Science and Engineering Department at University of Michigan, Ann Arbor in 2001. I earned a Bachelor of Science degree in Computer Science from Ohio University in 1989, and a Master of Science degree, also in Computer Science, from Ball State University in 1991.

7. Since 2022, I have been Tsun-Ming Shih Professor of Computer Sciences in the School of Computer, Data and Information Sciences at the University of Wisconsin-Madison. Prior to my move to Wisconsin, I was the William L. Weiss Professor of Information and Communications Technology in the School of Electrical Engineering and Computer Science at Pennsylvania State University in University Park, PA. I was also the director of the Institute for Network and Security Research, and founder and co-director of the Systems and Internet Infrastructure Security Laboratory, a research laboratory focused on the study of security in diverse network and computer environments. My research efforts primarily involve computer

systems, network management and authentication, systems security, and technical public policy.

8. Prior to 2017, I was an Assistant Professor (2004-2007), Associate Professor (2007-2011), Full Professor (2011-2015), and Distinguished Professor (2016-2017) of Computer Science and Engineering and the William L. Weiss Professor of Information and Communications Technology (2017-2022) at the Pennsylvania State University. Since 2004, I have taught courses in the field of computer systems, systems programming, mobile device security, networks, and network and computer security at both the undergraduate and graduate level. I created and maintained several of these courses at Penn State. I began teaching cybersecurity courses at the University of Wisconsin-Madison but will teach a network security course in Fall of 2023.

9. From 2003-2009, I was also an Adjunct Professor at the Stern School of Business at New York University in New York, NY. At the Stern School of Business, I taught courses in computer and network security and online privacy.

10. I am a Fellow of the Association for Computing Machinery (ACM, the leading professional association for computer science), a Fellow Institute for Electrical and Electronics Engineering (IEEE, the leading professional

association for engineering), and Fellow of the American Association for the Advancement of Science (AAAS, the leading professional association for science).

11. I am the director of the NSF Frontier Center for Trustworthy Machine Learning (CTML), a research organization exploring security and privacy of machine learning (and AI in general). Funded by the US National Science Foundation, the CTML is led by the University of Wisconsin-Madison and has members from Stanford, the University of California, Berkeley, The University of California-San Diego, and the University of Virginia.

12. I was the Program Manager (PM) and lead scientist for the Cyber Security Collaborative Research Alliance (CRA). The CRA is led by Penn State University and includes faculty and researchers from the Army Research Laboratory, Carnegie Mellon University, Indiana University, the University of California-Davis, and the University of California-Riverside. This initiative is a major research project aimed at developing a new science of cyber-security for military networks, computers, and installations.

13. I have served as an advisor to several Ph.D. and master's degree candidates, several of whom have gone on to become professors at various institutions such as North Carolina State University, Purdue University, the University of Toronto, the University of Oregon, and the Georgia Institute of

Technology and the University of Florida. I am currently an advisor to seven Ph.D. students.

14. Before joining Pennsylvania State University as a professor, I was a software developer and project manager for companies in the networking industry including Applied Innovation, Inc., and Primary Access Corporation. I was also a senior researcher at AT&T Research-Labs (previously known as Bell Labs). As part of my duties in these industrial positions, I informed, reviewed, and formed corporate policies and practices relating to the security of mobile devices, networks, and software systems.

15. As shown in Appendix A, I have published extensively in the field of mobile security, network and security management, computer systems, routing and queueing, authentication, systems security, applied cryptography and network security. In addition to writing several articles for industry journals and conferences, I have authored portions of numerous books related to computer systems, applied cryptography and network security. I have served on the editorial boards of several peer-reviewed journals including ACM Transactions on Internet Technology, for which I was the Editor-in-Chief. I was also an Associate Editor for ACM Transactions on Information and System Security and IEEE Transactions of Software Engineering, two highly regarded journals in the field. My curriculum vitae,

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

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

17. In writing this Declaration, I have considered the following: my own knowledge and experience, including my work experience in the fields of network and system design, mobile systems, and system policy; my experience in teaching those subjects; and my experience in working with others involved in those fields.

18. I have reviewed the '110 patent (SAMSUNG-1001), and relevant excerpts of the prosecution history (SAMSUNG-1002) of the '110 patent. In addition, I have analyzed the publications and materials listed below, in addition to other materials I cite in my declaration. Among various textbooks, documents, and publications, I have also reviewed the following prior art references:

- SAMSUNG-1005 U.S. Pat. App. Pub. No. 2007/0149252 ("Jobs")

- SAMSUNG-1006 U.S. Pat. No. 8,285,850 (“Jones”)
- SAMSUNG-1007 U.S. Pat. App. Pub. No. 2006/0039354 (“Rao”)
- SAMSUNG-1009 U.S. Pat. App. Pub. No. 2006/0075090
 (“Bocking”)
- SAMSUNG-1010 U.S. Pat. App. Pub. No. 2006/0019632
 (“Cunningham”)
- SAMSUNG-1011 U.S. Pat. App. Pub. No. 2006/0203739
 (“Padmanabhan”)
- SAMSUNG-1012 U.S. Pat. App. Pub. No. 2008/0026787
 (“Ibrahim”)
- SAMSUNG-1020 U.S. Pat. No. 5,987,611 (“Freund”)
- SAMSUNG-1021 Lobo, et. al., (1999). A policy description
 language. AAAI/IAAI, 1999, 291-298 (“Lobo”)
- SAMSUNG-1022 Verma, et. al., (2002). Policy-based
 management of content distribution networks. IEEE network,
 16(2), 34-39 (“Verma”)
- SAMSUNG-1023 Agrawal, et. al., 2005. Policy-based
 management of networked computing systems. IEEE
 Communications Magazine, 43(10), pp. 69-75 (“Agrawal”)

- SAMSUNG-1024 Blake, et al., IETF RFC 2475, “An Architecture for Differentiated Services,” December 1998, downloaded from the internet at <https://datatracker.ietf.org/doc/html/rfc2475> on July 29, 2023
- SAMSUNG-1025 Westerinen, et al., IETF RFC 3198, Terminology for Policy-Based Management, November 2001, downloaded from the Internet on May 27, 2024
- SAMSUNG-1026 Damianou, et al., 2001. The ponder policy specification language. In Policies for Distributed Systems and Networks: International Workshop, POLICY 2001 Bristol, UK, January 29–31, 2001 Proceedings (pp. 18-38). Springer Berlin Heidelberg (“Damianou”)
- SAMSUNG-1027 Stone, G.N., Lundy, B. and Xie, G.G., 2001. Network policy languages: a survey and a new approach, IEEE network, 15(1), pp.10-21 (“Stone”)
- SAMSUNG-1028 Agrawal, et. al., 2007, May. Issues in designing a policy language for distributed management of IT infrastructures. In 2007 10th IFIP/IEEE International Symposium on Integrated Network Management (pp. 30-39), IEEE (“Agrawal-2”)

- SAMSUNG-1029 Simplified Policy Language (CIM-SPL).
Document Number DSP0231, version, 1 (“CIM-SPL”)
- SAMSUNG-1030 Ponnappan, et al., 2002, June. A policy based
QoS management system for the IntServ/DiffServ based Internet.
In Proceedings Third International Workshop on Policies for
Distributed Systems and Networks (pp. 159-168), IEEE.
 (“Ponnappan”)
- SAMSUNG-1031 Gonçalves, et al., 2009, October. A
graphical user interface for policy composition in CIM-SPL. In
2009 International Conference on Ultra Modern
Telecommunications & Workshops (pp. 1-7), IEEE. (“Gonçalves”)
- SAMSUNG-1032 U.S. Pat. No. 6,947,723 (“Gurnani”)
- SAMSUNG-1033 U.S. Pat. App. Pub. No. 2008/0122796 (“Jobs-
796”)
- SAMSUNG-1034 U.S. Pat. App. Pub. No. 2009/0217065
 (“Araujo”)
- SAMSUNG-1035 U.S. Pat. No. 7,454,446 (“Leung”)
- SAMSUNG-1036 U.S. Pat. No. 8,799,242 (“Leonard”)
- SAMSUNG-1037 U.S. Pat. No. 7,860,964 (“Brady”)

- SAMSUNG-1038 Liao, S.H., 2005. Expert system methodologies and applications—a decade review from 1995 to 2004. *Expert systems with applications*, 28(1), pp. 93-103 (“Liao”)
- SAMSUNG-1039 U.S. Pat. App. Pub. No. 2008/0002652 (“Gupta”)
- SAMSUNG-1040 van Beek, et. al., 2004, January. Adaptive streaming of high-quality video over wireless LANs. In *Visual Communications and Image Processing 2004* (Vol. 5308, pp. 647-660). SPIE. (“van Beek”)
- SAMSUNG-1042 Reeder, R.W., Karat, C.M., Karat, J. and Brodie, C., 2007. Usability challenges in security and privacy policy-authoring interfaces. In *Human-Computer Interaction—INTERACT 2007: 11th IFIP TC 13 International Conference, Rio de Janeiro, Brazil, September 10-14, 2007, Proceedings, Part II* 11 (pp. 141-155). Springer Berlin Heidelberg. (“Reeder”)
- SAMSUNG-1043 Mansour, Y. and Patt-Shamir, B., 2001. Jitter control in QoS networks. *IEEE/ACM Transactions On Networking*, 9(4), pp.492-502. (“Mansour”)

- SAMSUNG-1044 U.S. Pat. No 5,481,735 (“Mortensen”)
- SAMSUNG-1045 U.S. Pat. No. 5,764,693 (“Taylor”)
- SAMSUNG-1046 IETF RFC 793, Transmission Control Protocol, September 1981, downloaded from the Internet on August 14, 2024 (“RFC 793”)
- SAMSUNG-1047 Prasad, et. al., 1998. An overview of CDMA evolution toward wideband CDMA. IEEE communications Surveys, 1(1), pp.2-29. (“Prasad”)
- SAMSUNG-1048 U.S. Pat. App. Pub. No. 2007/0117550 (“Boris”)
- SAMSUNG-1049 Excerpts, Garg, "An overview of wireless systems." Wireless Communications Networking, Morgan Kaufmann, 1st edition. ISBN 123735807 (2007). (“Garg”)
- SAMSUNG-1050 Li, et al., 2003, December. “Dynamic priority reallocation scheme for quality of service in IEEE 802.11e WLANs.” In Multimedia Computing and Networking 2004 (Vol. 5305, pp. 83-94). SPIE. (“Li”)

19. Counsel (Fish & Richardson) has informed me that I should consider these materials through the lens of one of ordinary skill in the art related to

the '110 patent at the time of the earliest possible priority date of the '110 patent, and I have done so during my review of these materials. I have been informed by Counsel to use the date January 29, 2009.

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

21. My opinions, as explained below, are based on my education, experience, and expertise in the fields relating to the '110 Patent. Unless otherwise stated, my testimony below refers to the knowledge of one of ordinary skill in the art as of the earliest possible priority date. Any figures that appear within this document have been prepared with the assistance of Counsel and reflect my understanding of the '110 Patent and the prior art discussed below.

III. OVERVIEW OF CONCLUSIONS FORMED

22. This declaration explains the conclusions that I have formed based on my analysis. To summarize those conclusions, based upon my knowledge and experience and my review of the prior art references listed above, I believe that:

- Ground 1A renders claims 1-16, 19, 21, 23-24, and 27-30 obvious;
- Ground 1B renders claims 17-18, and 24 obvious;
- Ground 1C renders claim 20 obvious;
- Ground 1D renders claim 22 obvious;
- Ground 1E renders claim 25 obvious; and
- Ground 2 renders claim 26 obvious.

23. In support of these conclusions, I provide an overview of the references in Section IX and more detailed comments regarding the obviousness of claims 1-30 (“**the Challenged Claims**”) of the ‘110 patent in Section X.

IV. LEVEL OF ORDINARY SKILL IN THE ART

24. In my opinion, a person of ordinary skill in the art (“POSITA”) relating to, and at the time of, the Priority Date would have been someone with (1) at least a bachelor’s degree in computer science, computer engineering, electrical engineering, or a related field, and (2) at least two years of industry experience in wireless communications security.

Additional advanced education could compensate for a deficiency in work experience, and *vice-versa*.

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

V. LEGAL STANDARDS

A. Terminology

26. 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 generally be given their ordinary and customary meaning to a person of ordinary skill in the art at the time of the invention, by considering the claims, specification, and prosecution history, as well as evidence extrinsic to the patent, when construing patent claims. 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, which I refer to as the “Critical Date” in this proceeding. Because I do not know at what date the invention as claimed was made, if ever, I have used the Critical Date of the ’110 patent as the point in time for claim interpretation purposes. My opinion does not change if the invention date is earlier.

B. Legal Standards

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

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

1. Anticipation

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

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

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

2. Obviousness

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

33. I have been informed by Counsel and understand that a claim is unpatentable for obviousness and that obviousness may be based upon a combination of references. I am informed by Counsel and understand that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. However, I am informed by Counsel and understand that a patent claim composed of

several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art.

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

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

36. I am informed by Counsel and understand that an obviousness inquiry requires consideration of the following factors: (1) the scope and content of the prior art, (2) the differences between the prior art and the claims, (3) the level of ordinary skill in the art, and (4) any so called “secondary considerations” of non-obviousness, which include: (i) “long felt need” for the claimed invention, (ii) commercial success attributable to the claimed invention, (iii) unexpected results of the claimed invention, and (iv) “copying” of the claimed invention by others.

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

38. I have been informed by Counsel and understand that if a technique has been used to improve one device, and a person of ordinary skill at the time of invention would have recognized that it would improve similar

devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.

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

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

41. I have been informed by Counsel and understand that a claim can be obvious in light of a single reference, without the need to combine references, if the elements of the claim that are not found explicitly or

inherently in the reference can be supplied by the common sense of one of skill in the art.

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

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

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

VI. RELEVANT CLAIM CONSTRUCTIONS

Overview

45. I have been asked to provide my interpretation of the terms from claim 26 of the '110 patent listed below as functional or structural limitations as they pertain to §112, ¶6 (also referred to as means-plus-function limitations), which I have been informed applies when claim limitations are recited in terms of their function instead of their structure. I have additionally been informed that, for terms that are subject to interpretation as means-plus-function limitations, the corresponding structure in the specification is what defines the scope of the limitation. I have also been informed that, for means-plus-function limitations that are performed by a generic computing device or processor, the corresponding structure includes a processor programmed to perform an algorithm to perform the recited function as disclosed in the specification.

46. Below I have presented interpretations for each of the terms I believe should be interpreted as means-plus-function limitations, which are applied to the prior art below. The interpretations represent my analysis regarding a POSITA's understanding and interpretation of these claim terms.

47. For all claims, I use the claim construction standard referred to in §V.

Means-plus-function elements (claim 26)

48. I address four means-plus-function claim elements below. This declaration identifies the specific portions of the specification that describe structures that correspond to the recited function.

49. Claim 26 describes a device, not a method. SAMSUNG-1001, 165:20-38. Elements [26.2] and [22.6]-[22.8] each refer to a “means for” performing a function without any recitation of structure. Counsel has informed me that the claim elements “shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.” 35 U.S.C. §112(6).

50. The ’110 patent discloses a device that “includes a processor 930, sometimes referred to as a CPU or central processor unit, an APU or application processor unit, a core processor, a computing device, or many other well known terms.” SAMSUNG-1001, FIGS. 9-15; 26:43-45, 26:52-26; *see generally id.*, 26:43-36:64 (describing device embodiments). The ’110 patent explains that, in some embodiments, “the service processor 115 is implemented on the processor 930 of the device” and “this implementation can be in part or whole accomplished in software stored, implemented and/or executed on the processor 930.” SAMSUNG-1001, 28:51-55.

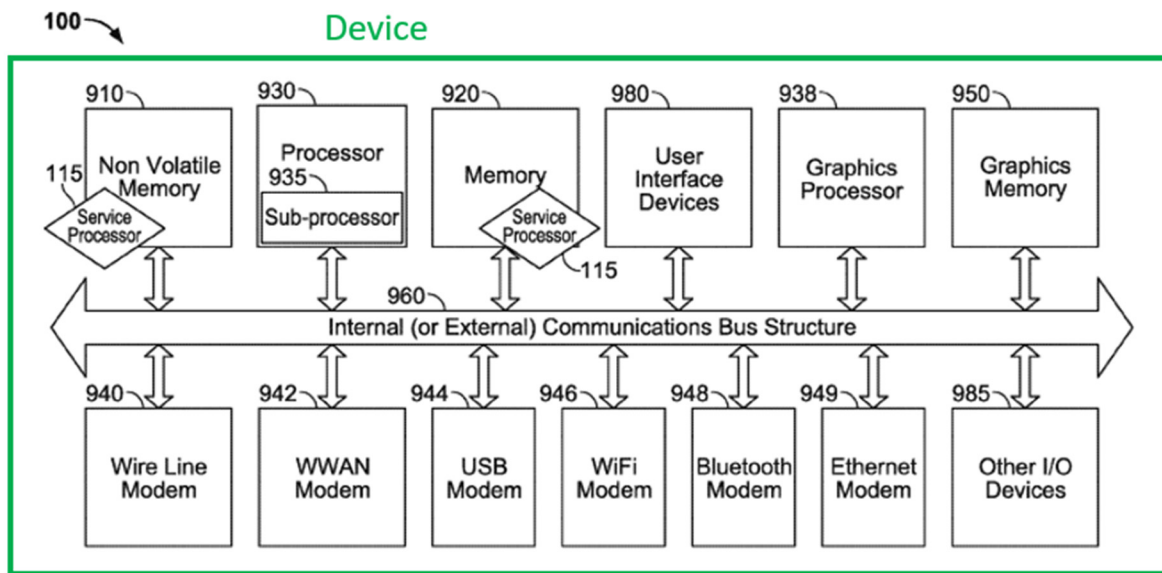


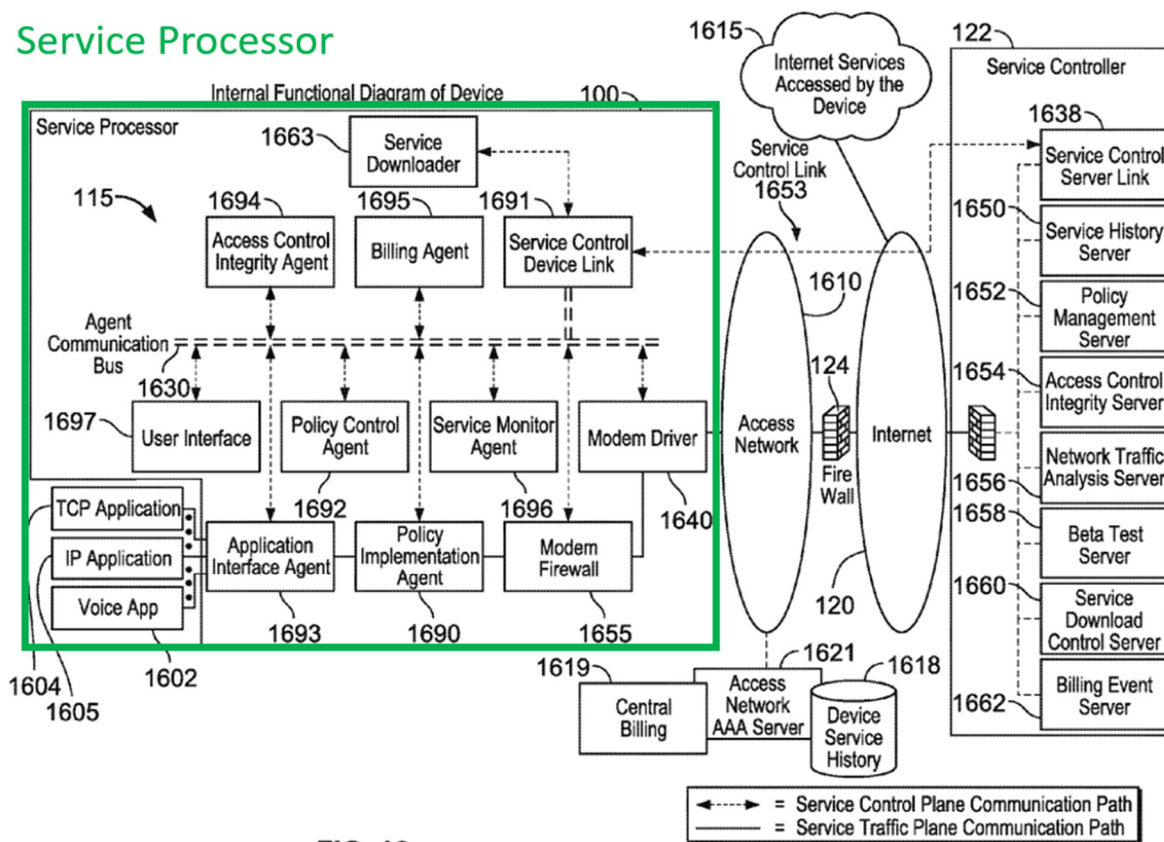
FIG. 9

SAMSUNG-1001, FIG. 9 (annotated).

51. FIG. 16 is “a functional diagram illustrating a device-based service processor 115 and a service controller 122 in accordance with some embodiments” that “provides relatively full featured device based service processor implementation and service controller implementation.”

SAMSUNG-1001, 36:65-37:2.

Service Processor



SAMSUNG-1001, FIG. 16 (annotated)

52. Since the service processor 115 is implemented on the processor, it follows that the corresponding structure for each of the “means for” elements is a processor configured to perform respective algorithm steps for the recited function corresponding to each element.

[26.2] means for obtaining, through a user interface of the wireless device, a user input specifying at least an aspect of a first service policy

53. [26.2] recites the function of obtaining, through a user interface of the wireless device, a user input specifying at least an aspect of a first service policy. Processor 930 and user interface device(s), such as a touch screen,

are collectively responsible for obtaining a user input specifying at least an aspect of a first service policy. SAMSUNG-1001, 27:15-29; 28:41-48.

54. The '110 patent states that the device “includes a user interfaces device component 980 for communicating with user interface devices,” such as touch screens. SAMSUNG-1001, 28:41-48. The patent explains that ***“the user interface 1697 provides the user with information and accepts user choices or preferences*** on one or more of the following: ... ***service plan selection or change*** ... and/or other service related information, settings, and/or options.” SAMSUNG-1001, 65:41-51.¹ The '110 patent further states that service policy functionality includes “notifying user of service overages,” which “[s]ends a notification message or screen to the UI to inform the user that the one or more aspects of service usage has exceeded the specified limits of one or more service plans.” SAMSUNG-1001, FIG. 42D. Since the service plan selection or change defines the plan’s “specified limits,” a POSITA would have understood that user input specifying a service plan selection or change specifies an aspect of the service policy.

55. Based on the '110 patent’s disclosure, the corresponding structure for the “means for obtaining” includes a user interface and a processor

¹ All emphasis is added unless otherwise indicated.

configured to perform the algorithm steps of providing the user with information and accepting user choices or preferences on, e.g., service plan selection or change, and/or other service related information, settings, and/or options. SAMSUNG-1001, 27:15-29; 28:41-48, 65:41-51.

[26.6] means for identifying that the wireless device is connected to the first wireless network

56. [26.6] recites the function of identifying that the wireless device is connected to the first wireless network.

57. Processor 930 is responsible for identifying that the wireless device is connected to the first wireless network. SAMSUNG-1001, 27:15-29.

58. The '110 patent discloses algorithm steps for identifying that the device is connected to the first wireless network. For example, it states that “the device recognizes which type of network it is currently connecting to (e.g., looking up in a local or network table for the current base station connected to, and/or the information is broadcast to the device upon the connection with the base station), that is, whether it is a macrocell, microcell, picocell or femtocell.” SAMSUNG-1001, 51:4-13.

59. Based on the '110 patent's disclosure, the corresponding structure for the “means for identifying” of [26.6] includes a processor configured to perform the algorithm steps of recognizing the type of network to which the

device is currently connecting, e.g., by looking up the information in a local or network table. SAMSUNG-1001, 51:4-13.

[26.7] means for identifying an intended, attempted, or successful data communication over the first wireless network, the intended, attempted, or successful data communication being associated with the first service activity

60. [26.7] recites the function of identifying an intended, attempted, or successful data communication over the first wireless network, the intended, attempted, or successful data communication being associated with the first service activity.

61. Processor 930 is responsible for identifying an intended, attempted, or successful data communication over the first wireless network.

62. The '110 patent provides algorithm steps for performing the function: for example, “the service monitor agent 1696 ***implements traffic inspection points between the applications and the networking stack application interface***, such as the sockets API.” SAMSUNG-1001, 53:51-55. The '110 patent explains that “***[t]raffic inspection can be accomplished in several ways, including, for example, implementing a T-buffer at each socket connection and feeding the side traffic into a traffic flow analyzer***, which in combination with a mapping of application to socket provides much of the information listed above.” *Id.*, 53:58-63.

63. The service monitoring agent runs on the service processor, which is implemented on processor 930. SAMSUNG-1001, 29:10-32, FIG. 16.

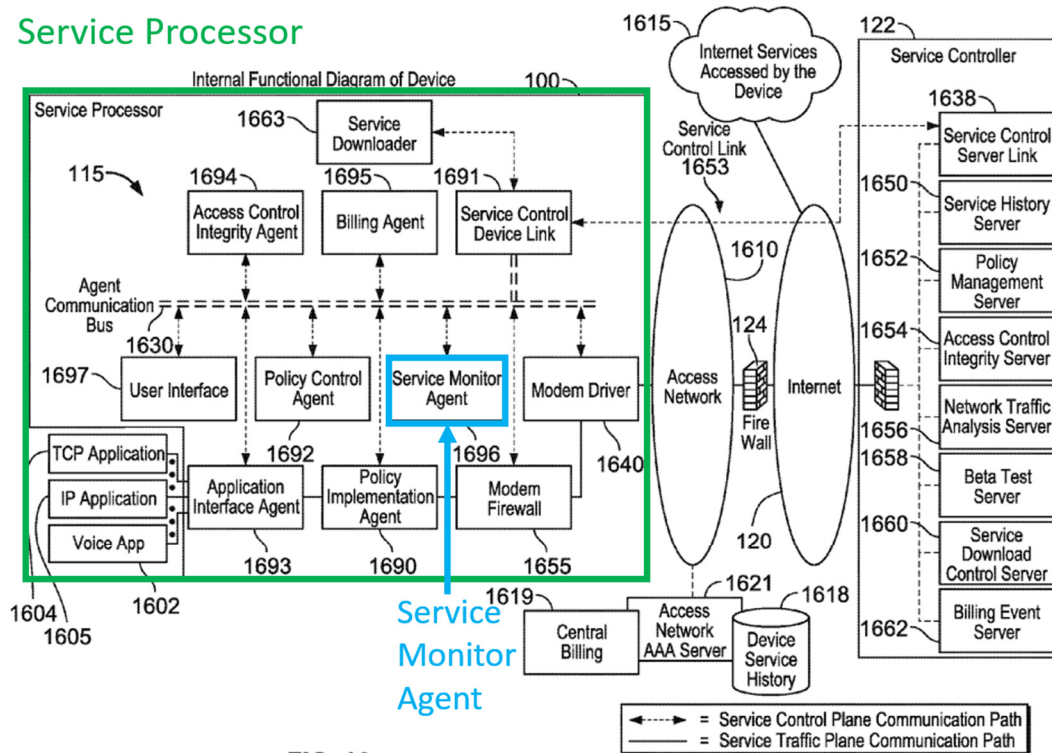


FIG. 16

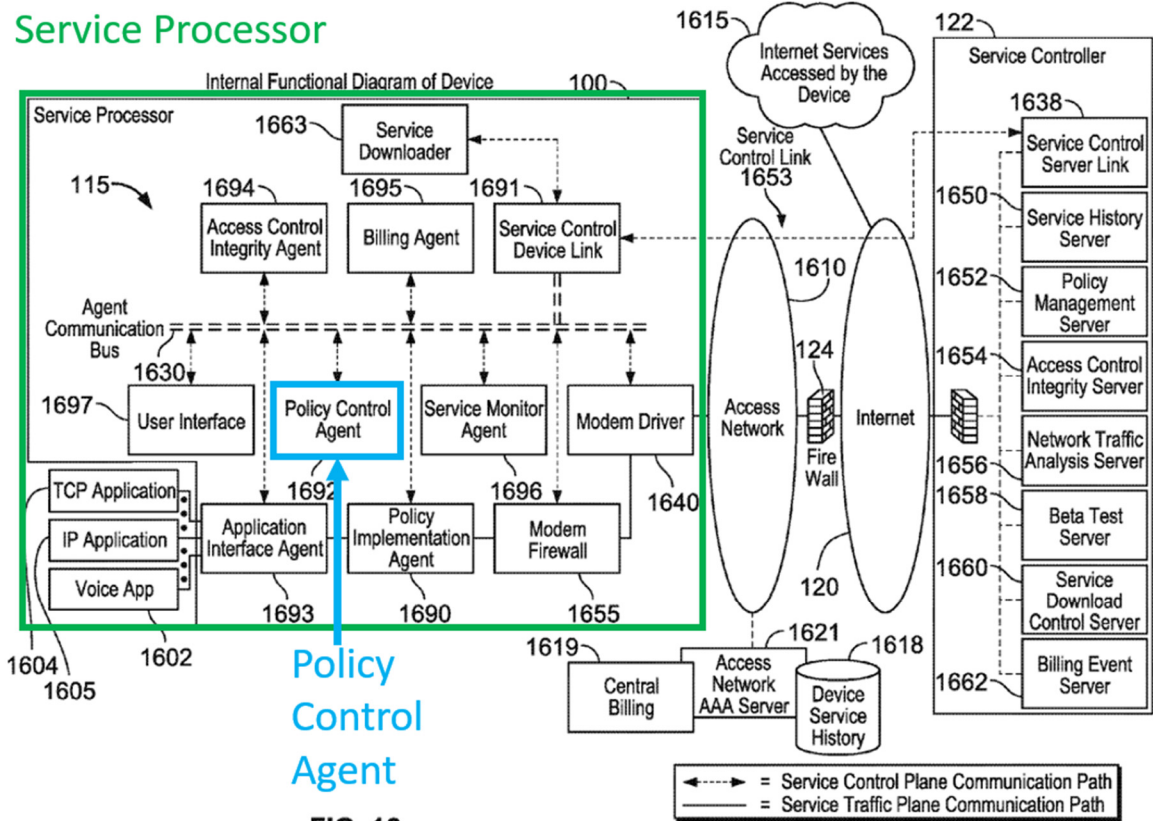
SAMSUNG-1001, FIG. 16 (annotated).

64. Based on the '110 patent's disclosure, the corresponding structure for the "means for identifying" of [26.7] includes a processor configured to perform the algorithm steps of implementing traffic inspection points between the applications and the networking stack application interface using a T-buffer at socket connections and feeding the side traffic into a traffic flow analyzer. SAMSUNG-1001, 29:10-32, 53:51-55, 58-63, FIG. 16.

[26.8] means for applying the first service policy

65. [28.8] recites the function of applying the first service policy.

66. Processor 930 is responsible for applying the first service policy. For example, the '110 patent states that “the policy control agent 1692 is instructed, for example, by the user, through billing agent 1695 to **perform a service control algorithm.**” SAMSUNG-1001, 48:38-40. The policy control agent executes on the processor.



SAMSUNG-1001, FIG. 16 (annotated).

67. The '110 patent provides multiple algorithms that apply policies. Examples include: (i) “the traffic shaping algorithm can simply reduce traffic speed for all applications and traffic types successively until the service usage projections are within service usage limits for the present service billing period,” and (ii) “the traffic shaping algorithm can identify the highest traffic usage applications and/or websites and successively reduce traffic speed just for the highest usage applications and/or websites until the service usage projections are within service usage limits for the present service billing period.” SAMSUNG-1001, 48:38-49:1.

68. Based on the '110 patent's disclosure, the corresponding structure for the “means for applying” includes a processor configured to perform the algorithm steps of performing a service control that reduces traffic speed for all applications and traffic types successively until the service usage projections are within service usage limits for the present service billing period. SAMSUNG-1001, 48:38-49:1.

VII. TECHNOLOGY OVERVIEW

69. In this section I provide a broad overview of the relevant technology and state of the technical community before the priority date of the '110 patent. This description is not intended to be exhaustive, but to provide sufficient background to support and contextualize my analysis below.

A. Mobile Devices

1. Mobile Technology

70. In 2009, use of smartphones experienced a significant surge, marking a pivotal moment in the evolution of mobile technology. The year saw a growing number of consumers transitioning from traditional feature phones (e.g., flip phones) to more capable and versatile smartphones. Key factors driving this uptake included advancements in mobile operating systems such as Apple's iOS and Google's Android, offering a user-friendly interface and access to a burgeoning app² ecosystem. Additionally, the earlier introduction of 3G networks enabled faster mobile data speeds, prompting users to embrace smartphones for tasks beyond voice and messaging. As a result, smartphone sales soared, laying the groundwork for the transformative impact they would have on communication, productivity, and entertainment in the years to come.

² The “app” refers to software applications that generally run on smartphones, e.g., email, browsers, streaming, and social media applications. An app market is the application and developer infrastructure for creating and providing apps to smartphone users.

71. However, smartphones in 2009 were resource-limited compared to the current devices. For example, smartphones of 2009 were equipped with single-core processors, usually running at speeds below 1 GHz. These processors lacked the computing power of today's multi-core CPUs found in modern smartphones. As a result, tasks that required significant processing, such as running complex applications or playing graphically intensive games, were often slow and less efficient. Similarly, memory capacities in smartphones of 2009 were generally limited, typically ranging from 128 MB to 512 MB. Long term storage was also limited, consisting of between 4 to 16GB of space.

72. Devices were connected to wireless networks using WWAN (cellular) and WLAN (Wi-Fi) modems,³ among other techniques. For example, Jobs⁴ describes a device that includes, "RF circuitry 108 may

³ The term modem refers to a *modulator/demodulator*, which is a device to process electrical signals received and sent over a physical media (e.g., copper wire) or over the air. In mobile devices, modems are software supported radios that process specific network access protocols.

⁴ Steven Jobs, co-founder of Apple, is the lead inventor of both SAMSUNG-1005 and SAMSUNG-1033.

communicate with networks, such as the Internet, also referred to as the World Wide Web (WWW), an intranet and/or a wireless network, such as a cellular telephone network, a wireless local area network (LAN) and/or a metropolitan area network (MAN), and other devices by wireless communication,” which “may use any of a plurality of communications standards, protocols and technologies, including but not limited to Global System for Mobile Communications (GSM), Enhanced Data GSM Environment (EDGE), high-speed downlink packet access (HSDPA), wideband code division multiple access (W-CDMA), code division multiple access (CDMA), time division multiple access (TDMA), Bluetooth, Wireless Fidelity (Wi-Fi) (e.g., IEEE 802.11a, IEEE 802.11b, IEEE 802.11g and/or IEEE 802.11n), voice over Internet Protocol (VoIP), Wi-MAX, a protocol for email (e.g., Internet message access protocol (IMAP) and/or post office protocol (POP)), instant messaging (e.g., extensible messaging and presence protocol (XMPP), Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE), and/or Instant Messaging and Presence Service (IMPS)), and/or Short Message Service (SMS)), or any other suitable communication protocol, including communication protocols not yet developed as of the filing date of this document.” SAMSUNG-1033, [0100].

73. The networks that were being used in 2009 were also limited in speed and throughput. In 2009, wide-area (WWAN) cellular 3G networks, as implemented by the Global System for Mobile Communications (GSM)⁵ and Code Division Multiple Access (CDMA) protocols were becoming widespread, but 4G networks were still in the early stages of deployment. This meant slower internet speeds and limited coverage for mobile data, affecting the overall online experience. Wi-Fi technology as implemented in the 802.11 suite of protocols complemented cellular networks. Smartphones, laptops, and other devices could connect to Wi-Fi hotspots in homes, offices, cafes, and public spaces to access the internet at much higher speeds than what 3G networks could offer. Wi-Fi also allowed users to offload data usage from their cellular plans, which was particularly helpful due to the relatively limited data caps on mobile plans during that time. Regardless of the network protocol it was running on, the IP protocol was used to connect each device with the Internet.

⁵ Note that GSM predates 3G networks (actually back to 1991), but, for the purposes of this report, I will focus only on those variants of GSM which were classified as 3G.

74. While 2009 smartphone displays were already evolving towards touchscreens, they were smaller, less vibrant, and had lower resolutions compared to modern displays. Common screen resolutions were around 320x480 pixels, making it challenging to display content with high visual fidelity. Devices operating systems provided windowed environments which would generally have a single application being displayed (and prioritized by the operating system) and interacting with the users. These applications were referred to as having focus (of the user interface). Users could switch between applications as needed but could only interact with the one application with focus at a time.

2. Billing Plans

75. As of the Critical Date, service plans for mobile devices were common. For example, Jobs explains that “[u]sers of portable communication devices (e.g., mobile telephones, handhelds, media players, personal digital assistants (PDAs), BlackBerry™, pocket PCs, Smart Phones, etc.) typically enter into service contracts with service providers for voice and/or data services.” SAMSUNG-1005, [0002]. Jobs notes that a “data service plan, for example, may have a flat monthly fee for a certain amount of data storage capacity (e.g., 100 MB) for email and other data, as

well as a surcharge rate (e.g., \$0.01/MB) if the user consumes additional capacity during the month.” *Id.*

76. Further, a broad range of service plans were known as of the Critical Date. For example, Cunningham discloses a “business model that is dedicated to supporting a wireless messaging device, where the “model offers unlimited services on a dependent device, including mixed limited/unlimited usage models, pre-and post-pay models, and models not found in a conventional monthly recurring charge system,” and can further includes components that address service selection, suspension, resumption, service add-ons, account limitations and restrictions, detect device compatibility with support services, account analysis, charging cycles, billing methods, third-party add-ons and interfacing, and troubleshooting support.” SAMSUNG-1010, Abstract. In one example, Cunningham states that “when the usage exceeds the expected payment, the service can be limited or disabled until the next payment cycle.” SAMSUNG-1010, [0050]. Gurnani similarly explains that “[w]hen the customer reaches the limit based on estimated charges, further usage is prohibited, even if the customer reaches the limit during an ongoing call or communication session.” SAMSUNG-1033, Abstract. In another example, Boris teaches that:

There are also calling/billing systems in the art which include SIM cards on which a running total is kept of the user's minutes and rating occurs on the card. Such SIM cards can be for calling plans where the user pays for minutes and services prior to using the minutes and services. In such SIM cards, a tariff table within the *SIM card keeps track of the minutes and service and shuts off service itself when the user's paid minutes and/or services have been used up*. SAMSUNG-1048, [0006](emphasis added).

Thus, it was well-known as of the Critical Date to block transmissions once an allocation threshold has been reached. SAMSUNG-1032, [0050]; SAMSUNG-1033, Abstract.

B. Policy-based Management

77. A key challenge in 2009 was finding ways to address the rapidly increasing needs of mobile users using the resource-limited devices and networks. Solutions to these problems were developed by adapting known techniques in computer systems and networks (e.g., priority queuing), as well as developing new, faster devices and networks.

78. One such approach was to use policies, often expressed as rules, to manage competing demand for resources. Policy for computational systems has been a part of the technical landscape since the 1970s, and policy has been applied to numerous domains. For example, Araujo described managing device power based on policy; Leung describes “data based upon storage policies;” Leonard describes policy-based content management; and Brady describes policy-based content delivery network selection. *Generally*, SAMSUNG-1034; SAMSUNG-1035; SAMSUNG-1036; SAMSUNG-1037. In addition, by the Critical Date, rule-based expert systems had been long-since been researched and developed. SAMSUNG-1038, 2.

79. One primary focus of policy-based systems was on differentiating resource usage in various environments. For example, a policy might specify that data from interactive applications, such as multi-player games, are assigned the highest priority to ensure the best user experience. For example, Stone explains that “a mission-critical application may be given priority over all other network traffic, or all users in the silver class (differentiated services) have priority over the bronze class, but must succumb to the gold class.” SAMSUNG-1027, 2. (See also, *e.g.*, SAMSUNG-1007, [0003].)

80. These policies were implemented to manage and allocate computing resources efficiently in diverse computing environments. For instance, differentiated services emerged as a crucial policy in this context, especially as mobile devices such as phones began to traverse heterogeneous environments, transitioning between Wi-Fi and cellular networks seamlessly. (SAMSUNG-1024 is an RFC that discusses DiffServ, “An Architecture for Differentiated Services.”) By employing policies like differentiated services, computing systems could optimize resource allocation, ensuring a smooth and reliable user experience while adapting to changing network conditions and device capabilities in these dynamic environments. Such techniques were particularly important to address the challenges faced by early mobile devices.

81. A policy can be defined as a set of rules to administer, manage, and control access to network resources.⁶ There are many alternatives for specifying policies, but one common approach is to specify a policy as a condition and corresponding action. For example, Verma defines a policy as an expression of the form “if condition then action” where “the conditional part describes a specific situation that can be encountered by a network

⁶ See, e.g., SAMSUNG-1025.

device, and the action component specifies the action that is to be performed by the device in that situation.” SAMSUNG-1022, 2. Lobo extends condition-action to “event-condition-action” such that “[a]n event-condition-action rule is triggered when the event occurs, and if the condition is true the action is executed.” SAMSUNG-1021, 1. For simplicity, I describe the condition-action example, but a POSITA would have understood that event-condition-action and other forms were known and could have been used.

82. In this construction, the two aspects of a policy, a condition aspect and an action aspect, influence how the system under management operates. The condition is typically a Boolean expression that compares some measurable state of the computing system to a value or to another measurable state. Rao suggests typical examples such as “if the application name is ‘App1’,” “if the application type is VoIP,” and “if the application is running in the Background,” although a POSITA would have recognized that virtually any condition could be used. SAMSUNG-1007, [0182]. For example, provisioning systems might specify conditions related to CPU utilization, caching systems might specify conditions relates to cache hit rate, a content distribution network (CDN) might measure popularity of a piece of content, an access control system might define access levels based on a user’s ID and/or role, and so on.

83. Conditions can be simple Boolean expression (e.g., “if X equals Y”) or more complex expressions that include multiple clauses (e.g., “if ((X equals Y) OR (A is less than B)”). Stone gives an example, in which:

```
{traffic_class = {video, voice}, used_bw <= allotted_bw}
{allotted_bw = 50M, loss_rate (data) > 40% : allotted_bw :=
40M}
```

SAMSUNG-1027, 10.

84. In this example, “[v]oice and video traffic are provided with an allotted bandwidth of 50 Mb/s, but when the network loss rate is greater than 40 percent, a compromise will be made to lower the allotted bandwidth to 40 Mb/s.” *Id.* (Lowering the allotted bandwidth is an action taken when the condition is true.)

85. Gonçalves’s similarly describe policy conditions that are “ORed or ANDed.” SAMSUNG-1031, 4. Further, CIM-SPL defined conditions as Boolean expressions of arbitrary complexity. SAMSUNG-1028, 5; SAMSUNG-1029, 51. In summary, Boolean conditions including multiple clauses were well-known as of the Critical Date.

86. The action aspect determines how the system reacts when the condition evaluates to TRUE. Verma teaches that an “action may be construed as a procedure that is defined and stored in the repository (e.g. a

piece of Java code, or a program in a language like CacheL or PONDER)” or a “set of simple operations that need to be performed.” SAMSUNG-1022, 2. Such reactions depend both on the type of a system and its goals. For example, when a provisioning system determines that CPU utilization of a system exceeds a threshold, it might provision a new server, providing additional computing capacity; a CDN might replicate a piece of content to more distribution nodes; and, in the context of Rao, packets are assigned priority, which determines queue placement. SAMSUNG-1007, [0184].

87. As is apparent in the discussion above, the terms “policy” and “rule” are often used interchangeably.⁷ For example, Agrawal writes that the “key idea of policy-based management is to allow system administrators to specify *declarative policy rules* that govern the behavior of their IT systems instead of relying on ad hoc mechanisms such as running customized scripts based on experience and rules of thumb.” SAMSUNG-1028, 2 (emphasis

⁷ Note that the use of these terms is entirely consistent with the use in the art at the priority date (and today). Broadly speaking, a “rule” is generally one statement or directive relating to policy, and policy is generally the set of rules that direct the behavior of the system. However, in common use the two terms are often used interchangeably.

added). Verma similarly discusses “the *application of policy based techniques* to content distribution networks, and discuss[es] the form that *typical policy rules* for such an environment would take.” SAMSUNG-1022, 1.

88. Mobile device service plans and policy-based management are overlapping concepts. For example, a service plan that blocked data beyond (e.g.) 100 MB can be written as a condition aspect, “if (data_used > 100MB)”, and an action aspect, “block_traffic.” In another example, a service plan with differentiated pricing (e.g., the plan described in Jobs), could be written as two policies: (i) if (data_sent ≤ 100 MB) then (charge is zero); (ii) if (data_sent > 100 MB) then (charge is \$0.01/MB). SAMSUNG-1005, [0002]. A plan that further included an absolute limit of 500 MB could be written as three policies: (i) if (data_sent ≤ 100 MB) then (charge is zero); (ii) if (100 MB < data_sent ≤ 500 MB) then (charge is \$0.01/MB); (iii) if (data_sent > 500 MB) then (block_traffic). These are, of course, only a small number of examples of the many policies that can be used as a part of a service plan, and, more generally, to govern device operation.

89. However, in some cases, if-then rules are insufficient since they allow for policy conflict, which occurs when two policies specify conflicting actions. Consider a simple case where one policy specifies that network

access is allowed if data use is below a threshold value, and a second policy specifies that network access is now allowed if the device is roaming. If the device is both below its data use threshold and roaming, the two policies would provide conflicting results. For example, Agrawal gives an example in which one policy permits data access and a second policy denies it.

SAMSUNG-1023, 2.

90. A common approach was to include a priority with each policy. The priority can indicate “the relative importance of the associated policy” and determine “which policy must be applied when there are multiple applicable policies with potentially conflicting actions.” SAMSUNG-1023, 2. CIM-SPL is one example of a policy systems that included priority. SAMSUNG-1029, 14, 16, 21-23.

91. The policy system can evaluate the condition aspects of each policy and enforce the highest-priority policy for which the condition aspect evaluated to TRUE. Or, more efficiently, the policy system can simply evaluate policies in priority order and enforce the first policy for which the condition evaluates to TRUE. Thus, the policy reflects a user (who can be an administrator) preference for how policies are to be applied.

92. Some policy systems automatically detected conflicts, along with dominance (a policy will never be enforced because it is dominated by other

policies) and coverage (for a set of input parameters, ensure that at least one policy applies, which can be important, e.g., for security policies).

SAMSUNG-1023, 5-6. Such systems allowed users to “debug” their policies before they were deployed. For example, Agrawal explains that “Policies can interact with each other, often with undesirable effects; therefore a policy administrator needs to be aware of such relations among policies,” and “[u]nderstanding and controlling the overall effect of policies is particularly important in a distributed system, where a policy author may only have a partial view of the entire system, and multiple authors may write policies for the same set of resources without coordination.” SAMSUNG-1023, 4-5.

93. The policies can be specified using many different syntaxes.⁸ Among the many examples are PDL,⁹ Ponder,¹⁰ and CIM-SPL,¹¹ and hardware and software vendors often defined their own proprietary policy-specification languages.

⁸ Stone provides one overview of policy languages in SAMSUNG-1027.

⁹ See, generally, SAMSUNG-1021.

¹⁰ See, generally, SAMSUNG-1026.

¹¹ See, generally, SAMSUNG-1028, SAMSUNG-1029.

94. In some systems, rules were simply coded by administrators using the appropriate syntax, such as PDL, Ponder, or a vendor-specific syntax. Some systems also provided users interfaces that permitted users to specify policies. For example, Agrawal writes that “[a] policy definition tool (PDT) is a user interface by which policy authors create and modify policies.”

SAMSUNG-1023, 3.

95. In its simplest form, a POSITA would have recognized that a user interface includes widgets (e.g., text boxes) that allow a user to provide input specifying the condition and action aspects of a policy, as illustrated below.¹²

Policy specification

Condition:

Action:

¹² This example is merely illustrative; user interfaces of actual systems were typically far more complex.

96. Ponnappan includes an example that “shows the Policy Editor developed in the system, and an example of a policy rule.” SAMSUNG-1030, 7.

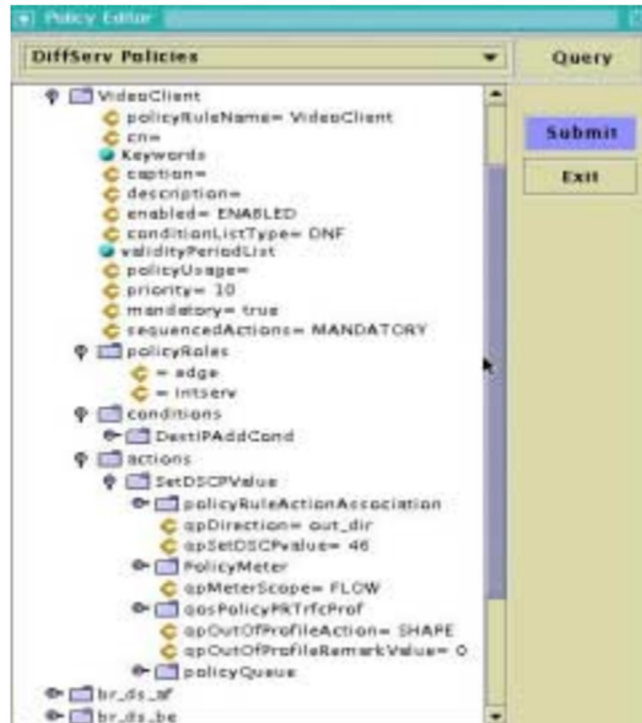


Figure 3: Policy Editor and a Policy Rule example

Id.

97. Gonçalves’s Figure 3 (reproduced below), shows a “graphical composition window” that can be used to specify conditions and actions. The condition component of the UI contains “a radio button where it can be defined how to compose the policy conditions (e.g. ORed or ANDed) and a list of simple conditions where condition usage can be suspended in the check box. SAMSUNG-1031, Figure 3.

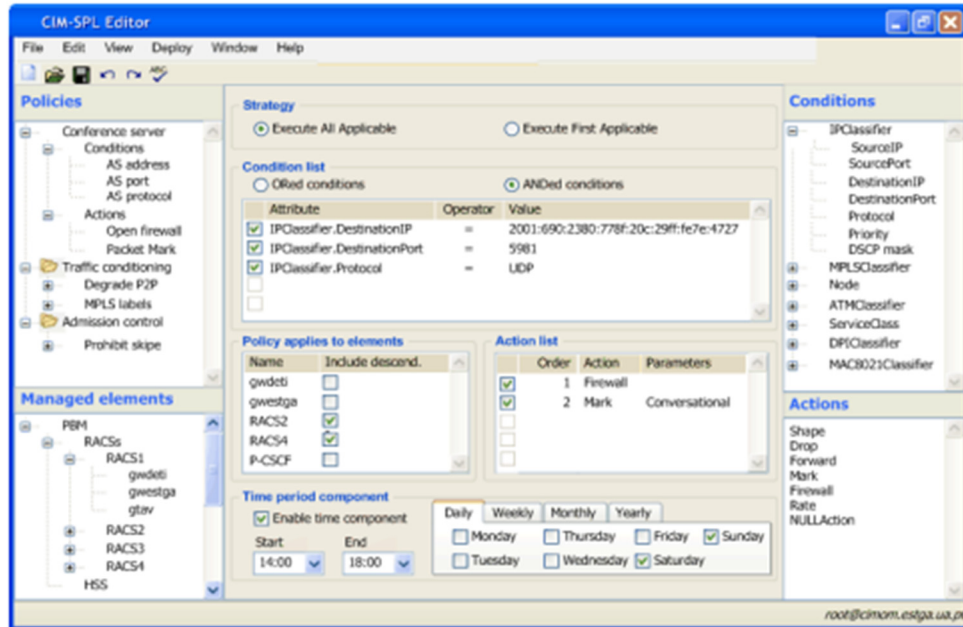


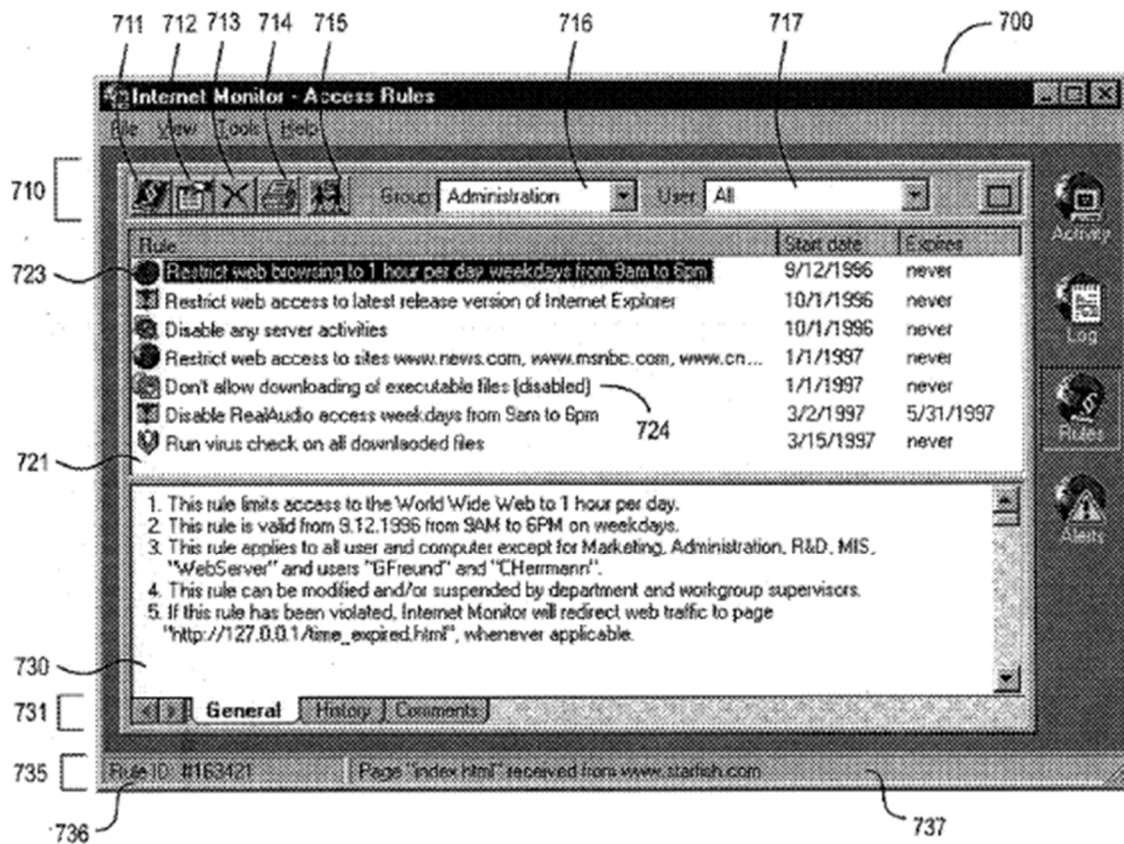
Figure 3 - Graphical editor view

Id.

98. Reeder similarly discussed policy authoring in the context of security and privacy and performed “a laboratory user study using the SPARCLE application to identify usability problems experienced by users in policy-authoring tasks.” SAMSUNG-1042, 5.

99. To further simplify policy specification, some systems provided wizard dialogs. For example, Freund provides rule configuration using “a preferred user interface or ‘wizard’ dialogs for configuring rules” displays “rules governing operation of the Internet access monitor” and rules that “are available for a current configuration” and allows a user to create, edit, or

delete rules. SAMSUNG-1020, 24:16-24. Figure 7A (below) shows an example UI panel.



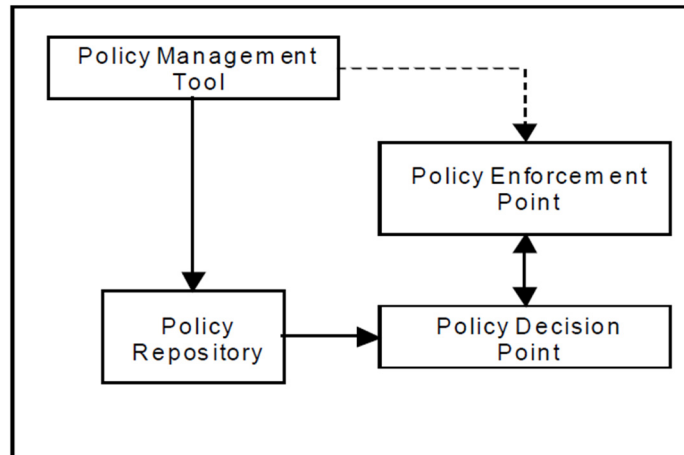
SAMSUNG-1020, FIG. 7A.

100. Gonçalves also describes a policy wizard that “made up of a set of dialog windows that ask for the policy component information, typically organized according to SPL policy components.” SAMSUNG-1031, 4.

101. In policy management, it was common to separate the concept of policy decisions (does the policy apply, which is determined by the condition) from policy enforcement (actuate the policy action). Policy

decisions are made at a Policy Decision Point (PDP) and policy enforcement occurs at a Policy Enforcement Point (PEP). For example, Verma writes that “[t]he policy decision point is an entity that is responsible for retrieving the policies from the repository, and for interpreting them and deciding on which set of policies ought to be enforced by the PEP” and “[t]he logical entities that can take actions to enforce the policies are known as the policy enforcement points (PEPs).” SAMSUNG-1022, 2. Verma further explains that the PEP and PDP can exist on the same device or on different devices, writing “the PEP would be the function inside the router that makes QoS decisions” and “[t]he PDP would be a software module inside the same router (or another router).” *Id.* In the example given above, the PDP would determine whether data are from an interactive game, and if so, the PEP would assign the highest priority to the data, e.g., by adding the data to a high-priority queue. Again, this would ensure the user does not experience performance problems (e.g., lag).

102. Verma also explains that a “policy repository is used to store the policies generated by the management tool.” *Id.* Verma provides the following schematic:



SAMSUNG-1022, Figure 1.

A Policy Decision Point (PDP) and Policy Enforcement Point (PEP) are essential components in policy-based systems.¹³ The PDP functions as the determining logic of the system, responsible for evaluating policy rules and making decisions based on the input received from sources. Conversely, the PEP serves to enforce policy. PEPs are located at the point where policies are applied. The PEP communicates with the PDP (which need not be co-located) to obtain the relevant policy decisions and then enacts them by controlling access to resources.

¹³ SAMSUNG-1022, 1-2.

C. Network Bandwidth Management

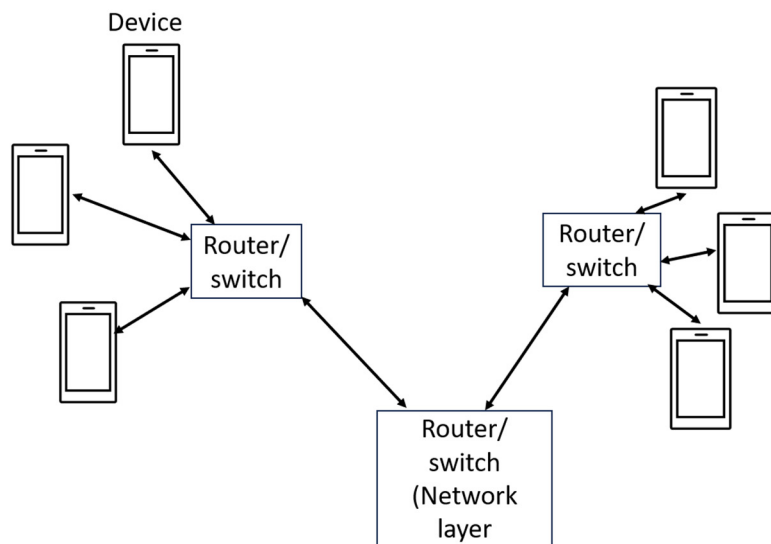
103. In addition, when the demands of apps and services on the phone overwhelmed the available network bandwidth, techniques were needed to allocate bandwidth in an optimal and fair¹⁴ way. These techniques were broadly characterized as network bandwidth management (or just bandwidth management for simplicity). Like policy-based management, techniques for bandwidth management were known long before mobile computing devices were widely deployed. As just one example, the IETF defined “DiffServ” in 1998, which “is based on a simple model where traffic entering a network is classified and possibly conditioned at the boundaries of the network, and assigned to different behavior aggregates.” SAMSUNG-1024, 12.

104. The goal of bandwidth management is to ensure that every user, device, and app receives a fair share of network resources, and to handle cases where there is not sufficient network bandwidth to support all requests—even when network failures occur that prevent serving those requests.

105. Bandwidth management occurs, generally, at three layers: within the devices, within network devices such as routers and switches, and at the

¹⁴ Fair does not necessarily mean equal, as discussed below.

network layer. As illustrated below, devices (laptops, desktops, servers, printers, mobile devices, etc.) connect to network elements such as routers and/or switches, which in turn connect to other network elements. The number of layers often depends on the size of the network. Large Cloud systems can have thousands or tens of thousands of network elements organized in a multi-layer hierarchy.



Example Network Architecture

106. At the device layer, bandwidth management serves two primary objectives. The first goal is to ensure that bandwidth is allocated fairly among all applications, preventing any single application from monopolizing network resources. This fair allocation is crucial for maintaining a network

environment where multiple applications can operate simultaneously without significant performance degradation. The second goal of bandwidth management at the device layer is to prioritize applications with real-time constraints, such as streaming media, to ensure they receive the necessary bandwidth for optimal performance. These applications require consistent¹⁵ and timely data delivery to maintain an adequate user experience (i.e., preventing buffering or stuttering during playback), and thus, they are given precedence in bandwidth allocation. By giving preferential treatment of these real-time applications, bandwidth management aims to minimize latency and buffering issues and provide a seamless and satisfactory experience for the end-users.

D. Bandwidth Management Policy

107. Well before the Critical Date, policies were commonly used to define and enforce bandwidth management policies. For example, in 1998, the DiffServ specification explained that “[n]etwork resources are allocated to

¹⁵ While only tangentially relevant to this declaration, a second factor, jitter, which measures changes in the amount of time required to deliver packets, can also influence user experience. Techniques for managing jitter were also well-known as of the critical date. *See, e.g.,* SAMSUNG-1043.

traffic *streams by service provisioning policies* which govern how traffic is marked and conditioned upon entry to a differentiated services-capable network, and how that traffic is forwarded within that network.”

SAMSUNG-1024, 1.

108. Generally speaking, there are three techniques used to control bandwidth: prioritization, quotas, and adaptive application controls.

109. Prioritization assigns each app a level of service it should be provided (e.g., high, medium, and low priority). Thereafter, when contention or other condition occurs, bandwidth is allocated apps by their assigned priority. For example, high priority apps would receive the most, followed by medium and finally low priority will receive the least. One special priority is none, where an app is blocked (that is, transmission is never allowed or allowed only when no other traffic is being transmitted) when contention or other condition (see below) occurs.

110. Prioritization is often implemented using weighted queueing, where outgoing data or incoming data packets are put into queues and processed according to the queue weights. For example, the high priority queue would have the heaviest weight, followed by medium, then low. The exact priorities used by the policy is again assigned by the user or network administrator, depending on the device and environment. In one example,

Blake teaches that “a priority queuing system is a combination of a set of queues and a scheduler that empties them in priority sequence.”

SAMSUNG-1024, 6. Blake explains that “when asked for a packet, the scheduler inspects the highest priority queue and, if there is data present, returns a packet from that queue” and “[f]ailing that, it inspects the next highest priority queue, and so on.” *Id*

111. Quotas set a maximum amount of bandwidth that each application can use per unit time (e.g., number of kilobytes per second). Unlike prioritization, which assigns different weights to applications, quotas establish specific bandwidth limits for each application. When an application is running, it can use bandwidth up to its assigned quota. Once this quota is reached, subsequent data packets are either queued or, in rare cases, dropped, based on the network policy. Queueing allows the application to continue functioning, albeit at a reduced rate, as it waits for additional bandwidth to become available. Another form of quotas at the network level allows for the reservation of a specified amount of bandwidth for future use by applications. An example of this is the “Resource ReSerVation Protocol (RSVP),” which is defined in the IETF RFC 2205 standard document. *See, generally*, SAMSUNG-1036. Reservations enables applications to request the network and other endpoints to reserve a certain

amount of bandwidth. The protocol facilitates these requests, ensuring that the required bandwidth is set aside and available when needed. The network actively manages and preserves these reservations, guaranteeing that the allocated resources remain available for the designated applications.

112. Adaptive application controls are a dynamic bandwidth management technique that adjusts bandwidth allocation based on real-time network conditions and application requirements. (*See, e.g., SAMSUNG-1007, Abstract, 5:66-6:12.*) These controls are particularly important for applications that can modify their resource usage in response to network congestion or availability.

113. A common example of adaptive controls is found in video streaming applications that adjust their video resolution when network or local device resources become congested—a process known as scaling. When network bandwidth or device resources are limited, applications reduce their resolution to maintain smooth playback and reduce the demand on the network. Conversely, when additional resources become available, the applications can increase their resolution, taking advantage of the improved conditions to enhance the user experience. To simplify, adaptive application controls work by continuously monitoring both local resources and network conditions. They use this data to make real-time adjustments, ensuring that

applications reduce their bandwidth usage during periods of high contention and increase it when more bandwidth becomes available.

114. Note that bandwidth policies are designed, not only to manage bandwidth in the face contention and congestion, but also to handle transient network errors that can cause bandwidth degradation or outages. These policies determine how traffic is managed during such events and play a key role in maintaining application resilience and user experience. For instance, during transient network errors (such as those caused by cellular tower handoffs) policies may dictate that traffic is delayed or dropped to prevent data loss or corruption.

115. Bandwidth policies can also be customized based on the hardware capabilities of devices, especially when devices have multiple interfaces accessing different networks, e.g., WiFi and cellular. Each network interface offers varying performance characteristics and cost structures and thus requires interface-specific policies. For example, policies can prioritize the use of fast WiFi networks over cellular networks for data-intensive applications. In extreme cases, bandwidth policies may even prohibit certain applications from using specific networks to avoid excessive costs or performance issues. For instance, an application may be restricted from transferring large data files over an expensive cellular network.

116. Where the network is controlled by a single administrative domain (e.g., a network for a corporation or a university), a network management system coordinates policy mechanisms within each device and network element to enforce a network-wide bandwidth management policy. This approach ensures that each device and the applications running on the devices receive optimal bandwidth allocation according to current network conditions, and across the entire network.

117. The network-wide policy can be enforced in one of two ways. First, it can leverage agents in devices such as mobile phones or desktop computers to help enforce bandwidth management policy. Second, it can operate independently of these device end-points, relying solely on the network elements to manage bandwidth. In some cases, enforcement is performed on both devices and network elements.

118. Bandwidth policies are typically created through user interfaces (command-line interfaces, scripting interfaces, graphical user interfaces, etc.) by either end users or network administrators. (See §VII.B.) User often create the policy by editing it on the local device through some provided application or interface. Conversely, administrators generally use network management tools to configure and distribute these policies across network elements and end-user devices. Once these policies are deployed,

end users may have the ability to modify them (as allowed by the network administrator policy) to meet their needs.

VIII. THE ‘110 PATENT

A. Overview of the ‘110 Patent

119. The ’110 Patent is directed to a “services policy communication system and method.” SAMSUNG-1001, Abstract. It further describes “a communications device [that] implements a service policy for assisting billing for the communications device use of a service on a network; and monitors use of the service based on the service policy, in which a local service usage is synchronized with a network based service usage.” *Id.*

B. Prosecution History of the ‘110 Patent

120. During prosecution, Applicant amended the claims only in response to a restriction requirement. SAMSUNG-1002, 454-470. No further office actions were entered, and the amended claims were allowed. *Id.*, 704.

Notably, the Office never considered Jones, Bocking, Padmanabhan or Ibrahim and therefore did not consider the combinations forming Grounds 1A-1E or 2. *Generally*, SAMSUNG-1002. These Grounds render the Challenged Claims obvious, as discussed below.

IX. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES

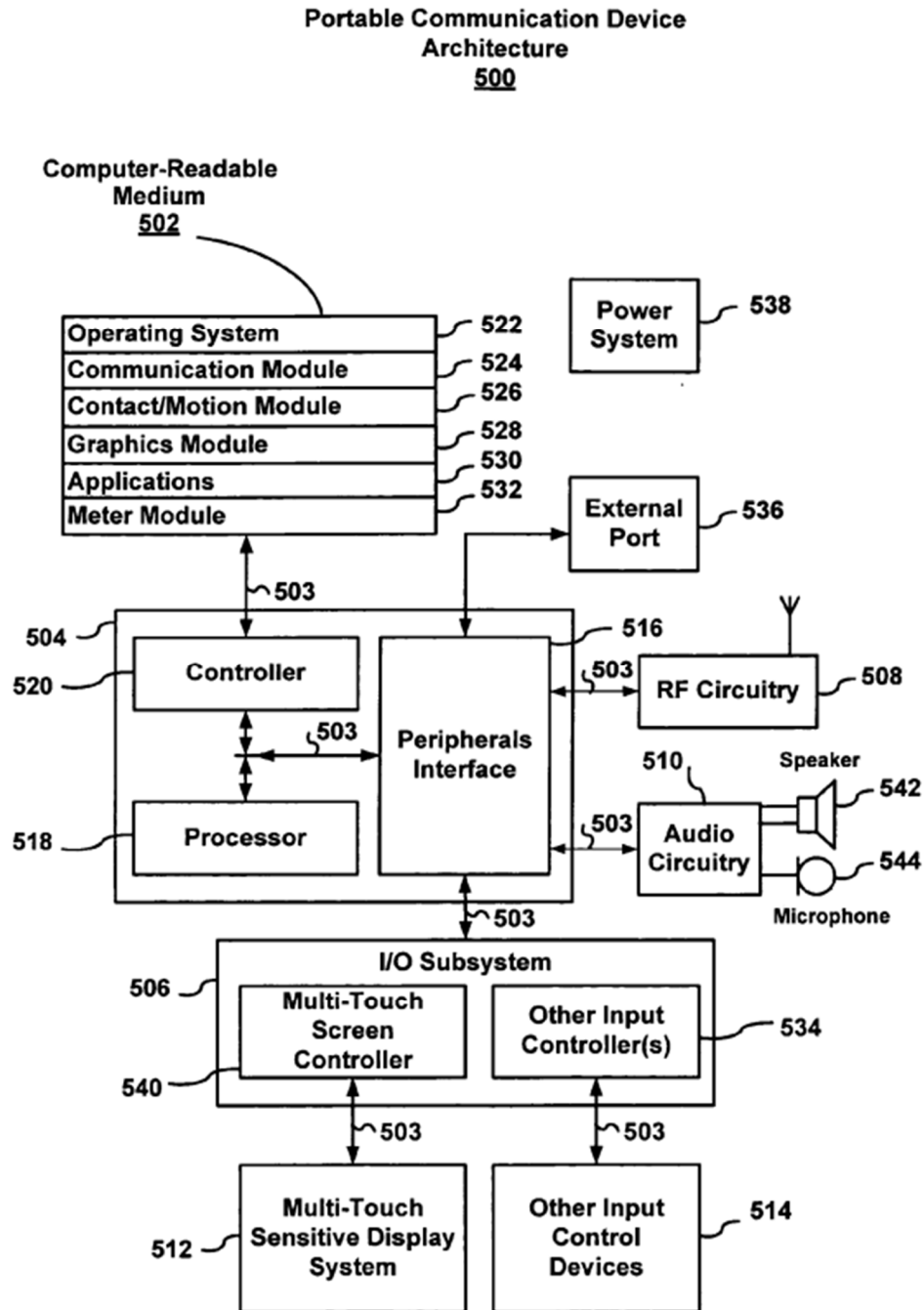
A. Jobs

121. Jobs explains, “[u]sers of portable communication devices (e.g., mobile telephones, handhelds, media players, personal digital assistants (PDAs), BlackBerry™, pocket PCs, Smart Phones, etc.) typically enter into service contracts with service providers for voice and/or data services.”

SAMSUNG-1005, [0002]. The “[s]ervice plans can provide data services, voice services or a combination of voice and data services” and “typically allocate limited amounts of minutes, bandwidth or storage based on the price of the plan.” *Id.* However, Jobs notes that users did “not have a convenient way to review the current account balance(s) of service plans,” so there was “a need for improved access to user account balance and other account usage information.” SAMSUNG-1005, [0003].

122. In response, Jobs discloses a “portable communication device [that] includes a display and a processor coupled to the display,” where the processor “automatically and repeatedly present[s] an updated account usage metric for an account associated with usage of the portable communication device,” e.g., “an account balance associated with usage of the portable communication device.” SAMSUNG-1005, [0004].

123. Jobs’s device includes conventional components such as CPUs, memory, display, speaker, microphone, etc., as illustrated in FIG.5, reproduced below. SAMSUNG-1005, [0040]-[0049], FIG. 5.



SAMSUNG-1005, FIG. 5.

124. The Jobs device further includes “RF circuitry” used “to send and receive information over a wireless link or network to one or more other devices and includes well-known circuitry for performing this function,

including but not limited to an antenna system, an RF transceiver, one or more amplifiers, a tuner, one or more oscillators, a digital signal processor, a CODEC chipset, memory, etc.” SAMSUNG-1005, [0042]. The RF circuitry can establish and maintain “communications with other devices using one or more known RF communication protocols (e.g., TDMA, CDMA, etc.) and one or more known mobile networking protocols (e.g., GSM, ANSI-41, etc.),” and can communicate “with other devices over the Internet using Voice-Over-Internet Protocol (VoIP).” *Id.*

125. While Jobs does not specifically use the term “modem” or “wireless modem,” a POSITA would have recognized that Jobs’s RF circuitry either is a wireless modem or is functionally equivalent to a wireless modem since a wireless modem is necessary for Jobs’s device to operate wirelessly, e.g., “uploading and downloading various objects from the Internet over a wireless network.” SAMSUNG_1005, [0044]. For example, Taylor describes a “**wireless radio modem** that may be incorporated into a host system or connected through a PCMCIA or similar port to a host system **includes radio frequency modulation/demodulation circuitry** employing electronic device elements that operate in a frequency range that minimizes the RF interference between the radio modem and the host system.” SAMSUNG-1045, Abstract, emphasis added.

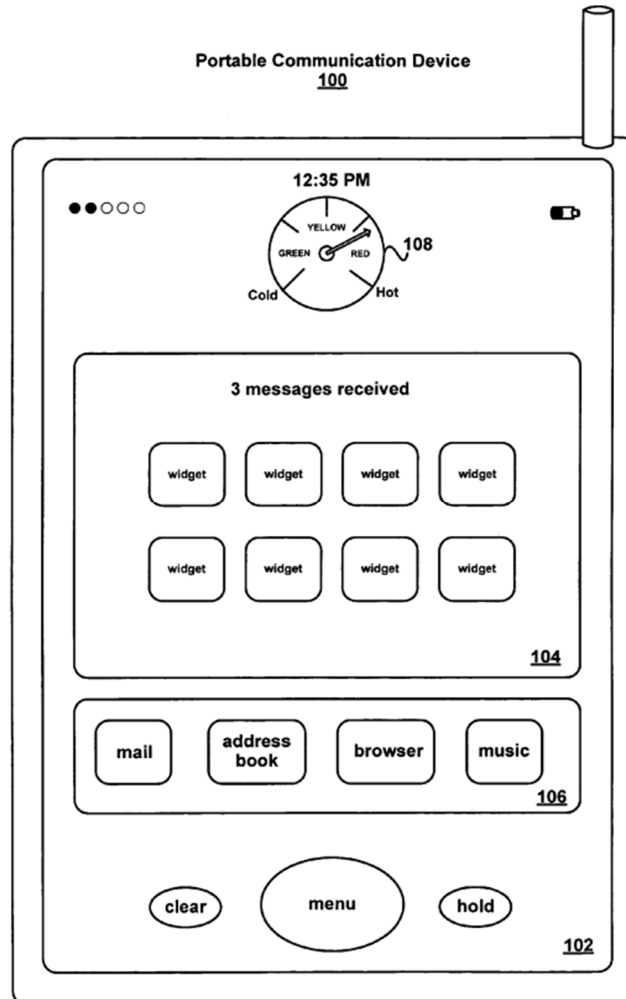
126. The device's operating system (e.g., LINUX, UNIX, OS X, WINDOWS, etc.) "includes various software components and/or drivers for controlling and managing general system tasks (e.g., memory management, storage device control, power management, etc.) and facilitates communication between various hardware and software components."

SAMSUNG-1005, [0047]. The device also includes "applications installed on the device 500, including without limitation, a browser, address book application, contact list application, email client, instant messaging client, word processing application, keyboard emulation application, widgets, JAVA-enabled applications, encryption application(s), digital rights management, etc." SAMSUNG-1005, [0050].

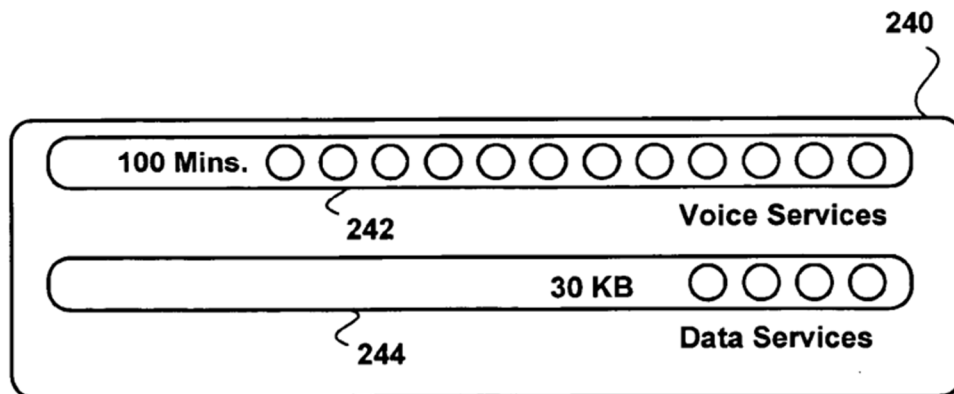
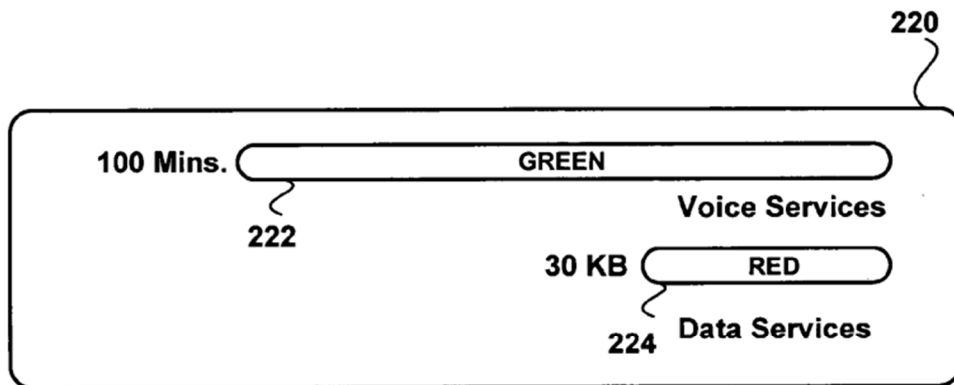
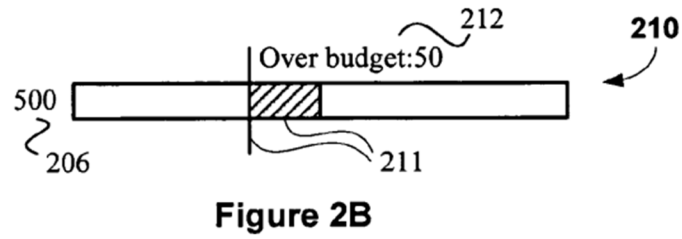
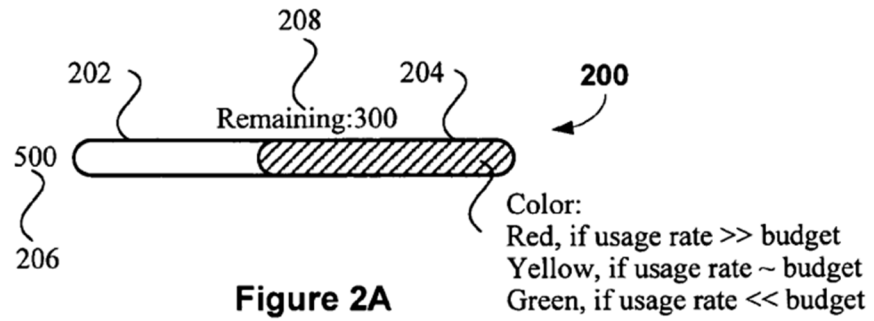
127. The device further includes a meter module to display usage information, e.g., including "arrow that indicates (A) a remaining balance on an account, and/or (B) whether the user's resource usage rate (sometimes called the "burn rate") is less than, approximately equal to, or greater than an average resource usage rate associated with a predefined or user-selected budget for the account." SAMSUNG-1005, [0018], [0052]. Jobs FIG. 1, reproduced below, "is a schematic diagram of one embodiment of a portable communication device for displaying one or more account balances."

SAMSUNG-1005, [0010]. FIGS. 2A-3 show additional "embodiments of

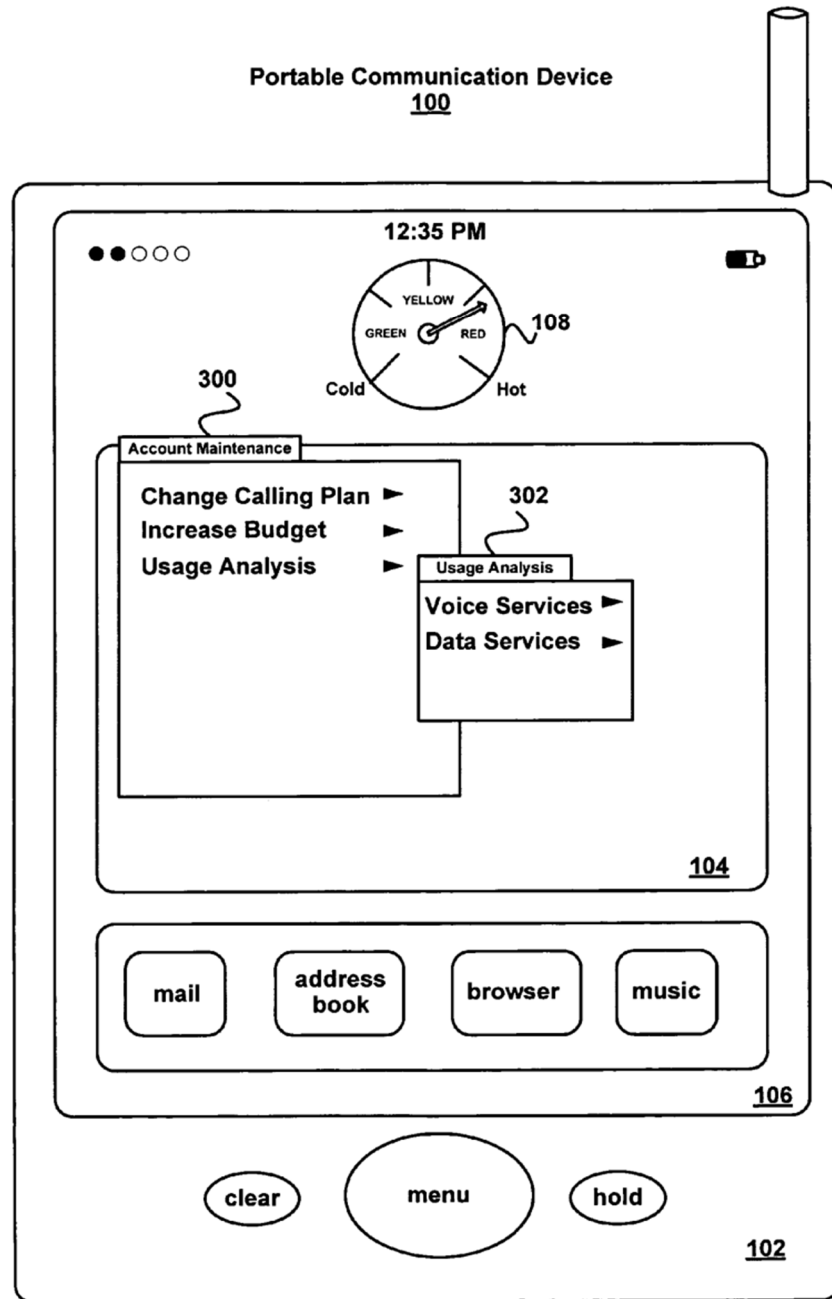
meters for displaying account balances.” SAMSUNG-1005, [0011]-[0012],
FIGS. 2A-3.



SAMSUNG-1005, FIG. 1



SAMSUNG-1005, FIGS. 2A-2D



SAMSUNG-1005, FIG. 3

128. When the device's "account balance drops below a respective threshold value (e.g., determined by the user's account time, or determined by a user selection in a preference pane)," a menu "is automatically

displayed and the user is prompted to make a selection,” such as changing calling plan or increasing budget. SAMSUNG-1005, [0029], [0034], FIG. 3.

B. Jones

129. Jones discloses techniques for “managing data transfers between client computers and a computer network” in which client devices include a “data transfer controller” and “data transfer rules.” SAMSUNG-1006, Abstract, 5:13-6:23. (As I explained in §VII.B, the term “rule” and “policy” are used interchangeably, so a POSITA would have recognized Jones’s use of rules as examples of policies.)

130. Jones explains that “it has become common for client computers to be dynamically connected to the enterprise network through a variety of connection types” and that the “method of connection to the enterprise network may change frequently as the mobile user travels from place to place.” *Id.*, 1:11-17. Jones notes that “each mobile computer may connect to a network via modem, wireless local area network (LAN), direct wired LAN, wireless connection through a wide area network (WAN),” etc., and the capabilities of each connection, such as connection speed, vary from one type to another. *Id.*, 3:17-29. A POSITA would have understood (e.g., from Taylor) that Jones’s modem can be a wireless modem since “[w]ireless radio modems are used to permit remotely located computers and other data

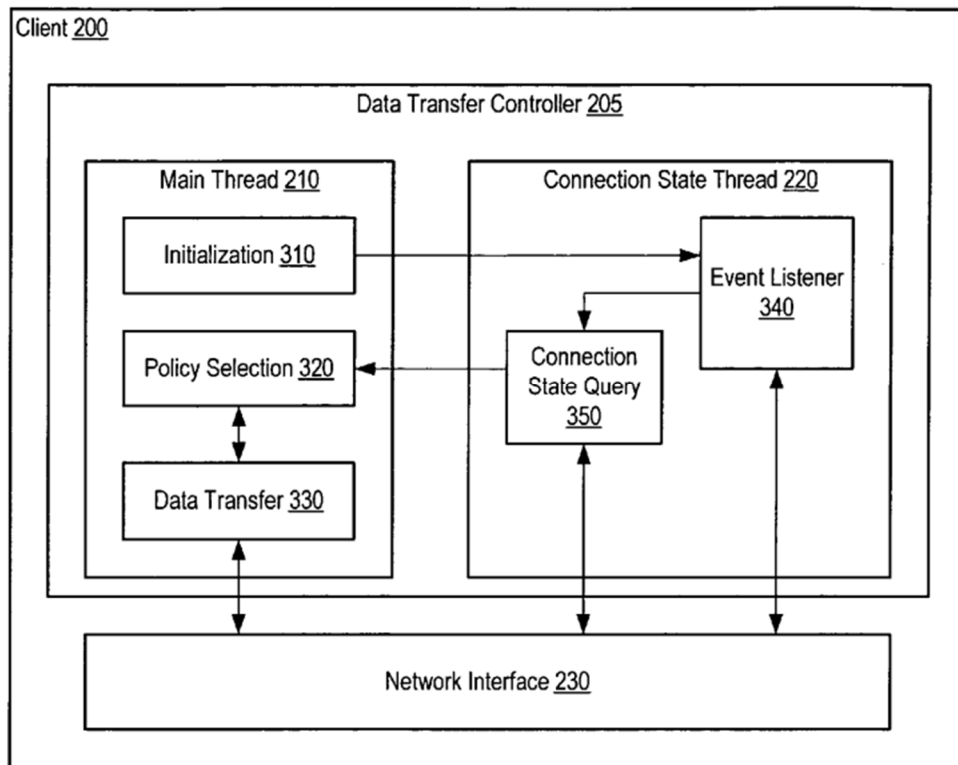
communications equipment to communicate with one or more other computers or equipment for data communications, usually as part of a computer network.” SAMSUNG-1045, 1:53-57.

131. Jones further explains that “[b]ecause of the differing capabilities of various connection types, it is generally desirable for software applications to be able to determine if and when a network connection changes” and that “[t]here are a variety of ways to determine the characteristics of a network connection,” such as using API calls. SAMSUNG-1006, 1:30-36. Jones notes that knowledge of the connection type is important since “it is generally desirable for enterprises to protect the data that resides on mobile computing devices via some type of backup mechanism,” but “changes to the connection type by mobile users tend to complicate any backup mechanism.” *Id.*, 3:30-32, 47-51. In one example, Jones states that, “if the connection type is slow, such as via a modem, a user who is attempting to access e-mail or browse the internet may be frustrated as the available bandwidth is consumed by backup data transfers.” *Id.*, 3:55-58. Therefore, Jones explains that it is desirable for policies to “adjust the frequency of data backups according to the identity of the user, the type of connection, and/or the bandwidth of the connection” and “to determine whether to backup individual files based on the combination of file size and connection type.”

Id., 3:60-67. Jones further explains that rules can prohibit data transfer over certain connection types. *Id.*, 5:25-26.

132. To provide such policy-based management, Jones teaches a client that includes a main thread and a connection state thread, as illustrated in FIG. 3 (below). SAMSUNG-1006, 4:27-32, FIG. 3. The main thread includes code to perform initialization, policy selection, and data transfer. *Id.*, 4:32-35.

The connection state thread includes an event listener and a connection state query. *Id.*, 4:34-36. When the event listener recognizes an event, it causes the connection state query to fetch the current state of network interface and forwards the current connection state to a policy selection component of the main thread. *Id.*, 4:40-45. In response, the policy selection component applies one or more rules for data transfer. *Id.*, 4:45-48.



SAMSUNG-1006, FIG. 3

C. Rao

133. Rao discloses a “remote access architecture” for “peer-to-peer communications and remote access connectivity” on a computing device. SAMSUNG-1007, Abstract, [0098]. The system (e.g., Figure 1A, below) includes clients (e.g., computing devices 102) that communicate over a network to other devices, such as servers and server farms. *Id.*, [0086]-[0096].

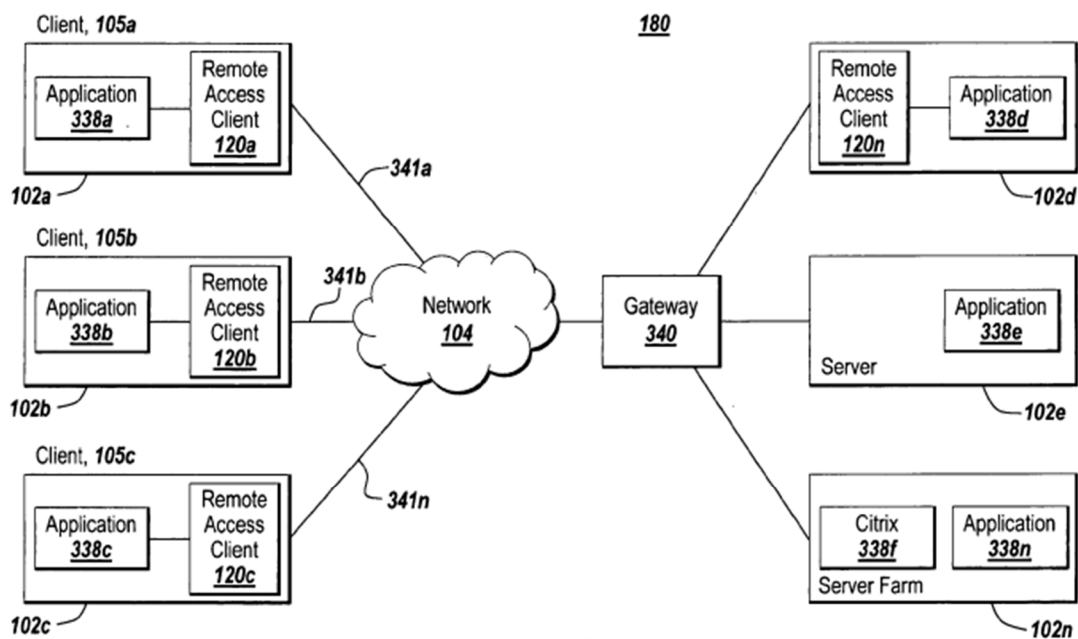


Fig. 1A

SAMSUNG-1007, FIG. 1A

134. Rao addresses inefficient use of network resources when network communications between devices are “processed in the order generated by the activity of a user and applications of the client,” which is not “always desirable” because network packets for background applications may be processed ahead of network packets for foreground applications, resulting in applications experiencing increased latency and reduced quality of voice communication. SAMSUNG-1007, [0003].

135. Rao addresses these inefficiencies through a prioritization scheme that “provide[s] application-aware, client-specific prioritization of packet

traffic,” which is achieved by augmenting the client with a remote access client (RAC) that interacts with the applications and network stack.

SAMSUNG-1007, [0003], [0089], [0098]-[0100].

136. Figure 5A shows an example RAC:

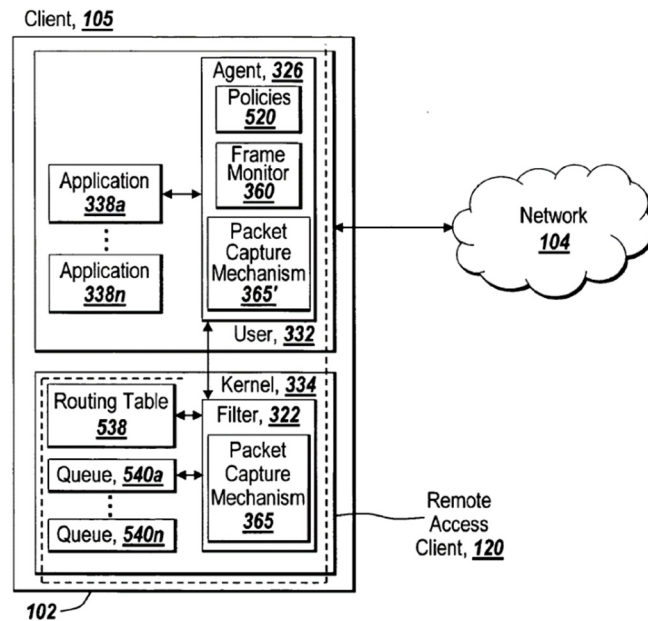


Fig. 5A

SAMSUNG-1007, FIG. 5A

137. RAC can include agent 326 with frame monitor 360 that “include[s] policies and logic for applying a policy to a received packet.” SAMSUNG-1007, [0108]. The “agent 326 uses the policies 520 to apply a priority to network packets of applications 338a-338n in accordance with the prioritization rules specified or indicated by the policies 520.” SAMSUNG-1007, [0189].

138. Rao offers non-limiting disclosure relating to policy specification and how its system leverages policies for prioritization. SAMSUNG-1007, [0182]-[0184]. Rao describes that policies can be specified, e.g., by name or type of application and type of “protocols used by the applications.” SAMSUNG-1007, [0182]. To enable configuration of such policies, Rao’s agent “may provide a configuration mechanism such as a user interface, graphical or otherwise, design[ed] and constructed for configuring or specifying the policies.” SAMSUNG-1007, [0183]. Policies can further be downloaded from a gateway. SAMSUNG-1007, [0183].

139. RAC’s agent indicates the priority to a low-level filter 322 “by any suitable means and/or mechanism such as via an application programming interface (API).” SAMSUNG-1007, [0190]. RAC’s filter then “place[s], arrange[s], or coordinate[s] network packets into queues 540a-540n in support of the priorities” and “the network packets are communicated from the queues 540a-540n according to the determined priorities for the network packets.” SAMSUNG-1007, [0191], [0194].

140. Thus, the use of policies guides efficient use of network resources and enables Rao’s system to address the inefficiencies Rao identifies.

141. Rao’s system further enables 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], [0182]-[0184], FIG. 5A. To perform prioritization, Rao’s system “appl[ies] a policy to determine a condition” of the client, or endpoint, at the time of transmission of the packet.” *Id.*, [0109]. Rao’s frame monitor can identify an application that generated the packet. *Id.*, [0109].

D. Jobs-Rao-Jones Combination

Jobs-Jones

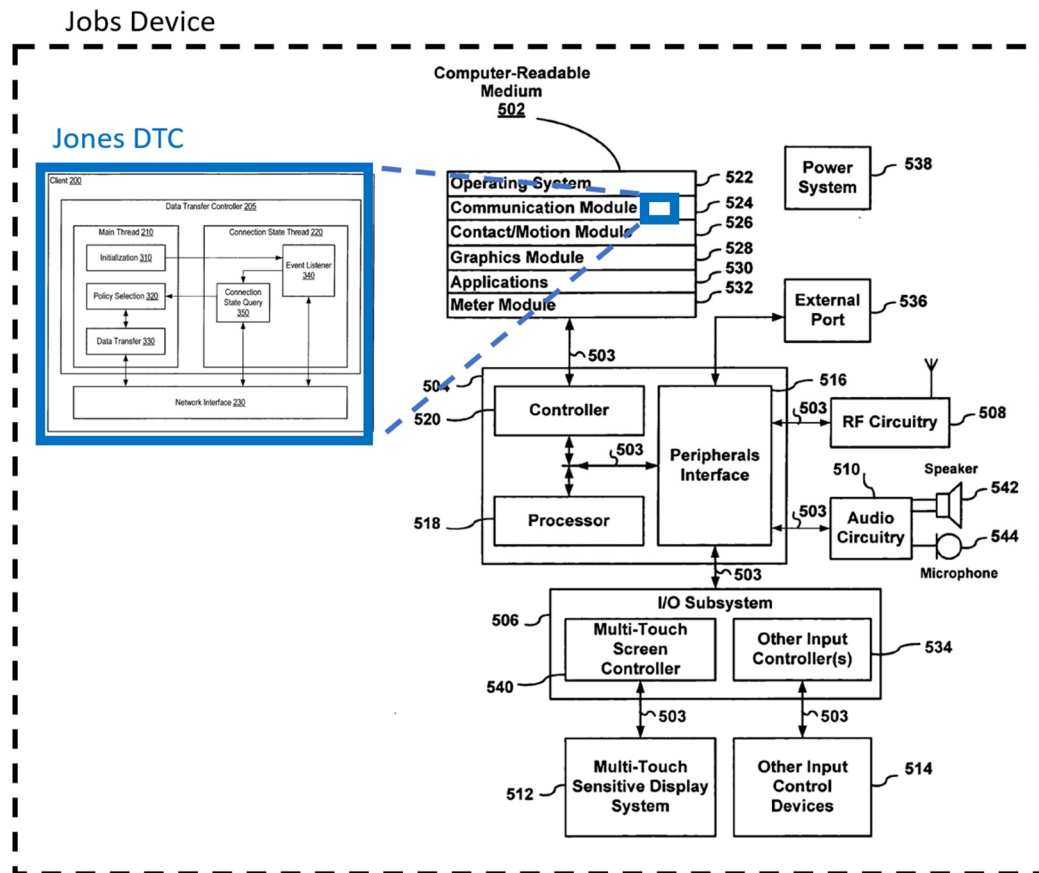
142. Jobs describes a portable device such as a mobile telephone that includes applications, e.g., web browser, email, music, instant messaging, a telephone communication client, VoIP, etc., and can upload and download videos, images, songs, etc. SAMSUNG-1005, [0017], [0040], [0042], [0044], [0050].

143. As explained in Jones, it is desirable “to protect the data that resides on mobile computing devices via some type of backup mechanism.”

SAMSUNG-1006, 1:47-50. A POSITA would have understood that Jobs’s device is a mobile device, and therefore it is desirable to back up its data, as explained in Jones. *Id.*.

144. The resulting Jobs-Jones Device (JJD) is a wireless device that includes components such as memory, processor(s), wireless modems (RF circuitry), an operating system (e.g., Unix or Linux), etc., as taught by Jobs,

augmented with a data transfer controller (DTC), as taught by Jones, that detects connection state and applies policies (e.g., allowing or prohibiting data transfer), as taught by Jones, e.g., as illustrated below. §IX.A; SAMSUNG-1006, Abstract, 2:5-15, 2: 29-40, 5:13-32.



JJD, SAMSUNG-1005, FIG. 5 (annotated); SAMSUNG-1006, FIG. 3 (annotated).

145. While the DTC is illustrated as being in the Communication Module 524, a POSITA would have understood that other design choices are

possible. For example, the entire DTC could be part of the Operating System 522; components of the DTC could run in the Operating System and other components as part of the Communication Module; various components of the DTC could run in the Operating System, Communication Module, and other device subsystems; and so on.

146. JJD includes a modem as taught by Jobs. For example, Jobs describes a device that includes “RF circuitry [that] is used to send and receive information over a wireless link or network to one or more other devices and includes well-known circuitry for performing this function, including but not limited to an antenna system, an RF transceiver, one or more amplifiers, a tuner, one or more oscillators, a digital signal processor, a CODEC chipset, memory, etc.” SAMSUNG-1005, [0042].

147. Per Jobs, JJD’s network access is enabled by a service provider through a service plan that includes data and/or voice services and corresponding resource limits. SAMSUNG-1005, [0002]. Note that a service plan can be a policy or can define one or more policies since service plans can govern device access to a network. For example, as I explained in §VII.A.2, Cunningham gives an example in which, “when the usage exceeds the expected payment, the service can be limited or disabled until the next payment cycle.” SAMSUNG-1010, [0050]. Limiting and/or disabling

services are examples of actions that are taken when a condition (e.g., usage exceeds the expected payment) is satisfied.

148. In JJD, when a trigger occurs, JJD presents usage metrics.

SAMSUNG-1005, [0034], [0036]. Triggers can occur when predefined amount of resource usage occurs and/or when usage rates exceed a threshold. SAMSUNG-1005, [0036]. Per Jobs, JJD includes a user interface that enables users to alter resource limits. SAMSUNG-1005, [0033], FIG. 3. Per Jobs, applications that access JJD resources include, without limitation, SMS, browsers, VoIP, email, etc. SAMSUNG-1005, [0019], [0042], [0050].

149. JJD further includes backup software, per Jones, since a POSITA would have understood that devices, such as the Jobs's device, can become disabled, and thus would have been motivated to include a backup capability so data from applications (e.g., contacts, photos, etc.), as taught by Jobs, are protected. SAMSUNG-1006, 1:47-49. Further, for example, on slow connections, "a user who is attempting to access e-mail or browse the internet may be frustrated as the available bandwidth is consumed by backup data transfers" (per Jones); JJD addresses this concern by reducing network usage on certain networks by altering the frequency of data transfer and/or

by prohibiting data transfer depending on policy decisions. SAMSUNG-1006, 1:55-58; §IX.B.

150. Also per Jones, JJD includes policies that prohibit data transfer over certain connection types. SAMSUNG-1006, 5:25-26; SAMSUNG-1005, [0002]. Thus, JJD has multiple types of policies, including prohibit data transfer over certain connection types (per Jones) and service plan policies (per Jobs). SAMSUNG-1006, 5:25-26. As I discuss below, in the Jobs-Jones-Rao combination, additional policy types are included.

151. In operation, JJD “monitors the state of [the] network interface” and applies rules to data transfers based on “the desired functionality, type of connection, connection bandwidth, user priorities, etc.” SAMSUNG-1006, 4:37-48, 5:13-15. Examples of rules include prohibiting data transfer on a connection type (e.g., GSM), reducing the frequency of backup on a connection type (e.g., CDMA), and permitting data transfer on another connection type (e.g., wi-fi). SAMSUNG-1006, 1:60-64, 5:13-15, 5:25-32. (As I described in §VII.B, in this context, “rule” and “policy” can be used interchangeably.) JJD rules can also be specified based on both connection type and user priority. SAMSUNG-1006, 5:13-15. JJD policies are configured through a GUI, as taught by Jones, which states “a user may be presented with a graphical user interface through which each policy may be

selected and configured in successive operations.” SAMSUNG-1006, 6:38-41.

152. A POSITA would have a reasonable expectation of success in creating a combination, which would have required only routine programming knowledge well within the skill of a POSITA. *Id.* For example, components of JJD from the Jobs device executes applications, and the DTC (from Jones) applies policies based on network conditions. §IX.A; §IX.B. Integrating such components is a routine programming task for a POSITA. Indeed, the change would have amounted to nothing more than the use of a known technique to improve similar mobile devices in a similar way and combining prior art elements according to known methods to yield the predictable results described above.

Jobs-Jones-Rao

153. Jones explains that on slow connections “a user who is attempting to access e-mail or browse the internet may be frustrated as the available bandwidth is consumed by backup data transfers.” SAMSUNG-1006, 1:55-58. In response to such resource contention, Jones describes altering the frequency of some network operations and prohibiting others. SAMSUNG-1006, 3:60-67; 5:25-26.

154. However, a POSITA would have understood that, in some cases, such responses are inappropriate. For example, if a user is on a voice call while streaming video, the device cannot run the video streaming application less often (running a streaming application less often would result in the video stuttering, likely to the point of being unwatchable), and if bandwidth is sufficient for both applications, blocking the streaming is an unnecessarily harsh response since less drastic alternatives exist. For example, as I describe in §VII.D, video application can adapt to available bandwidth, and doing so allows the e-mail application to be responsive to user while still allowing the video to play (perhaps at reduced quality).

155. Of course, there can be situations in which the aggregate bandwidth requirements of applications exceeds available bandwidth. As a simple example, if three applications each require a minimum of 5 Mbs, and the total bandwidth is 10 Mbs, bandwidth will be exhausted. This situation requires the system determine which apps/traffic to prioritize.

156. In one example, van Beek explains that “[t]he maximum throughput of an 802.11b system is barely 6 Mbps,” which is “approximately the rate of a single standard-definition video signal at DVD quality.” SAMSUNG-1040, 1. Gupta similarly explains that “CDMA2000 Evolution Data Only (EVDO) networks that provide up to 2 Mbps and Third Generation GSM

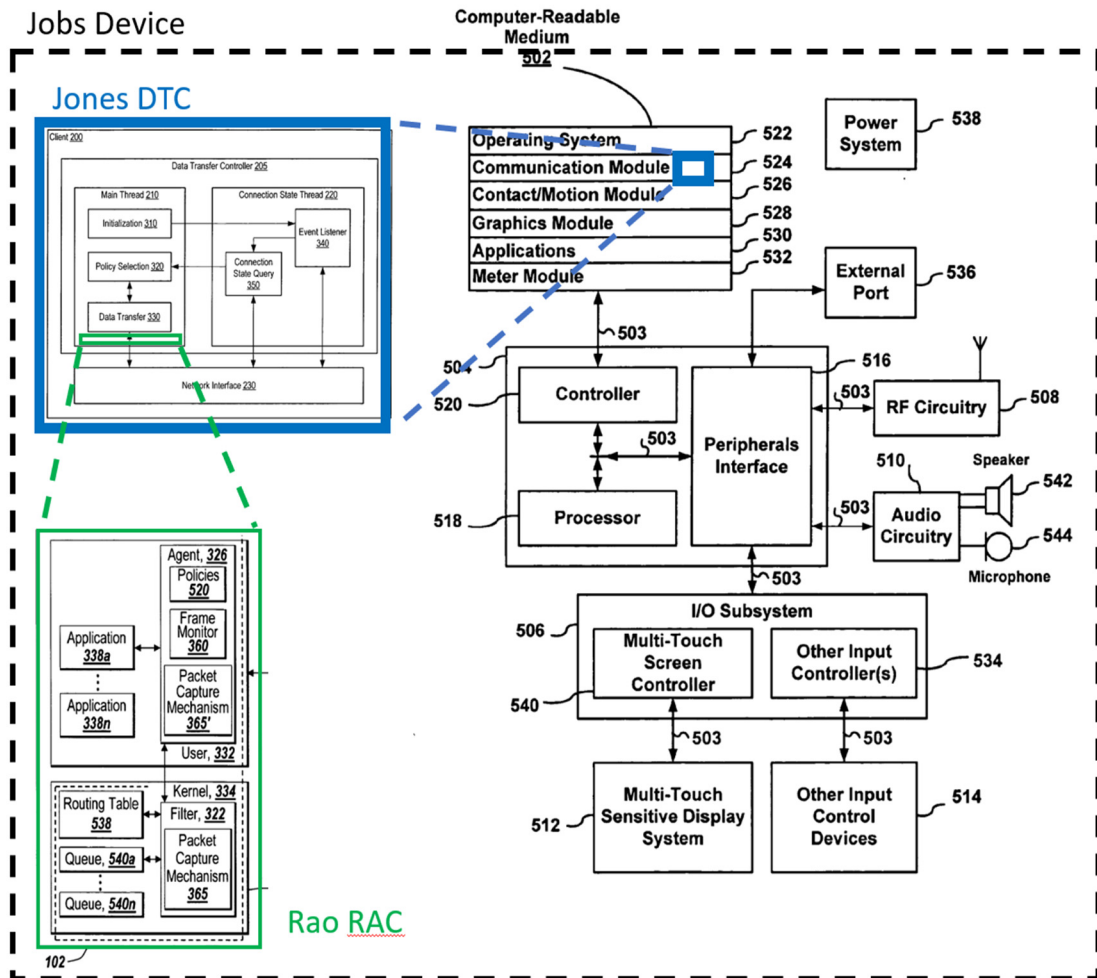
(3GSM) that provide approximately 300 kbps data rates.” SAMSUNG-1039, [0004]. While Rao explains that it is advantageous to prioritize VoIP packets ahead of packets from other applications, a POSITA would have understood that if the other application is streaming a video signal at DVD quality over an 802.11b system, then the connection bandwidth is insufficient to handle packets from both applications since the video streaming would saturate the network. SAMSUNG-1007, [0003]. A POSITA would have further understood that streaming DVD-quality signal over an EVDO or 3GSM network would fail for insufficient bandwidth. SAMSUNG-1039, [0004], SAMSUNG-1040, 1. In such cases, to avoid overwhelming network capacity, adversely impacting all device applications, denying network access to some applications (e.g., as taught in Jones) is necessary. SAMSUNG-1006, 5:13-15.

157. To address cases where multiple applications on JJD (e.g., backup, video conferencing, telephony) are competing for network bandwidth, a POSITA would have further looked to references such as Rao, which teaches that it is also beneficial to share bandwidth by prioritizing traffic from some applications over traffic from other applications to improve device efficiency, e.g., to avoid “increasing the latency and reducing the

quality” for applications such as voice communication. SAMSUNG-1005, [0044]; SAMSUNG-1007, [0003].

158. Rao explains that the network is used inefficiently when packets are “processed in the order generated by the activity of a user and applications of the client,” since network packets for background applications may be processed ahead of network packets for foreground applications, resulting in applications experiencing increased latency and reduced quality of voice communication. SAMSUNG-1005, [0040]; SAMSUNG-1007, [0003], [0130]. As described above, a POSITA would have understood that JJD would suffer such inefficiencies and would have looked to references such as Rao to improve the user experience by prioritizing packets.

159. The resulting Jobs-Jones-Rao Device (JJRD), illustrated below, is a wireless device that includes components of JJD, further including a RAC, as Rao teaches, which provides policy-based, priority queuing based on factors such as application name, application type, whether the application is running in the foreground or background, among other of “the multitude of ways to define client-side application priorities.” SAMSUNG-1007, [0182].



JJRD, SAMSUNG-1005, FIG. 5 (annotated); SAMSUNG-1006, FIG. 3 (annotated); SAMSUNG-1007, FIG. 5A (excerpt, annotated)

160. As I described in ¶[145], components for DTC and/or RAC can be implemented in the Communication Module, Operating System, in other elements of the system, and/or split among various system elements.

161. In operation, JJRD “monitors the state of [the] network interface” and applies data transfer rules, e.g., permitting or prohibiting the transmission.

SAMSUNG-1006, 1:60-64, 5:13-15, 5:25-32. When a transfer is permitted, JJRD passes the data to the RAC, which includes a policy-control agent (RAC's agent) and a low-level policy control agent (RAC's filter). §IX.C.

162. JJRD policies can be specified, e.g., based on connection type, bandwidth, user priority, name or type of application and type of protocols used by the applications. SAMSUNG-1006, 5:13-15; SAMSUNG-1007, [0182]; §IX.B, §IX.C. A POSITA would have understood that, at least in some cases, connection type and protocol are related concepts. For example, the 802.11 protocols are used for wireless LAN connections, and GSM and CDMA are used for cellular (wireless WAN) connections.

163. Examples of policies include, per Jones, prohibiting data transfer on a connection type (e.g., GSM), reducing the frequency of backup on a connection type (e.g., CDMA), and permitting data transfer on another connection type (e.g., wi-fi), and, per Rao, setting priority based on application name or type, based on protocols used by the application, network factors (host name, destination port, etc.) among a “multitude of ways to define client-side application priorities.” SAMSUNG-1006, 1:60-64, 5:13-15, 5:25-32; SAMSUNG-1007, [0182].

164. Based on such policies, JJRD's DTC, which includes a RAC, determines actions for network activities, which can include, for example,

prohibiting a transfer, delaying a backup, and queuing packets. SAMSUNG-1006, 1:60-65, 5:25-32; SAMSUNG-1007, [0184]. When packets are to be queued, JJRD's agent (per Rao) determines the priority based on the policies and passes the priority to a low-level agent (filter, per Rao), which assigns the packets to the appropriate priority-based queue. SAMSUNG-1007, [0184]; §IX.C. JJRD then transmits the packets according to the assigned priority. SAMSUNG-1007, [0184]. Because the transmission is priority-based, lower-priority packets receive less bandwidth than higher-priority packets. SAMSUNG-1007, [0184].

165. JJRD policies are configured through a GUI, as taught by Jones and Rao. For example, Jones teaches that “a user may be presented with a graphical user interface through which each policy may be selected and configured in successive operations,” and Rao similarly teaches that “the agent 326 may provide a configuration mechanism such as a user interface, graphical or otherwise, design and constructed for configuring or specifying the policies 520.” SAMSUNG-1006, 6:38-41; SAMSUNG-1007, [0183]. Policies can further be downloaded (e.g., from network devices such as gateways), as taught by Rao. SAMSUNG-1007, [0183].

166. Thus, the components of JJRD each operate similarly to as they would in isolation. For example, per Jones, JJRD's DTC, which applies policies to

determine (e.g.) whether to permit data transfer. SAMSUNG-1006, 5:13-6:23. Per Rao, RAC within JJRD's DTC applies policy to assign traffic to priority queues. SAMSUNG-1007, [0184].

167. More generally, computing devices, including mobile devices include at least dozens of hardware components (e.g., CPU(s), memory, storage, modems, etc.) and thousands (or more) software components. In cases where a software component was already implemented in one device, integrating that component, or the functions of that component, into a new device was well within the skill of a POSITA and required only routine programming skill.

168. In this particular combination, Jobs-Jones-Rao, the Jobs reference describes a general mobile device that is controlled by a service plan, and computes and presents account metrics. SAMSUNG-1005, Abstract, [0002], [0021]-[0022]. A POSITA would have understood that as of the Critical Date, mobile devices includes numerous other functions that could be integrated with the Jobs device using only routine programming skill.

169. Further, a POSITA would have understood that Jobs does not discuss details regarding optimizations since such optimizations were known and common in computing devices, and therefore POSITA would have naturally included such optimizations in devices, which requires only routine

programming skill. As one example, a POSITA would have understood that task scheduling was well known as of the Critical Date (and long before), and therefore, including task scheduling would have been both natural and routine.

170. The analysis applies to the techniques of Rao and of Jones, which a POSITA would have understood as straightforward device improvements that would naturally be integrated into a device such as the Jobs device. As I stated above, such integrations require at most the skill of a POSITA.

171. This observation applies to all combinations discussed in this document, all of which simply integrate software components from one device into other devices.

172. For at least these reasons, a POSITA would have a reasonable expectation of success in creating a combination, which would have required only routine programming knowledge well within the skill of a POSITA.

For example, integrating Rao's RAC into Jones's DTC requires only routing knowledge. Indeed, the change would have amounted to nothing more than the use of a known technique to improve similar mobile devices in a similar way and combining prior art elements according to known methods to yield the predictable results described above.

173. JJRD's processor would be configured to perform or assist in performing the operations discussed in this Ground, as taught by Jobs. SAMSUNG-1007 [0046] ("The one or more processors 518 run various software components stored in the medium 502 to perform various functions for the device 500."). More generally, processors, such as the one in JJRD (per Jobs), are the device components that perform operations, an observation that applies to all of the Grounds.

E. Bocking

174. Bocking explains that "[m]any handheld electronic devices include wireless telephone and data (e.g., email, SMS, Internet) functionality," and "wireless services, such as telephone and data services, are provided by way of an air interface involving radio frequency (RF) communications between wireless enabled equipment, such as a handheld electronic device" and land based radio transmitters or base stations commonly referred to as a public land mobile networks (PLMNs). SAMSUNG-1009, [0006]. "PLMNs interconnect with other PLMNs and the public switched telephone network (PSTN) for telephone communications or with Internet service providers for data and Internet access." *Id.*

175. Bocking further explains that "to use wireless communications functionality, a user must subscribe with a wireless service provider or

operator,” which permits “the user to utilize the PLMN operated by the service provider or operator (referred to as the ‘home PLMN’).”

SAMSUNG-1009, [0007]. Additionally, Bocking notes that “roaming is a service offered by PLMN operators which allows a subscriber to use his or her wireless enabled equipment while in the service area of another operator (and outside of the user's home PLMN), and that “[r]oaming requires an agreement between operators of technologically compatible systems to permit customers of either operator to access the other’s PLMN.”

SAMSUNG-1009, [0007].

176. With that context, Bocking describes a “handheld electronic device adapted to display a listing of known networks, scan for available networks, display a listing of the available networks and enable the entry of information relating to manually entered networks.” SAMSUNG-1009, Abstract, [0028]. The device stores a list of preferred networks and enables “the assignment of a priority value to each of the preferred networks,” and uses “the preferred networks for performing wireless communications when the device is in a roaming situation,” where the preferred network is determined from the priority ordering. SAMSUNG-1009, Abstract.

F. Jobs-Jones-Rao-Bocking Combination

177. JJRD is a wireless device where network access is governed by service policies comprising access privileges. §IX.D. Such privileges are granted by a particular service provider, per Jobs. SAMSUNG-1005, [0002]. A POSITA would have understood that, when a device moves to a location lacking service from the service provider, network connectivity is lost unless the device obtains service from an alternate service provider. To avoid connectivity loss, a POSITA would therefore have looked to references such as Bocking, which teaches techniques for connecting a device to roaming networks. SAMSUNG-1009, Abstract, [0024], [0028].

178. The resulting Jobs-Jones-Rao-Bocking Device (JJRBD) is a wireless device (per Jobs, Jones, Rao, and Bocking) that supports the service plans of Jobs. §IX.D. When JJRBD moves outside the service provider's coverage, it uses techniques, such as those described in Bocking, to connect to a roaming network, enhancing the connectivity range of the device. SAMSUNG-1009, Abstract, [0024], [0028].

179. Thus, the components of JJRBD each operate as they would in isolation. For example, the components of JJRBD provide wireless device functions, including accessing cellular networks, and use the techniques of Bocking (e.g., network scanning and prioritization) when accessing a roaming cellular network. §IX.D; §IX.A. A POSITA would have a

reasonable expectation of success in creating a combination, which would have required only routine programming knowledge well within the skill of a POSITA. Indeed, the change would have amounted to nothing more than the use of a known technique to improve similar mobile devices in a similar way and combining prior art elements according to known methods to yield the predictable results described above.

180. JJRBD's processor would be configured to perform or assist in performing the operations discussed in this Ground, as taught by Jobs.

SAMSUNG-1005 [0046] ("The one or more processors 518 run various software components stored in the medium 502 to perform various functions for the device 500.").

G. Cunningham

181. Cunningham explains that "mobile users to desire access to mail and communicate in a data-centric manner while mobile," and describes a "business model that is dedicated to supporting a wireless messaging device." SAMSUNG-1010, Abstract, [0006]. In Cunningham, "limitations or restrictions that can be placed on the account based on account history information, current user behavior, subscribed services, services that can or cannot be employed according to the particular user device, and so on," and

“when the usage exceeds the expected payment, the service can be limited or disabled until the next payment cycle.” SAMSUNG-1010, [0050].

H. Jobs-Jones-Rao-Cunningham Combination

182. JJRD is a network device where network access is enabled by a service provider through a service plan that includes data and/or voice services and includes resource limits. SAMSUNG-1005, [0002]; §IX.D.

As I described in §IX.D, service plans are policies (or define policies) related to resource usage.

183. Jobs’s examples include fees for excess usage. SAMSUNG-1005, [0002]. However, since such plans impose no cap on use, the network is exposed to overloading, which diminishes user experience for the connected devices. While different networks have different bandwidth limits, no network offers unlimited bandwidth. For example, van Beek explains that “WLANs based on IEEE 802.11 can operate at several data link rates” and the 802.11b standard operates at 1, 2, 5.5 or 11 Mbps, while the 802.11a standard operates at 6, 9, 12, 18, 24, 36, 48 or 54 Mbps.” SAMSUNG-1040, 1. Once that bandwidth is exhausted, users will experience degraded performance, such as dropped packets and delays. This is true of all networks.

184. Additionally, this single plan does not enable “differentiating access between unlimited included access and other billing models,” as described in Cunningham. SAMSUNG-1010, [0050]. As a result, a POSITA would have looked to references such as Cunningham, which provides alternate service plan structures, such as placing a hard cap on resource consumption.

SAMSUNG-1010, [0050].

185. The resulting Jobs-Jones-Rao-Cunningham device (JJRCD) includes the components of JJRD and is governed by service plans such as hard usage limits after which access is denied. §IX.D; SAMSUNG-1010, [0050]. In operation, when JJRCD hits a resource limit set by the service plan, further usage is denied, per Cunningham. Additionally, per Jobs, JJRCD presents a UI allowing the user to change plans and resume usage. SAMSUNG-1005, [0029].

186. Thus, the components of JJRCD each operate as they would in isolation. For example, components of JJRD continue to provide a functional wireless device, which in JJRCD cellular network access is governed by the service plans of Jobs and Cunningham. §IX.D; §IX.G. A POSITA would have a reasonable expectation of success in creating a combination, which would have required only routine programming knowledge well within the skill of a POSITA. Indeed, the change would

have amounted to nothing more than the use of a known technique (e.g., enforcing additional service plans) to improve similar mobile devices in a similar way and combining prior art elements according to known methods to yield the predictable results described above.

187. JJRCD's processor would be configured to perform or assist in performing the operations discussed in this Ground, as taught by Jobs.

SAMSUNG-1005 [0046] ("The one or more processors 518 run various software components stored in the medium 502 to perform various functions for the device 500.").

I. Padmanabhan

188. Padmanabhan describes a peer-to-peer system that enables monitoring and diagnosing of network problems. SAMSUNG-1011, Abstract. In Padmanabhan, information related to both performance and reliability are gathered from multiple vantage points, correlated, and then analyzed to diagnose problems. SAMSUNG-1011, [0009]. For example, "information describing the performance of the connection includes both the speed of the connection and information about the failure of the connection," and "[r]eliability information is collected across several connections, but it may include the same type of data such as speed and the history of session failures with particular network resources." SAMSUNG-1011, [0009].

189. In Padmanabhan, the information is collected using “[p]assive observations [that] are made at end hosts of end-to-end transactions and shared with other end hosts in the network, either via an infrastructural service or via peer-to-peer communications techniques.” SAMSUNG-1011, [0011].

J. Jobs-Jones-Rao-Padmanabhan Combination

190. Per Rao, JJRD’s RAC considers “network factors in determining what network packets to communicate from what queue,” e.g., RAC can “receive an indication of network congestion” and/or “recognize a high number of retransmits to a particular destination.” SAMSUNG-1007, [0195]. In response, RAC may “throttle back or not communicate network packets related to other networks factors, such as congestion, even though the network packets may have a higher priority than other network packets.” *Id.*

191. A POSITA would have understood that, while RAC reacts to network degradations, it is preferable to proactively identify and address errors, allowing higher-priority packets to be transmitted before lower-priority packets, thus improving performance of applications such as VoIP.

SAMSUNG-1007, [0003]. In such a system, when an error occurs (e.g., a software fault in a router), the system identifies the error so that it can be corrected, and while the corrective actions (e.g., restarting the router) are

being taken, the system adapts its behavior so that it operates well given the degraded operational circumstances, and once the error is remediated, the system returns to normal operation. In contrast, if the error is not identified, the system would continue to operate in the degraded state indefinitely. Consequently, a POSITA would have been motivated to look to references such as Padmanabhan, which teaches techniques for identifying causes of error and other issues to improve performance.

192. The resulting Jobs-Jones-Rao-Padmanabhan Device (JJRPD) is a wireless device (per Jobs, Jones, and Rao) that reports performance metrics to network elements, allowing diagnosis of network issues, per Padmanabhan. §IX.D, §IX.I. Thus, when issues occur, JJRPD adjusts packet transmission order to best use the impaired network (per Rao), and provides reports to other network elements (per Padmanabhan), enabling error remediation. SAMSUNG-1007, [0003], [0195]; §IX.a.

193. The components of JJRPD each operate as they would in isolation. For example, the components of JJRPD from JJRD each operate as they would in isolation, as do the information reporting techniques as taught in Padmanabhan. §IX.D.

194. A POSITA would have a reasonable expectation of success in creating a combination, including the information reporting techniques per

Padmanabhan, which would have required only routine programming knowledge well within the skill of a POSITA. Indeed, the change would have amounted to nothing more than the use of a known technique to improve similar devices in a similar way and combining prior art elements according to known methods to yield the predictable results described above.

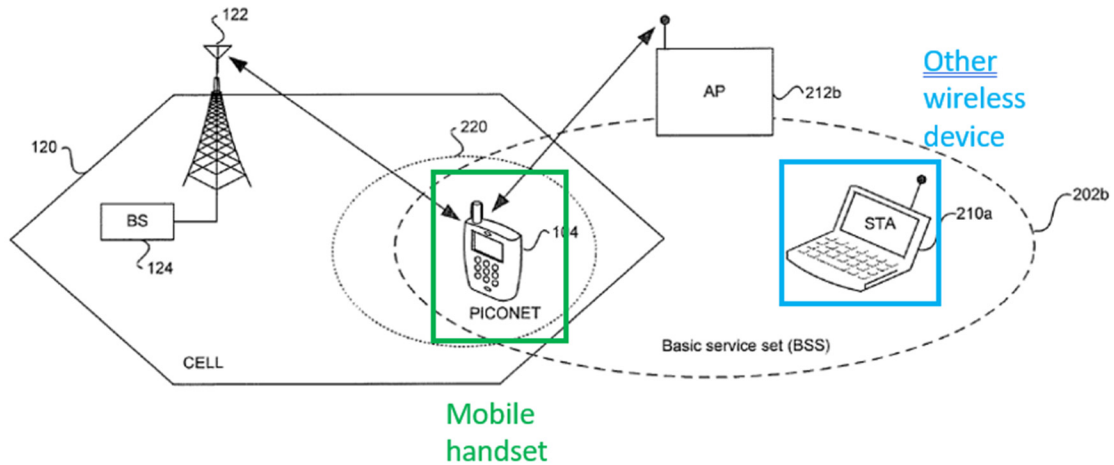
195. JJRPD's processor would be configured to perform or assist in performing the operations discussed in this Ground, as taught by Jobs.

SAMSUNG-1005 [0046] ("The one or more processors 518 run various software components stored in the medium 502 to perform various functions for the device 500.").

K. Ibrahim

196. As shown in FIG. 2A and 4A below, Ibrahim teaches a mobile handset operating as a base station that enables "wireless devices to communicate with each other and/or with a wireless network via the mobile handset," such that the "mobile handset operates as a base station for wireless devices within a personal area or piconet," enabling "access to the cellular network 100 by closely located wireless devices that do not have direct access to the cellular network." SAMSUNG-1012, Abstract, [0029], [0040]. The mobile handset enables "switching and/or routing operations to

enable communication between the cellular network 100 and at least a portion of the closely located wireless devices.” SAMSUNG-1012, [0027].



SAMSUNG-1012, FIG. 2A(annotated).

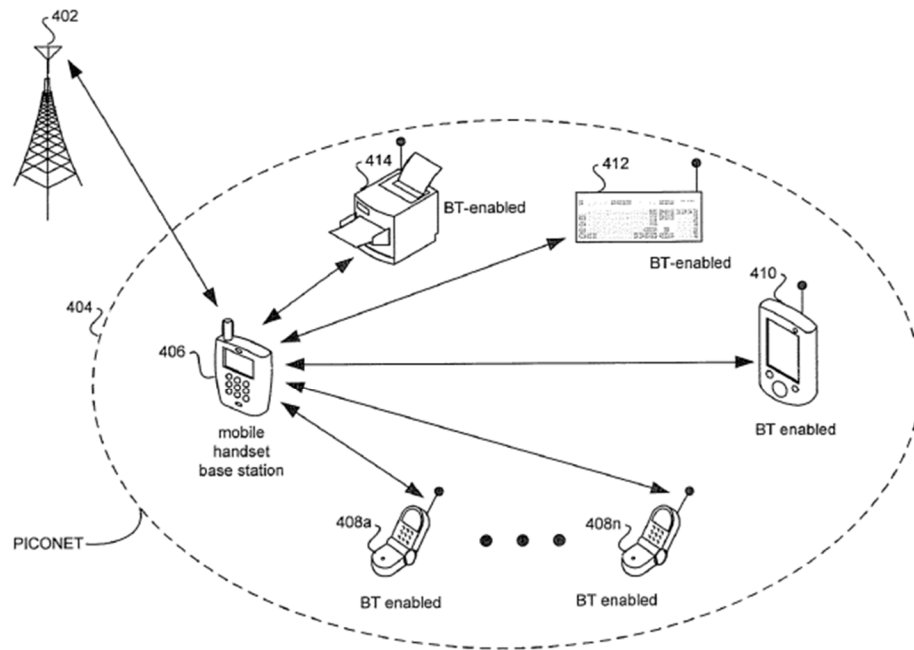
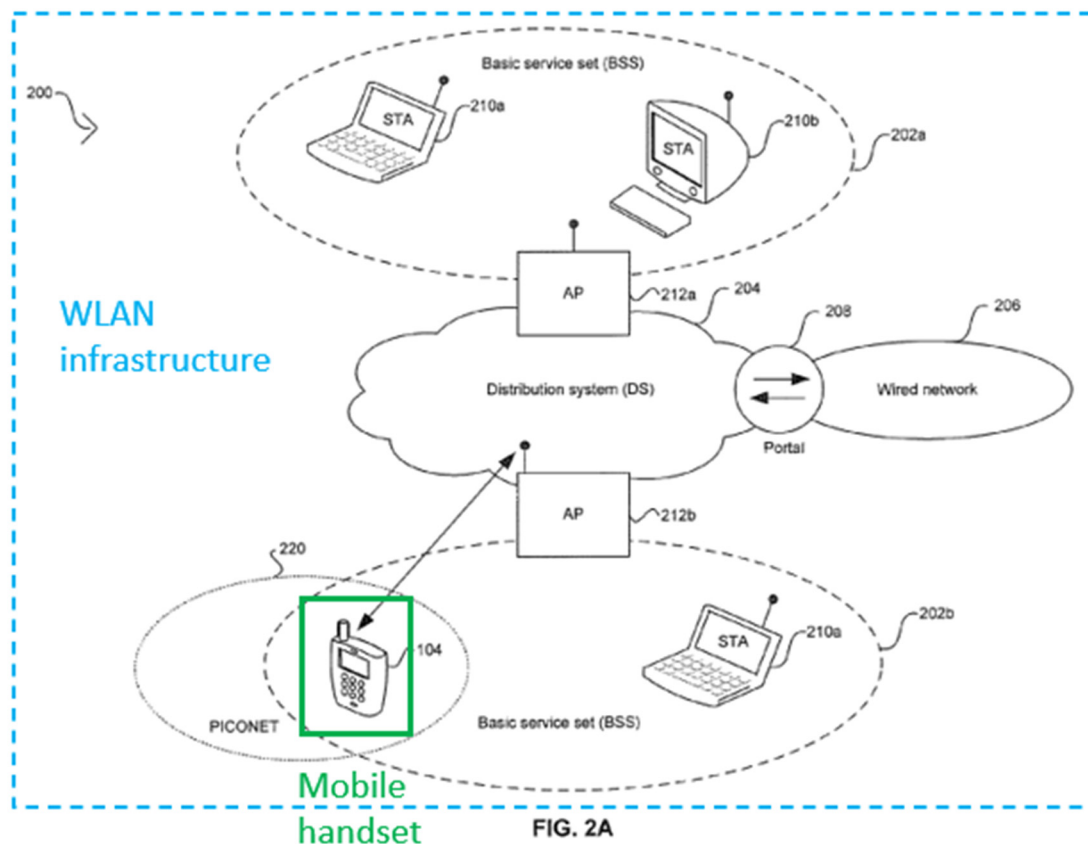


FIG. 4A

SAMSUNG-1012, FIG. 4A.

197. Communication between the wireless devices and mobile handset can use Bluetooth or “another type of wireless technology.” SAMSUNG-1012, Abstract. The mobile handset communicates with the cellular network “over a plurality of radio access technologies, such as GSM and/or WCDMA technologies.” SAMSUNG-1012, [0026]. Additionally, the “wireless connection between the mobile handset base station” and a WLAN infrastructure network can “be utilized for voice and/or data communication.” SAMSUNG-1012, [0038].



SAMSUNG-1012, FIG. 2A(annotated).

L. Jobs-Jones-Rao-Ibrahim Combination

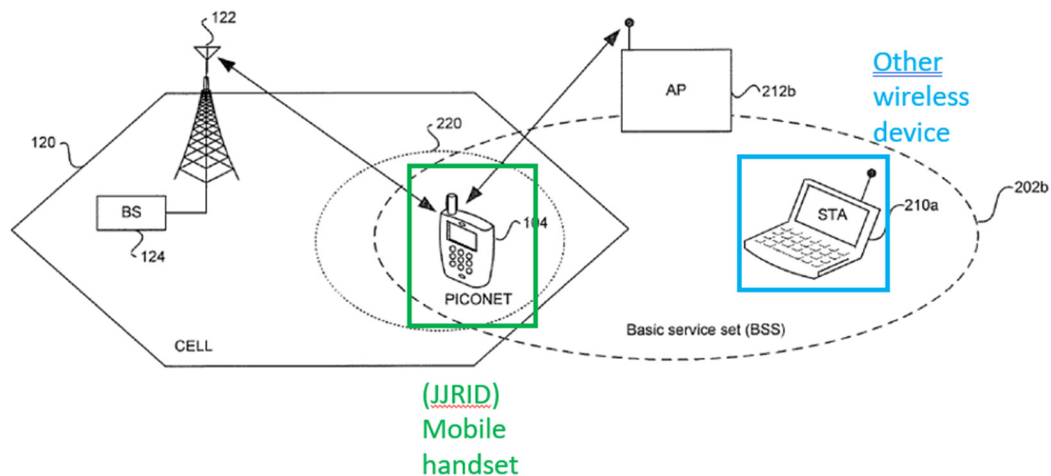
198. JJRD is a computing device with applications including telephony, messaging, etc. §IX.D. To enable JJRD to extend the communication range of other devices, a POSITA would have been motivated to include the mobile base station function disclosed in Ibrahim with the mobile device function of JJRD.

199. The resulting Jobs-Jones-Rao-Ibrahim Device (JJRID) is a wireless device (per Jobs, Jones, Rao and Ibrahim) that serves as a base station relaying traffic between other wireless devices and a cellular network or WLAN (per Ibrahim), thereby increasing the network coverage area for nearby devices. §IX.D; SAMSUNG-1012, Abstract, [0029], [0040]. While including base station functionality does not benefit a particular JJRID instance that is acting as a base station, JJRID does benefit when other devices, include devices owned by the same enterprise (or another cooperating group, such as a family) are able to connect to a network that is otherwise inaccessible. Therefore, a POSITA would have understood that including the base station functionality (per Ibrahim) benefits the enterprise computing environment (or any cooperating group) by enabling devices lacking cellular capability to connect to a cellular network. SAMSUNG-

1006, 1:11-17, 1:47-50, FIG. 1; SAMSUNG-1012, [0022], [0033];

§III.E.1.a.

200. Per Ibrahim, JJRID communicates with other wireless devices over “Bluetooth, WLAN, ZigBee, and/or ultra-wideband.” SAMSUNG-1012, [0056]. JJRID communicates with a downstream network using “cellular radio or a WLAN radio,” e.g., using GSM, CDMA, etc., per Ibrahim. SAMSUNG-1012, [0045].



SAMSUNG-1012, FIG. 2B(modified).

201. Thus, the components of JJRID each operate as they would in isolation. For example, the components of JJRD provide network access for applications on the device, as do the relay techniques as taught in Ibrahim, providing a forwarding service for other wireless devices, including other instances of JJRID. §IX.D; §IX.K.

202. A POSITA would have a reasonable expectation of success in creating a combination, which would have required only routine programming knowledge well within the skill of a POSITA. Indeed, the change would have amounted to nothing more than the use of a known technique to improve similar mobile devices in a similar way and combining prior art elements according to known methods to yield the predictable results described above.

203. JJRID's processor would be configured to perform or assist in performing the operations discussed in this Ground, as taught by Jobs. SAMSUNG-1005 [0046] ("The one or more processors 518 run various software components stored in the medium 502 to perform various functions for the device 500.").

M. Jobs-Jones-Rao-Bocking-Cunningham Combination

204. As discussed in §IX.E, JJRBD is a mobile device. While Jobs provides a single example service plan, Jobs, Jones, Rao, and Bocking are otherwise silent with respect to other service plan options. SAMSUNG-1005, [0002]. For at least the reasons discussed in §IX.H, a POSITA would have looked to references such as Cunningham, which describes various calling plans used by mobile devices, to allow the mobile devices to use different types of calling plans. SAMSUNG-1010, [0012]; §IX.H. For

example, Jobs explains that “[u]sers of portable communication devices (e.g., mobile telephones, handhelds, media players, personal digital assistants (PDAs), BlackBerry™, pocket PCs, Smart Phones, etc.) typically enter into service contracts with service providers for voice and/or data services.” SAMSUNG-1005, [0002]. For a description of such service plans, a POSITA would have looked to references such as Cunningham, which discloses a business model that “offers unlimited services on a dependent device, including mixed limited/unlimited usage models, pre-and post-pay models, and models not found in a conventional monthly recurring charge system,” and addresses service suspension. SAMSUNG-1010, Abstract.

205. The components of JJRBCD each operate as they would in isolation. For example, JJRBCD includes the components of JJRBD that are governed by the service plans of Cunningham. §IX.F; §IX.G.

206. A POSITA would have a reasonable expectation of success in creating a combination, which would have required only routine programming knowledge well within the skill of a POSITA. As described in ¶[167], integrating such components is a straightforward programming task. Indeed, the change would have amounted to nothing more than the use of a known technique to improve similar mobile devices in a similar way and combining

prior art elements according to known methods to yield the predictable results described above.

207. JJRBCD's processor would be configured to perform or assist in performing the operations discussed in this Ground, as taught by Jobs.

SAMSUNG-1005 [0046] ("The one or more processors 518 run various software components stored in the medium 502 to perform various functions for the device 500.").

X. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '110 CLAIMS UNPATENTABLE

A. Ground 1A: Jobs in view of Jones and Rao renders claims 1-16, 19, 21, 23-24, and 27-30 obvious

[1.1] A wireless device comprising:

208. To the extent the preamble is limiting, JJRD renders it obvious.

209. JJRD is a wireless device. §IX.D. For example, Jobs teaches a "portable communication device" that "establish[es] and maintain[s] communications with other devices using one or more known RF communication protocols (e.g., TDMA, CDMA, etc.) and one or more known mobile networking protocols (e.g., GSM, ANSI-41, etc.)" and "is capable of uploading and downloading various objects from the Internet over a wireless network or an external port 536, such as files, songs, digital images, videos, emails, instant messages, widgets (i.e., application programs), and the like." SAMSUNG-1005, [0040], [0042], [0044]. Jobs

further teaches that the device can couple to the Internet and wireless LAN.

SAMSUNG-1005, [0048]. Similarly, Jones's client can be "a mobile client." SAMSUNG-1006, 3:58.

[1.2] one or more modems for enabling the wireless device to communicate over at least two wireless networks, the at least two wireless networks comprising a first wireless network and a second wireless network;

210. JJRD renders [1.2] obvious. §IX.D.

211. JJRD includes a modem(s) that enables the device to communicate over at least two wireless networks, such as a cellular network running GSM, a cellular network running CDMA, and a WLAN. SAMSUNG-1005, [0042]; §IX.D. For example, Jobs describes a device that includes "RF circuitry [that] is used to send and receive information over a wireless link or network to one or more other devices and includes well-known circuitry for performing this function, including but not limited to an antenna system, an RF transceiver, one or more amplifiers, a tuner, one or more oscillators, a digital signal processor, a CODEC chipset, memory, etc." SAMSUNG-1005, [0042]. As I describe in ¶[125], a POSITA would have understood Jobs's RF circuitry as a wireless modem.

212. Jobs further teaches that the device's "one or more processors" communicate with communications network "such as the Internet, intranet(s), Local Area Networks (LANs), Wide Local Area Networks

(WLANs), Storage Area Networks (SANs) and the like, or any suitable combination thereof.” SAMSUNG-1005, [0045]. Similarly, Rao’s “computing device 102 may include a network interface 118 to interface to a Local Area Network (LAN), Wide Area Network (WAN) or the Internet through a variety of connections including, but not limited to ... wireless connections, or some combination,” where the network interface comprises a modem. SAMSUNG-1007, [0125].

213. Thus, a POSITA would have understood from Jobs’s disclosure of RF circuitry and its functionality, and/or Rao’s discussion of its network interface, that JJRD includes one or more modems that communicates over a first and second network, e.g., GSM, CDMA, WLAN.

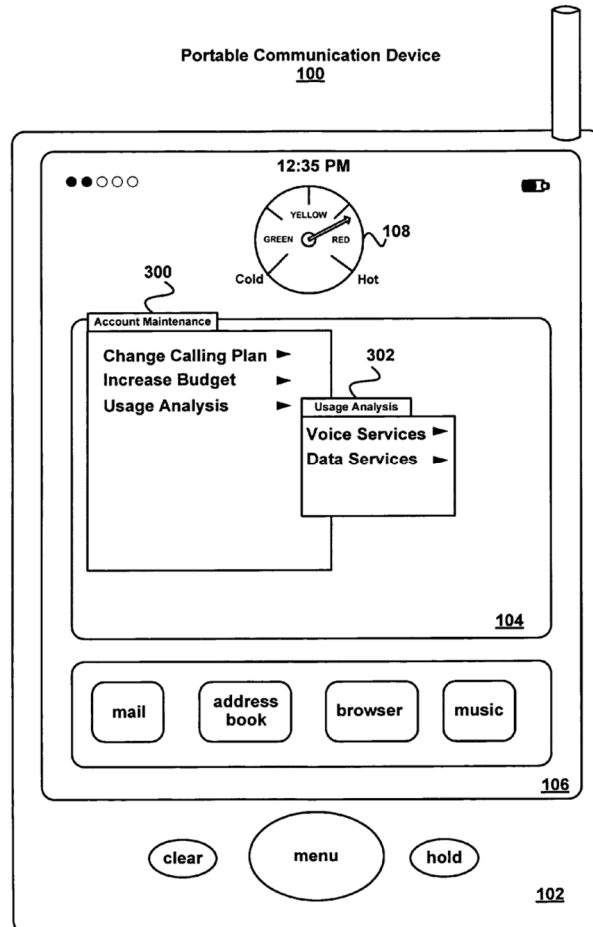
[1.3] a user interface;

214. JJRD renders [1.3] obvious.

215. JJRD includes a user interface, as described in Jobs, Jones, and Rao.

§IX.D. For example, Jobs describes “user interfaces for portable communication devices.” SAMSUNG-1005, [0001]. The device “includes a display surface/graphical user interface (GUI) 102 and one or more graphical objects 108 for displaying information associated with a service account.” SAMSUNG-1005, [0016]. In FIG. 3 (reproduced below), Jobs

illustrates “a user interface that includes a pull-down menu containing account-related actions.” SAMSUNG-1005, [0012].



SAMSUNG-1005, FIG. 3.

216. Further, Jones teaches that “a user may be presented with a graphical user interface through which each policy may be selected and configured in successive operations,” and Rao similarly teaches that “the agent 326 may provide a configuration mechanism such as a user interface, graphical or

otherwise, design and constructed for configuring or specifying the policies 520.” SAMSUNG-1006, 6:38-41; SAMSUNG-1007, [0183].

[1.4] memory configured to store: a first service policy associated with the first wireless network,

217. JJRD renders [1.4] obvious.

218. Per Jobs, JJRD includes “one or more computer-readable mediums 502 (often called memory or storage devices)” and the “computer-readable medium 502 can be any device or medium that can store code and/or data for use by the one or more processors 518.” SAMSUNG-1005, [0040], [0045]. A POSITA would have understood from Jones’s and Rao’s discussions of policies that service policies (e.g., policies taught by Jobs, Jones, and Rao) are sets of instructions stored in memory. SAMSUNG-1006, 5:13-19. For example, Rao teaches that “central processing unit 102 is any logic circuitry that responds to and processes instructions fetched from the main memory unit.” SAMSUNG-1007, [0119]. A POSITA would have understood that policies are an example of such instructions. As I explained in §VII.B, policies are commonly expressed as if-then rules, and such rules would be stored in memory. For example, to evaluate such rules on a CPU-based system (such as Jobs), the rule would be stored in memory. SAMSUNG-1005, [0045]-[0046].

219. Per Jones, in JJRD, service policies are applied to data transfer based on the type of connection, such as GSM, CDMA, WLAN. SAMSUNG-1006, 1:17-22; 5:13-15. Therefore, since Jones teaches that rules can be applied based on type of connection, a POSITA would have understood or found obvious that service policies are associated with wireless networks (GSM, CDMA, WLAN, which are types of connections), including the first wireless network (GSM). SAMSUNG-1006, 5:13-15.

220. JJRD's service policies can specify a variety of action aspects. For example, per Jones, services policies can alter data transfer (e.g., backup) frequency or prohibit transfers; per Rao, service policies can determine transmission priority, and per Jobs, service policies can set resource usage thresholds. SAMSUNG-1005, [0002], [0018]-[0019]; SAMSUNG-1006, 1:60-64, 5:25-26, claim 7; SAMSUNG-1007, [0179]-[0195].

[1.5] the first service policy configured to at least assist in reducing data usage associated with a first service activity over the first wireless network,

221. JJRD renders [1.5] obvious.

222. In JJRD, a first service policy is associated with the first wireless network (GSM). See §X.A.[1.4].

223. JJRD policies reduce data usage associated with service activities.

For example, Jones teaches backup policies that adjust the frequency of, or prohibit, data backups (first service activity) according to the type of

connection. SAMSUNG-1006, 1:60-67, 5:25-26 A POSITA would have understood that, since backups result in data usage, reducing the frequency of backups (which results in data being used less often) and prohibiting backups both reduce data usage over time. Such limitations can be desirable, e.g., on a limited data plan where backup can exhaust the plan's data allocation.

224. Therefore, a POSITA would have understood from Jones' teaching concerning backup policies that JJRD's first service policy reduces the frequency of data backup or prohibits data transfer when on a GSM cellular network, which reduces data usage over the first network.

[1.6] the first service activity being less than all service activities available to the wireless device,

225. JJRD renders [1.6] obvious.

226. JJRD can perform numerous service activities including instant messaging, email, web browsing, downloading media (files, songs, videos, etc.), per Jobs, and backup, per Jones. SAMSUNG-1005, [0044];

SAMSUNG-1006, 5:4-12. Therefore, a first service activity (e.g., media download or backup) is less than all available service activities.

[1.7] the first service policy for enabling control of the first service activity on the first wireless network that is different from how the first service activity is controlled on the second wireless network; and

227. JJRD renders [1.7] obvious.

228. Per Jones, in JJRD, a first service policy enables a first control of a first service activity (e.g., reducing backup frequency) when JJRD is on a first wireless network of a particular type, e.g., GSM cellular). SAMSUNG-1005, [0042]; SAMSUNG-1006, 1:60-64, claim 7. Jones provides examples of network types, e.g., in claim 4, which states, “first connection type and second connection type comprise a modem connection, a wireless LAN connection, a WAN connection, or a cabled LAN connection.” SAMSUNG-1006, claim 4. (See also SAMSUNG-1006, 1:17-29.)

229. Jones further teaches that connection type is used at least to determine connection speed, writing, e.g., “applying the first data backup rule to the client device, in response to detecting said connection state *corresponds to a first connection type transmitting data at a first speed.*” SAMSUNG-1006, claim 7. Jones similarly writes that, “[w]hile it is generally useful to be able to use a variety of *connection types, the capabilities of each connection vary* from one type to another,” e.g., “*modem connections are generally slower than wireless connections*, which may be slower than directly cabled connections.” SAMSUNG-1006, 1:22-27. Jones further writes that “if the *connection type is slow*, such as via a modem, a user who is attempting to access e-mail or browse the internet may be frustrated as the available bandwidth is consumed by backup data transfers.” SAMSUNG-1006, 1:55-

59. A POSITA would have understood from these teachings in Jones that the connection speed is a key characteristic of each network type, which aligns with Jones's teaching that backups on slow networks impair user experience. SAMSUNG-1006, 1:55-59.

230. JJRD supports additional connection types including cellular connection types such as GSM and CDMA. SAMSUNG-1005, [0042]; §IX.D. A POSITA would have understood from Jones's discussion of how policy relates to network types ("it may not be necessary to require the same backup *policy for every user regardless of connection type*") that, when a device (such as JJRD) supports additional or different connection types (e.g., JJRD's GSM and CDMA), the device has policies configured for each of those network types. SAMSUNG-1006, 1:58-60.

231. Thus, in one example, the policy can specify that, when JJRD is on a GSM network, backup frequency is adjusted according to the connection bandwidth (speed), per Jones. SAMSUNG-1006, 1:60-64. However, when JJRD is on a second network (e.g., CDMA cellular), the backup frequency is also adjusted, but since the bandwidth of CDMA and GSM networks differ, the frequency of backup will also differ. SAMSUNG-1006, 1:60-64, claim 7; SAMSUNG-1049, 8-10, 12, 14. Therefore, the control (backup

frequency) of the first service activity (backup) differs between the first and second network.

232. While CDMA cellular is used as an example of a second wireless network, a POSITA would have understood that other wireless network types can be the second wireless network. One example is a WLAN using the 802.11 protocol. Similarly, other cellular protocols can be used.

233. Further, a POSITA would have understood that one purpose of policies is to ensure that resources (compute, storage, bandwidth, etc.) are used efficiently.¹⁶ In this particular case, an administrator can set backup policies such that backups occur more frequently on faster networks, and less frequently (or not at all) on slower networks. In fact, Jones explains that “[d]epending on a number of factors, it may not be necessary to require the same backup policy for every user regardless of connection type,” and “enterprise data protection strategy may prefer to adjust the frequency of data backups according to ... the type of connection, and/or the bandwidth of the connection.” SAMSUNG-1006, 1:58-64.

¹⁶ Policies are also used to maintain security, efficiency and reliability, among other reasons.

234. In this case, where one policy applies to GSM networks, and another policy applies to CDMA network (or a different network type such as wi-fi or a different cellular protocol), JJRD's policies are set to account for factors such as differences in bandwidth, e.g., as explained in Jones, between GSM and CDMA. *Id.*

235. Additionally, as described in Jones claim 7, the device performs differently depending on the connection type:

applying the first data backup rule to the client device, *in response to detecting said connection state corresponds to a first connection type transmitting data at a first speed;*

applying the second data backup rule to the client device, *in response to detecting said connection state corresponds to a second connection type transmitting data at a second speed which is lower than the first connection speed*

SAMSUNG-1006, claim 7, annotated.

236. Such a policy is naturally expressed as a condition-action rule (also known as an if-then rule), as described in section §VII.B. For example, the first rule could be written, "IF connection state EQUALS first connection type, THEN transmit at first speed," and "IF connection state EQUALS

second connection type, THEN transmit at second speed,” where the second speed would be defined to be slower than the first speed.

237. In another example, a first policy (applicable to GSM networks) can specify that backup is not permitted, and a second policy (applicable to CDMA networks) can specify that backup is permitted. SAMSUNG-1006, 5:25-26; §IX.D. Thus, control of the first service activity differs between GSM (first network) and CDMA (second network).

238. In a further example, a first policy (applicable to GSM networks as determined by protocol, per Rao) can specify that packets are assigned to one queue, and a second policy (applicable to CDMA networks as determined by protocol per Rao) can specify that packets are assigned to a different queue. SAMSUNG-1007, [0182], [0184].

[1.8] one or more processors for executing one or more agents, the one or more agents configured to:

239. JJRD renders [1.8] obvious.

240. A POSITA would have understood from the '110 patent that “agent” refers to software components, which are “software components stored in the medium 502 to perform various functions for the device 500.”

SAMSUNG-1005, [0046]. For example, the '110 patent describes a service processor that includes “policy control agent,” “service monitor agent,” “billing agent,” etc., and “all or substantially all of the service processor 115

functionality (as discussed herein) is implemented and stored in software that can be performed on (e.g., executed by) various components in device 100.” SAMSUNG-1001, 28:7-11, FIG. 16.

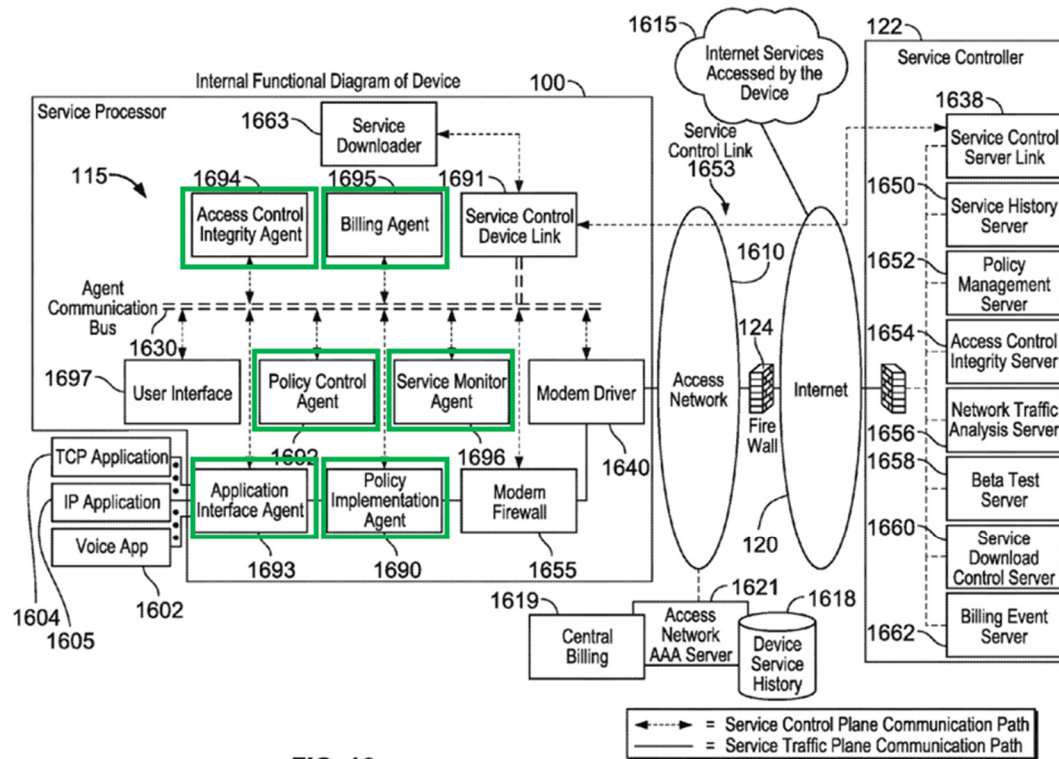
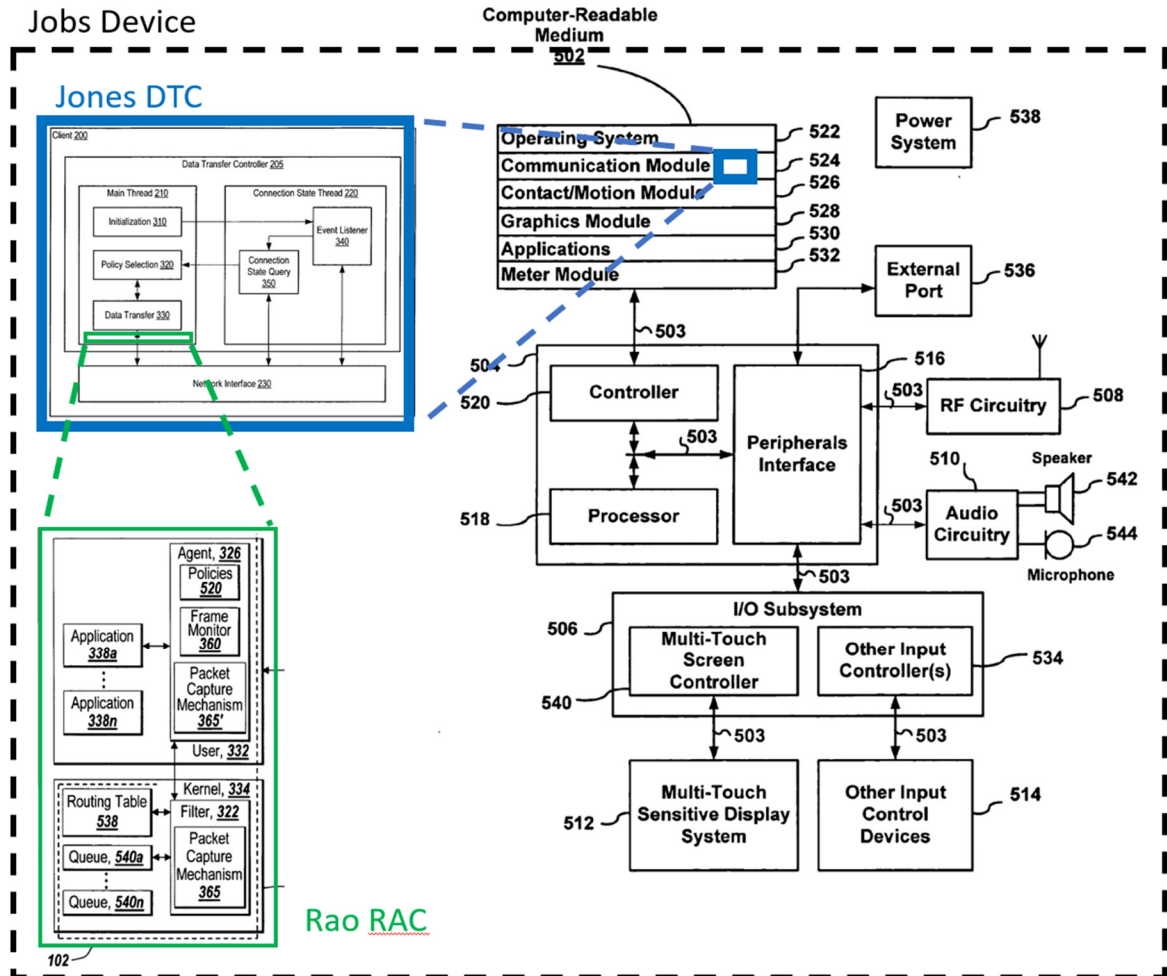


FIG. 16

SAMSUNG-1001, FIG. 16 (annotated).

241. Per Jobs, JJRD includes “one or more processors 518 [that] run various software components stored in the medium 502 to perform various functions for the device 500.” SAMSUNG-1005, [0046]. JJRD includes agents such as, e.g., policy selection and data transfer (per Jones’s DTC), and frame monitor and packet capture mechanism (per Rao’s RAC).

SAMSUNG-1006, 4:27-36, FIG. 3; SAMSUNG-1007, [0179]-[0180], FIGS. 1C, 5A.



JJRD, SAMSUNG-1005, FIG. 5 (annotated); SAMSUNG-1006, FIG. 3 (annotated); SAMSUNG-1007, FIG. 5A (excerpt, annotated).

242. Structures such as the one illustrated above are common in software design. A component that performs multiple functions, such as communication module 524 will be designed as an aggregation of smaller

modules, e.g., including the DTC and many of other communication functions. In addition, the DTC itself will have multiple components, including Rao's RAC and other DTC components. Such hierarchical structures such as this containing components and sub- and sub-sub components allow functional isolation. Hierarchical designs make implementing and testing significantly easier than monolithic designs, and are thus widely used in software systems.

243. Consistent with this design philosophy, both DTC and RAC are agents that can be viewed as containing other agents. For example, the RAC has a frame monitor and packet capture mechanism, and DTC has even listener and policy selection, among other components that can be agents.

244. Further, as described above, the various components (DTC, RAC, etc.) can be implemented in various way, including as part of the operating system.

[1.9] obtain, through the user interface, a user input specifying at least an aspect of the first service policy,

245. JJRD renders [1.9] obvious.

246. JJRD includes a user interface for obtaining user input specifying a policy, per Jones and Rao. §IX.D. For example, Jones teaches that "a user such as a system administrator may ***configure policies*** for data transfers such as backups, updates, etc. that are sensitive to the type of connection and

various characteristics of the network connection” and “a user may be presented with a graphical user interface through which each policy may be selected and *configured in successive operations.*” SAMSUNG-1006, 5:15-29. Rao similarly teaches that “the agent 326 may provide a configuration mechanism such as a user interface, graphical or otherwise, design and constructed for configuring or specifying the policies 520.” SAMSUNG-1007, [0183].

247. In JJRD, policies, which are obtained as user input from the user interface (per Rao and Jones), consist of condition aspects (e.g., device is using GSM cellular) and action aspects (e.g., reduce backup frequency per Jones). SAMSUNG-1006, 1:60-64, 5:15-29; SAMSUNG-1007, [0183].

JJRD policies can also include prioritization policies (per Rao) and service plan policies (per Jobs), among other examples. SAMSUNG-1007, [0179]-[0195]; SAMSUNG-1005, [0002].

248. As I described in §VII.B (e.g., ¶¶[94]-[100]), it was common (and indeed ubiquitous) as of the Critical Date to define policies using a user interface. Since the purpose of a user interface is to present to a user and to obtain information from a user, a POSITA would have known that policy user interfaces are used to specify aspects of policies, and such aspects are

specified by the user input obtained from the policy user interface. In JJRD, such aspects are condition and action aspects.

[1.10] identify that the wireless device is connected to the first wireless network,

249. JJRD renders [1.10] obvious.

250. Per Jones, JJRD identifies that it is connected to the first wireless network (GSM). For example, Jones's DTC "also detects a connection state," which "corresponds to a connection type." SAMSUNG-1006, Abstract, claim 7. Jones provides one example in which, "[f]or a modem policy, a system administrator may decide that modem connections have lower bandwidth than non-modem connections," so "the system administrator may apply a rule that distinguishes between connections that use a modem and connections that do not," e.g., "a first rule may prohibit data transfers over a modem connection." SAMSUNG-1006, 5:20-26.

While Jones lists only one example (modem) in this passage, a POSITA would have known that such policies can apply to other network types, including network types such as " various combinations of modem banks, direct LAN connections, wireless connections, WAN links, etc." as explained in Jones. SAMSUNG-1006, 3:8-36. In addition, Jones explains that mobile clients can be connected to the enterprise network via wireless connections. SAMSUNG-1006, 3:28-32.

251. Therefore, when the connection type is GSM cellular, JJRD identifies that the wireless device is connected to the first wireless network (GSM), per Jones.

[1.11] identify an intended, attempted, or successful data communication over the first wireless network, the intended, attempted, or successful data communication over the first wireless network being associated with the first service activity, and

252. JJRD renders [1.11] obvious.

253. Per Jones, JJRD data transfers move data between a client and other network-connected devices, including transfers of data to a backup medium over the enterprise network, and file sharing, software updates, virus definition updates, which transfer data either from the client to the enterprise network or from the enterprise network to the client. SAMSUNG-1006, 5:4-12. Per Jones, JJRD applies policies to such data transfers. SAMSUNG-1006, 4:46-47, FIG. 3. Therefore, in view of Jones' discussion of data policies, a POSITA would have understood that JJRD identifies an intended or attempted data transfer so that it can apply the policies.

254. In fact, a POSITA would have understood that any policy that limits bandwidth that is consumed by an application or device is operating on a successful data communication – that is, the communication that was limited. Jones explains that “[f]or a modem policy, a system administrator may decide that modem connections have lower bandwidth than non-modem

connections.” SAMSUNG-1006, 5:20-22. That a connection has lower bandwidth indicates that the bandwidth is used for successful communication.

255. Typically, a policy is applied when communication is attempted, for at least the reason that if the policy prohibits the transmission, applying the policy after the transmission is successful would not implement the intent of the policy – that is, to block the transmission. In one example, Rao teaches that its client intercepts packets (attempted data communication) from an application (first service activity), assigns the packet to a priority queue, and communicates the packets according to the priority. SAMSUNG-1007, [0179]-[0195].

256. Per Jobs and Jones, JJRD can communicate data over a first network (e.g., GSM cellular) associated with a first activity (e.g., backup), among other network types (e.g., CDMA cellular). SAMSUNG-1005, [0042] SAMSUNG-1006, 5:25-26.

[1.12] apply the first service policy.

257. JJRD renders [1.12] obvious.

258. Per Jones, JJRD “associates each of at least two connection states with one of the data transfer rules,” “detects a connection state of a client device,” and “applies a first data transfer rule to the client device in response to

detecting a first connection state.” SAMSUNG-1006, 2:8-13. Jones further explains that data backup frequency can be adjusted based on network type, which can be GSM (per Jobs). SAMSUNG-1005, [0042]; SAMSUNG-1006, 1:61-64; *supra* [1.7]. Since Jones explains that backup frequency can depend on enterprise policies, a POSITA would have understood that reducing backup frequency (e.g., on the first network, GSM) is applying the first service policy. SAMSUNG-1005, [0042]; SAMSUNG-1006, 3:48-51.

259. Additionally, Rao teaches that its client intercepts packets (attempted data communication) from an application (first service activity), assigns the packet to a priority queue (applying the policy), and communicates the packets according to their priority. SAMSUNG-1007, [0184].

[2] The wireless device recited in claim 1, wherein the first service activity is associated with an application on the wireless device, a network communication end point, a traffic type, a content type, a download, an upload, or a combination of these.

260. JJRD renders [2] obvious.

261. JJRD associates the first service activity with a content type (e.g., backup data or virus definition), a download, and/or an upload.

SAMSUNG-1006, 5:7-12. For example, Jones teaches that a rule can apply to data backup (which a POSITA would have understood as upload since files are moving from the device being backed up to a backup service), file sharing (which a POSITA would have understood as upload and/or

download since the files are being shared among computer, which indicated bidirectional file movement), and virus definition updates (which a POSITA would have understood as download since they are delivered from the server that has the virus definitions to the device running the antivirus program).

SAMSUNG-1006, 5:7-12; 26-29. For example, files can be shared from JJRD to other devices, which is a file upload and/or files from other devices can be shared with JJRD, which is a file download. Additionally, virus definition update requires at least a download of the new virus definitions and can also include an upload of the definitions previously installed on JJRD, e.g., to determine which virus definition updates are required on JJRD. Similarly, Rao explains that policies can be based on application name or type and destination network address (communication end point). SAMSUNG-1007, [0182].

262. Note further that even if the intent is to transfer a file in one direction (upload or download), network traffic flows in both directions. For example, using the Transmission Control Protocol (TCP), when a packet is transmitted from device 1 to device 2, upon receipt of the packet, device 2 will send an acknowledgement that the packet was received. *See, generally*, SAMSUNG-1046; *discussion of* [22.1].

[3.1] The wireless device recited in claim 1, wherein the one or more agents are further configured to: identify that the wireless device is connected to the second wireless network,

263. Counsel has informed me that duplicated claim elements do not carry independent patentable significance. A POSITA would have understood that if a device can identify that it is connected to a first wireless network, as recited in [1.10], then it can identify that it is connected to a second wireless network. Thus, for at least the reasons discussed in [1.10], JJRD renders [3.1] obvious. This analysis is applies to elements [3.2] and [3.3], which mimic the language of [1.11] and [1.12], respectively.

264. Additionally, JJRD identifies that it is connected to a second wireless network (e.g., CDMA cellular). SAMSUNG-1005, [0042]. For example, Jones's DTC "also detects a connection state," which "corresponds to a connection type." SAMSUNG-1006, Abstract, claim 7. Therefore, when the connection type is CDMA cellular, JJRD identifies that the wireless device is connected to the second wireless network (CDMA cellular).

SAMSUNG-1005, [0042]. As I explained in reference to [1.7], a POSITA would have understood that administrators set different policies for different network types, e.g., as explained in Jones. SAMSUNG-1006, 1:58-64.

[3.2] identify an intended, attempted, or successful data communication over the second wireless network, the intended, attempted, or successful data communication over the second wireless network being associated with the first service activity, and

265. For at least the reasons discussed in [1.11], JJRD renders [3.2] obvious.

266. Additionally, per Jones, JJRD applies policies to data transfers. SAMSUNG-1006, 4:46-47, FIG. 3; §X.A.[1.11]. Therefore, a POSITA would have understood that JJRD identifies an intended or attempted data transfer so that it can apply the policies, per Jones. Per Jobs, JJRD can communicate data associated with a first activity (backup) over a second network (e.g., CDMA cellular). SAMSUNG-1005, [0042].

267. Further, Rao teaches that its client intercepts packets (attempted data communication) from an application (first service activity), assigns the packet to a priority queue (applying the policy), and communicates the packets according to the priority. SAMSUNG-1007, [0184].

[3.3] apply the first service policy.

268. For at least the reasons discussed in [1.12]. JJRD renders [3.3] obvious.

269. Additionally, per Jones, in JJRD, a first service policy enables a first control of a first service activity (e.g., reducing backup frequency). SAMSUNG-1006, 1:60-64; §X.A.[1.7]. For example, the policy can specify that backup frequency is adjusted according to the connection bandwidth, so when JJRD is on a second network (e.g., CDMA cellular), the

policy is applied, adjusting the backup frequency according to the second network's bandwidth. SAMSUNG-1006, 1:60-64.

[4.1] The wireless device recited in claim 1, wherein the memory is further configured to store a second service policy associated with the second wireless network, the second service policy configured to assist in reducing data usage over the second wireless network associated with the first service activity, and wherein the one or more agents are further configured to:

270. For at least the reasons discussed in [1.4] and [1.5], JJRD renders [4.1] obvious. §X.A.[1.4]-[1.5]. A POSITA would have understood that if a device can perform the operations cited in this element on a first wireless network, it can also perform them on a second wireless network. This analysis also applies to limitations [4.2], [4.3], and [4.4], which duplicate the elements recited in [1.10], [1.11], and [1.12],

271. Additionally, in JJRD, the memory stores a second policy associated with the second wireless network. For example, per Jones, in JJRD, service policies are applied to data transfer based on the type of connection (e.g., GSM and CDMA, per Jobs). SAMSUNG-1005, [0042]; SAMSUNG-1006, 1:17-22; 5:13-15. Therefore, a POSITA would have understood that service policies are associated with wireless networks including the second wireless network (CDMA cellular). §X.A.[1.4].

272. The second policy can be further specified based on user priority, per Jones. SAMSUNG-1006, 5:13-15. In one example, the second policy

specifies that, if connected to a second network (CDMA) and the user priority is low, backup is prohibited, reducing data usage. SAMSUNG-1006, 5:13-15, 25-26. A POSITA would have understood that the second policy has a higher priority than the first policy, and therefore, only the second policy would be applied. As I discussed in §VII.B, assigning priorities to policies was common as of the Critical Date, e.g., to resolve cases where the condition aspects of multiple policies evaluate to TRUE.” SAMSUNG-1023, 2; SAMSUNG-1029, 14, 16, 21-23; ¶[90].

273. The second policy would be assigned a higher priority since it is more specific than the first policy since it depends not only on network type, but also on use priority. For example, the first policy generally specifies backup frequency on a network type for all users, while the second policy applies only to a specific subset of users, and thus is assigned a lower priority. Here the first general policy serves as a default, while the second, more specific policy overrides the default (via the higher priority) only for a specific subset of users.

[4.2] identify that the wireless device is connected to the second wireless network,

274. For at least the reasons discussed in [1.10], JJRD renders [4.2] obvious.

275. Additionally, per Jones, JJRD identifies that it is connected to the second wireless network (CDMA). §X.A.[1.10]. For example, Jones’s DTC “also detects a connection state,” which “corresponds to a connection type.” SAMSUNG-1006, Abstract, claim 7. Therefore, when the connection type is CDMA cellular, JJRD identifies that the wireless device is connected to the second wireless network (CDMA cellular). §X.A.[1.10].

[4.3] identify an intended, attempted, or successful data communication over the second wireless network, the intended, attempted, or successful data communication over the second wireless network being associated with the first service activity, and

276. For at least the reasons discussed in [1.11], JJRD renders [4.3] obvious. §X.A.[1.11].

277. Per Jones, JJRD applies policies to data transfers. SAMSUNG-1006, 4:46-47, FIG. 3; §X.A.[1.11]. Therefore, a POSITA would have understood that JJRD identifies an intended or attempted data transfer so that it can apply the policies, per Jones. Per Jobs, JJRD communicates data associated with a first activity over a second network (e.g., CDMA). SAMSUNG-1005, [0042].

[4.4] apply the second service policy.

278. For at least the reasons discussed in [1.12], JJRD renders [4.4] obvious. §X.A.[1.12].

279. Per Jones, JJRD “associates each of at least two connection states with one of the data transfer rules,” “detects a connection state of a client device,” and “applies a first data transfer rule to the client device in response to detecting a first connection state.” SAMSUNG-1006, 2:8-13. Per Jones, when the second policy is applied, backup can be prohibited. SAMSUNG-1006, 5:25-26; §X.A.[1.12]. Per Rao, backup can also be delayed, e.g., by assigning packets to a lower-priority queue. SAMSUNG-1007, [0179]-[0195]. A POSITA would have understood that since packets in higher-priority queues are transmitted ahead of packets in lower-priority queues (which naturally results from queue priority), packets in the lower-priority queue are delayed. SAMSUNG-1007, [0184].

[5] The wireless device recited in claim 1, wherein reducing data usage comprises blocking the first service activity.

280. JJRD renders [5] obvious.

281. Per Jones, JJRD blocks service activities to reduce data usage. For example, Jones teaches that “a first rule may prohibit data transfers” when on a particular network type, such as “in the case of data backup.”

SAMSUNG-1006, 5:25-27. A POSITA would have understood that a prohibited backup is blocked.

[6] The wireless device recited in claim 1, wherein reducing data usage comprises blocking the first service activity when the wireless device is connected

to the first wireless network and allowing the first service activity when the wireless device is connected to the second wireless network.

282. JJRD renders [6] obvious.

283. Per Jones, JJRD blocks service activities when connected to the first wireless network (e.g., when on GSM). For example, Jones teaches that “a first rule may prohibit data transfers” when on a particular network type, such as “in the case of data backup.” SAMSUNG-1006, 5:25-27. Jones further teaches that service activities can continue when connected to a second network (e.g., CDMA), e.g., explaining that, if the client connection changes to a different connection, the “policy rule prohibiting data transfers may no longer apply and remote copying may resume.” SAMSUNG-1006, 5:29-32. Jones further teaches that data backup frequency can be adjusted based on network type (e.g., CDMA cellular), and therefore a POSITA would have understood that data backup is allowed to occur at a frequency that depends on network bandwidth. SAMSUNG-1006, 1:61-64.

284. As I discussed in [1.7], systems administrators commonly set policies based on resource capabilities and constraints. In cases where the first wireless network does not have sufficient bandwidth to support a backup, and the second wireless network does have sufficient bandwidth, the backup frequency would naturally differ, e.g., as taught by Jones. SAMSUNG-1006, 1:58-64. If the first network simply lacks bandwidth needed for a

backup, the policy would prohibit the backup, also as taught by Jones.

SAMSUNG-1006, 5:25-26.

285. In this example, the GSM network is assumed to have insufficient bandwidth to support a backup, while CDMA is assume to have sufficient bandwidth. In fact, over time, bandwidth available over various network types will evolve over time (see, e.g., SAMSUNG-1047, generally), and the policies set by the administrators will reflect the bandwidth available at a point in time. However, a POSITA would have understood (and as taught by Jones) that some networks will have insufficient bandwidth to support a backup, while other networks will have sufficient bandwidth. SAMSUNG-1006, 1:58-64, 5:25-26.

[7] The wireless device recited in claim 1, wherein reducing data usage comprises throttling or traffic shaping the first service activity.

286. JJRD renders [7] obvious.

287. Per Rao, JJRD assigns packets to priority queues based on policy and transmits the packets from the queues according to the priority.

SAMSUNG-1007, [0184]; §IX.D. JJRD policies determine priority using, e.g., the application name or type, or other suitable means. SAMSUNG-1007, [0182]; §IX.D. JJRD assigns packets from a backup application (an application type) to a lower priority queue, thereby reducing data usage by throttling and shaping backup traffic. SAMSUNG-1007, [0182], [0184];

§IX.D.. For example, Rao’s priority queuing is a form of traffic shaping since higher-priority packets are transmitted ahead of lower-priority packets.

288. Additionally, per Jones, JJRD throttles backup traffic by reducing backup frequency. SAMSUNG-1006, 1:58-64. For example, Jones states that “[d]epending on a number of factors, it may not be necessary to require the same backup policy for every user regardless of connection type,” e.g., “an enterprise data protection strategy may prefer to adjust the frequency of data backups according to the identity of the user, the type of connection, and/or the bandwidth of the connection.” *Id.*

[8] The wireless device recited in claim 1, wherein reducing data usage comprises delaying the first service activity, or assigning the first service activity to a lower-priority traffic queue than a traffic queue to which the first service activity would otherwise be assigned.

289. JJRD renders [8] obvious.

290. Per Jones, JJRD delays a first service activity (backup). For example, Jones explains that data backup frequency can be adjusted, and a POSITA would have understood that when backups are made less frequently, backups are delayed. SAMSUNG-1006, 1:61-64.

291. Further, per Rao, JJRD assigns packets to priority queues based on policy and transmits the packets from the queues according to the priority. SAMSUNG-1007, [0184]; §IX.D. JJRD policies determine priority using, e.g., the application name or type, or other suitable means. SAMSUNG-

1007, [0182]; §IX.D. JJRD assigns packets from a backup application (an application type) to a lower priority queue than it would be assigned if a different policy applied (e.g., for higher-priority traffic), thereby reducing data usage by throttling backup traffic. SAMSUNG-1007, [0182], [0184]; §IX.D.

292. As described in Jones, policies can “be configured by a user such as a system administrator.” SAMSUNG-1006, 6:37-38. Rao similarly explains that policies “may be configurable by a user by any suitable means and/or mechanism. For example, the agent 326 may provide a configuration mechanism such as a user interface, graphical or otherwise, design and constructed for configuring or specifying the policies 520.” SAMSUNG-1007, [0183]. Therefore, since JJRD policies are set by an administrator (per Jones), the policies reflect priority as set by the administrator. Thus, a packet of the first service activity is assigned by JJRD to a lower-priority traffic queue (per the policy set by an administrator) than a traffic queue to which the first service activity would otherwise be assigned (e.g., if the administrator had set a different policy).

[9] The wireless device recited in claim 1, wherein the first service policy is dependent on a network type, a roaming network connection condition, a WiFi network condition, a background download condition, a user designation that the first service activity is non-critical, a geographic location, or a combination of these.

293. JJRD renders [9] obvious.

294. In JJRD, the policy is dependent on network type, background download condition, and/or a designation that the activity is non-critical.

§IX.D. For example, Jones explains that policies “may be applied to data transfers depending on the desired functionality, type of connection, connection bandwidth, user priorities, etc.” SAMSUNG-1006, 5:13-15. A

POSITA would have understood or found obvious that “a type of connection” is a “network type” (i.e., a type of network connection).

Additionally, Jones teaches that data protection software on client devices can “execute in the background to perform data backups.” SAMSUNG-

1006, 3:45-47. Jones further teaches that policies can depend on user

priorities. SAMSUNG-1006, 5:13-15. A POSITA would have understood

or found obvious that “non-critical” is a user priority.¹⁷ Finally, Rao teaches

that policy can be “based on whether an application is running in the ...

background.” SAMSUNG-1007, [0182].

[10] The wireless device recited in claim 1, wherein the first service activity comprises a background activity or a software update, and wherein reducing

¹⁷ Non-critical can be called “best effort,” which indicates that the traffic receives no performance guarantees and is assigned the lowest priority. See, e.g., SAMSUNG-1050, Table 1.

data usage comprises delaying, deferring, throttling, or blocking the first service activity.

295. JJRD renders [10] obvious.

296. In JJRD, backup (first service activity) can run as a background activity and can involve a software update, per Jones, which explains that data protection software on client devices can “execute in the background to perform data backups.” SAMSUNG-1006, 3:45-47; 5:4-12.

297. In addition, Jones’s data transfers include virus updates, which a POSITA would understand to be a software update since the virus definitions are an integral component of an antivirus program. SAMSUNG-1006, 5:9-10.

298. Further, in JJRD, reducing data usage can comprise delaying a service activity, e.g., backup. For example, Jones explains that data backup frequency can be adjusted, and a POSITA would have understood that when backups are made less frequently, backups are delayed, deferred, and/or throttled (i.e., not occurring at the same frequency that they otherwise would be). SAMSUNG-1006, 1:61-64. Further, in JJRD, reducing data usage can comprise blocking (prohibiting) a service activity, e.g., backup.

SAMSUNG-1006, 5:25-26.

299. Additionally, Rao teaches that policies determine priority and can be applied “based on whether an application is running in the foreground or the

background.” SAMSUNG-1007, [0179], [0182], [0184]. Rao further teaches that “packets are communicated according to the determined priority.” SAMSUNG-1007, [0184]. A POSITA would have understood from Rao’s discussion of priority queuing that lower-priority traffic (e.g., from background applications) will be delayed in favor of higher-priority traffic. SAMSUNG-1007, [0003], [0179]-[0195].

[11] The wireless device recited in claim 1, wherein reducing data usage comprises directing communications associated with the first service activity to a particular network end point, route, or tunnel.

300. JJRD renders [11] obvious.

301. In JJRD, a policy can specify that only local backup can occur, which a POSITA would have understood as directing communication to a particular network endpoint, JJRD itself. A POSITA would have understood that JJRD is a network endpoint since it runs applications that send and receive network data. §IX.D.

302. For example, Jones explains that “a mobile client such as client 128 may take advantage of local backups when it is not connected to enterprise network” and that when a policy prohibits data transfer over a network, the policy can allow local backup to continue. SAMSUNG-1006, 3:51-55; 5:26-32.

303. Per Rao, JJRD applications can transmit data over TCP/IP.

SAMSUNG-1007, [0184].¹⁸ A POSITA would have understood that TCP traffic is directed to a network endpoint identified by hostname or IP address. One such choice is “localhost,” which directs traffic to the device sending the data. Similarly, the IP Address 127.0.0.1 is called a “loopback address” that directs traffic to the sender. Thus, even for a local backup (per Jones), traffic is directed to a network endpoint, e.g., localhost or 127.0.0.1.

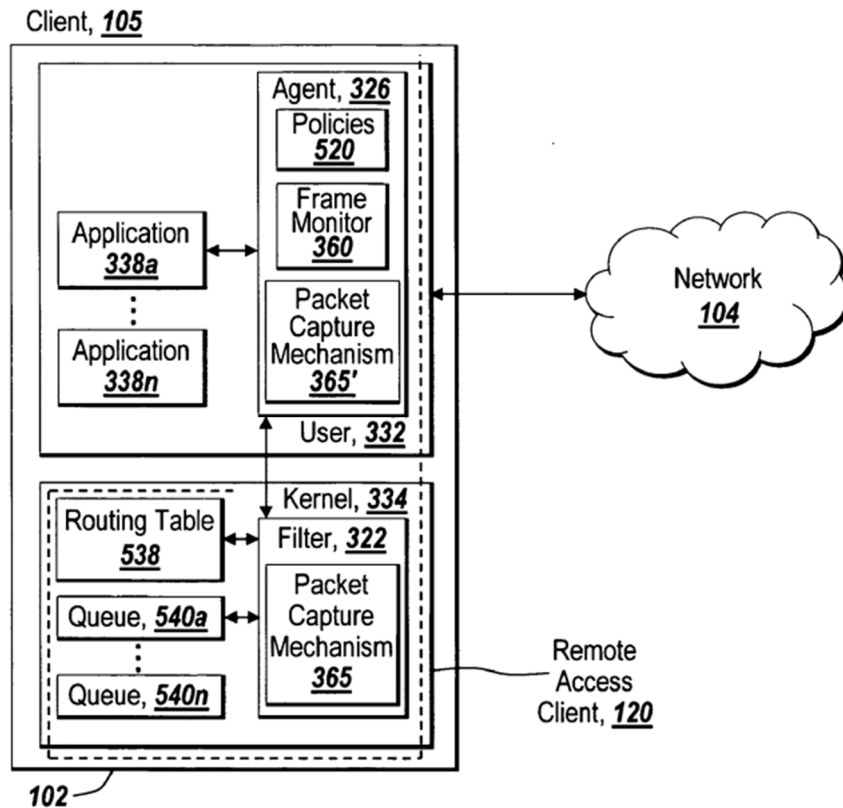
304. In another example, when, per Jones, “a mobile client such as client 128 may take advantage of local backups when it is not connected to enterprise network,” the local backup can be directed to a network endpoint such as a SAN (storage area network) backup device that does uses a separate, non-public network. SAMSUNG-1006, 3:51-55; 5:26-32.

[12.1] The wireless device recited in claim 1, wherein the one or more agents comprise a policy control agent and one or more low-level policy agents, and the policy control agent is configured to:

305. JJRD renders [12.1] obvious.

¹⁸ Additionally, Jobs explains that the device can couple “directly to other devices or indirectly over a network (e.g., the Internet, wireless LAN, etc.).” SAMSUNG-1005, [0048]. A POSITA would have recognized that TCP/IP is the protocol used most commonly on the Internet.

306. In JJRD, per Rao, agents comprise a policy control agent (Rao's agent) and a low-level policy agent (a filter, per Rao), e.g., as illustrated in Rao's FIG. 5A, reproduced below.



SAMSUNG-1007, FIG. 5A.

307. Rao explains that “the agent 326 indicates the priority to the filter 322 for management of network packet queues 540 a-540 n to apply the indicated priorities.” SAMSUNG-1007, [0190].

[12.2] obtain the first service policy,

308. JJRD renders [12.2] obvious.

309. JJRD's agent obtains the first service policy, per Rao. For example, Rao teaches that "policies 520 may be accessible by the agent 326, configured into the agent 326, or loaded by the agent 326," e.g., "the policies 520 may be provided by or downloaded via the gateway 340." SAMSUNG-1007, [0183].

[12.3] obtain information about the first service activity,

310. JJRD renders [12.3] obvious.

311. In JJRD, the agent obtains information about the service activity. For example, Rao teaches that policy can be specified based on the name or type of application, protocols used by the application, whether the service is in the foreground or background, etc. SAMSUNG-1007, [0182]. Per Rao, when JJRD intercepts a packet, it determines the application associated with the packet and "uses the policies 520 to apply a priority to network packets of applications 338a-338n in accordance with the prioritization rules specified or indicated by the policies 520." SAMSUNG-1007, [0187], [0189]. A POSITA would have understood that the application determined to be associated with the packet is information associated with the service activity.

[12.4] based on the information about the first service activity and the first service policy, determine a low-level policy rule or setting for the one or more low-level policy agents, the low-level policy rule or setting for assisting in achieving the first service policy, and

312. JJRD renders [12.4] obvious.

313. Per Rao, based on the information about the service activity, JJRD determines a priority (setting for assisting in achieving the first service policy). For example, per Rao, JJRD intercepts a packet, determines the application associated with the packet and “uses the policies 520 to apply a priority to network packets of applications 338a-338n in accordance with the prioritization rules specified or indicated by the policies 520.” SAMSUNG-1007, [0187], [0189].

[12.5] provide the low-level policy rule or setting to the one or more low-level agents.

314. JJRD renders [12.5] obvious.

315. JJRD’s agent communicates the policy setting (packet priority) to the low-level agent (filter). For example, Rao teaches that the agent “communicate[s] the priority of network packets to the filter 322 by any suitable means and/or mechanism such as via an application programming interface (API), such an IOCTL interface, or any other type and/or form of interface known to those ordinarily skilled in the art.” SAMSUNG-1007, [0190].

[13] The wireless device recited in claim 12, wherein the one or more low-level policy agents comprise an application interface agent, a policy implementation agent, a service monitor agent, or a combination of these.

316. JJRD renders [13] obvious.

317. Per Rao, JJRD's filter is a policy implementation agent since it implements the policy by queuing packets according to priority. For example, Rao teaches that "the filter 322 may place, arrange, or coordinate network packets into queues 540 a-540 n in support of the priorities." SAMSUNG-1007, [0191].

[14.1] The wireless device recited in claim 1, wherein the first service policy is further configured to assist the one or more agents in: determining a usage measure associated with the first service activity, and

318. JJRD renders [14.1] obvious.

319. Per Jobs, JJRD's service policy assists one or more agents on JJRD in determining a usage measure associated with the first service activity. As I described in §VII.B, Jobs's service plans are examples of service policies since they constrain a device's use of (at least) network resources. For example, Jobs explains that a service plan can include resource limits (e.g., voice and/or data), and once those limits are exceeded, additional charges can occur. SAMSUNG-1005, [0002]. Thus, Jobs's data monitoring against the thresholds set by the service plan is an example of the policy assisting (by setting the threshold) in determining a usage measure (against that threshold).

320. Jobs further explains that, in multi-service accounts, the user's resource budget is defined by a linear combination of resource usage

amounts, e.g., “a particular account may provide a user with a combined monthly budget for voice and data transmission services, where transmission of N megabytes (MB) of data (e.g., 20 megabytes) is treated as equivalent to one minute of voice transmission usage.” SAMSUNG-1005, [0019]. In such cases, the “device may compute a ‘combined usage metric’ indicative of the total resources used during an accounting period (e.g., a current or prior accounting period) as follows:

$$usage_metric = \sum_i w_i \times (usage\ of\ resource\ i) \quad (1)$$

where i is an index having distinct values associated with two or more distinct resources, w_i is a weight associated with resource i , and ‘*usage of resource i* ’ is a measurement of the amount of resource i used during the relevant accounting period. Per Jobs, resources include “voice transmission services, data transmission services, SMS messaging services, data storage services, and perhaps other services as well.” SAMSUNG-1005, [0019]. In some embodiments, the weights, w_i may correspond to the monetary cost per unit of resource i used, and the combined usage metric may be a monetary value indicating either a total cost, or the amount of the user’s budget that has been consumed.” SAMSUNG-1005, [0019].

321. Therefore, a POSITA would have understood that the policy specifying a “combined usage metric” is assisting in determining a usage metric (aggregate data use) associated first service activity (backup).

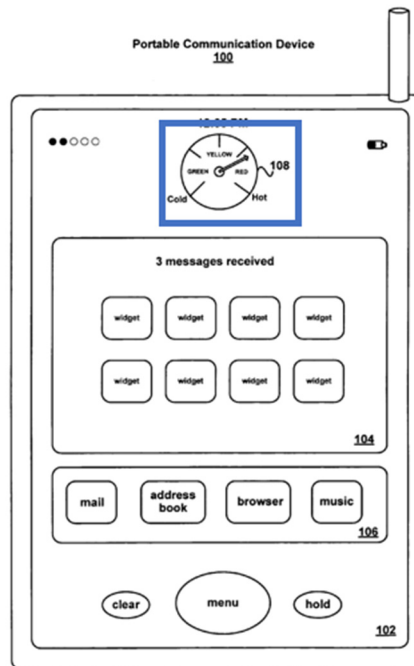
[14.2] presenting information about the usage measure through the user interface.

322. JJRD renders [14.2] obvious.

323. JJRD presents information about the usage measure associated with the first service activity in the user interface, as taught by Jobs.

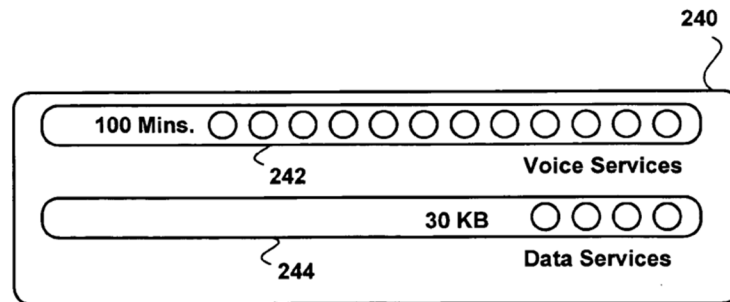
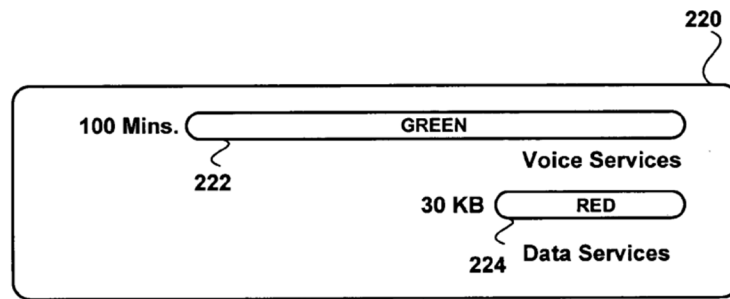
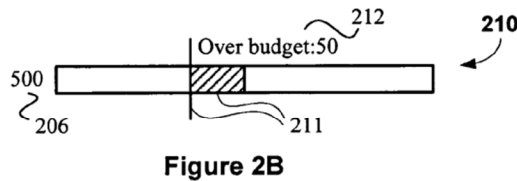
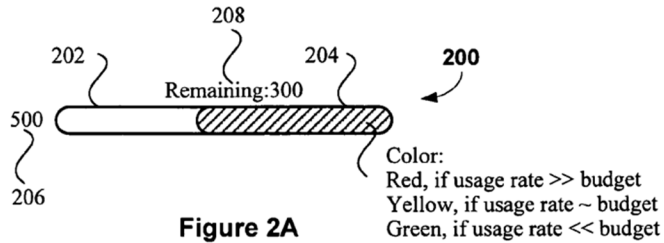
SAMSUNG-1005, [0004], [0018]. For example, per Jobs, JJRD “automatically and repeatedly present[s] an updated account usage metric for an account associated with usage of the portable communication device” in a usage meter, such as “an ‘analog’ type meter (e.g., similar to a heat gauge) that includes an arrow that indicates (A) a remaining balance on an account, and/or (B) whether the user’s resource usage rate (sometimes called the ‘burn rate’) is less than, approximately equal to, or greater than an average resource usage rate associated with a predefined or user-selected budget for the account,” where, “as the user uses account resources (minutes, bandwidth, data storage capacity or any other asset or resource for which there is an account balance), the meter is automatically, without user action, updated to reflect the corresponding change in account status.” *Id.* A POSITA would have understood from Jobs’s description of the account

usage metric that “resource usage rate” is associated with the first service activity since the first service activity consumes resources and thus contributes to the usage rate.



SAMSUNG-1005, FIG. 1 (annotated)

324. Jobs further explains that “the graphical object 108 can be any type of object, such as a gauge, meter, dial, bar, graph, chart, animation, button, etc.,” and “the user can be provided with a preference pane for selecting among a list of predefined meter types,” e.g., as illustrated in FIGS. 2A, 2B, 2C and 2D, reproduced below. SAMSUNG-1005, [0029].



SAMSUNG-1005, FIGS. 2A-2D

[15.1] The wireless device recited in claim 1, wherein the first service policy is further configured to assist the one or more agents to: detect that a service usage pattern associated with the first service activity has occurred, or that a service usage amount associated with the first service activity has been consumed, and

325. JJRD renders [15.1] obvious.

326. Similar to the description in [14.1], Jobs’s data monitoring against the thresholds set by the service plan is an example of the policy (the service plan) assisting (by setting the threshold) in detecting that a service usage has been consumed. For example, per Jobs, JJRD detects that a service usage amount (overall data use) associated with the service activity (backup) has been consumed. Jobs includes a meter “that indicates ... a remaining balance on an account.” SAMSUNG-1005, [0018]. A POSITA would have understood from Jobs’s discussion of account usage metrics that JJRD is detecting that a usage amount associated with the first service activity has been consumed when JJRD meter indicates a remaining balance since the remaining balance is simply the plan amount minus service usage, including usage by the first service activity.

327. Further, the total service usage is “associated with” the first service activity (and the first service usage is associated with the total service usage) since that service activity contributes to the total service usage.

328. Additionally, to the extent that the claim requires that the system detects when the usage amount is fully consumed, JJRD performs such measurement when the meter reads zero (e.g., the account balance reaches zero). SAMSUNG-1005, [0025].

[15.2] in response to detecting that the service usage pattern associated with the first service activity has occurred, or that the service usage amount associated

with the first service activity has been consumed, present a notification through the user interface.

329. JJRD renders [15.2] obvious.

330. Per Jobs, when JJRD detects that a service usage amount (which is associated with the first service activity) has been consumed, JJRD presents a notification through the user interface. For example, per Jobs, JJRD “automatically initiate[s] certain actions when an account balance or resource usage rate reaches a threshold level,” including generating a notification, e.g., “an audio or visual message to indicate that a condition has been triggered, such as, for example, one or more tones, a music clip, a computer-generated announcement or a text message displayed in the window 104.” SAMSUNG-1005, [0034].

[16] The wireless device recited in claim 1, wherein the first service policy is further configured to assist the one or more agents in presenting a notification through the user interface, the notification comprising information associated with the first service activity.

331. JJRD renders [16] obvious.

332. Per Jobs, “certain trigger conditions can result in an action being performed by the device,” which can include a “visual message to indicate that a condition has been triggered.” SAMSUNG-1005, [0034]. The “trigger condition can occur whenever a predefined amount of resource usage (e.g., one minute of voice transmission, 20 MB of data have been

transmitted,” and/or “when an account balance reaches or falls below a threshold.)” SAMSUNG-1005, [0036]. A POSITA would have understood that the resource usage threshold (e.g., 20 MB of data transmitted) can be reached when a particular service activity (e.g., backup) is transmitting data. Therefore, a POSITA would have understood that the notification (e.g., use threshold satisfied) is associated at least with a service activity (e.g., backup).

333. Thus, the first service policy (access privileges specifying a data use threshold) assists device agents in presenting a notification through the user interface (visual message), the notification comprising information associated with the first service activity (indication that an account balance trigger has occurred, e.g., during a service activity such as a backup).

[19] The wireless device recited in claim 1, wherein the first service policy is further configured to assist the one or more agents in presenting a notification through the interface, the notification for providing an indication that data usage over the first wireless network associated with the first service activity has reached a particular amount or a limit.

334. JJRD renders [19] obvious.

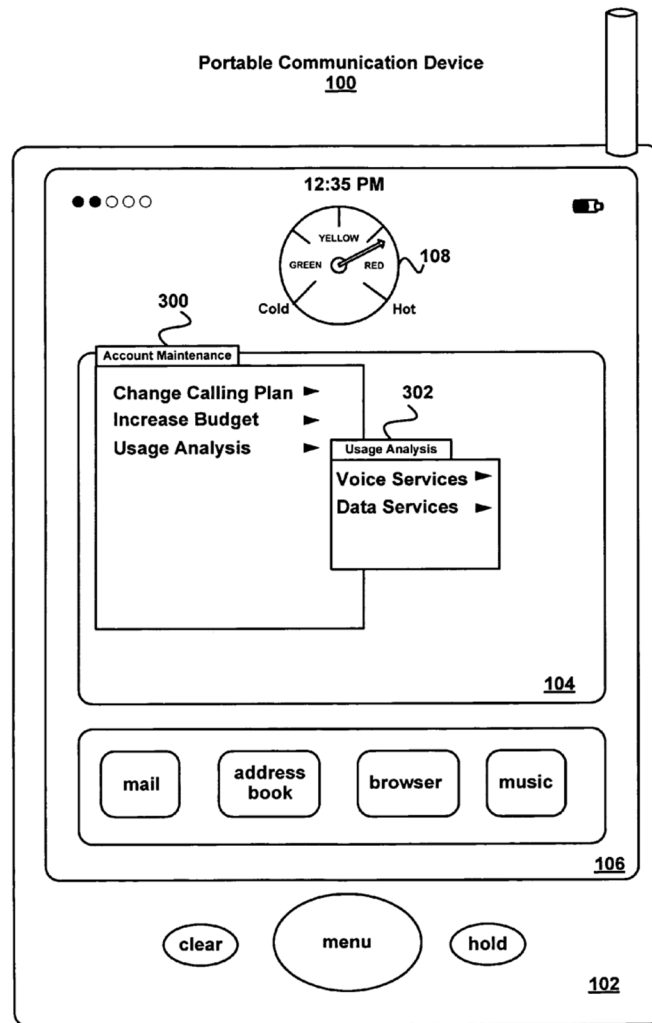
335. In JJRD, the first service policy is further configured to assist the one or more agents in presenting a notification through the interface. *See* [16].

336. As described above for claim [16], resource usage can include “volume limitations,” e.g., “20 MB of data have been transmitted.”

SAMSUNG-1005, [0036]. In one example, when a network service activity transmits data causing the account data balance to fall below a threshold, a trigger will occur. SAMSUNG-1005, [0036].

337. Thus, the first service policy (specifying a resource usage threshold) assists device agents in presenting a notification through the user interface (visual message indicating that an account balance trigger has occurred), that data usage over the first wireless network associated with the first service activity (backup) has reached a particular amount or a limit (the threshold) which is reached during a first service activity (backup).

338. In this example, the device is backing up data, and that use of data causes the device to hit the data limit set in the service plan. In response, JJRD displays a message, e.g., the user interface panel of Jobs, which explains that when “account balance drops below a respective threshold value (e.g., determined by the user’s account time, or determined by a user selection in a preference pane),” a menu “is automatically displayed and the user is prompted to make a selection,” such as changing calling plan or increasing budget. SAMSUNG-1005, [0029], [0034], FIG. 3.



SAMSUNG-1005, FIG. 3

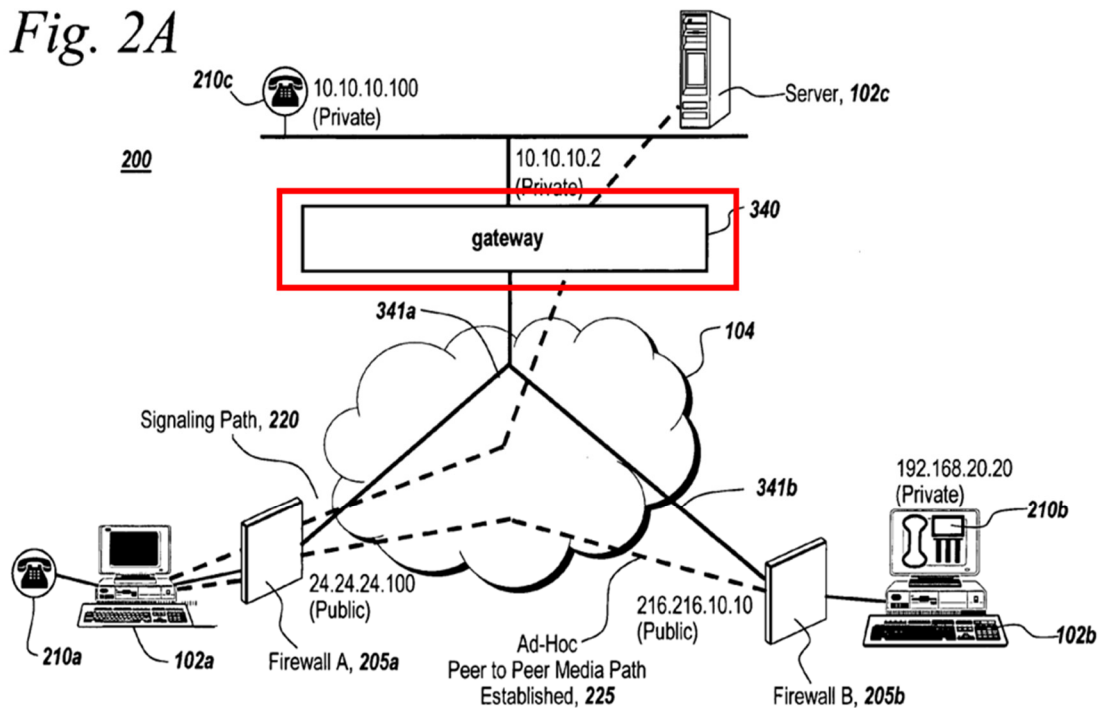
[21] The wireless device recited in claim 1, wherein the one or more agents are further configured to obtain at least a portion of the first service policy from a network element.

339. JJRD renders [21] obvious.

340. For example, Rao teaches that “[t]he policies 520 may be accessible by the agent 326, configured into the agent 326, or loaded by the agent 326”

and that “the policies 520 may be provided by or downloaded via the gateway 340.” SAMSUNG-1007, [0183].

Fig. 2A



SAMSUNG-1007, FIG. 2A(annotated).

341. A POSITA would have understood from Rao’s disclosure of a gateway that a gateway is a network element:

Still referring to FIG. 1A, the gateway 340 may comprise any type and/or form of gateway, such as a remote access server, that *may be used to connect one or more computing devices on one network to other networks*. In another aspect, the gateway 340

may be *used to provide a virtual private network connection to give a client 105 a-105 c access to a private network*. In a further aspect, the gateway 340 may be a hardware or software set-up that *translates between two dissimilar protocols or disjoint or disconnected networks or systems*. The gateway 340 may comprise a specialized hardware or networking device, or may be a computing device configured to act as a gateway. As such, the gateway 340 may comprise software, hardware, or any combination of software and hardware. In one embodiment, *the client 105 and the gateway 340 communicate via any type and/or form of gateway or tunneling protocol 341 a-341 n*, such as SSL or TLS, or the Citrix Gateway Protocol manufactured by Citrix Systems, Inc. of Ft. Lauderdale, Fla.

SAMSUNG-1007, [0092](emphasis added).

342. A POSITA would have understood that Rao's gateway is a network device. For example, Rao explains that its gateway "may comprise any type and/or form of gateway, such as a remote access server, that may be used to connect one or more computing devices on one network to other networks."

[23.1] The wireless device recited in claim 1, wherein, after obtaining the user input, the one or more agents are further configured to: send a message to a network element, the message configured to provide information about the user input, and

343. JJRD renders [23.1] obvious.

344. Per Jobs, JJRD's UI includes a pull-down menu "containing account-related options ... including but not limited to changing a billing plan [and] increasing budget for a service account," through which JJRD obtains user input specifying (e.g.) access privileges. SAMSUNG-1005, [0029]. As I described in [1.4], Jobs's service plans are examples of service policies. SAMSUNG-1005, [0002], [0018]-[0019].

345. Also, per Jobs, JJRD creates a trigger event, which occurs when "the user manually selects a menu option (e.g., analyze device or service usage, change calling plans)" (obtaining the user input, which is related to the service plan and therefore to the service policy). SAMSUNG-1005, [0036]. In response, JJRD "establishes a secure network connection (e.g., SSL connectivity) with a service provider computer," and sends a "message requesting the user's account information," where the message includes "identifying information (e.g., MSID) that can be used by the service provider to verify the device and the user." SAMSUNG-1005, [0037]. A POSITA would have understood from Jobs that the MSID (Mobile Station Identifier) provides information about the user input (e.g., the device from which the user input originated).

[23.2] obtain at least a portion of the first service policy from the network element.

346. JJRD renders [23.2] obvious.

347. Per Jobs, when a “trigger condition is detected[,] the device downloads (404) account information from the service provider for the account.” SAMSUNG-1005, [0038]. In response, the device updates “one or more account metrics,” e.g., the data budget. SAMSUNG-1005, [0002], [0038]. Therefore, the device obtains from the server provider’s server (network element) at least a portion of the service policy (the data budget).

[24] The wireless device recited in claim 1, wherein the first wireless network is a cellular network or a roaming network.

348. JJRD renders [24] obvious.

349. For example, per Jobs, the network can be GSM (cellular).

SAMSUNG-1005, [0042]; §X.A.[1.4].

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

350. JJRD renders [27.1] obvious.

351. For example, Jobs teaches that the processors “communicate with the one or more computer-readable mediums,” where the “computer-readable medium 502 can be any device or medium that can store code and/or data for use by the one or more processors. SAMSUNG-1005, [0045]. Jobs further teaches that “[t]he one or more processors 518 run various software

components stored in the medium 502 to perform various functions for the device.” SAMSUNG-1005, [0046].

[27.2] obtain, through a user interface of the wireless device, a user input specifying at least an aspect of a first service policy,

352. See [1.9].

[27.3] the first service policy configured to at least assist in reducing data usage associated with a first service activity over the first wireless network,

353. See [1.5].

[27.4] the first service activity being less than all service activities available to the wireless device,

354. See [1.6].

[27.5] the first service policy for enabling control of the first service activity on the first wireless network that is different from how the first service activity is controlled on a second wireless network;

355. See [1.7].

[27.6] identify that the wireless device is connected to the first wireless network;

356. See [1.10].

[27.7] identify an intended, attempted, or successful data communication over the first wireless network, the intended, attempted, or successful data communication being associated with the first service activity; and

357. See [1.11].

[27.8] apply the first service policy.

358. See [1.12]

[28] The non-transitory computer-readable storage medium recited in claim 27, wherein reducing data usage comprises blocking the first service activity.

359. See [1.4], [5].

[29] The non-transitory computer-readable storage medium recited in claim 27, wherein the first service activity comprises a background activity or a software update, and wherein reducing data usage comprises delaying, deferring, throttling, or blocking the first service activity.

360. See [10].

[30.1] The non-transitory computer-readable storage medium recited in claim 27, wherein, when executed by the one or more processors of the wireless device, the machine-executable instructions further cause the one or more processors to: determine a usage measure associated with the first service activity; and

361. See [14.1].

[30.2] cause information about the usage measure to be presented through a user interface of the wireless device.

362. See [14.2]

B. Ground 1B: Jobs in view of Jones, Rao and Bocking renders claims 17, 18, and 24 obvious

[17] The wireless device recited in claim 1, wherein the first service policy is further configured to assist the one or more agents in presenting a notification through the user interface, the notification providing information about a roaming network or a roaming condition of the wireless device.

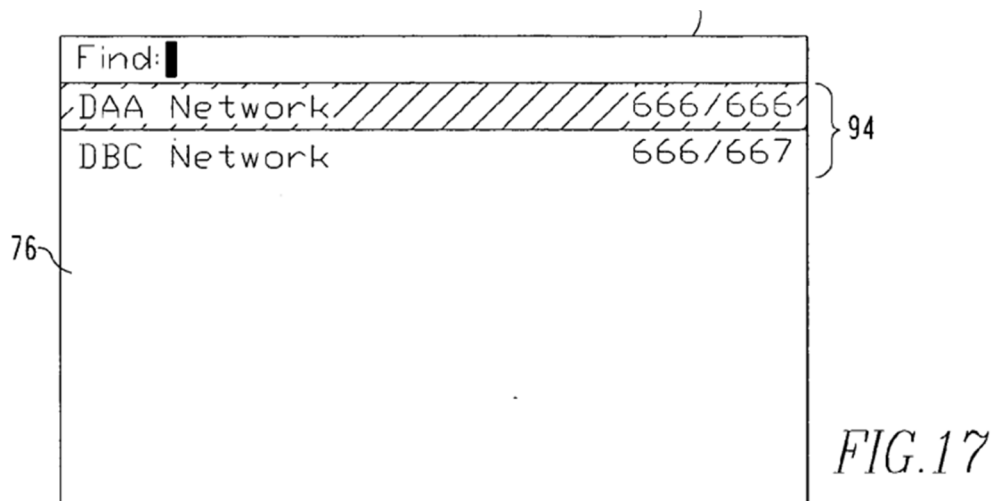
363. JJRBD renders [17] obvious.

364. Per Jones, JJRBD's policies determine backup frequency based on network type, bandwidth, etc. SAMSUNG-1006, 1:60-64. Jones further explains that "the structure of each policy and the mapping of the policy structure to a set of data transfer rules may be configured by a user such as a system administrator," e.g., "a user may be presented with a graphical user

interface through which each policy may be selected and configured in successive operations.” SAMSUNG-1006, 6:36-42.

365. Per Bocking, JJRBD “establish[es] a prioritized list of preferred PLMNs to be used in roaming situations.” SAMSUNG-1009, [0024].

When roaming, in response to a user selecting “Select From Available Networks,” JJRBD performs a scan to locate available networks and displays “a listing 94 of all of the ‘available networks’ located during the scanning procedure.” SAMSUNG-1009, [0028], FIG. 17.



SAMSUNG-1009, FIG. 17.

366. A POSITA would have understood that, to appropriately protect enterprise data, backup policies must be configured for each network type, including JJRBD’s preferred roaming networks. SAMSUNG-1006, 1:46-50. For example, when (per Bocking) JJRBD scans for roaming networks and

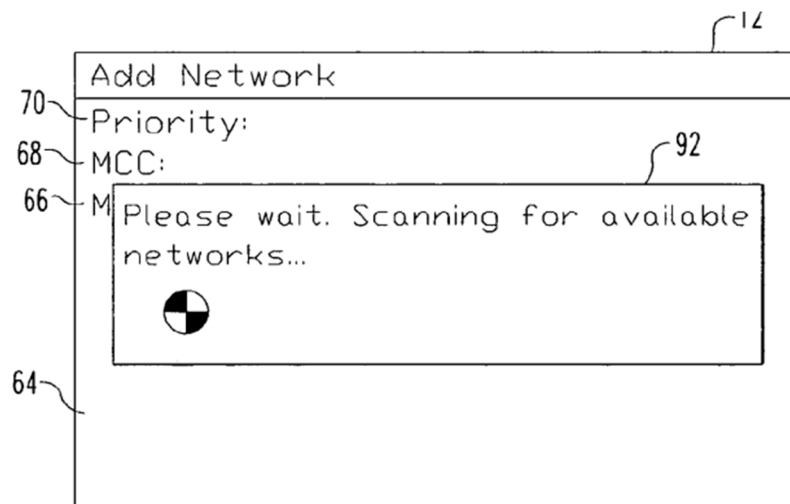
the user can add an available network to the preferred roaming list for which JIRBD does not have a configured backup policy. SAMSUNG-1009, [0028], FIG. 17. In such cases, to protect the data, JIRBD might perform a backup, incurring large roaming fees, or JIRBD might not perform a backup when such fees do not exist, putting data at risk. SAMSUNG-1006, 1:46-50. In one example, a device might have access to high-speed network that incurs no costs, and the corresponding policy might initiated backups on the device similarly to the backup policy for other high-speed networks. In another example, the device might roam to a network type that, while fast, incurs substantial costs for data usage, so the enterprise might specify a policy that backs up less often, fewer files, or even not at all. SAMSUNG-1006, 1:60-67.

367. Therefore, to ensure all networks are configured, the first service policy (backup frequency) assists in presenting a notification through the user interface (policy configuration GUI) that provides information about a roaming network (preferred roaming networks, per Bocking).

[18.1] The wireless device recited in claim 1, wherein the first service policy is further configured to assist the one or more agents in: presenting a notification through the user interface, the notification providing information about one or more available wireless networks, and

368. JIRBD renders [18.1] obvious.

369. For example, Bocking teaches that a user “can add a PLMN to the listing 58 by selecting the PLMN from a group of ‘available networks,’ which handheld electronic device 4 is able to locate from its current location using communications subsystem 45 and a known network scanning procedure.” SAMSUNG-1009, [0028].



SAMSUNG-1009, FIG. 16

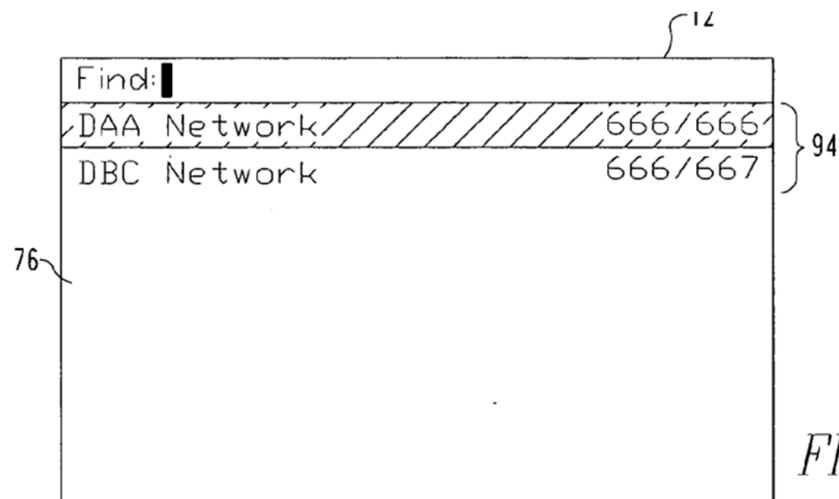


FIG.17

SAMSUNG-1009, FIG. 17.

[18.2] obtaining a first user response through the user interface, the first user response indicating a selection of one of the one or more available wireless networks.

370. JIRBD renders [18.2] obvious.

371. Per Bocking, when JIRBD displays the list of available networks, the “user may then select a particular PLMN for inclusion” in the list “used to determine which and in what order PLMNs are to be used by handheld electronic device 4, if available, in roaming situations.” SAMSUNG-1009, [0028].

372. Further, per Bocking, “the user may easily reorder, and thus change the priority of, the PLMNs listed in listing 58 by selectively moving their location in listing 58.” SAMSUNG-1009, [0029]. A POSITA would have understood from Bocking that when a user reorders the list to place the selected “particular PLMN” first in the list (giving it highest priority), the user is indicating a selection of that network. By the nature of priority, the first (highest priority) network is the network selected by the user, which is indicated by the order set by the user via the user response.

[24] The wireless device recited in claim 1, wherein the first wireless network is a cellular network or a roaming network.

373. JIRBD renders [24] obvious.

374. For example, per Bocking, JIRBD “establish[es] a prioritized list of preferred PLMNs to be used in roaming situations,” and the “respective

priorities assigned to the PLMNs listed on listing 58 determines the order in which the PLMNs are to be used by handheld electronic device 4, if available, in roaming situations.” SAMSUNG-1009, [0024], [0026].

Therefore, a POSITA would have understood that, when the JJRBD is roaming, per Bocking, the network is a roaming network.

375. Bocking further teaches that a device can be connected to a cellular network. SAMSUNG-1009, [0004], [0007]. For example, Bocking explains that “[n]umerous types of handheld electronic devices are known, including “cellular telephones.” SAMSUNG-1009, [0004]. Bocking further notes that “to use wireless communications functionality, a user must subscribe with a wireless service provider or operator.” SAMSUNG-1009, [0007]. A POSITA would have understood that cellular telephones (e.g., JJRBD) use cellular wireless communication.

C. Ground 1C: Jobs in view of Jones, Rao, and Cunningham renders claim 20 obvious

[20.1] The wireless device recited in claim 1, wherein the first service policy is further configured to assist the one or more agents in presenting a notification through the user interface, the notification for notifying a user about a particular condition associated with the first service activity, and wherein the one or more agents are further configured to:

376. JJRCD renders [20.1] obvious.

377. For example, Jobs teaches that, “when an account balance drops below a respective threshold value” (a particular condition associated with the first service activity, e.g., the threshold being reached during a backup), the menu is “automatically displayed and the user is prompted to make a selection.” SAMSUNG-1005, [0034]. A POSITA would have understood that the account balance (e.g., data limit) reaches a maximum threshold when some service activity is occurring. Since the JJRCD performs backup (per Jones), the backup service activity can cause the data limit to be reached.

378. In addition, “the device 100 generates an audio or visual message to indicate that a condition has been triggered, such as, for example, one or more tones, a music clip, a computer-generated announcement or a text message displayed in the window 104.” *Id.* A POSITA would have understood that displaying a menu and/or message is presenting a notification. Further, since the resource use threshold value is set by the policy, a POSITA would have understood that the policy assists in presenting the notification.

[20.2] assist in presenting the notification through the user interface,

379. JJRCD renders [20.2] obvious.

380. For example, Jobs teaches that, “when an account balance drops below a respective threshold value,” the menu is “automatically displayed and the user is prompted to make a selection.” SAMSUNG-1005, [0034]. In addition, “the device 100 generates an audio or visual message to indicate that a condition has been triggered, such as, for example, one or more tones, a music clip, a computer-generated announcement or a text message displayed in the window 104.” *Id.* A POSITA would have understood that displaying a menu and/or message is presenting a notification.

[20.3] obtain a user response to the notification through the user interface, and

381. JJRCD renders [20.3] obvious.

382. For example, Jobs teaches that “when an account balance drops below a respective threshold value,” the menu “automatically displayed and the user is prompted to make a selection.” SAMSUNG-1005, [0034]. A POSITA would have understood that the user’s selection is a user response to the notification (displayed menu and/or visual message).

[20.4] restrict or quarantine communications over the first wireless network or over the second wireless network unless the user response comprises an acknowledgment of the particular condition associated with the first service activity.

383. JJRCD renders [20.4] obvious.

384. For example, per Cunningham, when JJRCD reaches the usage limit, service is disabled (restricted). SAMSUNG-1010, [0050]. Additionally, per

Jobs, when JJRCD's account balances reaches a threshold (e.g., the usage limit), a menu "is automatically displayed and the user is prompted to make a selection," which can include "changing a billing plan, increasing budget for a service account." SAMSUNG-1005, [0029], [0034]. A POSITA would have understood that, by increasing budget or by selecting a new plan, the user is acknowledging the condition (insufficient data remaining). SAMSUNG-1001, 59: 23-32.

385. Note that JJRCD discloses a scenario quite similar (if not identical) to the one described in the '110 patent, which states:

In some embodiments, device based service billing includes recording billing option response history. For example, this approach can be particularly important for service plan overage conditions (e.g., when the use of the device is exceeding the service plan associated with the device in some manner, such as service data usage, bandwidth, service or transaction access and/or in some other manner). In some embodiments, in a service plan overage condition, the user is requested to confirm that user has acknowledged notification of service plan overage, such as via the user interface 1697.

SAMSUNG-1001, 59: 23-32.

386. Further, if the user does not acknowledge the condition, access remains disabled, per Cunningham, which explains that “when the usage exceeds the expected payment, the service can be limited or **disabled** until the next payment cycle.” SAMSUNG-1010, [0050].

387. In addition, the acknowledgement is associated with the first service activity, such as a backup activity that results in the usage threshold (set by the service plan) being exhausted.

Ground 1D: Jobs in view of Jones, Rao, and Padmanabhan renders claim 22 obvious

[22.1] The wireless device recited in claim 1, wherein the first service policy is further configured to assist the one or more agents to: determine a usage measure associated with the first service activity,

388. JJRPD renders [22.1] obvious.

389. Per Padmanabhan JJRPD determines usage measures (e.g., round-trip time) associated with applications, e.g., the backup application.

SAMSUNG-1011, [0052]. For example, per Padmanabhan, JJRPD “collects data derived from monitoring the activity of [] application programs” using sensors that “passively observe existing network traffic.” SAMSUNG-1011, [0035], [0047]. A POSITA would have understood that the “passively observe[d] existing network traffic” from the backup application includes network service activities of the backup application, e.g., backup data transmitted from JJRPD to the backup device, and protocol messages (e.g.,

“ACK” messages) sent to JJRPD in response. SAMSUNG-1011, [0051]-[0053].

390. Since the Transmission Control Protocol (TCP) guarantees delivery of packets (unlike, e.g., UDP), it includes a mechanism for the receiver to inform the sender that packets have arrived, e.g., a TCP “ACK.”

SAMSUNG-1046, 7. In the simplest form, to guarantee delivery, the sender could transmit one packet; the receiver could receive the packets, and reply with an ACK (acknowledgement) message; the sender could receive the ACK and transmit the next packet. If the sender does not receive an ACK within some set amount of time, the sender retransmits the packet.

However, in this simple example, since the sender cannot send a second packet until the receiver acknowledges the receipt of the first packet, such a protocol would be highly inefficient. Instead, TCP includes more complex techniques that enable multiple packets to be sent concurrently, but the general technique is the same: if the sender does not receive a ACK for a packet, the sender retransmits the packet. SAMSUNG-1046, *generally*.¹⁹

¹⁹ The TCP specification includes additional examples of bidirectional traffic, e.g. 3-way handshake, SAMSUNG-1046, 28-29, *generally*.

391. Thus, JJRPD determines usage measures (e.g., round-trip time) associated with the first service activity (e.g., transmitted backup data).

392. Additionally, per Jones, JJRPD's backup frequency is set by policy. SAMSUNG-1006, 1:60-64. Therefore, JJRPD's first service policy (backup frequency) assists in determining a usage measure (e.g., round-trip time) associated with the first service activity (e.g., transmitted backup data) since the policy determines when the data are sent. SAMSUNG-1006, 1:60-64.

[22.2] generate a report based on the usage measure, and

393. JJRPD renders [22.2] obvious.

394. For example, per Padmanabhan, JJPRD "passively collects data derived from monitoring the activity of other application programs" and processes and correlates the data "with attributes of the client machine in order to provide contextual information describing the performance of the machine during network communications." SAMSUNG-1011, [0035]. The collected data are then normalized before sharing with other nodes.

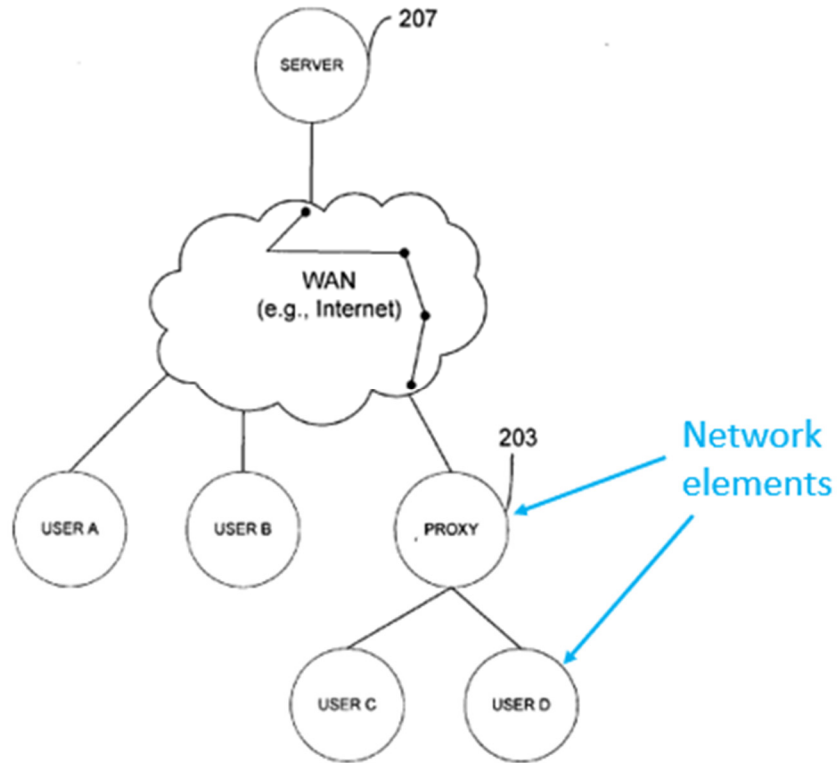
SAMSUNG-1011, [0060]. A POSITA would have understood from Padmanabhan's discussion of data collection and processing that collected and normalized data comprise a report based on usage measures, or would have otherwise found generating a report from the collected/processed data to at least be obvious. Since Padmanabhan's collected and normalized data

provide information about network state, such data are a report, or report data. In fact, a POSITA would recognize that, per Padmanabhan, JJRPD “reports on” its state to other network devices, which is done using a report. In fact, Padmanabhan states that “[p]eriodically, each USER node *reports* aggregated views of information to a parent node.” SAMSUNG-1011, [0083].

[22.3] assist in sending the report to a network element over the first wireless network or over the second wireless network.

395. JJRPD renders [22.3] obvious.

396. For example, per Padmanabhan, JJRPD’s “performance information is shared with other end hosts in the network (e.g., USERS B, C and D) in a manner in keeping with either a peer-to-peer or server-based infrastructure to which the USERS A, B, C and D belong,” and can use infrastructural service or peer-to-peer communications techniques. SAMSUNG-1011, [0011], [0035].



SAMSUNG-1011, FIG. 2b(annotated)

397. Further, as described above Padmanabhan states that “[p]eriodically, each USER node reports aggregated views of information to a parent node.” SAMSUNG-1011, [0083].

398. A POSITA would have understood that at least proxies, other networked devices (end hosts), server-based infrastructure and infrastructural services are network elements.

D. Ground 1E: Jobs in view of Jones, Rao, and Ibrahim renders claim 25 obvious

[25.1] The wireless device recited in claim 1, wherein the one or more modems include a wireless wide-area network modem for enabling the wireless device to communicate over at least the first wireless network and a local-area network

modem for enabling the wireless device to communicate with one or more end-user devices over a local-area network

399. JJRID renders [25.1] obvious.

400. Per Ibrahim, Jobs and Rao, JJRID includes a modem, e.g., a WAN “cellular radio” (per Ibrahim) enabling JJRID to communicate over the first wireless network (GSM). SAMSUNG-1012, [0045]; [1.2]; §IX.L. (I discuss Jobs’s modem in §IX.A.)

401. JJRID also includes a WLAN modem enabling JJRID to communicate with devices over the WLAN. Per Ibrahim, JJRID communicates with other wireless devices over “Bluetooth, WLAN, ZigBee, and/or ultra-wideband.” SAMSUNG-1012, [0056]. A POSITA would have understood JJRID includes a WLAN modem since it communicates with other wireless devices over a WLAN. SAMSUNG-1012, [0056].

[25.2] wherein the one or more agents are further configured to assist in providing an intermediate networking device forwarding service for forwarding traffic between a particular end-user device of the one or more end-user devices and at least one network communication end point over the first wireless network,

402. JJRID renders [25.2] obvious.

403. Per Ibrahim, JJRID serves as an intermediate networking device providing forwarding service by enabling “access to the cellular network 100 by closely located wireless devices that do not have direct access to the cellular network” by providing “switching and/or routing operations to

enable communication between the cellular network 100 and at least a portion of the closely located wireless devices.” SAMSUNG-1012, [0027], [0029], [0040]. A POSITA would have understood that providing switching and/or routing operations is providing a forwarding service. SAMSUNG-1001, 29:59-67, 33:47-53, 152: 37-50. For example, the ’110 patent explains that “a PCIe modem card running over USB or PCIe, a GPIO connection running from a processor 930 chipset to a modem chipset inside a mobile device, or a Wi-Fi connection running from a Wi-Fi modem inside of device 100 to *an intermediate modem or networking device combination that forwards the access network traffic between the access network connection and the device via the Wi-Fi connection.*” SAMSUNG-1001, 29:59-67. More generally, JJRID is serving as a base station that bridges another wireless device to a network, a POSITA would have recognized that JJRID forward traffic to/from that other wireless device since that is a core function of such a base station.

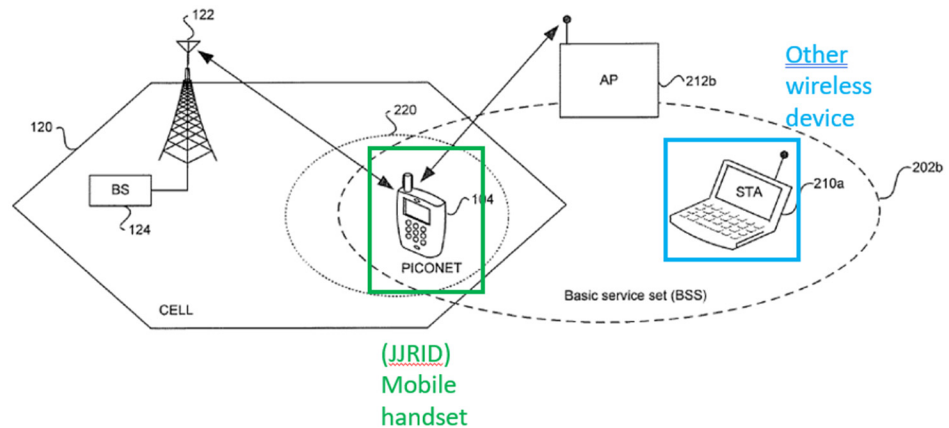
[25.3] wherein the first service activity includes traffic associated with the particular end-user device.

404. JJRID renders [25.3] obvious.

405. JJRID both forwards traffic from other devices and transmits data generated on JJRID, including backup data (first service activity).

§III.A.1.d; §III.E.1.b.

406. A POSITA would have understood that the destination of backup from JJRID can be any suitable computing device, including “[an]other wireless device.”



SAMSUNG-1012, FIG. 2B(modified).

407. For example, JJRID backs up personal data (contacts, favorites, etc.) to the “other wireless device,” such as a laptop assigned to the same employee. While backing up to a laptop might not be optimally suited for all types of data (e.g., for data subject to regulatory control such as HIPAA, or for enormous files, such as large software projects), they are well-suited for backing up things like personal files where they are easily accessible if it is necessary to restore the files from the laptop to the mobile device.

408. A POSITA would have understood that, to protect data, backing up data requires a reliable protocol, such as TCP/IP. SAMSUNG-1006, 1:47-

49. A POSITA would have further understood that TCP includes

bidirectional traffic, e.g., the payload (backup data) flowing from JJRID to the backup server, and acknowledgements flowing from the backup server to JJRID. For example the TCP RFC states that the “TCP must recover from data that is damaged, lost, duplicated, or delivered out of order by the internet communication system,” which “is achieved by assigning a sequence number to each octet transmitted, and requiring a positive acknowledgment (ACK) from the receiving TCP.” SAMSUNG-1046, 7, *generally; discussion of* [22.1].

409. Therefore, the first service activity (backup from JJRID to the “other wireless device,” which is a particular end-user device) includes traffic associated with (e.g., directed to) the particular end-user device (e.g., TCP “ACK” packets). SAMSUNG-1046, 7.

E. Ground 2: Jobs in view of Jones, Rao, Bocking, and Cunningham renders claim 26 obvious

[26.1] A wireless device comprising:

410. For at least the reasons described in §X.A.[1.1], JJRBCD is a wireless device that renders [26.1] obvious. SAMSUNG-1005, [0016]; §IX.M; §X.A.[1.1].

[26.2] means for obtaining, through a user interface of the wireless device, a user input specifying at least an aspect of a first service policy,

411. The structure for the “means for obtaining” includes a user interface and a processor configured to perform the algorithm steps of providing the

user with information and accepting user choices or preferences on, e.g., service plan selection or change, and/or other service related information, settings, and/or options. SAMSUNG-1001, 27:15-29; 28:41-48, 65:41-51; §I.C.2.[26.2]. The JIRBCD renders obvious this element. §I.C.2.[26.2].

412. For example, per Jobs, JIRBCD includes “one or more ***processors*** 518 [that] run various software components stored in the medium 502 to perform various functions for the device 500,” which “include an operating system 522, a communication module 524, a contact/motion module 526, a graphics module 528, one or more applications 530 and a meter module 532.”

SAMSUNG-1005, [0046]. The “graphics module 528 includes various known software components for rendering, animating and ***displaying graphical objects in a GUI/display surface*** of the multi-touch sensitive display system 512.” SAMSUNG-1005, [0049]. Additionally, “[t]he multi-touch sensitive display 512 communicates with the processing system 504 via a multi-touch sensitive screen controller 540 which includes various components for ***processing user input*** (e.g., scanning hardware).”

SAMSUNG-1005, [0053].

413. JIRBCD includes a user interface for obtaining user input specifying a policy, per Jobs. For example, per Jobs, JIRBCD’s UI includes a pull-down menu “containing account-related options ... including but not limited to

changing a billing plan [and] increasing budget for a service account.”

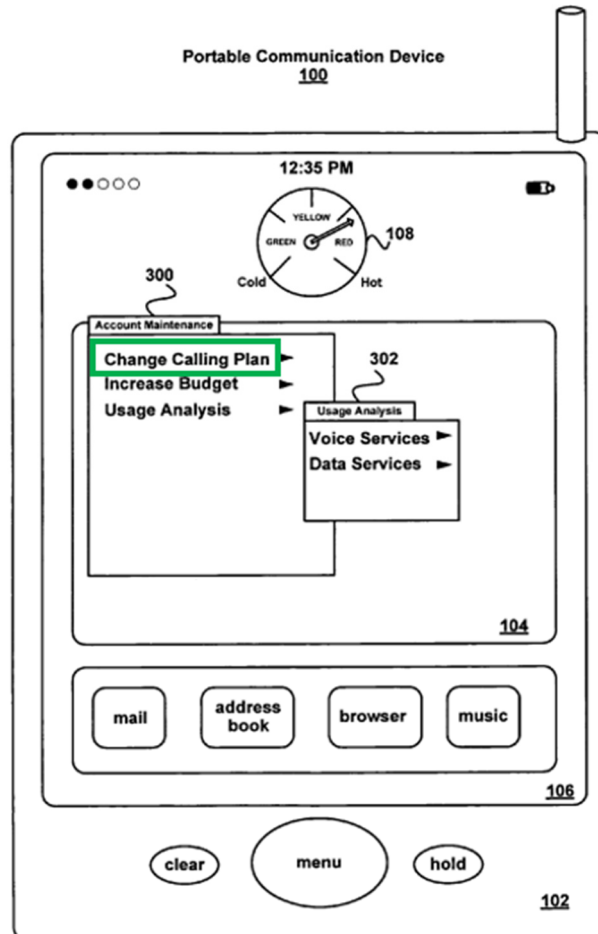
SAMSUNG-1005, [0029]. A POSITA would have understood or found obvious that JJRBCD’s pull-down menu (per Jobs) causes JJRBCD to obtain user input from the pull-down menu. SAMSUNG-1005, [0029].

414. That a pull-down menu provides user input (in this case to JJRBCD) was well-known in the art. In general, user interface widgets serve two purposes: to provide information to the user and to obtain input from the user. Menus do both: they display a list of choices to a user, and obtain the user’s selection from the list. For example, Mortensen explains that:

A pull-down menu is a selection which is accessible by depressing the selection button when the cursor is pointing at a menu bar (typically at the top of a computer screen), and "dragging" (moving cursor control device 123 while the selection button is depressed) until the selection the user wishes to access is reached on the pull-down menu. An item is indicated as being selected on a pull-down menu when the item is displayed in " reverse video" or white text on a black background. *The selection is performed by the user releasing the selection button when the selection he wishes to make is displayed in this reverse video format.* Other selections and

options are available using standard GUI functions.

SAMSUNG-1044, 5:12-25 (emphasis added).



SAMSUNG-1005, FIG. 3(annotated).

415. Thus, JJRBCD's user interface and processor obtain, through a user interface, user input specifying an aspect of the service policy (access privileges, e.g., "volume limitations"). SAMSUNG-1005, [0029].

[26.3] the first service policy configured to at least assist in reducing data usage associated with a first service activity over the first wireless network,

416. For at least the reasons discussed in §X.A.[1.5], JJRBCD renders [26.3] obvious. Additionally, per Cunningham, which explains that “when the usage exceeds the expected payment, the service can be limited or disabled until the next payment cycle,” when JJRBCD exhausts its data allocation (set by policy), JJRBCD blocks further transmission, reducing data usage. SAMSUNG-1010, [0050].

[26.4] the first service activity being less than all service activities available to the wireless device,

417. For at least the reasons discussed in §X.A.[1.6], JJRBDC renders [26.4] obvious.

418. Additionally, per Jobs, JJRBDC includes service activities such as data access (e.g., backup, per Jones), SMS, and telephony. SAMSUNG-1005, [0019]; SAMSUNG-1006, 5:4-19; §IX.A; §IX.B; §IX.D. Therefore, a POSITA would have understood that the first service activity (backup), is less than all service activities.

[26.5] the first service policy for enabling control of the first service activity on the first wireless network that is different from how the first service activity is controlled on a second wireless network;

419. For at least the reasons discussed in §X.A.[1.7], JJRBCD renders [26.5] obvious.

420. Additionally, for example, Jobs explains that users of mobile devices “typically enter into service contracts with service providers for voice and/or

data services,” and Cunningham similarly describes a “dedicated wireless device business model 100 of a wireless provider.” SAMSUNG-1005, [0002]; SAMSUNG-1010, [0039]. A POSITA would have understood that, since the service contract applies to a particular service provider (per Jobs), the service contract does not apply to a different provider. SAMSUNG-1005, [0002]; SAMSUNG-1010, [0043]. Therefore, the first service activity (e.g., backup) is controlled differently on the first network (to which the contract applies) than on a second network (to which the contract does not apply).

[26.6] means for identifying that the wireless device is connected to the first wireless network;

421. For at least the reasons discussed in §X.A.[1.10], JIRBCD renders [26.6] obvious.

422. Additionally, the structure for the “means for identifying” of [26.6] includes a processor configured to perform the algorithm steps of recognizing the type of network to which the device is currently connecting, e.g., by looking up the information in a local or network table. SAMSUNG-1001, 51:4-13; §I.C.2.[26.6]. JIRBCD renders obvious this element.

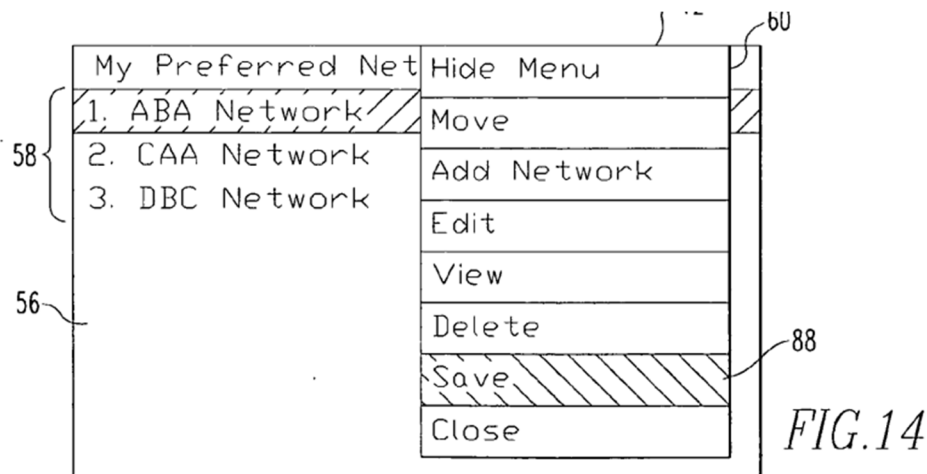
423. For example, per Jobs, JIRBCD includes “one or more ***processors*** 518 [that] run various software components stored in the medium 502 to perform various functions for the device 500,” which “include an operating system

522, a communication module 524, a contact/motion module 526, a graphics module 528, one or more applications 530 and a meter module 532.”

SAMSUNG-1005, [0046]. The “communication module 524 facilitates communication with other devices over one or more external ports 536 and the RF circuitry 508, [and] includes various software components for handling the transmission and receipt of data via the RF circuitry 508 and/or the external port 536.” SAMSUNG-1005, [0048]. A POSITA would have understood that identifying a wireless network is an example of facilitating communication.

424. Per Bocking, JJRBCD maintains a table of preferred networks.

SAMSUNG-1009, [0024]-[0029], FIGS. 14, 18-20.



SAMSUNG-1009, FIG. 14.

425. For example, Bocking explains that a user can (i) “manually add a PLMN to the listing” of preferred networks; (ii) “add a PLMN to the listing

58 by selecting the PLMN from a group of ‘known networks’ stored in memory 44 of handheld electronic device 4 (the MNC and MCC is stored for each such ‘known network’); and (iii) “add a PLMN to the listing 58 by selecting the PLMN from a group of ‘available networks,’ which handheld electronic device 4 is able to locate from its current location using communications subsystem 45 and a known network scanning procedure.” SAMSUNG-1009, [0026]-[0028]. An example list is illustrated in FIG. 19. SAMSUNG-1009, [0029], FIG. 19.

My Preferred Network List	
1. CAA Network	666/664
2. ABA Network	666/660
3. DAA Network	666/666
4. DBC Network	666/667

SAMSUNG-1009, FIG. 19.

426. A POSITA would have recognized that while Bocking refers to such data as a roaming list, “table” is a more accurate description since the each row includes multiple columns, e.g., “CAA Network” and “666/664.”

427. Per Bocking, JJRBCD “utilize[s] the preferred networks for performing wireless communications when the device is in a roaming situation, wherein the preferred networks are utilized in a priority order that is based on the priority value assigned to each of the preferred networks.” SAMSUNG-1009, Abstract, [0010], [0013]. A POSITA would have understood that when the device is connecting to a network, the device does so based on the list of preferred networks that are “utilized in priority order,” per Bocking. SAMSUNG-1009, Abstract, [0010], [0013], [0026]-[0028]. In the example above, JJRBCD first attempts to connect to “CAA Network,” and if it succeeds, it recognized that it has connected to “CAA Network,” and ceases the connection process. If JJRBCD cannot connect to “CAA Network, it attempts to connect to “ABA Network,” and if it succeeds, it recognized that it has connected to “ABA Network,” and ceases the connection process. JJRBCD continues the process until it connects or exhausts the list of available roaming networks.

428. Therefore, a POSITA would have understood that JJRBCD recognizes, or identifies, the network it is currently connecting to by looking up the network in the list of preferred networks.

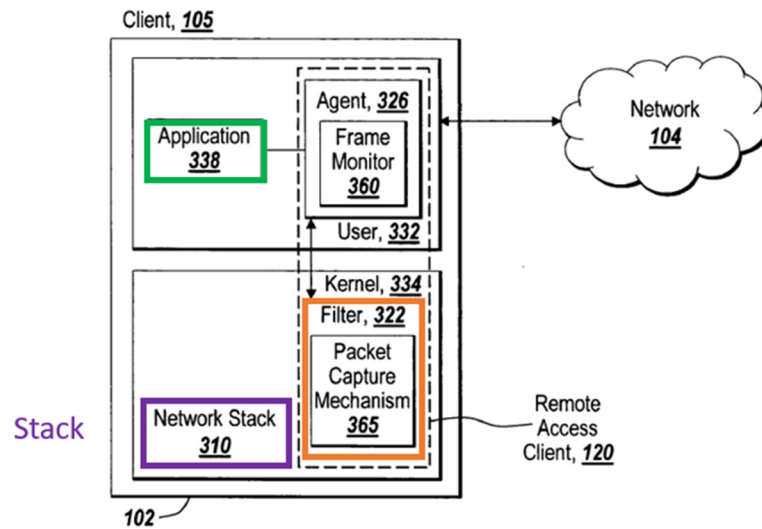
[26.7] means for identifying an intended, attempted, or successful data communication over the first wireless network, the intended, attempted, or successful data communication being associated with the first service activity; and

429. The structure for the “means for identifying” of [26.7] includes a processor configured to perform the algorithm steps of implementing traffic inspection points between the applications and the networking stack application interface using a T-buffer at socket connections and feeding the side traffic into a traffic flow analyzer. SAMSUNG-1001, 29:10-32, 53:51-55, 53:58-63, FIG. 16; §VI.[26.7]. JJRBCD renders obvious this element.

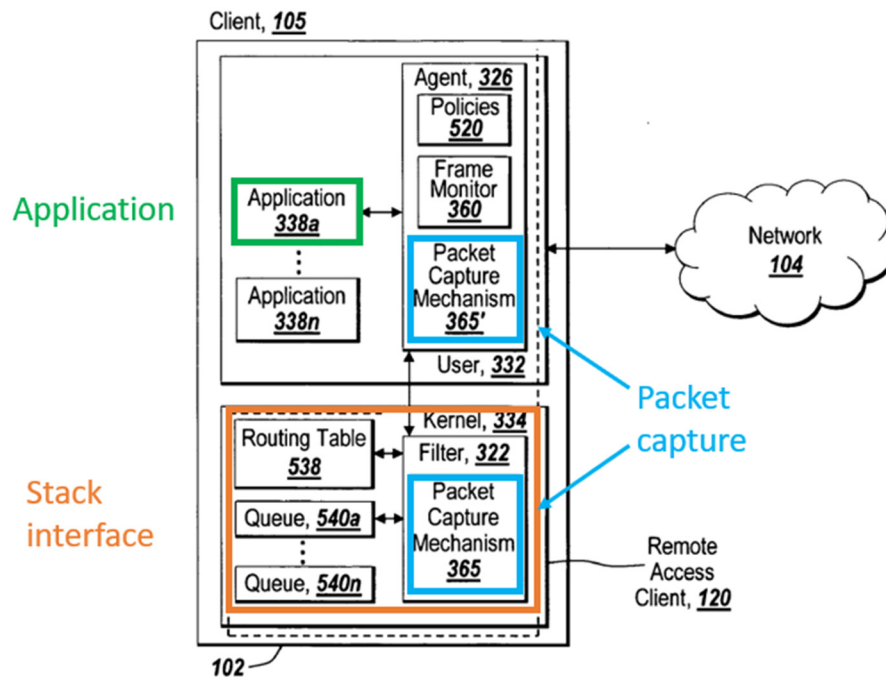
430. For example, per Jobs, JJRBCD includes “one or more *processors* 518 [that] run various software components stored in the medium 502 to perform various functions for the device 500.” SAMSUNG-1005, [0046]. A POSITA would have understood that identifying attempted data communication is a device function.

431. Per Rao, JJRBCD implements traffic inspection points between the applications and the networking stack application interface. For example, Rao explains that the “the filter 322 intercepts all outbound packets of the client 105 for inspection” and the “filtering table is used to determine what action to take against packets, such as packets intercepted by the packet capture mechanism 365.” SAMSUNG-1007, [0102], [0105]. Per Rao, JJRBCD’s RAC “store[s] a captured IP packet in a buffer.” SAMSUNG-1007, [0111]. Rao illustrates the packet capture mechanism and filter

(which together serve as traffic inspection points), in FIGS. 1C and 5A, reproduced below. SAMSUNG-1007, FIGS. 1C, 5A.



SAMSUNG-1007, FIG. 1C(annotated).



SAMSUNG-1007, FIG. 5A(annotated)

432. Thus, per Rao, JJRBCD's RAC implements a traffic inspection point (packet capture) between the applications and the networking stack application interface uses a buffer ("store[s] a captured IP packet in a buffer") at a socket connection ("network stack 310 may comprise one or more protocols, such as the TCP/IP protocol"), and feeds the side traffic into a traffic flow analyzer ("packet capture mechanism 365 may forward the packets to ... a frame monitor mechanism 360 of the agent 326").

SAMSUNG-1007, [0100], [0104], [0111]. A POSITA would have recognized that the TCP protocol (as used in Rao) provides network sockets. E.g., RFC 793 states that "[c]oncatenated with the network and host addresses from the internet communication layer, this forms a socket," and "[a] pair of sockets uniquely identifies each connection." SAMSUNG-1046, 8.

433. A POSITA would have further understood that packets sent by an application 338 and captured before reaching the network stack 310 are attempted and/or successful data communication from the application.

[26.8] means for applying the first service policy.

434. The structure for the "means for applying" includes a processor configured to perform the algorithm steps of performing a service control

that reduces traffic speed for all applications and traffic types successively until the service usage projections are within service usage limits for the present service billing period. SAMSUNG-1001, 48:38-49:1; §VI.[26.8]. JJRBCD renders obvious this element.

435. For example, per Jobs, JJRBCD includes “one or more *processors* 518 [that] run various software components stored in the medium 502 to perform various functions for the device 500.” SAMSUNG-1005, [0046]. A POSITA would have understood that applying policy is a device function.

436. Per Cunningham, JJRBCD evaluates the data access threshold (first service policy), and in response to determining that usage exceeds the threshold, applies the policy by reducing traffic speed to zero (blocking access). SAMSUNG-1010, [0050]. Thus, by disabling access for the remainder of the month, JJRBCD is reducing traffic speed (to zero) for all applications and service types for present service billing period. SAMSUNG-1010, [0050].

F. CONCLUSION

437. For all the reasons I have noted in the foregoing paragraphs, claims 1-30 of the ‘110 Patent are obvious in view of the references discussed above.

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

APPENDIX A

PATRICK DREW MCDANIEL

Tsun-Ming Shih Professor of Computer Sciences
School of Computer, Data and Information Sciences ◊ University of Wisconsin-Madison
Office : Room 7387, 1210 W. Dayton St. ◊ Madison, WI 53706 ◊ (608) 263-1008
email: mcdaniel@cs.wisc.edu ◊ *Homepage*: <https://patrickmcdaniel.org/>

ACADEMIC AND RESEARCH APPOINTMENTS

Tsun-Ming Shih Professor of Computer Sciences, University of Wisconsin-Madison, Madison, WI	2022-Present
William L. Weiss Professor of Information and Communications Technology Computer Science and Engineering, Pennsylvania State University, University Park, PA	2017-2022
Distinguished Professor Computer Science and Engineering, Pennsylvania State University, University Park, PA	2016-2017
Professor Computer Science and Engineering, Pennsylvania State University, University Park, PA	2011-2015
Associate Professor Computer Science and Engineering, Pennsylvania State University, University Park, PA	2007-2011
Hartz Family Career Development Assistant Professor Computer Science and Engineering, Pennsylvania State University, University Park, PA	2004-2007
Adjunct Professor Stern School of Business, New York University, New York, NY	2003-2009
Senior Research Staff Member AT&T Labs - Research, Florham Park, NJ	2001-2004

RESEARCH LEADERSHIP APPOINTMENTS

Director, National Science Foundation, Center for Trustworthy Machine Learning Participants: Penn State, Stanford, UC Berkeley, UC San Diego, Univ. of Wisconsin, Univ. of Virginia	2018-present
Director, Institute for Networking and Security Research College of Engineering, Pennsylvania State University, University Park, Pennsylvania	2016-2022
Program Manager, Cyber-Security Collaborative Research Alliance (CRA) College of Engineering, Pennsylvania State University, University Park, Pennsylvania	2013-2018
Co-Director, Systems and Internet Infrastructure Laboratory College of Engineering, Pennsylvania State University, University Park, Pennsylvania	2004-2022

EDUCATION

Ph.D., Computer Science and Engineering, University of Michigan , Ann Arbor, MI	2001
M.S., Computer Science, Ball State University , Muncie, IN	1991
B.S., Computer Science Ohio University , Athens, OH	1989

AFFILIATIONS

Association for Computing Machinery (ACM), *Fellow*
The Institute of Electrical and Electronics Engineers (IEEE), *Fellow*
American Association for the Advancement of Science (AAAS), *Fellow*
USENIX Advanced Computing Systems Association (USENIX)

STUDENTS

Past PhD Students

- *Z. Berkay Celik*, Spring 2019, now **Assistant Professor**, Purdue University

-
- *Nicolas Papernot*, Spring 2018, now **Assistant Professor**, University of Toronto
 - *Wenhui Hu*, Fall 2016, now **Senior Member of Technical Staff**, Oracle
 - *Devin Pohly*, Spring 2016, now **Assistant Professor**, Wheaton College
 - *Damien Oceau*, Summer 2014, now **Software Engineer in Security**, Google
 - *Steve McLaughlin*, Spring 2014, now **Senior Software Engineer**, Samsung Research America
 - *Thomas Moyer*, Summer 2011, now **Assistant Professor**, University of North Carolina-Charlotte
 - *William Enck*, Spring 2011, now **Professor**, North Carolina State University
 - *Kevin Butler*, Summer 2010, now **Professor**, University of Florida
 - *Machigar Ongtang*, Summer 2010, now **Assistant Professor**, Dhurakij Pundit University
 - *Patrick Traynor*, Spring 2008, now **John and Mary Lou Dasberg Preeminent Chair, Professor**, University of Florida, co-advisor
 - *Fr. Boniface Hicks*, Fall 2007, now **Assistant Professor**, St. Vincent College

Current PhD Students

- *Jean-Charles Noirot Ferrand*, University of Wisconsin, Spring 2028
- *Kyle Domico*, University of Wisconsin, Spring 2028
- *Kunyang Li*, University of Wisconsin, Spring 2027
- *Rachel King*, University of Wisconsin, Spring 2027
- *Yohan Beugin*, University of Wisconsin, Spring 2026
- *Blaine Hoak*, University of Wisconsin, Spring 2026
- *Quinn Burke*, University of Wisconsin, Spring 2026
- *Eric Pauley*, University of Wisconsin, Spring 2025
- *Ryan Sheatsley*, University of Wisconsin, Spring 2024

Past Masters Students

- *Blaine Hoak*, Pennsylvania State University, Summer 2022
- *Rachel King*, Pennsylvania State University, Summer 2022
- *Alban Heon*, Pennsylvania State University, Summer 2022
- *Yohan Beugin*, Pennsylvania State University, Spring 2021
- *Ahmed Abdou*, Pennsylvania State University, Spring 2021
- *Adrien Cosson*, Pennsylvania State University, Summer 2020
- *Bolor Zolbayar*, Pennsylvania State University, Summer 2020
- *Alejandro Andrade*, Pennsylvania State University, Summer 2020
- *Quinn Burke*, Pennsylvania State University, Spring 2020
- *Eric Pauley*, Pennsylvania State University, Spring 2020
- *Sushrut Shringarputal*, Pennsylvania State University, Fall 2019
- *Raquel Alvarez*, Pennsylvania State University, Spring 2019
- *Valentin Vie*, Pennsylvania State University, Spring 2019
- *Ryan Sheatsley*, Pennsylvania State University, Fall 2018
- *Eric Kilmer*, Pennsylvania State University, Spring 2016
- *Nathan Lagerman*, Pennsylvania State University, Spring 2016
- *Matthew Dering*, Pennsylvania State University, Spring 2014
- *Phil Koshy*, M.S. Pennsylvania State University, Fall 2013
- *Diana Koshy*, M.S. Pennsylvania State University, Fall 2013
- *Steve McLaughlin*, M.S. Pennsylvania State University, Spring 2011
- *Sergei Miadzvezhanka*, M.S. Pennsylvania State University, Spring 2011
- *Adam Delozier*, M.S. Pennsylvania State University, Spring 2011
- *Juliet Uhloff*, M.Eng. Pennsylvania State University, Fall 2010

-
- *Damien Octeau*, M.S. Pennsylvania State University, Spring 2010
 - *Thomas Moyer*, M.S. Pennsylvania State University, Spring 2009
 - *Luke St. Clair*, M.S. Pennsylvania State University, Summer 2008
 - *Lisa Johansen*, M.S. Pennsylvania State University, Spring 2008
 - *Sunam Ryu*, M.S. Pennsylvania State University, Spring 2007
 - *Dhananjay Bapat*, M.S. Pennsylvania State University (Electrical Engineering), Fall 2006
 - *Jennifer Plasterr*, M.Eng. Pennsylvania State University, Summer 2006
 - *Adam Kerr*, M.Eng. Pennsylvania State University, Fall 2006
 - *William Enck*, M.S. Pennsylvania State University, Spring 2006
 - *Wesam Lootah*, M.S. Pennsylvania State University, Spring 2006
 - *Jon Hansford*, M.Eng. Pennsylvania State University, Fall 2005
 - *John van Bremer*, M.Eng. Pennsylvania State University, Spring 2005

Past Post-Docs

- *Vaibhav Rastogi*, graduated Northwestern University
- *Robert Walls*, graduated University of Massachusetts, Amherst

TEACHING

University of Wisconsin-Madison, College of Letters and Science

- **Intro to Information Security** - Fall 2023

Pennsylvania State University, College of Engineering

- **CMPSC311 - Introduction to Systems Programming** - Fall 2013, Fall 2014, Fall 2015, Fall 2016, Summer 2019, Spring 2020, Fall 2020, Fall 2021
- **CMPSC443 - Introduction to Computer and Network Security** - Spring 2006, Spring 2009, Fall 2017, Fall 2018
- **CSE543 - Computer and Network Security** - Fall 2004, Fall 2005, Fall 2008, Fall 2009, Fall 2011, Fall 2014
- **CSE544 - Advanced System Security** - Spring 2005, Spring 2007
- **CSE545 - Advanced Network Security** - Spring 2006, Spring 2008, Spring 2011
- **CSE597g - Principles, Analysis, and Applications of Computer Security** - Fall 2015
- **Security and Privacy of Machine Learning** - Fall 2016
- **Advanced Topics in the Security and Privacy of Machine Learning** - Spring 2017
- **CSE598 - Cell Phone Operating Systems** - Spring 2009
- **CSE598i - Web 2.0 Security** - Spring 2010
- **CSE598d - Topics in Applied Systems Security** - Fall 2010
- **CSE598e - Critical Infrastructure Security** - Fall 2011
- **CSE 597 – Emerging Trends in Computer Security** - Fall 2021
- **CMPSC297 – Introduction to C Programming in UNIX** - Fall 2021

New York University, Stern School of Business

- **B20.3157 Computer and Network Security** - Spring 2003, Summer 2004, Summer 2005
- **B20.3156 - Online Privacy** - Spring 2003, Summer 2004

HONORS, AWARDS, AND KEYNOTE ADDRESSES

SIGSAC Outstanding Innovation Award, for innovative research in mobile device security, trustworthiness of machine learning, and systems security, November 2021

Penn State Engineering Society Premier Research Award, Given to one faculty member per year, the Penn State Engineering Alumni Society Premier Research Award recognizes and rewards an individual whose contributions to scientific knowledge through research are exemplary and internationally acclaimed, April 2021

AAAS Fellow, for distinguished contributions to the field of computational security and privacy, particularly for advancing algorithms for the formal analysis of mobile devices and applications, November 2020

SIGOPS Hall of Fame Award, recognizing the paper "TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones" (Will Enck first author), "which sparked an important research agenda on smartphone privacy that continues to this day", November 2020

J. D. Williams student paper award, Nuclear Security and Physical Protection division, recognizing the best student papers by area in Proceedings of the Institute of Nuclear Materials Management Annual Meeting (INMM), July 2019

Penn State Engineering Society Outstanding Advising Award, highly selective award by the Penn State Engineering Society given to faculty in the College of Engineering who have made significant contributions as advisor, October 2018

Best Paper, 2017 EAI SECURECOMM 2018, with Sayed M. Saghaian, Tom La Porta, Trent Jaeger and Z. Berkay Celik, August 2018

Best Student Paper, 2017 ACM Symposium on SDN Research (SOSR), with Stefan Achleitner, Thomas La Porta and Trent Jaeger, April 2017

IEEE Technical Committee on Security and Privacy Outstanding Community Service Award, in recognition for leadership of the Technical Committee on Security and Privacy, May 2016

ACM Fellow, for contributions to computer and mobile systems security, December 2015

Science of Security Index of Significant Research in Cyber Security, acknowledging paper 'Toward a Science of Secure Environments', Science of Security Virtual Organization (SOS-VO), August 2015

IEEE Fellow, for contributions to the security of mobile communications, November 2014

Best Artifact Award, 20th International Symposium on the Foundations of Software Engineering (FSE), with advisee Damien Ocateau and collaborator Somesh Jha, November 2012

Best Paper, 25th Annual Computer Security Applications Conference, with advisees Machigar Ongtang, Stephen McLaughlin, and William Enck, December 2009

Faculty Marshal, College of Engineering, selected by student marshals for contributions to undergraduate education, leads procession into graduation ceremony, May 2009

Penn State Engineering Society Outstanding Research Award, highly selective award by the Penn State Engineering Society given to faculty in the College of Engineering who have made significant contributions to knowledge in their field, March 2009

Google Security and Product Safety Acknowledgement, in recognition of efforts in improving the security of Google Android cellular phone operating system, 2008

Commendation for Exceptional Leadership and Achievement, in recognition of efforts as PI of the EVEREST study, from Ohio Secretary of State Jennifer Brunner, August 2008

IEEE Technical Committee on Security and Privacy Outstanding Community Service Award, in recognition for technical program management of the IEEE Security and Privacy symposia, August 2008

National Science Foundation CAREER Award, Faculty early career development grant, August 2007

Penn State Computer Science and Engineering Outstanding Teaching Award, Given to best teacher in the department as selected by students, March 2007

ACM Certificate of Meritorious Service, Certificate acknowledging exemplary service as associate editor of ACM Transactions on Internet Technologies, April 2007

Best Student Paper, 22nd Annual Computer Security Applications Conference, as advisor, with Boniface Hicks and Kiyan Ahmadizadeh, December 2006

Best Paper, Innovations and Commercial Applications of Distributed Sensor Networks Symposia, Awarded for best paper in conference, October 2005.

Hartz Family Career Development Professor, Endowed Professorship, Pennsylvania State University, Fall 2004-2007

Bang for the Buck Award, DARPA Dynamic Coalitions Program, Award for most feature-rich/useful software system, April 2002

National Aeronautics and Space Administration, Kennedy Space Center Fellowship, Research Fellowship, September 1997 - August 2000

Electrical Engineering and Computer Science Summer Fellowship Award, University of Michigan, June 1997

Dean's Citation for Perfect Academic Record, Ball State University, June 1991

Keynote Addresses

1. Security's Role in Achieving Sustainability, 29th ACM Conference on Computer and Communications Security (CCS), Los Angeles, CA, November, 2022.
2. Security, Game Theory, and Their Role in Achieving Sustainability, Conference on Decision and Game Theory for Security, Pittsburgh, PA, October, 2022.
3. Prognosticating the Future of IoT Security, 2022 IEEE SafeThings Workshop, San Francisco, CA, May 2022.
4. The Challenges of Machine Learning in Adversarial Settings. Triangle Area Privacy and Security Day, Durham, NC, October, 2019.
5. The Challenges of Machine Learning in Adversarial Settings. 2019 Subversion and Assurance of AI Workshop, US National Reconnaissance Office, Washington, DC, March, 2019.
6. Attacks, Defenses, and Impacts of Machine Learning in Adversarial Settings. 2017 Conference on Security and Privacy in Communication Networks (SecureComm), Niagara Falls, Canada, October, 2017.
7. Tracing the Arc of Smartphone Application Security. 2017 ACM on International Workshop on Security And Privacy Analytics. Scottsdale, AZ, March, 2017.
8. Tracing the Arc of Smartphone Application Security. 12th International Conference on Information Systems Security, Jaipur, India, December, 2016.
9. The 25th International Conference on Computer Communication and Networks (ICCCN 2016), August, 2016, Waikoloa, Hawaii.
10. Learning from Ourselves: Where are we and where can we go in mobile systems security?. Mobile Security Technologies (MOST) 2016 Workshop, IEEE Computer Society Security and Privacy Workshops, San Jose, CA, May, 2016.
11. Eight Years of Mobile Smartphone Security. Center for Secure and Dependable Systems (CSDS) Cybersecurity Symposium, Coeur d'Alene, April, 2016.
12. The Importance of Measurement and Decision Making to a Science of Security, 2015 IEEE Conference on Communications and Network Security (CNS), September 2015, Florence, Italy.
13. The Importance of Measurement and Decision Making to a Science of Security. 3rd International Symposium on Resilient Cyber Systems, Philadelphia, PA, August, 2015.
14. The Importance of Measurement and Decision Making to a Science of Security, 2015 Symposium And Bootcamp on the Science of Security (Hotsos), April 2015, University of Illinois at Urbana-Champaign

-
15. Security and Science of Agility, ACM Workshop on Moving Target Defense (MTD 2014), November 2014, Scottsdale, AZ
 16. A Secondary Internet Revolution: How the Smart Device has Changed the Information Security Landscape, IEEE New Technology Industry Seminar (NTIS '13), Everett WA, August, 2013
 17. Permission-based Application Governance; A Step Forward or Backward?, 26th Annual WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'12), Paris, France, July 2012.
 18. Scalable Integrity-Guaranteed AJAX, The 14th Asia-Pacific Web Conference (APWeb), Kunming, China, April 2012.
 19. Security Challenges and Solutions in Mobile Smartphone Applications, IEEE Computer Security Foundations (CSF 2011), Abbaye des Vaux de Cernay, France, June 2012.
 20. Password Exhaustion: Predicting the End of Password Usefulness. 2nd International Conference on Information Systems Security, Kolkata India, December, 2006.
 21. Physical and Digital Convergence: Where the Internet is the Enemy. Eighth International Conference on Information and Communications Security (ICICS '06), Raleigh, NC, December, 2006.

Distinguished Lectures

1. The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, Michigan State University, Lansing, MI, November, 2023.
2. The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective. Computer Science Department, Temple University, Philadelphia, PA, February, 2022.
3. The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective. Computer Science Department, University of Wisconsin-Madison, Madison, WI, February, 2020.
4. Shutterstock Distinguished Lecture: The Challenges of Machine Learning in Adversarial Settings. Computer Science Department, Stonybrook University, Stonybrook, NY, December, 2019.
5. Distinguished Blockchain Lecture: The Challenges of Machine Learning in Adversarial Settings. Cylab Security and Privacy Institute, Carnegie Mellon University, Pittsburgh, PA, December, 2019.
6. Distinguished Speaker Series: The Challenges of Machine Learning in Adversarial Settings. Department of Computer Science, University at Buffalo, Buffalo, NY, November, 2018.
7. Samuel D. Conte Distinguished Lecture Series: The Challenges of Machine Learning in Adversarial Settings. Department of Computer Science, Purdue University, West Lafayette, Indiana, November, 2018.
8. The Challenges of Machine Learning in Adversarial Settings. Department of Software and Information Systems, University of North Carolina at Charlotte, Charlotte, NC, February, 2018.
9. Tracing the Arc of Smartphone Application Security. Celebrating 50 Years of Computer Science @ NC State, North Carolina State University, Raleigh, NC, October, 2017.
10. Tracing the Arc of Smartphone Application Security. Computer Science Department and the Electrical and Computer Engineering Department Seminar Series, Colorado State University, Fort Collins, CO, October, 2017.
11. Tracing the Arc of Smartphone Application Security. Rochester Institute of Technology, College of Computing and Information Sciences, Rochester, NY, September, 2017.
12. Tracing the Arc of Smartphone Application Security, University of Texas-Dallas Department of Computer Science, Dallas, TX, May 2017.
13. Tracing the Arc of Smartphone Application Security. Rochester Institute of Technology, College of Computing and Information Sciences, Rochester, NY, May 2017.

-
14. Tracing the Arc of Smartphone Application Security. University of California-Irvine, Computer Science Department, Irvine CA, March, 2017.
 15. Tracing the Arc of Smartphone Application Security. The Ohio State University, Department of Computer Science and Engineering, Columbus, OH, March, 2017.
 16. Tracing the Arc of Smartphone Application Security. Virginia Technical University, Department of Computer Science, Blacksburg, VA, March, 2017.
 17. Six Years of Mobile Smartphone Security, CISPA Distinguished Lecture Series, Max Planck Institute/Saarland University, Saarbrücken Germany, July, 2015.
 18. Six Years of Mobile Smartphone Security. Technische Universität Darmstadt, Darmstadt Germany, July, 2015.
 19. Security Challenges and Solutions in Mobile Smartphone Applications. Computer and Information Science Department, University of Oregon, Eugene, OR, April, 2011.
 20. Security Challenges and Solutions in Mobile Smartphone Applications. Department of Software Information Systems College of Computing and Informatics, UNC Charlotte, Charlotte, NC, December, 2010.

RESEARCH SUPPORT

co-PI, *MURI: Cohesive and Robust Human-Bot Cybersecurity Teams*, Army Research Office, \$6,000,000 (PSU award \$739,527), 07/01/2021-06/30/2026, Collaborators: Many.

co-PI, *SaTC: CORE: Small: Adversarial Network Reconnaissance in Software Defined Networking*, NSF (CNS), \$500,000 (PSU award \$500,000), 1/1/2020-12/31/2022, Collaborators: He (Penn State).

PI, *CNS Core: Medium: Automated IoT Safety and Security Analysis and Synthesis*, NSF (CNS), \$272,033 (PSU award \$272,033), 6/25/2019-6/24/2022, Collaborators: Tan (Penn State).

PI, *Mapping Black-Box Attack Metrics and Parameter Spaces in Machine Learning*, US Army Aviation and Missile Research, Development and Engineering Center, \$436,677 (PSU award \$436,677), 6/25/2019-6/24/2022, Collaborators: (single PI).

PI, *SaTC CORE: Frontier: Collaborative: End-to-End Trustworthiness of Machine-Learning Systems*, NSF (CNS), \$9,649,366 (PSU award \$2,044,550), 8/15/2018-3/31/2023, Collaborators: Boneh (Stanford), Chaudhuri (UCSD), Evans (Virginia), Jha (Wisconsin), Liang (Stanford), Song (Berkeley).

PI, *2017 SaTC PI Meeting*, NSF (CNS), \$99,999 (PSU award \$50,230), 8/15/2016-3/31/2017, Collaborators: Antonakakis (GaTech), Mason (UIUC).

PI, *TWC: Medium: Collaborative: Scaling and Prioritizing Market-Sized Application Analysis*, NSF (CNS), \$1,147,213 (PSU award \$547,213), 7/01/2016-6/30/2020, Collaborators: Jha (Wisconsin).

PI, *Student Travel Support for Symposium on Security and Privacy 2014*, Army Research Office, \$10,000 (PSU award \$10,000), 5/1/14-5/1/15.

PI, *Models for Enabling Continuous Reconfigurability of Secure Missions (MACRO) Cyber-Security Collaborative Research Alliance (CRA)*, Army Research Laboratory, \$24.1 million (\$48.2 million with renewal at 12/17), 9/20/2013-9/19/2023 (renewed at 5 years), Collaborators: PSU, Carnegie Mellon, Indiana, UC Davis, UC Riverside, ARL, CERDEC.

PI, *Google Faculty Research Award, Plotting a Map of Android Inter-App Communication*, Google, \$50,000, 3/1/2012-2/28/2013, Collaborators: PSU (McDaniel), TU Darmstadt (Bodden), University of Luxembourg (Traon), .

PI, *Battelle BGP Security Study (Phase 2)*, Battelle, \$102,815, 10/1/2012-9/30/2013, Collaborators: PSU (McDaniel), Oregon (Butler).

PI, *TWC: Medium: Collaborative: Extending Smart-Phone Application Analysis*, NSF (CNS), \$1,386,518 (plus 16k REU supplement) (PSU award \$534,748), 8/1/2012-7/31/2016, Collaborators: PSU (McDaniel), Wisconsin (Jha).

PI, *Battelle BGP Security Study (Phase 1)*, Battelle, \$94,400, 2/15/2012-9/30/2012, Collaborators: PSU (McDaniel).

co-PI, *TC: Medium: Collaborative Research: Building Trustworthy Applications for Mobile Devices*, NSF (CNS), \$1,386,518 (PSU award \$350,000), 8/1/2011-7/31/2014, Collaborators: PSU (McDaniel), Wisconsin (Banerjee, Jha, Swift).

PI, *Closing the Loop on Security Testing and Security Requirements*, Security and Software Engineering Research Center, \$31,000, 8/1/2011-7/31/2012.

co-PI, *Managing Security and Vulnerability Risks in the Smart Grid*, Institute for CyberScience and The Penn State Institutes of Energy and the Environment, \$31,000, 08/1/09-12/16/09, Collaborators: PSU (Blumsack, McDaniel).

PI, *Smart Grid Cyber Security Research*, Lockheed Martin, \$250,000, 1/1/10-12/16/10.

PI, *NSF HECURA: Collaborative Research: Secure Provenance in High-End Computing Systems*, NSF (CCF), \$1,000,000 (PSU award \$307,073), 08/1/09-8/31/13, Collaborators: PSU (McDaniel), UIUC (Winslett), Stonybrook (Sion, Zadok).

PI, *TC: Medium: Collaborative Research: Security Services in Open Telecommunications Networks*, NSF (CNS), \$1,386,518 (PSU award \$594,941), 08/01/09-08/01/12, Collaborators: PSU (McDaniel, La Porta), UPenn (Blaze), Columbia (Schulzrinne).

PI, *Characterizing and Mitigating Wireless Systems Vulnerabilities*, Defense University Research Instrumentation Program (DURIP), Army Research Office (ARO), \$150,000, 05/22/09-02/28/11, Collaborators: PSU (La Porta, McDaniel).

co-PI, *Integrity Management for ICT Development*, Bell Labs Network Reliability and Security Office, Alcatel-Lucent, \$100,000, 11/30/08-11/30/09, Collaborators: PSU (La Porta, McDaniel).

PI, *Utility Grid Automation and Risk Management*, Lockheed Martin, \$400,000, 11/30/08-12/16/09.

PI, *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards, and Testing*, The State of Ohio, \$716,336 (PSU award \$332,066), 10/01/07-01/07/08, Collaborators: PSU (McDaniel), UPenn (Blaze), UCSB (Kemmerer, Vigna), Berkeley (Hall, Quilter).

Co-PI, *Protecting Services for Emerging Wireless Telecommunications Infrastructure*, NSF (CNS), \$658,032, 09/01/07-08/31/11, Collaborators: PSU (La Porta, Jaeger, McDaniel).

Co-PI, *Security for Internet/IMS Convergence*, Cisco, \$100,000, 9/1/07-8/31/08, Collaborators: PSU (La Porta, McDaniel).

Co-PI, *System-Wide Information Flow Enforcement*, BAA 06-11-IFKA, "National Intelligence Community Enterprise Cyber Assurance Program", \$496,000, 2/1/07-8/1/08, Collaborators: PSU (Jaeger, McDaniel).

PI, *CAREER: Realizing Practical High Assurance through Security-Typed Information Flow Systems*, NSF (CNS), \$400,000, 1/2/07-1/1/12.

Co-PI, *CT-IS: Shamon: Systems Approaches for Constructing Distributed Trust*, NSF (CNS), \$400,000, 9/1/06-8/31/10, Collaborators: PSU (Jaeger, McDaniel).

Co-PI, *Center of Excellence*, Ben Franklin Technology Partners, \$75,000, 01/01/07-07/01/07, Collaborators: PSU (Cao, Jaeger, La Porta, McDaniel, Smith).

Co-PI, *Exploiting Asymmetry in Performance and Security Requirements for I/O in High-end Computing*, NSF (CFF), \$699,690, 9/1/06-8/31/10, Collaborators: PSU (McDaniel, Sivasubramaniam).

PI, *Automated Configuration with the PRESTO Network Management Platform*, AT&T, \$100,000, 6/1/06-5/31/07.

PI, *Testbed for Network-Scale Countermeasure Evaluation*, Cisco, \$45,938, 9/1/05-8/31/06.

PI, *Collaborative Research: CT-T: Flexible, Decentralized Information-flow Control for Dynamic Environments*, NSF (CFF), \$1,057,427 (PSU award \$234,585), 8/1/05-7/31/08, Collaborators: PSU (McDaniel), UPenn (Zdancewic), Maryland (Hicks), GMU (Winsborough).

PI, *Extending Developer Tools for Security-typed Languages*, Software Engineering Research Center, Sponsor: Motorola, \$23,200, 7/1/05-6/30/06.

PI, *Student Travel Support for ACM SIGCOMM 2005 Conference*, NSF, \$19,620, 4/1/05-3/31/06.

Co-PI, *NSF CyberTrust: Collaborative Research: Testing and Benchmarking Methodologies for Future Network Security Mechanisms (EMIST)*, NSF/DHS, \$5,344,459 (PSU award \$2,533,447), 8/1/04-8/31/06, Collaborators: PSU (Kesidis, Miller, Liu), Purdue (Fahmy, Rosenberg, Spafford, Shroff, Brodley), UCDavis (Wu, Levitt, Bishop, Rowe), ICSI/Berkeley (Paxson, Floyd, Weaver).

PROFESSIONAL ACTIVITIES

Editorial Positions, Panels, and Boards

IEEE Technical Committee on Security and Privacy

- *Chair*–January 2014–January 2016
- *Vice Chair*–January 2012–December 2014

ACM Transactions on Internet Technology (TOIT)

- *Editor in Chief*–September 2007–December 2012
- *Associate Editor*–April 2004–August 2007

IEEE Security and Privacy Magazine

- *Area Editor, Secure Systems*–January 2009–2015

IEEE Transactions on Computers (TC)

- *Associate Editor*–August 2008–2014

ACM Transactions on Information and System Security (TISSEC)

- *Associate Editor*–May 2007–May 2012

IEEE Transactions on Software Engineering (TSE)

- *Associate Editor*–January 2007–April 2012
- *Guest Editor, Special Issue on Topics in Security*–Fall 2006–April 2012

IEEE Transactions on Parallel and Distributed Systems (TPDS)

- *Guest Editor, Special Issue on Trust, Security and Privacy in Parallel and Distributed Systems*–Fall 2012

Elsevier Journal of Computer Networks

- *Guest Editor, Special Issue on Web Security*–Fall 2003–Spring 2005

Encyclopedia of Cryptography and Security

- *Editorial Board Member*–Fall 2002–Spring 2005

Journal of Defense Modeling and Simulation

- *Guest Editor, Special Issue on Cyber Risk and Vulnerability Estimation*–Winter 2018–

Other Professional Activities

IEEE Workshop on the Internet of Safe Things (SafeThings)

- *Steering Committee*–2022–present

Helmholtz Center for Information Security (CISPA), Scientific Advisory Board

- *Member*–2019–present

Ohio University College of Engineering, Board of Vistors

- *Member*–2018–present

Penn State CISO Advisory Board

- *Member*–2016–2022

Member, Technical Guideline Development Committee, U.S. Election Assistance Commission

- *Member*–2010–2011

Natural Sciences and Engineering Research Council of Canada, Internetworked Systems Security Network

- *Scientific Advisory Board*–2008–2013

Technology for Cyber Physical System Security Forum, Cyber Security Research and Development, (Senators Joseph I. Lieberman and Susan Collins, Chairs)

- *Speaker and Participant*–September 2008

ACM Student Organization Advisor

- *Penn State Computer Science and Engineering Department*–2006–2012

The Technology Collaborative

- *Penn State Representative (Pennsylvania economic development consortium)*–2007–2008

President's National Security Telecommunications Advisory Panel

- *Member, Next Generation Networks Task Force*–2005–2006

Abusable Technologies Awareness Center (ATAC)

- *Panelist*–October 2003–2010

AT&T IP Services Security Council

- *Member*–June 2003–August 2004

AT&T Internet Intellectual Property Review Team

- *Member*–September 2001–May 2002

ACM SIGCOMM Student Travel Grant Committee

- *Member*–August 2005

National Science Foundation, Grant Review Panel

- *Member*–2003–2004, 2006–2007, 2009–2021

Department of Energy SciDAC Review Panel

- *Member*–2001

Conference and Workshop Participation

IEEE Symposium on Security and Privacy

- *Technical Program Co-Chair*–2007, 2008
- *Program Committee*–2011, 2012, 2013, 2022, 2023, 2024

USENIX Security Symposium

- *Program Chair*–2005
- *Invited Talks Chair*–2006, 2009
- *Program Committee*–2001, 2003, 2004, 2007, 2014, 2018, 2019, 2020, 2021, 2022, 2023, 2024

ACM Conference on Computer and Communications Security (CCS)

- *Program Committee*–2006, 2008, 2009, 2010, 2012, 2018, 2019, 2020, 2021, 2022, 2023
- *Industry and Government Track Chair*–2004, 2007
- *Program Committee-Industry and Government Track*–2003, 2005, 2006
- *Test of Time Committee*–2019, 2020

IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)

- *Founding Program Co-Chair*–2023

IEEE European Symposium on Security and Privacy

- *Steering Committee*–2015–present
- *Program Committee*–2016, 2017

International Conference on Privacy, Security and Trust (PST)

- *Steering Committee*–2019–

ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)

- *Program Committee*–2017

Network and Distributed System Security Symposium (NDSS)

- *Program Committee*–2009, 2012, 2013, 2017

Annual Computer Security Applications Conference (ACSAC)

- *Program Committee*–2004, 2005, 2006, 2007, 2010, 2011, 2019
- *Test of Time Committee*–2019

Financial Cryptography

- *General Chair*–2006
- *Program Committee*–2007, 2008, 2012

Computer Security Foundations Symposium (CSF)

- *Program Committee*–2011, 2021

European Symposium on Research in Computer Security (ESORICS)

-
- *Program Committee*–2004, 2005, 2021
- ACM Symposium of SDx Research 2021 (SOSR)**
- *Program Committee*–2021
- International Symposium on Engineering Secure Software and Systems (ICISSP)**
- *Program Committee*–2015
- IEEE Conference on Communications and Network Security (CNS)**
- *Program Committee*–2015, 2017
- ACM Annual International Conference on Mobile Computing and Networking (MobiCom)**
- *Program Committee*–2010, 2011, 2012
 - *Program Committee, Distinguished Member*–2021
- ACM Annual International Conference on Mobile Systems, Applications, and Services (MobiSys)**
- *Program Committee*–2012
- ACM Symposium on Access Control Models and Technologies (SACMAT)**
- *Program Committee*–2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2011
- ACM Conference on ASIA Computer and Communications Security (ASIA CCS)**
- *Program Committee*–2008
- ACM Conference on Electronic Commerce (ACM EC)**
- *Program Committee*–2005
- EAI International Conf. on Security and Privacy in Communication Networks (SecureComm)**
- *Program Committee*–2020
- International Conference on Applied Cryptography and Network Security (ACNS)**
- *Program Committee*–2006
- ACM Annual Digital Forensics Conference**
- *Program Committee*–2012
- IEEE Workshop on the Internet of Safe Things**
- *Program Committee*–2019, 2022
- ACM Workshop on Moving Target Defense (MTD)**
- *Program Committee*–2015, 2016
- IEEE ICNP Workshop on Secure Network Protocols (NPSec)**
- *Program Committee*–2005, 2006
- Conference on Decision and Game Theory for Security (GameSec)**
- *Program Committee*–2012, 2018
- ACM Symposium on Applied Computing (SAC)**
- *Program Committee, Information Security Research and Applications* –2010
- USENIX Annual Technical Conference**
- *Program Committee*–2002, 2003
- World Wide Web Conference (WWW)**
- *Security and Privacy Track Vice-Chair*–2005
 - *Security and Privacy Track Deputy Vice-Chair*–2004
 - *Program Committee*–2003, 2007, 2010, 2011
- Intl. Conference on Emerging Trends in Information and Communication Security (ETRICS)**
- *Program Committee*–2006
- International Conference On Distributed Computing Systems (ICDCS)**
- *Program Committee*–2011
- IEEE INFOCOM**
- *Program Committee*–2007
- IEEE GLOBECOM**
- *Program Committee*–2010
- Military Communications Conference (MILCOM)**

-
- *Program Committee*–2015, 2016, 2017, 2018, 2019, 2021, 2022
- The Five Nines Workshop on Designing and Managing High Availability Internet Services (INM)**
- *Program Committee*–2007
- International Conference on Information Systems Security (ICISS)**
- *Steering Committee*–2007
 - *Program Co-Chair*–2007
 - *Program Committee*–2005, 2006, 2009, 2011
- International Conference on Parallel Processing**
- *Program Committee-Network Security*–2003
- USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)**
- *Program Committee*–2010
- ACM Workshop on Networking, Systems, Applications on Mobile Handhelds (MobiHand)**
- *Program Committee*–2009
- ACM Workshop on Cloud Computing Security**
- *Program Committee*–2009, 2010
- ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)**
- *Program Committee*–2011, 2012, 2013
- International Workshop on Security in Software Engineering**
- *Founding General Co-Chair*–2007
- USENIX Workshop On Offensive Technology (WOOT)**
- *Program Committee*–2007
- ACM Storage Security and Survivability Workshop**
- *Program Committee*–2006
- ACM SIGCOMM Workshop on Internet Network Management**
- *Program Committee*–2006, 2007
- Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec)**
- *Program Committee*–2006, 2007, 2008
- Workshop on Workshop on Telecommunications Infrastructure Protection and Security (TIPS)**
- *General Chair*–2009
- USENIX Workshop on Hot Topics in Security (HotSec)**
- *Program Chair*–2011
 - *Program Committee*–2007, 2008, 2009, 2010, 2012
- ACM Workshop TPC on Security and Privacy in Smartphones and Mobile Devices**
- *Program Committee*–2011
- International Workshop on Security (IWSEC)**
- *Program Committee*–2006
- International Workshop on Systems and Network Security (SNS)**
- *Program Committee*–2005, 2006

COLLABORATORS (Last 48 Months)

Bolor-Erdene Zolbayar, Ahmed Abdou, Stefan Achleitner, Hidayet Aksu, Leonardo Babun, Paul Barford, Novella Bartolini, Yohan Beugin, Hoak, Blaine, Christopher Burchard, Quinn Burke, Z. Berkay Celik, Kamalika Chaudhuri, Adrien Cosson, Kyle Denney, Genannt Dohmann, Kyle Domico, Kyle D Domico, Matthew Durbin, Pauley, Eric, David Evans, Jean-Charles Noirot Ferrand, Felix Freiling, Anshul Gandhi, Rahul George, Kanad Ghose, Kartik Gopalan, Ryan Guide, Amy Hasan, Ting He, Blaine Hoak, Thorsten Holz, Syed Rafiul Hussain, Syed Rafiul Hussain, Alban Héon, Trent Jaeger, Somesh Jha, Rachel King, Engin Kirda, Farinaz Koushanfar, Srikanth V. Krishnamurthy, Daniel E. Krych, Domico, Kyle, Thomas La Porta, Dongyoon Lee, Kunyang Li, Azaree Lintereur, David Liu, David Yu Liu, Zhenhua Liu, Andrea Matwyshyn, Patrick McDaniel, Paul Barford Patrick McDaniel, Patrick Mcdaniel, Fidan Mehmeti, Shuai Mu, Namitha Nambiar, Michael Norris, Kyle Ostrowski, Nicolas Papernot, McDaniel, Patrick, Eric Pauley, Jonathan Petit, Jingyuan Qi, Burke, Quinn, Konrad Rieck,

Sheatsley, Ryan, Ahmad-Reza Sadeghi, Alejandro Andrade Salazar, Ryan Sheatsley, Tyler Shipp, Amit Kumar Sikder, Anand Sivasubramaniam, Wenjia Song, Indra Spiecker, Michael Swift, Gang Tan, Sanchal Thakkar, Selcuk Uluagac, Prasanna Venkatesh, Gunjan Verma, Bimal Viswanath, Michael J. Weisman, Ya Xiao, Tian Xie, Danfeng Yao, Beugin, Yohan, Mingi Yu, Mingli Yu, Erez Zadok, Danfeng Zhang, Shulin Zhao, Sencun Zhu, Shitong Zhu, Bolor-Erdene Zolbayarn

CASES (Expert Witness)

DivX, LLC v. Hulu, LLC and Netflix, Inc., Expert for Expert for the Defence, Central District of California, Case no. Case No. 2:19-cv-01602.

Inter Partes Review, Expert for Expert for Apple Inc., United States Patent and Trademark Office, Case no. Patent Nos. 9,947,000, 9,928,495 and 10,163,103.

Trusted Knight Corporation v. International Business Machines Corporation, Expert for Expert for IBM Corporation, Northern District of California, Case no. Case No. 3:19-cv-01206-EMC.

Inter Partes Review, Expert for Expert for IBM Corporation, United States Patent and Trademark Office, Case no. Patent No. 9,503,473.

Finjan Inc., vs. Rapid7 Inc and Rapid7 LLC, Expert for Expert for Rapid7, District of Delaware, Case no. C.A. No. 1:18-CV-01519-MN.

Finjan Inc., vs. Cisco Systems, Inc., Expert for Expert for CISCO, Northern District of California, San Jose Division, Case no. Case No. 5:17-cv-00072-BLF-SVK.

Inter Partes Review, Expert for Expert for BlackBerry Limited, United States Patent and Trademark Office, Case no. Patent Nos. 8,825,084 and 8,326,327.

BlackBerry Limited v. Snap. Inc., Expert for Expert for BlackBerry Limited, Central District of California, Case no. Case No. 2: 18-cv-02693.

Rimini Street, Inc. v. Oracle International Corporation, Expert for Expert for Oracle, United States District Court, District of Nevada, Case no. Case No. 2:14-cv-01699.

Inter Partes Review, Expert for Expert for Google Inc., United States Patent and Trademark Office, Case no. Patent No. 9,444,812.

Good Technology Corporation et al., v. AirWatch, LLC, Expert for Expert for Airwatch LLC, United States District Court for the Northern District of California, Case no. 5-12-cv-05827.

Inter Partes Review, Expert for Duo Security Inc., United States Patent and Trademark Office, Case no. IPR2017-01041.

Inter Partes Review, Expert for Duo Security Inc., United States Patent and Trademark Office, Case no. IPR2017-01064.

Frederick Whalen, et al., v. SEI/AARON'S, INC., Expert for defense, United States District Court for the Northern District of Georgia, Case no. 1:2014-cv-01209.

Certain Portable Electronic Communications Devices, Including Mobile Phones and Components Thereof, Expert for plaintiff, International Trade Commission.

Secure Access, LLC v. Bank of America Corp., et al., Expert for defense, United States District Court for the Eastern District of Texas, Tyler Division, Case no. 6-10-cv-00670.

Intellectual Ventures I LLC, v. Check Point et al., Expert for plaintiff, United States District Court for the District of Delaware, Case no. 1-10-cv-01067.

NetMonitor LLC, v. Compuware et al., Expert for plaintiff, United States District Court for the District of Delaware, Case no. 1-10-cv-01061.

Amdocs Ltd. v. Openet Telecom Ltd., Expert for defense, United States District Court for the Eastern District of Virginia, Alexandria Division, Case no. 1-10-cv-00910.

PSI Systems Inc. v. Stamps.com, Expert for defense, United States District Court for the Central District of California, Case no. 2-08-cv-05233.

Stamps.com v. Endicia, Expert for plaintiff, United States District Court for the Central District of California, Case no. 2-06-cv-07499.

Kara Technologies v. Stamps.com, Expert for defense, United States District Court for the Central District of California, Case no. 2-05-cv-01890.

Coinstar Inc. v. Coinxchange, Expert for defense, United States District Court for the Eastern District of Virginia, Richmond Division, Case no. 3-06-cv-00299.

VCode Holdings Inc. v. Stamps.com, Expert for defense, United States District Court for the Central District of California.

Inter Partes Review, Expert for Google Inc., United States Patent and Trademark Office, Case no. (Patent No. 8,489,868).

Inter Partes Review, Expert for Cisco Systems, Inc., , Case no. (Patent No. 7,536,598).

Vir2us v. Cisco Systems, INC and Sourcefire, LLC, Expert for defense, United States District Court for the Eastern District of Virginia, Case no. 51:16cv1095.

Zito Vault, LLC V. International Business Machines Corporation, and Softlayer Technologies, Inc., Expert for defense, , Case no. 3:16-CV-962-M.

INDUSTRIAL EXPERIENCE

Software Developer	1994-1995
Applied Innovation, Inc., Columbus, OH	
Project Manager	1993-1994
Primary Access Corporation, San Diego, CA	
Software Developer	1991-1993
Primary Access Corporation, San Diego, CA	
Software Developer	1989
Integrated Technologies, Inc., Muncie, IN	

PUBLICATIONS

Books and Book Chapters

Patrick Traynor and Patrick McDaniel and Thomas La Porta, *Security for Telecommunications Networks*, Springer, Advances in Information Security, July, 2008, ISBN: 978-0-387-72441-6.

Bolor-Erdene Zolbayar and Ryan Sheatsley and Patrick McDaniel, *Evading Machine Learning based Network Intrusion Detection Systems with GANs*, Game Theory and Machine Learning for Cyber Security, John Wiley & Sons, 2021. Eds. Charles A Kamhoua and Christopher D. Kiekintveld and Fei Fang and Quanyan Zhu. Hoboken, New Jersey.

Kevin Butler and William Enck and Patrick Traynor and Jennifer Plasterr and Patrick McDaniel, *Privacy Preserving Web-Based Email*, Algorithms, Architectures and Information Systems Security, Statistical Science and Interdisciplinary Research, World Scientific Computing, 349-371, November, 2008. Eds. Bhargab Bhattacharya, Susmita Sur-Kolay, Subhas Nandy and Aditya Bagchi.

Patrick McDaniel, *Authentication*, Handbook of Computer Networks, Volume II, Chapter 171, John Wiley and Sons, May, 2007. Eds. Hossein Bidgoli.

Patrick McDaniel, *Computer and Network Authentication*, Handbook of Information Security, John Wiley and Sons, September, 2004. Eds. Hossein Bidgoli.

Patrick McDaniel, *IPsec*, Encyclopedia of Information Security, Kluwer, 2003. Eds. Hossein Bidgoli.

Patrick McDaniel, *Policy*, Encyclopedia of Information Security, Kluwer, 2003. Eds. Hossein Bidgoli.

Patrick McDaniel, *Authentication*, The Internet Encyclopedia, John Wiley and Sons, 2002.

Journal Articles

Mingi Yu and Quinn Burke and Thomas La Porta and Patrick McDaniel, *Stealthy Misreporting Attacks Against Load Balancing*, IEEE/ACM Transactions on Networking (TON), 2024.

Anshul Gandhi and Dongyoon Lee and Zhenhua Liu and Shuai Mu and Erez Zadok and Kanad Ghose and Kartik Gopalan and David Yu Liu and Syed Rafiul Hussain and Patrick McDaniel, *Metrics for Sustainability in Data Centers*, SIGENERGY Energy Inform. Rev., New York, NY, USA, ACM, 3, 3, 40–46, October, 2023.

Quinn Burke and Patrick McDaniel and Thomas La Porta and Mingli Yu and Ting He, *Misreporting Attacks Against Load Balancers in Software-Defined Networking*, Mobile Networks and Applications, Springer, 2023.

Tian Xie and Sanchal Thakkar and Ting He and Patrick McDaniel and Quinn Burke, *Joint Caching and Routing in Cache Networks with Arbitrary Topology*, IEEE Transactions on Parallel and Distributed Systems, May, 2023.

Ya Xiao and Wenjia Song and Jingyuan Qi and Bimal Viswanath and Patrick McDaniel and Danfeng Yao, *Specializing Neural Networks for Cryptographic Code Completion Applications*, IEEE Transactions on Software Engineering, IEEE, 2023.

Matthew Durbin and Ryan Sheatsley and Patrick McDaniel and Azaree Lintereur, *Experimental tests of Gamma-ray Localization Aided with Machine-learning (GLAM) capabilities*, Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment, 1038, 2022.

Amit Kumar Sikder and Leonardo Babun and Z. Berkay Celik and Hidayet Aksu and Patrick McDaniel and Engin Kirda and Selcuk Uluagac, *Who's Controlling My Device? Multi-User Multi-Device-Aware Access Control System for Shared Smart Home Environment*, ACM Transactions on Internet of Things, Association for Comput-

ing Machinery, May, 2022.

Michael Norris and Z. Berkay Celik and Prasanna Venkatesh and Shulin Zhao and Patrick McDaniel and Anand Sivasubramaniam and Gang Tan, *IoTRepair: Flexible Fault Handling in Diverse IoT Deployments*, ACM Transactions on Internet of Things, ACM, 2022.

Tian Xie and Namitha Nambiar and Ting He and Patrick McDaniel, *Attack Resilience of Cache Replacement Policies: A Study Based on TTL Approximation*, IEEE/ACM Transactions on Networking, 2022.

Quinn Burke and Fidan Mehmeti and Rahul George and Kyle Ostrowski and Trent Jaeger and Thomas La Porta and Patrick Mcdaniel, *Enforcing Multilevel Security Policies in Unstable Networks*, IEEE Transactions on Network and Service Management, IEEE, June, 2022.

Ryan Sheatsley and Nicolas Papernot and Michael J. Weisman and Gunjan Verma and Patrick McDaniel, *Adversarial Examples for Network Intrusion Detection Systems*, Journal of Computer Security (JCS), IOS Press, January, 2022.

Quinn Burke and Patrick McDaniel and Thomas La Porta and Mingli Yu and Ting He, *Misreporting Attacks Against Load Balancers in Software-Defined Networking*, Mobile Networks and Applications, Springer, 2021.

Daniel E. Krych and Patrick McDaniel, *Exposing Android Social Applications: Linking Data Leakage to Privacy Policies*, Journal of Cyber Security Technology, Taylor & Francis, 5, 3-4, 2021.

Alejandro Andrade Salazar and Ryan Sheatsley and Jonathan Petit and Patrick McDaniel, *Physics-based Misbehavior Detection System for V2X Communications*, SAE International Journal of Connected and Automated Vehicles, SAE International, June, 2021.

Mingli Yu and Tian Xie and Ting He and Patrick McDaniel and Quinn Burke, *Flow Table Security in SDN: Adversarial Reconnaissance and Intelligent Attacks*, IEEE/ACM Transactions on Networking, 29, 6, 1063-6692, December, 2021.

Leonardo Babun and Kyle Denney and Z. Berkay Celik and Patrick McDaniel and Selcuk Uluagac, *A Survey on IoT Platforms: Communication, Security, and Privacy Perspectives*, Computer Networks, 192, 19, June, 2021.

Ryan Sheatsley and Matthew Durbin and Azaree Lintereur and Patrick McDaniel, *Improving Radioactive Material Localization by Leveraging Cyber-Security Model Optimizations*, IEEE Sensors, 21, 8, April, 2021.

Stefan Achleitner and Quinn Burke and Patrick McDaniel and Trent Jaeger and Thomas La Porta and Srikanth V. Krishnamurthy, *MLSNet: A Policy Complying Multilevel Security Framework for Software Defined Networking*, IEEE Transactions on Network and Service Management, 18, 1, March, 2021.

Dan Boneh and Andrew J. Grotto and Patrick McDaniel and Nicolas Papernot, *Preparing for the Age of Deepfakes and Disinformation*, Stanford HAI Policy Brief, 2020.

Dan Boneh and Andrew J. Grotto and Patrick McDaniel and Nicolas Papernot, *How Relevant Is the Turing Test in the Age of Sophisbots?*, IEEE Security & Privacy Magazine, 17, 64-71, Nov/Dec, 2019.

Z. Berkay Celik and Patrick McDaniel and Thomas Bowen, *Malware Modeling and Experimentation through Parameterized Behavior*, Journal of Defense Modeling and Simulation (JDMS), 15, 1, 31-48, 2017.

Z. Berkay Celik and Earlence Fernandes and Eric Pauley and Gang Tan and Patrick McDaniel, *Program Analysis of Commodity IoT Applications for Security and Privacy: Opportunities and Challenges*, ACM Computing Surveys (CSUR), ACM, 42, 4, 2019.

Z. Berkay Celik and Patrick McDaniel and Gang Tan and Leonardo Babun and Selcuk Uluagac, *Verifying IoT Safety and Security in Physical Spaces*, IEEE Security & Privacy Magazine, IEEE, 17, 5, 30-37, 2019.

Ahmed Atya and Zhiyun Qian and Srikanth V. Krishnamurthy and Thomas La Porta and Patrick McDaniel and Lisa Marvel, *Catch Me if You Can: Malicious Co-Residency on the Cloud*, IEEE/ACM Transactions on Networking, 27, 2, April, 2019.

Ian Goodfellow and Patrick McDaniel and Nicolas Papernot, *Making machine learning robust against adversarial inputs*, Communications of the ACM, ACM, 61, 7, 56-6, June/July, 2018.

Dave Tian and Kevin Butler and Joseph Choi and Patrick McDaniel and Padma Krishnaswamy, *Securing ARP/NDP From the Ground Up*, IEEE Transactions on Information Forensics and Security, 12, 9, 2131-2143, April, 2017.

Stefan Achleitner and Thomas La Porta and Patrick McDaniel and Shridatt Sugrim and Srikanth V. Krishnamurthy and Ritu Chada, *Deceiving Network Reconnaissance Using SDN-based Virtual Topologies*, IEEE Transactions on Network and Service Management, Special Issue on Advances in Management of Softwarized Networks, 14, 4, July, 2017.

Chaz Lever and Robert Walls and Yacin Nadjji and David Dagon and Patrick McDaniel and Manos Antonakakis, *Dawn of the Dead Domain: Measuring the Exploitation of Residual Trust in Domains*, IEEE Security & Privacy Magazine (Secure Systems issue column), April, 2017.

Patrick McDaniel and Nicolas Papernot and Z. Berkay Celik, *Machine Learning in Adversarial Settings*, IEEE Security & Privacy Magazine, 14, 3, May/June, 2016.

Patrick McDaniel and Ananthram Swami, *The Cyber Security Collaborative Research Alliance: Unifying Detection, Agility, and Risk in Mission-Oriented Cyber Decision Making*, CSIAC Journal, Army Research Laboratory (ARL) Cyber Science and Technology, 5, 1, January, 2017.

Damien Ocateau and Daniel Luchaup and Somesh Jha and Patrick McDaniel, *Composite Constant Propagation and its Application to Android Program Analysis*, IEEE Transactions on Software Engineering, 42, 11, 999-1014, 2016.

Alexander Kott and Ananthram Swami and Patrick McDaniel, *Security Outlook: Six Cyber Game Changers for the Next 15 Years*, IEEE Computer, 47, 12, 104-106, 2014.

Zhenfu Cao and Keqiu Li and Xu Li and Patrick McDaniel and Radha Poovendran and Guojun Wang and Yang Xiang, *Guest Editors' Introduction: Special Issue on Trust, Security, and Privacy in Parallel and Distributed Systems*, IEEE Transactions on Parallel and Distributed Systems, 25, 2, 279-28, 2014.

Patrick McDaniel and Brian Rivera and Ananthram Swami, *Toward a Science of Secure Environments*, IEEE Security & Privacy Magazine, 12, 4, July/August, 2014.

William Enck and Peter Gilbert and Seungyeop Han and Vasant Tendulkar and Byung-Gon Chun and Landon Cox and Jaeyeon Jung and Patrick McDaniel and Anmol Sheth, *TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*, ACM Transactions on Computer Systems (TOCS), 32, 2, June, 2014.

William Enck and Peter Gilbert and Byung-Gon Chun and Landon Cox and Jaeyeon Jung and Patrick McDaniel and Anmol Sheth, *TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*, Communications of the ACM, 57, 3, March, 2014.

Machigar Ongtang and Stephen McLaughlin and William Enck and Patrick McDaniel, *Semantically Rich Application-Centric Security in Android*, Security and Communication Networks, 5, 6, 658-673, 2012.

Patrick McDaniel, *Bloatware Comes to the Smartphone*, IEEE Security & Privacy Magazine, 10, 4, July/August, 2011.

Thomas Moyer and Kevin Butler and Joshua Schiffman and Patrick McDaniel and Trent Jaeger, *Scalable Web Content Attestation*, IEEE Transactions on Computers, 61, 5, 686–699, April, 2011.

Patrick McDaniel, *Data Provenance and Security*, IEEE Security & Privacy Magazine, 9, 3, March/April, 2011.

Joshua Schiffman and Thomas Moyer and Trent Jaeger and Patrick McDaniel, *Network-based Root of Trust for Installation*, IEEE Security & Privacy Magazine, 40-48, Jan/Feb, 2011.

Kevin Butler and Stephen McLaughlin and Thomas Moyer and Patrick McDaniel, *New Security Architectures Based on Emerging Disk Functionality*, IEEE Security and Privacy Magazine, 8, 5, October, 2010.

Patrick McDaniel and William Enck, *Not So Great Expectations: Why Application Markets Haven't Failed Security*, IEEE Security & Privacy Magazine, 8, 5, 76–78, September/October, 2010.

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

Patrick Traynor and Kevin Butler and William Enck and 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, March, 2010.

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

Boniface Hicks and Sandra Rueda and Luke St. Clair and Trent Jaeger and Patrick McDaniel, *A Logical Specification and Analysis for SELinux MLS Policy*, ACM Transactions on Information and System Security (TISSEC), 13, 26, 2010.

Kevin Butler and Toni Farley and Patrick McDaniel and J. Rexford, *A Survey of BGP Security Issues and Solutions*, Proceedings of the IEEE, 2010, 1, 100-122, January, 2010.

Kevin Butler and Sunam Ryu and 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, December, 2009.

Patrick McDaniel and Stephen McLaughlin, *Security and Privacy Challenges in the Smart Grid*, IEEE Security & Privacy Magazine (Secure Systems issue column), 7, 3, 75-77, May/June, 2009.

Patrick Traynor and William Enck and Patrick McDaniel and Thomas La Porta, *Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks*, IEEE/ACM Transactions on Networking (TON), 17, 1, 40-53, February, 2009.

William Enck and Machigar Ongtang and Patrick McDaniel, *Understanding Android Security*, IEEE Security & Privacy Magazine, 7, 1, 50–57, January/February, 2009.

William Enck and Thomas Moyer and Patrick McDaniel and Shubho Sen and Panagiotis Sebos and Sylke Sporel and Albert Greenberg and Yu-Wei Sung and Sanjay Rao and William Aiello, *Configuration Management at Massive Scale: System Design and Experience*, IEEE Journal on Selected Areas in Communications (JSAC), 27, 3, 323-335, 2009.

Heesook Choi and William Enck and Jaesheung Shin and Patrick McDaniel and Thomas La Porta, *ASR: Anonymous and Secure Reporting of Traffic Forwarding Activity in Mobile Ad Hoc Networks*, Wireless Networks (WINET), ACM/Kluwer, 15, 4, 525-539, May, 2009.

Patrick Traynor and William Enck and Patrick McDaniel and Thomas La Porta, *Exploiting Open Functionality in SMS-Capable Cellular Networks*, Journal of Computer Security, 16, 6, 713-742, Febraury, 2009.

Patrick Traynor and Michael Chien and Scott Weaver and Boniface Hicks and Patrick McDaniel, *Non-Invasive Methods for Host Certification*, ACM Transactions on Information and System Security (TISSEC), 11, 3, 2008.

Patrick McDaniel and Bashar Nuseibeh, *Guest Editorial: Special Issue on Software Engineering for Secure Systems*, IEEE Transactions on Software Engineering, 34, 1, 3-4, 2008.

Wesam Lootah and William Enck and Patrick McDaniel, *TARP: Ticket-based Address Resolution Protocol*, Computer Networks, Elsevier, 51, 15, 4322-4337, October, 2007.

Patrick McDaniel and Avi Rubin, *Guest Editorial: Special Issue on Web Security*, Computer Networks, Elsevier, 22, 2, 2005.

Patrick McDaniel and Atul Prakash, *Enforcing Provisioning and Authorization Policy in the Antigone System*, Journal of Computer Security, 14, 6, 483-511, November, 2006.

Patrick McDaniel and Atul Prakash, *Methods and Limitations of Security Policy Reconciliation*, ACM Transactions on Information and System Security (TISSEC), Association for Computing Machinery, 9, 3, 259-291, August, 2006.

Patrick McDaniel and William Aiello and Kevin Butler and JohnIoannidis, *Origin Authentication in Interdomain Routing*, Journal of Communication Networks, Elsevier, 50, 16, 2953-2980, November, 2006.

Matthew Pirretti and Sencun Zhu and VijaykrishnanNarayanan and Patrick McDaniel and Mahmut Kandemir and Richard Brooks, *The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense*, International Journal of Distributed Sensor Networks, 2, 3, 267-287, June, 2005.

Simon Byers and Lorrie Cranor and Eric Cronin and DaveKormann and Patrick McDaniel, *Analysis of Security Vulnerabilities in the Movie Production and Distribution Process*, Telecommunications Policy, 28, 8, 619-644, August, 2004.

Conference Publications

Yohan Beugin and Patrick McDaniel, *Interest-disclosing Mechanisms for Advertising are Privacy-Exposing (not Preserving)*, Proceedings on Privacy Enhancing Technologies (PETS), July, 2024.

Blaine Hoak and Patrick McDaniel, *Explorations in Texture Learning*, 12th International Conference on Learning Representations, Tiny Papers Track (ICLR), May, 2024.

Tian Xie and Sanchal Thakkar and Ting He and Novella Bartolini and Patrick McDaniel, *Host-based Flow Table Size Inference in Multi-hop SDN*, Proceedings of the IEEE GLOBECOM, IEEE, December, 2023. Kuala Lumpur, Malaysia.

Eric Pauley and Paul Barford and Patrick McDaniel, *The CVE Wayback Machine: Measuring Coordinated Disclosure from Exploits Against Two Years of Zero-Days*, Proceedings of the ACM 2023 Internet Measurement Conference (IMC), October, 2023. Montreal, Canada. (**runner up-best paper award**)

Mingli Yu and Quinn Burke and Thomas La Porta and Patrick McDaniel, *mMLSnet: Multilevel Security Network With Mobility*, Proceedings of the Military Communications Conference (MILCOM), IEEE, October, 2023. Boston, MA.

Ryan Guide and Eric Pauley and Yohan Beugin and Ryan Sheatsley and Patrick McDaniel, *Characterizing the Modification Space of Signature IDS Rules*, MILCOM 2023 - 2023 IEEE Military Communications Conference

(MILCOM), IEEE, October, 2023. Boston, MA.

Eric Pauley and Paul Barford Patrick McDaniel, *DScope: A Cloud-Native Internet Telescope*, 32nd USENIX Security Symposium (USENIX Security 23), USENIX Association, August, 2023. Anaheim, CA.

Ryan Sheatsley and Blaine Hoak and Eric Pauley and Patrick McDaniel, *The Space of Adversarial Strategies*, 32nd USENIX Security Symposium (USENIX Security 23), USENIX Association, August, 2023.

Eric Pauley and Gang Tan and Danfeng Zhang and Patrick McDaniel, *Performant Binary Fuzzing without Source Code using Static Instrumentation*, Conference on Communications and Network Security (CNS), IEEE, October, 2022.

Patrick McDaniel, *Keynote Address: Sustainability is a Security Problem (extended abstract)*, Proceedings of the ACM Conference on Computer and Communications Security (CCS), ACM, November, 2022.

Kyle Domico and Ryan Sheatsley and Yohan Beugin and Quinn Burke and Patrick McDaniel, *A Machine Learning and Computer Vision Approach to Geomagnetic Storm Forecasting*, Machine Learning in Heliophysics (ML-Helio), AGU, November, 2022.

Tian Xie and Sanchal Thakkar and Ting He and Patrick McDaniel and Quinn Burke, *Joint Caching and Routing in Cache Networks with Arbitrary Topology*, Proceedings of the International Conference on Distributed Computing Systems (ICDCS), July, 2022.

Yohan Beugin and Quinn Burke and Blaine Hoak and Ryan Sheatsley and Eric Pauley and Gang Tan and Syed Rafiul Hussain and Patrick McDaniel, *Building a Privacy-Preserving Smart Camera System*, Proceedings on Privacy Enhancing Technologies (PETS), July, 2022.

Eric Pauley and Ryan Sheatsley and Blaine Hoak and Quinn Burke and Yohan Beugin and Patrick McDaniel, *Measuring and Mitigating the Risk of IP Reuse on Public Clouds*, 2022 IEEE Symposium on Security and Privacy (IEEE S&P), IEEE, May, 2022. San Francisco, CA.

Ahmed Abdou and Ryan Sheatsley and Yohan Beugin and Tyler Shipp and Patrick McDaniel, *HoneyModels: Machine Learning Honey Pots*, Proceedings of the Military Communications Conference (MILCOM), IEEE, November, 2021.

Ryan Sheatsley and Blaine Hoak and Eric Pauley and Yohan Beugin and Michael J. Weisman and Patrick McDaniel, *On the Robustness of Domain Constraints*, Proceedings of the ACM Conference on Computer and Communications Security (CCS), ACM, November, 2021.

Tian Xie and Ting He and Patrick McDaniel and Namitha Nambiar, *Attack Resilience of Cache Replacement Policies*, IEEE International Conference on Computer Communications (INFOCOM), IEEE, May, 2021.

Adrien Cosson and Amit Kumar Sikder and Leonardo Babun and Z. Berkay Celik and Patrick McDaniel and Selcuk Uluagac, *Sentinel: A Robust Intrusion Detection System for IoT Networks Using Kernel-Level System Information*, In 6th ACM/IEEE Conference on Internet of Things Design and Implementation (IoTDI), April, 2021.

Matthew Durbin and Ryan Sheatsley and Patrick McDaniel and Azaree Lintereur, *A Multi-Step Machine Learning Approach to Directional Gamma Ray Detection*, 2020 IEEE Nuclear Science Symposium and Medical Imaging Conference (NSS/MIC), October, 2020.

Sayed M. Saghaian and Thomas La Porta and Simone Silvestri and Patrick McDaniel, *Improving Robustness of a Popular Probabilistic Clustering Algorithm Against Insider Attacks*, International Conference on Security and Privacy in Communication Networks (SecureComm 2020), EAI, October, 2020.

Quinn Burke and Patrick McDaniel and Thomas La Porta and Mingli Yu and Ting He, *Misreporting Attacks in Software-Defined Networking*, International Conference on Security and Privacy in Communication Networks

(SecureComm 2020), EAI, October, 2020.

Amit Kumar Sikder and Leonardo Babun and Z. Berkay Celik and Abbas Acar and Hidayet Aksu and Patrick McDaniel and Engin Kirda and Selcuk Uluagac, *KRATOS: Multi-User Multi-Device-Aware Access Control System for the Smart Home*, 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '20), ACM, July, 2020.

Mingli Yu and Ting He and Patrick McDaniel and Quinn Burke, *Flow Table Security in SDN: Adversarial Reconnaissance and Intelligent Attacks*, IEEE INFOCOM, IEEE Conference on Computer Communications, June, 2020. Beijing, China.

Michael Norris and Z. Berkay Celik and Prasanna Venkatesh and Shulin Zhao and Patrick McDaniel and Anand Sivasubramaniam and Gang Tan, *IoTRepair: Systematically addressing device faults in commodity IoT*, In 5th ACM/IEEE Conference on Internet of Things Design and Implementation (IoTDI), April, 2020.

Raquel Alvarez and Jake Levenson and Ryan Sheatsley and Patrick McDaniel, *Application Transiency: Towards a Fair Trade of Personal Information for Application Services*, Proceedings of the EAI Conference on Security and Privacy in Communication Networks (SecureComm), October, 2019. Orlando, FL.

Giuseppe Petracca and Yuqiong Sun and Ahmad-Atamli Reineh and Jens Grossklags and Patrick McDaniel and Trent Jaeger, *EnTrust: Regulating Sensor Access by Cooperating Programs via Delegation Graphs*, Proceedings of the 28th USENIX Security Symposium, August, 2019. Santa Clara, CA.

Matthew Durbin and Ryan Sheatsley and Christopher Balbier and Tristan Grieve and Patrick McDaniel and Azaree Lintereur, *Development of Machine Learning Algorithms for Directional Gamma Ray Detection*, Proceedings of the Institute of Nuclear Materials Management Annual Meeting (INMM), July, 2019. Palm Desert, CA. (**J. D. Williams student paper award, Nuclear Security and Physical Protection division**)

Z. Berkay Celik and Abbas Acar and Hidayet Aksu and Abbas Acar and Ryan Sheatsley and Selcuk Uluagac and Patrick McDaniel, *Curie: Policy-based Secure Data Exchange*, ACM Conference on Data and Applications Security (CODASPY), March, 2019. Dallas, TX.

Z. Berkay Celik and Gang Tan and Patrick McDaniel, *IoTGuard: Dynamic Enforcement of Security and Safety Policy in Commodity IoT*, Network and Distributed System Security Symposium (NDSS), February, 2019. San Diego, CA.

Dang Tu Nguyen and Chengyu Song and Zhiyun Qian and Srikanth V. Krishnamurthy and Edward J. M. Colbert and Patrick McDaniel, *IoTSan: Fortifying the Safety of IoT Systems*, Proceedings of the 14th International Conference on emerging Networking EXperiments and Technologies (CoNEXT '18), December, 2018.

Z. Berkay Celik and Leonardo Babun and Amit Kumar Sikder and Hidayet Aksu and Gang Tan and Patrick McDaniel and Selcuk Uluagac, *Sensitive Information Tracking in Commodity IoT*, Proceedings of the 27th USENIX Security Symposium, August, 2018. Baltimore, MD.

Rauf Izmailov and Shridatt Sugrim and Ritu Chadha and Patrick McDaniel and Ananthram Swami, *Enablers Of Adversarial Attacks in Machine Learning*, Proceedings of the Military Communications Conference (MILCOM), IEEE, October, 2018.

Sayed M. Saghaian and Thomas La Porta and Trent Jaeger and Z. Berkay Celik and Patrick McDaniel, *Mission-oriented Security Model, Incorporating Security Risk, Cost and Payout*, Proceedings of EAI SECURECOMM 2018, August, 2018. (**best paper award**)

Z. Berkay Celik and Patrick McDaniel and Gang Tan, *Soteria: Automated IoT Safety and Security Analysis*, USENIX Annual Technical Conference (USENIX ATC), July, 2018. Boston, MA.

Z. Berkay Celik and Patrick McDaniel and Rauf Izmailov and Nicolas Papernot and Ryan Sheatsley and Raquel Alvarez and Ananthram Swami, *Detection under Privileged Information*, ACM Asia Conference on Computer and Communications Security (ASIACCS), June, 2018.

Florian Tramer and Alexey Kurakin and Nicolas Papernot and Ian Goodfellow and Dan Boneh and Patrick McDaniel, *Ensemble Adversarial Training: Attacks and Defenses*, International Conference on Learning Representations (ICLR), 2018. Vancouver, Canada.

Nicolas Papernot and Patrick McDaniel and Arunesh Sinha and Michael Wellman, *SoK: Security and Privacy in Machine Learning*, Security and Privacy (EuroS&P), 2018 IEEE European Symposium on on Security and Privacy (EuroS&P), IEEE, April, 2018. London, UK.

Chun-Ming Lai and Xiaoyun Wang and Yunfeng Hong and Yu-Cheng Lin and Felix Wu and Patrick McDaniel and Hasan Cam, *Attacking Strategies and Temporal Analysis Involving Facebook Discussion Groups*, 13th IEEE International Conference on Network and Service Management, November, 2017. Tokyo, Japan.

Kathrin Grosse and Nicolas Papernot and Praveen Manoharan and Michael Backes and Patrick McDaniel, *Adversarial Examples for Malware Detection*, 22nd European Symposium on Research in Computer Security (ESORICS '17), September, 2017. Oslo, Norway.

Z. Berkay Celik and David Lopez-Paz and Patrick McDaniel, *Patient-Driven Privacy Control through Generalized Distillation*, Proceedings of the Privacy-Aware Computing (PAC), IEEE, 2017.

Abbas Acar and Z. Berkay Celik and Hidayet Aksu and Selcuk Uluagac and Patrick McDaniel, *Achieving Secure and Differentially Private Computations in Multiparty Settings*, Proceedings of the Privacy-Aware Computing (PAC), IEEE, 2017.

Vaibhav Rastogi and Drew Davidson and Lorenzo De Carli and Somesh Jha and Patrick McDaniel, *Cimplifier: Automatically Debloating Containers*, 11Th Joint Meeting of the European Software Engineering Conference and the Acm Sigsoft Symposium on the Foundations of Software Engineering, September, 2017. Paderborn, Germany.

Yunfeng Hong and Yongjian Hu and Chun-Ming Lai and Felix Wu and Iulian Neamtii and Yu Paul and Patrick McDaniel and Hasan Cam and Gail-Joon Ahn, *Defining and Detecting Environment Discrimination in Android Apps*, The 13th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 17), October, 2017.

Nicolas Papernot and Patrick McDaniel and Ian Goodfellow and Somesh Jha and Z. Berkay Celik and Ananthram Swami, *Practical Black-Box Attacks against Machine Learning*, ACM Asia Conference on Computer and Communications Security (ASIACCS) 2017, April, 2017.

Stefan Achleitner and Thomas La Porta and Trent Jaeger and Patrick McDaniel, *Adversarial Network Forensics in Software Defined Networking*, ACM Symposium on SDN Research (SOSR), ACM, April, 2017. (**best student paper award**)

Stefan Achleitner and Thomas La Porta and Patrick McDaniel and Srikanth V. Krishnamurthy and Alexander Poylisher and Constantin Serban, *Stealth Migration: Hiding Virtual Machines on the Network*, IEEE International Conference on Computer Communications (INFOCOM), IEEE, 2017.

Ahmed Atya and Zhiyun Qian and Srikanth V. Krishnamurthy and Thomas La Porta and Patrick McDaniel and Lisa Marvel, *Malicious Co-Residency on the Cloud: Attacks and Defense*, IEEE International Conference on Computer Communications (INFOCOM), IEEE, 2017.

Nathaniel Lageman and Eric Kilmer and Robert Walls and Patrick McDaniel, *BinDNN: Resilient Function Matching Using Deep Learning*, 2016 International Conference on Security and Privacy in Communication Networks (SECURECOMM), October, 2016.

Z. Berkay Celik and Nan Hu and Yun Li and Nicolas Papernot and Patrick McDaniel and Jeff Rowe and Robert Walls and Karl Levitt and Novella Bartolini and Thomas La Porta and Ritu Chadha, *Mapping Sample Scenarios to Operational Models*, Proceedings of the Military Communications Conference (MILCOM), IEEE, 2016.

Nicolas Papernot and Patrick McDaniel and Ananthram Swami and Richard Harang, *Crafting Adversarial Input Sequences for Recurrent Neural Networks*, Proceedings of the Military Communications Conference (MILCOM), IEEE, 2016.

Michael Backes and Sven Bugiel and Erik Derr and Patrick McDaniel and Damien Ocateau and Sebastian Weisgerber, *On Demystifying the Android Application Framework: Re-Visiting Android Permission Specification Analysis*, Proceedings of the 25th USENIX Security Symposium, August, 2016.

Devin Pohly and Patrick McDaniel, *Modeling Privacy and Tradeoffs in Multichannel Secret Sharing Protocols*, 46th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), June, 2016.

Chaz Lever and Robert Walls and Yacin Nadji and David Dagon and Patrick McDaniel and Manos Antonakakis, *Domain-Z: 28 Registrations Later*, Proceedings of the 37th IEEE Symposium on Security and Privacy, May, 2016. San Francisco, CA.

Yasemin Acar and Michael Backes and Sven Bugiel and Sascha Fahl and Patrick McDaniel and Matthew Smith, *SoK: Lessons Learned From Android Security Research For Appified Software Platforms*, Proceedings of the 37th IEEE Symposium on Security and Privacy, May, 2016. San Francisco, CA.

Nicolas Papernot and Patrick McDaniel and Xi Wu and Somesh Jha and Ananthram Swami, *Distillation as a Defense to Adversarial Perturbations Against Deep Neural Networks*, Proceedings of the 37th IEEE Symposium on Security and Privacy, May, 2016. San Francisco, CA.

Charles Huber and Scott Brown and Patrick McDaniel and Lisa Marvel, *Cyber Fighter Associate: A Decision Support System for Cyber Agility*, Proceedings of the 50th Annual Conference on Information Sciences and Systems (CISS), March, 2016. Princeton, NJ.

Nicolas Papernot and Patrick McDaniel and Somesh Jha and Matthew Fredrikson and Z. Berkay Celik and Ananthram Swami, *The Limitations of Deep Learning in Adversarial Settings*, Proceedings of the 1st IEEE European Symposium on Security and Privacy, IEEE, 2016. Saarbrücken, Germany.

Damien Ocateau and Somesh Jha and Matthew Dering and Patrick McDaniel and Alexandre Bartel and Li Li and Jacques Klein and Yves Le Traon, *Combining Static Analysis with Probabilistic Models to Enable Market-Scale Android Inter-Component Analysis*, Proceedings of the 43rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL), January, 2016. St. Petersburg, Florida, USA.

Devin Pohly and Patrick McDaniel, *MICSS: A Realistic Multichannel Secrecy Protocol*, IEEE Global Communications Conference (GLOBECOM), December, 2015. San Diego, CA.

Robert Walls and Eric Kilmer and Nathaniel Lageman and Patrick McDaniel, *Measuring the Impact and Perception of Acceptable Advertisements*, Proceedings of the ACM 2015 Internet Measurement Conference (IMC), October, 2015. Tokyo, Japan.

Nicolas Papernot and Patrick McDaniel and Robert Walls, *Enforcing Agile Access Control Policies in Relational Databases using Views*, Proceedings of the Military Communications Conference (MILCOM), October, 2015. Tampa, FL.

Alessandro Oltramari and Lorrie Cranor and Robert Walls and Patrick McDaniel, *Computational Ontology of Network Operations*, Proceedings of the Military Communications Conference (MILCOM), October, 2015. Tampa, FL.

Z. Berkay Celik and Robert Walls and Patrick McDaniel and Ananthram Swami, *Malware Traffic Detection using Tamper Resistant Features*, Proceedings of the Military Communications Conference (MILCOM), October, 2015. Tampa, FL.

Devin Pohly and Charles Sestito and Patrick McDaniel, *Adaptive Protocol Switching Using Dynamically Insertable Bumps in the Stack*, Proceedings of the Military Communications Conference (MILCOM), October, 2015. Tampa, FL.

Azeem Aqil and Ahmed Atya and Trent Jaeger and Srikanth V. Krishnamurthy and Karl Levitt and Patrick McDaniel and Jeff Rowe and Ananthram Swami, *Detection of Stealthy TCP-based DoS Attacks*, Proceedings of the Military Communications Conference (MILCOM), October, 2015. Tampa, FL.

Daniel E. Krych and Stephen Lange-Maney and Patrick McDaniel and William Glodek, *Investigating Weaknesses in Android Certificate Security*, SPIE 9478, Modeling and Simulation for Defense Systems and Applications X, May, 2015.

Damien Oceau and Daniel Luchaup and Matthew Dering and Somesh Jha and Patrick McDaniel, *Composite Constant Propagation: Application to Android Inter-Component Communication Analysis*, Proceedings of the 37th International Conference on Software Engineering (ICSE), May, 2015. Florence, Italy.

Li Li and Alexandre Bartel and Tegawende Bissyande and Jacques Klein and Yves Le Traon and Steven Arzt and Siegfried Rasthofer and Eric Bodden and Damien Oceau and Patrick McDaniel, *IccTA: Detecting Inter-Component Privacy Leaks in Android Apps*, Proceedings of the 37th International Conference on Software Engineering (ICSE), May, 2015. Florence, Italy.

Jing Tian and Kevin Butler and Patrick McDaniel and Padma Krishnaswamy, *Securing ARP From the Ground Up*, CODASPY '15: Proceedings of the 5th ACM Conference on Data Application and Security and Privacy, March, 2015. San Antonio, TX, USA.

Alessandro Oltramari and Lorrie Cranor and Robert Walls and Patrick McDaniel, *Building an Ontology of Cyber Security*, Proc. Intl. Conference on Semantic Technologies for Intelligence, Defense, and Security (STIDS), November, 2014.

Matthew Dering and Patrick McDaniel, *Android Market Reconstruction and Analysis*, Proceedings of the Military Communications Conference (MILCOM), October, 2014. Baltimore, MD.

Wenhui Hu and Damien Oceau and Patrick McDaniel and Peng Liu, *Duet: Library Integrity Verification for Android Applications*, Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), July, 2014. Oxford, United Kingdom.

Steven Arzt and Siegfried Rasthofer and Christian Fritz and Eric Bodden and Alexandre Bartel and Jacques Klein and Yves Le Traon and Damien Oceau and Patrick McDaniel, *FlowDroid: Precise Context, Flow, Field, Object-sensitive and Lifecycle-aware Taint Analysis for Android Apps*, Proceedings of the 35th Conference on Programming Language Design and Implementation (PLDI), June, 2014. Edinburgh, UK.

Phillip Koshy and Diana Koshy and Patrick McDaniel, *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*, Proceedings of Financial Cryptography 2014, International Financial Cryptography Association (IFCA), February, 2014. Christ Church, Barbado.

Stephen McLaughlin and Devin Pohly and Patrick McDaniel and Saman Zonouz, *A Trusted Safety Verifier for Process Controller Code*, Proc. ISOC Network and Distributed Systems Security Symposium (NDSS), February, 2014. San Diego, CA.

Damien Oceau and Patrick McDaniel and Somesh Jha and Alexandre Bartel and Eric Bodden and Jacques Klein and Yves Le Traon, *Effective Inter-Component Communication Mapping in Android with Epiccc: An Essential Step Towards Holistic Security Analysis*, Proceedings of the 22th USENIX Security Symposium, August, 2013.

Washington, DC.

Devin J. Pohly and Stephen McLaughlin and Patrick McDaniel and Kevin Butler, *Hi-Fi: Collecting High-Fidelity Whole-System Provenance*, Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC), December, 2012. Orlando, Florida.

Stephen McLaughlin and Patrick McDaniel, *SABOT: Specification-based Payload Generation for Programmable Logic Controllers*, 19th ACM Conference on Computer and Communications Security (CCS), October, 2012.

Weining Yang and Ninghui Li and Yuan Qi and Wahbeh Qardaji and Stephen McLaughlin and Patrick McDaniel, *Minimizing Private Data Disclosures in the Smart Grid*, 19th ACM Conference on Computer and Communications Security (CCS), October, 2012.

Eun Kyoung Kim and Patrick McDaniel and Thomas La Porta, *A Detection Mechanism for SMS Flooding Attacks in Cellular Networks*, Proceedings of the 8th International Conference on Security and Privacy in Communication Networks (SECURECOMM 2012), September, 2012. Padua, Italy.

Damien Oceau and Somesh Jha and Patrick McDaniel, *Retargeting Android Applications to Java Bytecode*, 20th International Symposium on the Foundations of Software Engineering (FSE), November, 2012. Research Triangle Park, NC. (**best artifact award**)

Thomas Moyer and Trent Jaeger and Patrick McDaniel, *Scalable Integrity-Guaranteed AJAX*, Proceedings of the 14th Asia-Pacific Web Conference (APWeb), April, 2012. Kunming, China. (*Invited Paper*)

Patrick McDaniel and Stephen McLaughlin, *Structured Security Testing in the Smartgrid*, Proceedings of 5th International Symposium on Communications, Control, and Signal Processing, May, 2012. Rome, Italy. (*Invited Paper*)

Stephen McLaughlin and Patrick McDaniel and William Aiello, *Protecting Consumer Privacy from Electric Load Monitoring*, The 18th ACM Conference on Computer and Communications Security (CCS), October, 2011. Chicago, IL.

William Enck and Damien Oceau and Patrick McDaniel and Swarat Chaudhuri, *A Study of Android Application Security*, Proceedings of the 20th USENIX Security Symposium, August, 2011. San Francisco, CA.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Kells: A Protection Framework for Portable Data*, Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC), December, 2010. Austin, TX.

Stephen McLaughlin and Dmitry Podkuiko and Adam Delozier and Sergei Miadzvezhanka and Patrick McDaniel, *Multi-vendor Penetration Testing in the Advanced Metering Infrastructure*, Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC), December, 2010. Austin, TX.

Machigar Ongtang and Kevin Butler and Patrick McDaniel, *Porscha: Policy Oriented Secure Content Handling in Android*, Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC), December, 2010. Austin, TX.

Patrick Traynor and Joshua Schiffman and Thomas La Porta and Patrick McDaniel and Abhrajit Ghosh and Farooq Anjum, *Constructing Secure Localization Systems with Adjustable Granularity*, IEEE Global Communications Conference (GLOBECOM), December, 2010. Miami, FL.

William Enck and Peter Gilbert and Byung-Gon Chun and Landon Cox and Jaeyeon Jung and Patrick McDaniel and Anmol Sheth, *TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*, Proceedings of the 9th USENIX Symposium on Operating Systems Design and Implementation (OSDI), October, 2010. Vancouver, BC.

Toby Ehrenkranz and Jun Li and Patrick McDaniel, *Realizing A Source Authentic Internet*, Proceedings of the 6th International ICST Conference on Security and Privacy in Communications Networks (Securecomm), September, 2010. Singapore.

Boniface Hicks and Sandra Rueda and David King and Thomas Moyer and Joshua Schiffman and Yogesh Sreenivasan and Patrick McDaniel and Trent Jaeger, *An Architecture for Enforcing End-to-End Access Control over Web Applications*, Proceedings of the Fifteenth ACM Symposium on Access Control Models and Technologies (SACMAT 2010), 163-172, June, 2010. Pittsburgh, PA.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Disk-Enabled Authenticated Encryption*, Proceedings of the 26th IEEE Symposium on Massive Storage Systems and Technologies (MSST), May, 2010.

Machigar Ongtang and Stephen McLaughlin and William Enck and Patrick McDaniel, *Semantically Rich Application-Centric Security in Android*, Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC), 340-349, December, 2009. Honolulu, Hawaii. **(best paper)**

Thomas Moyer and Kevin Butler and Joshua Schiffman and Patrick McDaniel and Trent Jaeger, *Scalable Asynchronous Web Content Attestation*, Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC), 95-104, December, 2009. Honolulu, Hawaii.

Joshua Schiffman and Thomas Moyer and Christopher Shal and Trent Jaeger and Patrick McDaniel, *Justifying Integrity Using a Virtual Machine Verifier*, Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC), 83-92, December, 2009. Honolulu, Hawaii.

William Enck and Machigar Ongtang and Patrick McDaniel, *On Lightweight Mobile Phone App Certification*, Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS), 235-245, November, 2009.

Patrick Traynor and Michael Lin and Machigar Ongtang and Vikhyath Rao and Trent Jaeger and Thomas La Porta and Patrick McDaniel, *On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core*, Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS), 223-234, November, 2009.

William Enck and Patrick McDaniel and Trent Jaeger, *PinUP: Pinning User Files to Known Applications*, Proceedings of the 24th Annual Computer Security Applications Conference (ACSAC), December, 2008.

William Enck and Kevin Butler and Thomas Richardson and Patrick McDaniel and Adam Smith, *Defending Against Attacks on Main Memory Persistence*, Proceedings of the 24th Annual Computer Security Applications Conference (ACSAC), December, 2008.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Rootkit-Resistant Disks*, Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS), November, 2008. Alexandria, VA.

Patrick Traynor and Kevin Butler and William Enck and Patrick McDaniel, *Realizing Massive-Scale Conditional Access Systems Through Attribute-Based Cryptosystems*, ISOC Network & Distributed System Security Symposium (NDSS), February, 2008. San Diego, CA.

Luke St. Clair and Joshua Schiffman and Trent Jaeger and Patrick McDaniel, *Establishing and Sustaining System Integrity via Root of Trust Installation*, 23rd Annual Computer Security Applications Conference (ACSAC), 19-29, December, 2007. Miami, FL.

Boniface Hicks and Tim Misiak and Patrick McDaniel, *Channels: Runtime System Infrastructure for Security-typed Languages*, 23rd Annual Computer Security Applications Conference (ACSAC), 443-452, December, 2007. Miami, FL.

Dhananjay Bapat and Kevin Butler and Patrick McDaniel, *Towards Automated Privilege Separation*, Proceedings of 2nd International Conference on Information Systems Security (short paper), December, 2007. Delhi, India.

Lisa Johansen and Kevin Butler and Michael Rowell and Patrick McDaniel, *Email Communities of Interest*, Fourth Conference on Email and Anti-Spam (CEAS 2007, August, 2007. Mountain View, California.

Patrick Traynor and Patrick McDaniel and Thomas La Porta, *On Attack Causality in Internet-Connected Cellular Networks*, Proceedings of the 16th USENIX Security Symposium, 1–16, August, 2007. Boston, MA.

Boniface Hicks and Sandra Rueda and Trent Jaeger and Patrick McDaniel, *From Trusted to Secure: Building and Executing Applications that Enforce System Security*, Proceedings of the USENIX Annual Technical Conference, June, 2007. Santa Clara, CA.

William Enck and Patrick McDaniel and Shubho Sen and Panagiotis Sebos and Sylke Spoerel and Albert Greenberg and Sanjay Rao and William Aiello, *Configuration Management at Massive Scale: System Design and Experience*, Proceedings of the USENIX Annual Technical Conference, June, 2007. Santa Clara, CA.

Boniface Hicks and Sandra Rueda and Luke St. Clair and Trent Jaeger and Patrick McDaniel, *A Logical Specification and Analysis for SELinux MLS*, 12th ACM Symposium on Access Control Models and Technologies (SACMAT), ACM, June, 2007. Sophia Antipolis, France.

Anusha Sriraman and Kevin Butler and Patrick McDaniel and Padma Raghavan, *Analysis of IPv4 Address Space Delegation Structure*, 12th IEEE Symposium on Computers and Communications (ISCC), July, 2007. Aveiro, Portugal.

Heesook Choi and Thomas La Porta and Patrick McDaniel, *Privacy Preserving Communication in MANETs*, Proceedings of Fourth Annual IEEE Communications Society Conference on Sensor, Mesh, and Ad Hoc Communications and Networks (SECON 07), June, 2007. San Diego, CA.

Sophie Qiu and Patrick McDaniel and Fabian Monroe, *Toward Valley-Free Inter-domain Routing*, Proceedings of 2007 IEEE International Conference on Communications (ICC 2007), June, 2007. Glasgow, Scotland.

Sunam Ryu and Kevin Butler and Patrick Traynor and Patrick McDaniel, *Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems*, Proceedings of the 3rd IEEE International Symposium on Security in Networks and Distributed Systems (SSNDS-07), June, 2007. Niagara Falls, Canada.

Hosam Rowaihy and William Enck and Patrick McDaniel and Thomas La Porta, *Limiting Sybil Attacks in Structured Peer-to-Peer Networks*, Proceedings of IEEE INFOCOM 2007 MiniSymposium, May, 2007. Anchorage, AK.

Boniface Hicks and Kiyan Ahmadizadeh and Patrick McDaniel, *Understanding Practical Application Development in Security-Typed Languages*, 22st Annual Computer Security Applications Conference (ACSAC), 153–164, December, 2006. Miami, Fl. (**best student paper**)

Luke St. Clair and Lisa Johansen and William Enck and Matthew Pirretti and Patrick Traynor and Patrick McDaniel and Trent Jaeger, *Password Exhaustion: Predicting the End of Password Usefulness*, Proceedings of 2nd International Conference on Information Systems Security (ICISS), 37–55, December, 2006. Kolkata, India.

Kevin Butler and William Enck and Jennifer Plasterr and Patrick Traynor and Patrick McDaniel, *Privacy-Preserving Web-Based Email*, Proceedings of 2nd International Conference on Information Systems Security (ICISS), 116–131, December, 2006. Kolkata, India.

Matthew Pirretti and Patrick Traynor and Patrick McDaniel and Brent Waters, *Secure Attribute-Based Systems*, Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS), 99–112, November, 2006. Alexandria, VA.

Kevin Butler and William Aiello and Patrick McDaniel, *Optimizing BGP Security by Exploiting Path Stability*, Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS), 298-310, November, 2006. Alexandria, VA.

Patrick Traynor and William Enck and Patrick McDaniel and Thomas La Porta, *Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks*, Proceedings of the Twelfth Annual International Conference on Mobile Computing and Networking (MobiCom), 182-193, September, 2006. Los Angeles, CA.

Patrick Traynor and Michael Chien and Scott Weaver and Boniface Hicks and Patrick McDaniel, *Non-Invasive Methods for Host Certification*, Proceedings of the Second IEEE Communications Society/CreateNet International Conference on Security and Privacy in Communication Networks (SecureComm), August, 2006. Baltimore, MD.

Sophie Qiu and Patrick McDaniel and Fabian Monrose and Avi Rubin, *Characterizing Address Use Structure and Stability of Origin Advertisement in Interdomain Routing*, 11th IEEE Symposium on Computers and Communications, 489-496, June, 2006. Pula-Cagliari, Sardinia, Italy.

Patrick McDaniel and Shubho Sen and Oliver Spatscheck and Jacobus Van der Merwe and William Aiello and Charles Kalmanek, *Enterprise Security: A Community of Interest Based Approach*, Proceedings of Network and Distributed Systems Security 2006 (NDSS), February, 2006. San Diego, CA.

Kevin Butler and Patrick McDaniel, *Understanding Mutable Internet Pathogens, or How I Learned to Stop Worrying and Love Parasitic Behavior*, Proceedings of 1st International Conference on Information Systems Security (ICISS), Springer-Verlag Lecture Notes in Computer Science, volume 3803, 36-48, December, 2005. Kolkata, India. (*Invited Paper*)

Wesam Lootah and William Enck and Patrick McDaniel, *TARP: Ticket-Based Address Resolution Protocol*, 21st Annual Computer Security Applications Conference (ACSAC), 95-103, December, 2005. Tuscon, AZ.

William Enck and Patrick Traynor and Patrick McDaniel and Thomas La Porta, *Exploiting Open Functionality in SMS-Capable Cellular Networks*, Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS), 393-404, May, 2005. Alexandria, VA.

Matthew Pirretti and Sencun Zhu and Vijaykrishnan Narayanan and Patrick McDaniel and Mahmut Kandemir and Richard Brooks, *The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense*, Proceedings of the Innovations and Commercial Applications of Distributed Sensor Networks Symposium, October, 2005. Bethesda, Maryland. (**best paper**)

Louis Kruger and Somesh Jha and Patrick McDaniel, *Privacy Preserving Clustering*, 10th European Symposium on Research in Computer Security (ESORICS '05), September, 2005. Milan, Italy.

Heesook Choi and William Enck and Jaesheung Shin and Patrick McDaniel and Thomas La Porta, *Secure Reporting of Traffic Forwarding Activity in Mobile AdHoc Networks*, MobiQuitous 2005, July, 2005. San Diego, CA.

Simon Byers and Lorrie Cranor and Eric Cronin and Dave Kormann and Patrick McDaniel, *Exposing Digital Content Piracy: Approaches, Issues and Experiences*, Thirty-Eighth Conference on Signals, Systems, and Computers, 45-50, Nov, 2004. Monterey, CA. (*Invited paper*)

William Aiello and John Ioannidis and Patrick McDaniel, *Origin Authentication in Interdomain Routing*, Proceedings of 10th ACM Conference on Computer and Communications Security (CCS), ACM, 165-178, October, 2003. Washington, DC.

Eric Cronin and Sugih Jamin and Tal Malkin and Patrick McDaniel, *On the Performance, Feasibility, and Use of Forward Secure Signatures*, Proceedings of 10th ACM Conference on Computer and Communications Security (CCS), ACM, 131-144, October, 2003. Washington, DC.

Patrick McDaniel, *On Context in Authorization Policy*, 8th ACM Symposium on Access Control Models and Technologies (SACMAT), ACM, 80-8, June, 2003. Como, Italy.

Geoff Goodell and William Aiello and Tim Griffin and John Ioannidis and Patrick McDaniel and Avi Rubin, *Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing*, Proceedings of Network and Distributed Systems Security 2003 (NDSS), Internet Society, 75-8, February, 2003. San Diego, CA.

Patrick McDaniel and Atul Prakash, *Methods and Limitations of Security Policy Reconciliation*, 2002 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, 73-87, May, 2002. Oakland, CA.

Patrick McDaniel and Atul Prakash and Jim Irrer and Sharad Mittal and Thai-Chuin Thuang, *Flexibly Constructing Secure Groups in Antigone 2.0*, Proceedings of DARPA Information Survivability Conference and Exposition II, IEEE Computer Society Press, 55-67, June, 2001. Los Angeles, CA.

Hugh Harney and Andrea Colegrove and Patrick McDaniel, *Principles of Policy in Secure Groups*, Proceedings of Network and Distributed Systems Security 2001 (NDSS), Internet Society, 125-13, February, 2001. San Diego, CA.

Patrick McDaniel and Sugih Jamin, *Windowed Certificate Revocation*, Proceedings of IEEE INFOCOM 2000, IEEE, 1406-1414, March, 2000. Tel Aviv, Israel.

Patrick McDaniel and Avi Rubin, *A Response to ‘Can We Eliminate Certificate Revocation Lists?’*, Proceedings of Financial Cryptography 2000, International Financial Cryptography Association (IFCA), February, 2000. Anguilla, British West Indies.

Andrew Adamson and Charles J. Antonelli and Kevin Coffman and Patrick McDaniel and Jim Rees, *Secure Distributed Virtual Conferencing*, Proceedings of Communications and Multimedia Security (CMS ’99), 176-190, September, 1999. Katholieke Universiteit, Leuven, Belgium.

Patrick McDaniel and Atul Prakash and Peter Honeyman, *Antigone: A Flexible Framework for Secure Group Communication*, Proceedings of the 8th USENIX Security Symposium, 99-114, August, 1999. Washington, DC.

Workshop Papers

Yohan Beugin and Patrick McDaniel, *A Public and Reproducible Assessment of the Topics API on Real Data*, SecWeb 2024 Workshop, IEEE Security and Privacy Workshops (SPW), May, 2024.

Kunyang Li and Kyle D Domico and Jean-Charles Noirot Ferrand and Patrick McDaniel, *The Efficacy of Transformer-Based Adversarial Attacks in Security Domains*, Workshop on Artificial Intelligence for Cyber (MIL-COM 2023), October, 2023. Boston, MA.

Eric Pauley and Patrick McDaniel, *Understanding the Ethical Frameworks of Internet Measurement Studies*, The 2nd International Workshop on Ethics in Computer Security (EthiCS 2023), February, 2023. San Diego, CA. **(best paper award)**

Anshul Gandhi and Kanad Ghose and Kartik Gopalan and Syed Rafiul Hussain and Dongyoon Lee and David Liu and Zhenhua Liu and Patrick McDaniel and Shuai Mu and Erez Zadok, *Metrics for Sustainability in Data Centers*, Proceedings of the 1st Workshop on Sustainable Computer Systems Design and Implementation (Hot-Carbon’22), USENIX, July, 2022. San Diego, CA.

Leonardo Babun and Z. Berkay Celik and Patrick McDaniel and Selcuk Uluagac, *Real-time Analysis of Privacy-(un)aware IoT Applications*, Privacy Enhancing Technologies Symposium (PETS), 2021.

Sushrut Shringarputale and Patrick McDaniel and Kevin Butler and Thomas La Porta, *Co-residency Attacks on Containers are Real*, The ACM Cloud Computing Security Workshop (CCSW 2020), 2020.

Z. Berkay Celik and Patrick McDaniel, *Extending Detection with Privileged Information via Generalized Distillation*, IEEE Security & Privacy Workshop on Deep Learning and Security (IEEE S&P DLS), 2018.

Alexander Alexeev and Diane Henshel and Karl Levitt and Patrick McDaniel and Brian Rivera and Steve Templeton and Michael J. Weisma, *Constructing a Science of Cyber-Resilience for Military Systems*, Information Systems and Technology (IST) Panel, IST-153/RWS-21, CEUR Workshop Proceeding, 30-42, October, 2017.

Z. Berkay Celik and Patrick McDaniel and Rauf Izmailov, *Feature Cultivation in Privileged Information-augmented Detection*, Proceedings of the International Workshop on Security And Privacy Analytics (IWSPA 2017), 2017. (*Invited Paper*)

Stefan Achleitner and Thomas La Porta and Patrick McDaniel and Shridatt Sugrim and Srikanth V. Krishnamurthy and Ritu Chadha, *Cyber Deception: Virtual Networks to Defend Insider Reconnaissance*, Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats, ACM, 2016.

Patrick McDaniel and Robert Walls, *Estimating Attack Intent and Mission Impact from Detection Signals*, Proceedings of the NATO IST-128 Workshop: Assessing Mission Impact of Cyberattacks, Army Research Laboratory, July, 2015.

Patrick McDaniel and Trent Jaeger and Thomas La Porta and Nicolas Papernot and Robert Walls and Alexander Kott and Lisa Marvel and Ananthram Swami and Prasant Mohapatra and Srikanth V. Krishnamurthy and Iulian Neamtiu, *Security and Science of Agility*, First ACM Workshop on Moving Target Defense (MTD 2014), November, 2014. Scottsdale, AZ.

Joshua Schiffman and Thomas Moyer and Hayawardh Vijayakumar and Trent Jaeger and Patrick McDaniel, *Seeding Clouds with Trust Anchors*, Proceedings of CCSW 2010: The ACM Cloud Computing Security Workshop, October, 2010. Chicago, IL.

Stephen McLaughlin and Dmitry Podkuiko and Adam Delozier and Sergei Miadzvezhanka and Patrick McDaniel, *Embedded Firmware Diversity for Smart Electric Meters*, Proceedings of the 5th Workshop on Hot Topics in Security (HotSec '10), August, 2010. Washington, DC.

Patrick McDaniel and Kevin Butler and Stephen McLaughlin and Radu Sion and Erez Zadok and Marianne Winslett, *Towards a Secure and Efficient System for End-to-End Provenance*, the 2nd USENIX Workshop on the Theory and Practice of Provenance, February, 2010. San Jose, CA.

Thomas La Porta and Patrick McDaniel and Karl Rauscher and Jun Shu, *The Impact of Supply Chain on Information and Communications Technology Security*, In the 1st Workshop on Workshop on Telecommunications Infrastructure Protection and Security, December, 2009. Honolulu, Hawaii.

Stephen McLaughlin and Dmitry Podkuiko and Patrick McDaniel, *Energy Theft in the Advanced Metering Infrastructure*, In the 4th International Workshop on Critical Information Infrastructure Security, September, 2009. Bonn, Germany.

Matthew Blaze and Patrick McDaniel, *Below the Salt: The Dangers of Unfulfilled Physical Media Assumptions*, In Proceedings of Seventeenth International Workshop on Security Protocols, April, 2009. Cambridge, England.

Kevin Butler and William Enck and Harri Hursti and StephenMcLaughlin and Patrick Traynor and Patrick McDaniel, *Systemic Issues in the Hart InterCivic and Premier VotingSystems: Reflections Following Project EVEREST*, In Proceedings of the 3rd USENIX/ACCURATE ElectronicVoting Technology Workshop (EVT '08), July, 2008.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Non-Volatile Memory and Disks: Avenues for Policy Architectures*, Proceedings of the 1st ACM Computer Security Architectures Workshop, November, 2007.

Alexandria, VA.

William Enck and Sandra Rueda and Yogesh Sreenivasan and JoshuaSchiffman and Luke St. Clair and Trent Jaeger and Patrick McDaniel, *Protecting Users from "Themselves"*, Proceedings of the 1st ACM Computer Security Architectures Workshop, November, 2007. Alexandria, VA.

Boniface Hicks and David King and Patrick McDaniel, *Jifclipse: Development Tools for Security-Typed Applications*, Proceedings of the 2nd ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS '07), ACM Press, June, 2007. San Diego, CA.

Boniface Hicks and Sandra Rueda and Trent Jaeger andPatrick McDaniel, *Integration of SELinux and Security-typed Languages*, Proceedings of the 2007 Security-Enhanced Linux Workshop, March, 2007. Baltimore, MD.

Sophie Qiu and Fabian Monroe and Andreas Terzis and Patrick McDaniel, *Efficient Techniques for Detecting False Origin Advertisements in Inter-domain Routing*, Proceedings of The Second Workshop on Secure Network Protocols (NPSec), November, 2006. Santa Barbara.

Shiva Chaitanya and Kevin Butler and Patrick McDaniel andAnand Sivasubramaniam, *Design, Implementation and Evaluation of Security iniSCSI-based Network Storage Systems*, Proceedings of 2nd International Workshop on StorageSecurity and Survivability (StorageSS 2006), October, 2006. Alexandria, Virginia.

Trent Jaeger and Patrick McDaniel and Luke St. Clair and RamonCaceres and Reiner Sailer, *Shame on Trust in Distributed Systems*, Proceedings of the First Workshop on Hot Topics inSecurity (HotSec '06), July, 2006. Vancouver, B.C., Canada.

Kevin Butler and Patrick McDaniel and Sophie Qiu, *BGPRV: A Library for Fast and Efficient Routing Data Manipulation*, Proceedings of DETER Community Workshop, June, 2006. Arlington, VA.

Kevin Butler and Patrick McDaniel, *Testing Large Scale BGP Security in Replayable NetworkEnvironments*, Proceedings of DETER Community Workshop, June, 2006. Arlington, VA.

Boniface Hicks and David King and Patrick McDaniel andMichael Hicks, *Trusted Declassification: High-level Policy for aSecurity-Typed Language*, Proceedings of ACM SIGPLAN Workshop on ProgrammingLanguages and Analysis for Security, 65-74, June, 2006. Ottawa, Canada.

Ali Al-Lawati and Dongwon Lee and Patrick McDaniel, *Blocking in Private Information Matching*, Proceedings of Second International ACM SIGMOD Workshopon Information Quality in Information Systems, June, 2005. Baltimore, MD.

William Aiello and Charles Kalmanek and Patrick McDaniel andShubho Sen and Oliver Spatscheck and Jacobus Van der Merwe, *Analysis of Communities Of Interest in Data Networks*, Passive and Active Measurement Workshop 2005, March, 2005. Boston, M.

Simon Byers and Lorrie Cranor and David Kormann andPatrick McDaniel, *Searching for Privacy: Design and Implementation of aP3P-Enabled Search Engine*, Proceedings of 2004 Workshop on Privacy EnhancingTechnologies (PETS), May, 2004. Toronto, Canad.

Hao Wang and Somesh Jha and Patrick McDaniel and MironLivn, *Security Policy Reconciliation in Distributed ComputingEnvironments*, Proceedings of 5th International Workshop on Policiesfor Distributed Systems and Networks (Policy 2004), IEEE Computer Society Press, 137-146, June, 2004. Yorktown Heights, N.

Simon Byers and Lorrie Cranor and Eric Cronin and DaveKormann and Patrick McDaniel, *Analysis of Security Vulnerabilities in the Movie Productionand Distribution Process*, Proceedings of 2003 ACM Workshop on Digital RightsManagement, ACM, October, 2003. Washington, DC, also appeared in Telecommunications PolicyResearch Conference – September 2003.

Patents

U.S. Patent No. 7,873,350, Patrick McDaniel and Martin Strauss, *End-to-end secure wireless communication for requesting a more secure channel*, January, 2011.

U.S. Patent No. 7,975,044, Oliver Spatscheck and Subhabrata Sen and Jacobus Van der Merwe and Patrick McDaniel, *Automated disambiguation of fixed-serverport-based applications from ephemeral applications*, July, 2011.

U.S. Patent No. 8,175,580, Patrick McDaniel and Martin Strauss, *End-to-end secure wireless communication for requesting a more secure channel*, May, 2012.

U.S. Patent No. 8,453,227, William Aiello and Charles Kalmanek and William Leighton III and Patrick McDaniel and Subhabrata Sen and Oliver Spatscheck and Jacobus Van der Merwe, *Reverse firewall with self-provisioning*, May, 2013.

U.S. Patent No. 8,732,293, Patrick McDaniel and Subhabrata Sen and Oliver Spatscheck and Jacobus Van der Merwe, *System and method for tracking individuals on a data network using communities of interest*, May, 2014.

U.S. Patent No. 8,813,213, William Aiello and Charles Kalmanek and William Leighton III and Patrick McDaniel and Subhabrata Sen and Oliver Spatscheck and Jacobus Van der Merwe, *Reverse firewall with self-provisioning*, August, 2014.

Other Publications

Patrick McDaniel and Farinaz Koushanfar, *NSF Secure and Trustworthy Computing 2.0 Vision Statement*, Public Report, August, 2023.

Patrick McDaniel and Thorsten Holz and Indra Spiecker and Genannt Dohmann and Christopher Burchard and Ahmad-Reza Sadeghi and Konrad Rieck and Kamalika Chaudhuri and Somesh Jha and Andrea Matwyshyn and David Evans and Felix Freiling and Amy Hasan, *Cybersecurity and Machine Learning: Vision Document, Report on the joint NSF/DFG Cybersecurity and Machine Learning Research Workshop*, Public Report, National Science Foundation/Deutsche Forschungsgemeinschaft, December, 2021.

Patrick McDaniel and John Launchbury, *Artificial Intelligence and Cybersecurity: Opportunities and Challenges 2019 Technical Workshop Report*, Public Report, Networking and Information Technology Research and Development Subcommittee, Machine Learning and Artificial Intelligence Subcommittee, and the Special Cyber Operations Research and Engineering Subcommittee of the National Science and Technology Council, 2020.

Patrick McDaniel and Avi Rubin, *Conference Proceedings*, 2008 IEEE Symposium on Security and Privacy, IEEE, May, 2008. Oakland, CA.

Patrick McDaniel and Kevin Butler and William Enck and Harri Hursti and Stephen McLaughlin and Patrick Traynor and Matthew Blaze and Adam Aviv and Pavol Cerny and Sandy Clark and Eric Cronin and Gaurav Shah and Micah Sherr and Giovanni Vigna and Richard Kemmerer and David Balzarotti and Greg Banks and Marco Cova and Viktoria Felmetzger and William Robertson and Fredrik Valeur and Joseph Lorenzo Hall and Laura Quilter, *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing*, Ohio Secretary of State, Public Report, 2007.

Patrick McDaniel and Shyam K. Gupta, *Conference Proceedings*, The Third International Conference Information Systems Security, Springer, December, 2007. Delhi, India.

Birgit Pfitzmann and Patrick McDaniel, *Conference Proceedings*, 2007 IEEE Symposium on Security and Privacy, IEEE, May, 2007. Oakland, CA.

Patrick McDaniel, *Conference Proceedings*, The 14th USENIX Security Symposium, USENIX, August, 2005.

Baltimore, MD.

Patrick McDaniel, *Policy Evolution: Autonomic Environmental Security*, Software Engineering Research Center Showcase, USA, December, 2004.

Hugh Harney and Uri Meth and Andrea Colegrove and Angela Schuett and Patrick McDaniel and Gavin Kenny and Haitham Cruickshank and Sunil Iyengar, *GSAKMP (Draft)*, Internet Research Task Force, August, 2003.

Patrick McDaniel and Atul Prakash, *A Flexible Architecture for Security Policy Enforcement*, Proceedings of DARPA Information Survivability Conference and Exposition III, Research Summaries, 234-239, April, 2003.

Jim Irrer and Atul Prakash and Patrick McDaniel, *Antigone: Policy-Based Secure Group Communications Systems and AMirD: Antigone-Based Secure File Mirroring System*, Proceedings of DARPA Information Survivability Conference and Exposition III, Demo Summaries, 44-4, April, 2003.

Patrick McDaniel and Sugih Jamin, *Windowed Key Revocation in Public Key Infrastructures*, NASA Tech Briefs, 55, August, 2002.

Patrick McDaniel and Atul Prakash, *Antigone Secure Group Communication System*, NASA Tech Briefs, 2001.

Patrick McDaniel, *Policy Management in Secure Group Communication*, PhD Thesis, University of Michigan, Ann Arbor, MI, August, 2001.

Patrick McDaniel and Hugh Harney and Andrea Colegrove and Atul Prakash and Peter Dinsmore, *Multicast Security Policy Requirements and Building Blocks (Draft)*, Internet Research Task Force, Secure Multicast Research Group (SMuG), November, 2000.

Tom Hardjono and Hugh Harney and Patrick McDaniel and Andrea Colegrove and Peter Dinsmore, *Group Security Policy Token (Draft)*, Internet Research Task Force, Secure Multicast Research Group (SMuG), November, 2001.

Patrick McDaniel and Hugh Harney and Peter Dinsmore and Atul Prakash, *Multicast Security Policy (Draft)*, Internet Research Task Force, Secure Multicast Research Group (SMuG), June, 2000.

Patrick McDaniel, *8th USENIX Security Symposium Conference Summaries, Potpourri Session*, USENIX Login Magazine, 9-12, November, 1999.

Patrick McDaniel, *The Analysis of D_i , a Detailed Design Metric on Large Scale Software*, Masters Thesis, Ball State University, Muncie, IN, June, 1991.

Technical Reports

Quinn Burke and Ryan Sheatsley and Rachel King and Michael Swift and Patrick McDaniel, *Cloud Storage Integrity at Scale: A Case for Dynamic Hash Trees*, Technical Report 2405.03830, arXiv preprint, May, 2024.

Alban Héon and Ryan Sheatsley and Quinn Burke and Blaine Hoak and Eric Pauley and Yohan Beugin and Patrick McDaniel, *Systematic Evaluation of Geolocation Privacy Mechanisms*, Technical Report 2309.06263, arXiv preprint, September, 2023.

Yohan Beugin and Patrick McDaniel, *Interest-disclosing Mechanisms for Advertising are Privacy-Exposing (Not Preserving)*, Technical Report 2306.03825, arXiv preprint, May, 2023.

Quinn Burke and Yohan Beugin and Blaine Hoak and Rachel King and Eric Pauley and Ryan Sheatsley and Mingli Yu and Ting He and Thomas La Porta and Patrick McDaniel, *Securing Cloud File Systems using Shielded Execution*, Technical Report 2305.18639, arXiv preprint, May, 2023.

Yohan Beugin and Quinn Burke and Blaine Hoak and Ryan Sheatsley and Eric Pauley and Gang Tan and Syed Rafiul Hussain and Patrick McDaniel, *Privacy-Preserving Protocols for Smart Cameras and Other IoT Devices*, Technical Report 2208.09776, arXiv preprint, August, 2022.

Pauley, Eric and Domico, Kyle and Hoak, Blaine and Sheatsley, Ryan and Burke, Quinn and Beugin, Yohan and McDaniel, Patrick, *EIPSIM: Modeling Secure IP Address Allocation at Cloud Scale*, Technical Report arXiv:2210.14999, arXiv preprint, 2022.

Bolor-Erdene Zolbayarn and Ryan Sheatsley and Patrick McDaniel and Michael J. Weisman and Sencun Zhu and Shitong Zhu and Srikanth V. Krishnamurthy, *Generating Practical Adversarial Network Traffic Flows using NIDSGAN*, Technical Report arXiv:2203.06694, arXiv preprint, March, 2022.

Ryan Sheatsley and Blaine Hoak and Eric Pauley and Yohan Beugin and Michael J. Weisman and Patrick McDaniel, *On the Robustness of Domain Constraints*, Technical Report arXiv:2105.08619, arXiv preprint, 2021.

Ryan Sheatsley and Nicolas Papernot and Michael J. Weisman and Gunjan Verma and Patrick McDaniel, *Adversarial Examples in Constrained Domains*, Technical Report arXiv:2011.01183, arXiv preprint, 2020.

Stefan Achleitner and Quinn Burke and Patrick McDaniel and Trent Jaeger and Thomas La Porta and Srikanth V. Krishnamurthy, *MLSNet: A Policy Complying Multilevel Security Framework for Software Defined Networking*, Technical Report INSR-500-TR-0500-2019, Institute of Networking and Security Research, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, January, 2019.

Michael Norris and Z. Berkay Celik and Patrick McDaniel and Gang Tan and Prasanna Venkatesh and Shulin Zhao and Anand Sivasubramaniam, *IoTRepair: Systematically Addressing Device Faults in Commodity IoT (Extended Paper)*, Technical Report arXiv:2002.07641, arXiv preprint, 2020.

Amit Kumar Sikder and Leonardo Babun and Z. Berkay Celik and Abbas Acar and Hidayet Aksu and Patrick McDaniel and Engin Kirda and Selcuk Uluagac, *KRATOS: Multi-User Multi-Device-Aware Access Control System for the Smart Home*, Technical Report arXiv:1911.10186, arXiv preprint, 2020.

Leonardo Babun and Z. Berkay Celik and Patrick McDaniel and Selcuk Uluagac, *Real-time Analysis of Privacy-(un)aware IoT Applications*, Technical Report arXiv:1911.10461, arXiv preprint, 2019.

Dan Boneh and Andrew J. Grotto and Patrick McDaniel and Nicolas Papernot, *How Relevant is the Turing Test in the Age of Sophisbots?*, Technical Report arXiv:1909.00056, arXiv preprint, 2019.

Chun-Ming Lai and Xiaoyun Wang and Jon W. Chapman and Yu-Cheng Lin and Yu-Chang Ho and Felix Wu and Patrick McDaniel and Hasan Cam, *More or Less? Predict the Social Influence of Malicious URLs on Social Media*, Technical Report arXiv:1812.02978, arXiv preprint, 2018.

Dang Tu Nguyen and Chengyu Song and Zhiyun Qian and Srikanth V. Krishnamurthy and Edward J. M. Colbert and Patrick McDaniel, *IoTSan: Fortifying the Safety of IoT Systems*, Technical Report arXiv:1810.09551, arXiv preprint, 2018.

Z. Berkay Celik and Earlence Fernandes and Eric Pauley and Gang Tan and Patrick McDaniel, *Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities*, Technical Report arXiv:1809.06962, arXiv preprint, 2018.

Giuseppe Petracca and Jens Grossklags and Patrick McDaniel and Trent Jaeger, *Regulating Access to System Sensors in Cooperating Programs*, Technical Report arXiv:1808.05579, arXiv preprint, 2018.

Z. Berkay Celik and Patrick McDaniel and Gang Tan, *Soteria: Automated IoT Safety and Security Analysis*, Technical Report arXiv:1805.08876, arXiv preprint, 2018.

Nicolas Papernot and Patrick McDaniel, *Deep k-Nearest Neighbors: Towards Confident, Interpretable and Robust Deep Learning*, Technical Report arXiv:1803.04765, arXiv preprint, 2018.

Z. Berkay Celik and Leonardo Babun and Amit Kumar Sikder and Hidayet Aksu and Gang Tan and Patrick McDaniel and Selcuk Uluagac, *Sensitive Information Tracking in Commodity IoT*, Technical Report arXiv:1802.08307, arXiv preprint, 2018.

Chun-Ming Lai and Xiaoyun Wang and Yunfeng Hong and Yu-Cheng Lin and Felix Wu and Patrick McDaniel and Hasan Cam, *Attacking Strategies and Temporal Analysis Involving Facebook Discussion Groups*, Technical Report arXiv:1802.04500, arXiv preprint, 2017.

Abbas Acar and Z. Berkay Celik and Hidayet Aksu and Selcuk Uluagac and Patrick McDaniel, *Achieving Secure and Differentially Private Computations in Multiparty Settings*, Technical Report arXiv:1707.01871, arXiv preprint, 2017.

Florian Tramer and Alexey Kurakin and Nicolas Papernot and Ian Goodfellow and Dan Boneh and Patrick McDaniel, *Ensemble Adversarial Training: Attacks and Defenses*, Technical Report arXiv:1705.07204, arXiv preprint, 2017.

Nicolas Papernot and Patrick McDaniel, *Extending Defensive Distillation*, Technical Report arXiv:1705.05264, arXiv preprint, 2017.

Florian Tramer and Nicolas Papernot and Ian Goodfellow and Dan Boneh and Patrick McDaniel, *The Space of Transferable Adversarial Examples*, Technical Report arXiv:1704.03453, arXiv preprint, 2017.

Z. Berkay Celik and Hidayet Aksu and Abbas Acar and Ryan Sheatsley and Selcuk Uluagac and Patrick McDaniel, *Curie: Policy-based Secure Data Exchange*, Technical Report arXiv:1702.08342, arXiv preprint, 2017.

Kathrin Grosse and Praveen Manoharan and Nicolas Papernot and Michael Backes and Patrick McDaniel, *On the (Statistical) Detection of Adversarial Examples*, Technical Report arXiv:1702.06280, arXiv preprint, 2017.

Z. Berkay Celik and David Lopez-Paz and Patrick McDaniel, *Patient-Driven Privacy Control through Generalized Distillation*, Technical Report arXiv:1611.08648, arXiv preprint, 2017.

Nicolas Papernot and Patrick McDaniel and Arunesh Sinha and Michael Wellman, *Towards the Science of Security and Privacy in Machine Learning*, Technical Report arXiv:1611.03814, arXiv preprint, 2016.

Nicolas Papernot and Ian Goodfellow and Ryan Sheatsley and Reuben Feinman and Patrick McDaniel, *cleverhans v1.0.0: an adversarial machine learning library*, Technical Report arXiv:1610.0076, arXiv preprint, 2016.

Nicolas Papernot and Patrick McDaniel, *On the Effectiveness of Defensive Distillation*, Technical Report arXiv:1607.05113, arXiv preprint, 2016.

Kathrin Grosse and Nicolas Papernot and Praveen Manoharan and Michael Backes and Patrick McDaniel, *Adversarial Perturbations Against Deep Neural Networks for Malware Classification*, Technical Report arXiv:1606.04435, arXiv preprint, 2016.

Nicolas Papernot and Patrick McDaniel and Ian Goodfellow, *Transferability in Machine Learning: from Phenomena to Black-Box Attacks using Adversarial Samples*, Technical Report arXiv:1605.07277, arXiv preprint, 2016.

Nicolas Papernot and Patrick McDaniel and Ananthram Swami and Richard Harang, *Crafting Adversarial Input Sequences for Recurrent Neural Networks*, Technical Report arXiv:1604.08275, arXiv preprint, 2016.

Z. Berkay Celik and Patrick McDaniel and Rauf Izmailov and Nicolas Papernot and Ryan Sheatsley and Raquel Alvarez and Ananthram Swami, *Detection under Privileged Information*, Technical Report arXiv:1603.09638,

arXiv preprint, 2016.

Vaibhav Rastogi and Drew Davidson and Lorenzo De Carli and Somesh Jha and Patrick McDaniel, *Towards Least Privilege Containers with Cimplifier*, Technical Report arXiv:1602.08410, arXiv preprint, 2016.

Nicolas Papernot and Patrick McDaniel and Ian Goodfellow and Somesh Jha and Z. Berkay Celik and Ananthram Swami, *Practical Black-Box Attacks against Machine Learning*, Technical Report arXiv:1602.02697, arXiv preprint, 2016.

Nicolas Papernot and Patrick McDaniel and Somesh Jha and Matthew Fredrikson and Z. Berkay Celik and Ananthram Swami, *The Limitations of Deep Learning in Adversarial Settings*, Technical Report arXiv:1511.07528, arXiv preprint, 2015.

Nicolas Papernot and Patrick McDaniel and Xi Wu and Somesh Jha and Ananthram Swami, *Distillation as a Defense to Adversarial Perturbations against Deep Neural Networks*, Technical Report arXiv:1511.04508, arXiv preprint, 2015.

Alexander Kott and Ananthram Swami and Patrick McDaniel, *Six Potential Game-Changers in Cyber Security: Towards Priorities in Cyber Science and Engineering*, Technical Report arXiv:1511.00509, arXiv preprint, 2015.

Li Li and Alexandre Bartel and Jacques Klein and Yves Le Traon and Steven Arzt and Siegfried Rasthofer and Eric Bodden and Damien Ochteau and Patrick McDaniel, *I know what leaked in your pocket: uncovering privacy leaks on Android Apps with Static Taint Analysis*, Technical Report arXiv:1404.7431, arXiv preprint, 2014.

Devin Pohly and Patrick McDaniel, *Modeling Privacy and Tradeoffs in Multichannel Secret Sharing Protocols*, Technical Report NAS-TR-0188-2016, Institute of Networking and Security Research, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, January, 2016.

Nicolas Papernot and Patrick McDaniel and Somesh Jha and Matthew Fredrikson and Z. Berkay Celik and Ananthram Swami, *The Limitations of Deep Learning in Adversarial Settings*, Technical Report NAS-TR-0172-2014, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, October, 2016.

Wenhui Hu and Damien Ochteau and Patrick McDaniel and Peng Liu, *Duet: Library Integrity Verification for Android Applications*, Technical Report NAS-TR-0172-2014, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2016.

Devin Pohly and Stephen McLaughlin and Patrick McDaniel and Kevin Butler, *Hi-Fi: Collecting High-Fidelity Whole-System Provenance*, Technical Report NAS-TR-0160-2012, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2016.

Damien Ochteau and Somesh Jha and Patrick McDaniel, *Retargeting Android Applications to Java Bytecode*, Technical Report NAS-TR-0150-2011, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, September, 2011.

Stephen McLaughlin and Patrick McDaniel, *Protecting Consumer Privacy from Electric Load Monitoring*, Technical Report NAS-TR-0147-2011, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, March, 2011.

William Enck and Patrick McDaniel, *Federated Information Flow Control for Mobile Phones*, Technical Report NAS-TR-0136-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, July, 2010.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Kells: A Protection Framework for Portable Data*, Technical Report NAS-TR-0134-2010, Network and Security Research Center, Department of Computer Science

and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2010.

Stephen McLaughlin and Dmitry Podkuiko and Adam Delozier and Sergei Miadzvezhanka and Patrick McDaniel, *Multi-vendor Penetration Testing in the Advanced Metering Infrastructure*, Technical Report NAS-TR-0133-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2010.

Machigar Ongtang and Kevin Butler and Patrick McDaniel, *Porscha: Policy Oriented Secure Content Handling in Android*, Technical Report NAS-TR-0132-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2010.

Joshua Schiffman and Thomas Moyer and Hayawardh Vijayakumar and Trent Jaeger and Patrick McDaniel, *Seeding Clouds with Trust Anchors*, Technical Report NAS-TR-0127-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, April, 2010.

William Enck and Machigar Ongtang and Patrick McDaniel, *TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*, Technical Report NAS-TR-0120-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2010.

Joshua Schiffman and Thomas Moyer and Christopher Shal and Trent Jaeger and Patrick McDaniel, *Justifying Integrity Using a Virtual Machine Verifier*, Technical Report NAS-TR-0119-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, August, 2010.

Machigar Ongtang and Stephen McLaughlin and William Enck and Patrick McDaniel, *Semantically Rich Application-Centric Security in Android*, Technical Report NAS-TR-0116-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2010.

Stephen McLaughlin and Dmitry Podkuiko and Patrick McDaniel, *Energy Theft in the Advanced Metering Infrastructure*, Technical Report NAS-TR-0115-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2010.

Kevin Butler and Stephen McLaughlin and Thomas Moyer and Joshua Schiffman and Patrick McDaniel and Trent Jaeger, *Firma: Disk-Based Foundations for Trusted Operating Systems*, Technical Report NAS-TR-0114-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, April, 2010.

William Enck and Machigar Ongtang and Patrick McDaniel, *On Lightweight Mobile Phone App Certification*, Technical Report NAS-TR-0113-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, April, 2010.

Patrick Traynor and Michael Lin and Machigar Ongtang and Vikhyath Rao and Thomas La Porta and Patrick McDaniel, *On Cellular Botnets: Measuring the Impact of Malicious Devices on the Network Core*, Technical Report NAS-TR-0110-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, March, 2010.

Boniface Hicks and Sandra Rueda and Yogesh Sreenivasan and Guruprasad Jakka and David King and Trent Jaeger and Patrick McDaniel, *An Architecture for Enforcing End-to-End Security Over Web Applications*, Technical Report NAS-TR-0104-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, January, 2009.

Joshua Schiffman and Thomas Moyer and Christopher Shal and Trent Jaeger and Patrick McDaniel, *No Node Is an Island: Shamon Integrity Monitoring Approach*, Technical Report NAS-TR-0103-2009, Network and Security

Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2009.

Patrick Traynor and Michael Lin and Machigar Ongtang and Vikhyath Rao and Trent Jaeger and Thomas La Porta and Patrick McDaniel, *On Cellular Botnets: Measuring the Impact of Malicious Devices on the Network Core*, Technical Report NAS-TR-0099-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, November, 2008.

Kevin Butler and Stephen McLaughlin and Thomas Moyer and Patrick McDaniel and Trent Jaeger, *SwitchBlade: Policy-Driven Disk Segmentation*, Technical Report NAS-TR-0098-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, November, 2008.

Thomas Moyer and Kevin Butler and Joshua Schiffman and Patrick McDaniel and Trent Jaeger, *Scalable Asynchronous Web Content Attestation*, Technical Report NAS-TR-0095-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, September, 2008.

William Enck and Machigar Ongtang and Patrick McDaniel, *Automated Cellphone Application Certification in Android (or) Mitigating Phone Software Misuse Before It Happens*, Technical Report NAS-TR-0094-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, September, 2008.

Boniface Hicks and Sandra Rueda and Luke St. Clair and Trent Jaeger and Patrick McDaniel, *A Logical Specification and Analysis for SELinux MLS Policy*, Technical Report NAS-TR-0091-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, July, 2008.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Rootkit-Resistant Disks*, Technical Report NAS-TR-0089-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, April, 2008.

Patrick Traynor and Joshua Schiffman and Thomas La Porta and Patrick McDaniel and Abhrajit Ghosh and Farooq Anjum, *Constructing Secure Localization Systems with Adjustable Granularity*, Technical Report NAS-TR-0084-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, December, 2007.

Stephen McLaughlin and Kevin Butler and William Enck and Patrick McDaniel, *Genbd - A Generic Block Device*, Technical Report NAS-TR-0082-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, November, 2007.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Non-Volatile Memory and Disks: Avenues for Policy Architectures*, Technical Report NAS-TR-0074-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2007.

William Enck and Sandra Rueda and Joshua Schiffman and Yogesh Sreenivasan and Luke St. Clair and Trent Jaeger and Patrick McDaniel, *Protecting Users From "Themselves"*, Technical Report NAS-TR-0073-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2007.

Dhananjay Bapat and Kevin Butler and Patrick McDaniel, *Towards Automated Privilege Separation*, Technical Report NAS-TR-0071-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, May, 2007.

Patrick Traynor and Kevin Butler and William Enck and Patrick McDaniel, *Realizing Massive-Scale Conditional Access Systems Through Attribute-Based Cryptosystems*, Technical Report NAS-TR-0070-2007, Network

and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, May, 2007.

Luke St. Clair and Joshua Schiffman and Trent Jaeger and Patrick McDaniel, *Establishing and Sustaining System Integrity via Root of Trust Installation*, Technical Report NAS-TR-0067-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, April, 2007.

Boniface Hicks and David King and Patrick McDaniel, *Jifclipse: Development Tools for Security-Typed Language*, Technical Report NAS-TR-0065-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, April, 2007.

William Enck and Patrick McDaniel and Trent Jaeger, *Protecting User Files by Reducing Application Access*, Technical Report NAS-TR-0063-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2007.

Boniface Hicks and Sandra Rueda and Trent Jaeger and Patrick McDaniel, *A Logical Specification and Analysis for SELinux MLSPolicy*, Technical Report NAS-TR-0058-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, January, 2007.

Boniface Hicks and Sandra Rueda and Trent Jaeger and Patrick McDaniel, *From Trusted to Secure: Building and Executing Applications that Enforce System Security*, Technical Report NAS-TR-0061-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, January, 2007.

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

Patrick Traynor and Vikhyath Rao and Trent Jaeger and Patrick McDaniel and Thomas La Porta, *From Mobile Phones to Responsible Devices*, Technical Report NAS-TR-0059-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, January, 2007.

Anusha Sriraman and Kevin Butler and Patrick McDaniel and Padma Raghavan, *Analysis of the IPv4 Address Space Delegation Structure*, Technical Report NAS-TR-0057-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, December, 2006.

Luke St. Clair and Joshua Schiffman and Trent Jaeger and Patrick McDaniel, *Sum of the Parts: Composing Trust from Validation Primitives*, Technical Report NAS-TR-0056-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, November, 2006.

Sophie Qiu and Patrick McDaniel and Fabian Monrose, *Toward Valley-Free Inter-domain Routing*, Technical Report NAS-TR-0054-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, October, 2006.

Boniface Hicks and Sandra Rueda and Trent Jaeger and Patrick McDaniel, *Integrating SELinux with Security-typed Languages*, Technical Report NAS-TR-0052-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, October, 2006.

Patrick Traynor and William Enck and Patrick McDaniel and Thomas La Porta, *Mitigating Attacks on Open Functionality in SMS-Capable Networks*, Technical Report NAS-TR-0051-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, October, 2006.

USA, October, 2006.

Patrick Traynor and Kevin Butler and William Enck and Kevin Borders and Patrick McDaniel, *malnets: Large-Scale Malicious Networks via Compromised Wireless Access Points*, Technical Report NAS-TR-0048-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, September, 2006.

Boniface Hicks and Sandra Rueda and Trent Jaeger and Patrick McDaniel, *Breaking Down the Walls of Mutual Distrust: Security-typed Email Using Labeled IPsec*, Technical Report NAS-TR-0049-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, September, 2006.

Sunam Ryu and Kevin Butler and Patrick Traynor and Patrick McDaniel, *Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems*, Technical Report NAS-TR-0043-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, August, 2006.

Wesam Lootah and William Enck and Patrick McDaniel, *TARP: Ticket-based Address Resolution Protocol (extended version)*, Technical Report NAS-TR-0046-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, August, 2006.

Patrick McDaniel, *Understanding Equivalence in High-Level and Information Flow Policy*, Technical Report NAS-TR-0042-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, July, 2006.

Trent Jaeger and Patrick McDaniel and Luke St. Clair and Ramon Caceres and Reiner Sailer, *Shame on Trust in Distributed Systems*, Technical Report RC239664 (W0605-129), IBM Research Division, Yorktown Heights, NY, May, 2006.

Lisa Johansen and Kevin Butler and Michael Rowell and Patrick McDaniel, *Email Communities of Interest*, Technical Report NAS-TR-0040-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, May, 2006.

Boniface Hicks and Kiyam Ahmadizadeh and Patrick McDaniel, *From Languages to Systems: Understanding Practical Application Development in Security-typed Languages*, Technical Report NAS-TR-0035-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, April, 2006.

Boniface Hicks and David King and Patrick McDaniel and Michael Hicks, *Trusted Declassification: High-level policy for a security-typed language*, Technical Report NAS-TR-0033-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, March, 2006.

Matthew Pirretti and Patrick Traynor and Patrick McDaniel and Brent Waters, *Secure Attribute-Based Systems*, Technical Report NAS-TR-0028-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2006.

William Enck and Kevin Butler and Thomas Richardson and Patrick McDaniel, *Securing Non-Volatile Main Memory*, Technical Report NAS-TR-0029-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2006.

Luke St. Clair and Lisa Johansen and William Enck and Matthew Pirretti and Patrick Traynor and Patrick McDaniel and Trent Jaeger, *Password Exhaustion: Predicting the End of Password Usefulness*, Technical Report NAS-TR-0030-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2006.

Heesook Choi and Patrick McDaniel and Thomas La Porta, *Privacy Preserving Communication in MANETs*, Technical Report NAS-TR-0031-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, December, 2005.

Matthew Pirretti and Vijaykrishnan Narayanan and PatrickMcDaniel and Bharat Madan, *SLAT: Secure Localization with Attack Tolerance*, Technical Report NAS-TR-0024-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, August, 2005.

Patrick Traynor and Michael Chien and Scott Weaver andBoniface Hicks and Patrick McDaniel, *Non-Invasive Methods for Host Certification*, Technical Report NAS-TR-0025-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, September, 2005.

Sophie Qiu and Patrick McDaniel and Fabian Monroe andAvi Rubin, *Characterizing Address Use Structure and Stabillity ofOrigin Advertizement in Interdomain Routing*, Technical Report NAS-TR-0018-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, July, 2005.

Hosam Rowaihy and William Enck and Patrick McDaniel andThomas La Porta, *Limiting Sybil Attacks in Structured Peer-to-Peer Networks*, Technical Report NAS-TR-0017-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, July, 2005.

Boniface Hicks and Patrick McDaniel and Ali Hurson, *Information Flow Control in Database Security: A CaseStudy for Secure Programming with Jif*, Technical Report NAS-TR-0011-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, April, 2005.

Wesam Lootah and William Enck and Patrick McDaniel, *TARP: Ticket-Based Address Resolution Protocol*, Technical Report NAS-TR-0010-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, June, 2005.

Patrick Traynor and Kevin Butler and William Enck andJennifer Plasterr and Scott Weaver and John van Bramer and PatrickMcDaniel, *Privacy-Preserving Web-Based Email*, Technical Report NAS-TR-0009-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, June, 2005.

William Enck and Patrick Traynor and Patrick McDaniel andThomas La Porta, *Exploiting Open Functionality in SMS-Capable Cellular Networks*, Technical Report NAS-TR-0007-2005, Network and Security Center, Department of Computer Science, Pennsylvania State University, May, 2005.

Boniface Hicks and David King and Patrick McDaniel, *Declassification with Cryptographic Functions in aSecurity-Typed Language*, Technical Report NAS-TR-0004-2005, Network and Security Center, Department of Computer Science, Pennsylvania State University, January, 2005.

William Aiello and Kevin Butler and Patrick McDaniel, *Path Authentication in Interdomain Routing*, Technical Report TR NAS-TR-0002-2004, Network and Security Center, Department of Computer Science and Engineering, Penn State University, November, 2004.

Dan Pei and William Aiello and Anna Gilbert and PatrickMcDaniel, *Origin Disturbances in BGP*, Technical Report TD-62TJJF8, AT&T Labs - Research, Florham Park, NJ, July, 2004.

Kevin Butler and Toni Farley and Patrick McDaniel andJennifer Rexford, *A Survey of BGP Security Issues and Solutions*, Technical Report TD-5UGJ33, AT&T Labs - Research, Florham Park, NJ, February, 2004.

Patrick McDaniel and Atul Prakash, *Securing Distributed Applications Using a Policy-based Approach*, Technical Report TD-5UDKVD, AT&T Labs - Research, Florham Park, NJ, December, 2003.

William Aiello and John Ioannidis and Patrick McDaniel, *Origin Authentication in Interdomain Routing*, Technical Report TD-5QHG2G, AT&T Labs - Research, Florham Park, NJ, August, 2003.

Eric Cronin and Sugih Jamin and Tal Malkin and Patrick McDaniel, *On the Performance, Feasibility, and Use of Forward Secure Signatures*, Technical Report TD-5QHGBK, AT&T Labs - Research, Florham Park, NJ, August, 2003.

Simon Byers and Lorrie Cranor and Eric Cronin and Dave Kormann and Patrick McDaniel, *Analysis of Security Vulnerabilities in the Movie Production and Distribution Process*, Technical Report TD-5N6SJ4, AT&T Labs - Research, Florham Park, NJ, August, 2003.

Patrick McDaniel, *On Context in Authorization Policy*, Technical Report TD-5JCJCK, AT&T Labs - Research, Florham Park, NJ, January, 2003.

Patrick McDaniel and Atul Prakash, *An Architecture for Security Policy Enforcement*, Technical Report TD-5C6JFV, AT&T Labs - Research, Florham Park, NJ, July, 2002.

Patrick McDaniel and Atul Prakash, *Methods and Limitations of Security Policy Reconciliation*, Technical Report TD57-PAW, AT&T Labs - Research, Florham Park, NJ, February, 2002.

Patrick McDaniel and Atul Prakash, *Ismene: Provisioning and Policy Reconciliation in Secure Group Communication*, Technical Report CSE-TR-438-00, Electrical Engineering and Computer Science, University of Michigan, December, 2000.

Patrick McDaniel and Atul Prakash, *Lightweight Failure Detection in Secure Group Communication*, Technical Report CSE-TR-428-00, Electrical Engineering and Computer Science, University of Michigan, June, 2000.

Patrick McDaniel and Atul Prakash, *Antigone: Implementing Policy in Secure Group Communication*, Technical Report CSE-TR-426-00, Electrical Engineering and Computer Science, University of Michigan, May, 2000.

Patrick McDaniel and Sugih Jamin, *Windowed Certificate Revocation*, Technical Report CSE-TR-413-99, Electrical Engineering and Computer Science, University of Michigan, November, 1999.

Patrick McDaniel and Atul Prakash and Peter Honeyman, *Antigone: A Flexible Framework for Secure Group Communication*, Technical Report 99-2, Center for Information Technology Integration, September, 1999.

Patrick McDaniel and Avi Rubin, *A Response to "Can We Eliminate Certificate Revocation Lists?"*, Technical Report 99.8.1, AT&T Labs - Research, Florham Park, NJ, August, 1999.

Andrew Adamson and Charles J. Antonelli and Kevin Coffman and Patrick McDaniel and Jim Rees, *Secure Distributed Virtual Conferencing: Multicast or Bust*, Technical Report 99-1, Center for Information Technology Integration, January, 1999.

Patrick McDaniel and Sugih Jamin, *Windowed Key Revocation in Public Key Infrastructures*, Technical Report CSE-TR-376-98, Electrical Engineering and Computer Science, University of Michigan, , 1998.

Patrick McDaniel and Sugih Jamin, *A Scalable Key Distribution Hierarchy*, Technical Report CSE-TR-366-98, Electrical Engineering and Computer Science, University of Michigan, , 1998.

Patrick McDaniel and Peter Honeyman and Atul Prakash, *Lightweight Secure Group Communication*, Technical Report 98-2, Center for Information Technology Integration, University of Michigan, April, 1998.

Wayne Zage and Delores Zage and Patrick McDaniel and IrshadKhan, *Evaluating Design Metrics on Large-Scale Software*, Technical Report SERC-TR-106-P, Software Engineering Resource Center, PurdueUniversity, September, 1991.

PUBLIC SPEAKING

The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, University of California, Los Angeles, Los Angeles, CA, December, 2023.

The Security of AI (what organizations need to know), TEDxUWMadison, Madison, WI, November, 2023.

The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, Michigan State University, Lansing, MI, November, 2023.

The Security of AI (what organizations need to know), Greater Madison Chamber of Commerce, Madison, WI, September, 2023.

Security's Role in Achieving Sustainability, Center for Sustainability and the Global Environment, Madison, WI, February, 2023.

Security's Role in Achieving Sustainability, 29th ACM Conference on Computer and Communications Security (CCS), Los Angeles, CA, November, 2022.

Security, Game Theory, and Their Role in Achieving Sustainability, Conference on Decision and Game Theory for Security, Pittsburgh, PA, October, 2022.

NSF Funding: Why, What and How, School of Computer, Data & Information Sciences, UW-Madison, Madison, WI, October, 2022.

Prognosticating the Future of IoT Security, 2022 IEEE SafeThings Workshop, San Francisco, CA, May, 2022.

The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, Temple University, Philadelphia, PA, March, 2022.

The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, CACR Security Speaker Series, Indiana University, Online, August, 2021.

The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, Robustness of AI Systems to Adversarial Attacks (RAISA3), Online, August, 2020.

The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, Computer Science Department, University of Wisconsin-Madison, Madison, WI, February, 2020.

The Challenges of Machine Learning in Adversarial Settings, Computer Science Department, Stonybrook University, Stonybrook, NY, December, 2019.

The Challenges of Machine Learning in Adversarial Settings, Cylab Security and Privacy Institute, Carnegie Mellon University, Pittsburgh, PA, December, 2019.

The Challenges of Machine Learning in Adversarial Settings, S2ERC, Ball State University, Muncie, IN, November, 2019.

The Challenges of Machine Learning in Adversarial Settings, Triangle Area Privacy and Security Day, Durham, NC, October, 2019.

AI-Cybersecurity Workshop Briefing to the NITRD and MLAI Subcommittees, NITRD and MLAI Subcommittees Quarterly Meeting, Washington, DC, July, 2019.

Workshop on the Security and Privacy of Machine Learning, Workshop on the Security and Privacy of Machine Learning, International Conference on Machine Learning, Long Beach, CA, June, 2019.

The Challenges of Machine Learning in Adversarial Settings, 2019 Subversion and Assurance of AI Workshop, US National Reconnaissance Office, Washington, DC, March, 2019.

The Challenges of Machine Learning in Adversarial Settings, National Science Foundation, Alexandria, VA, March, 2019.

Convergence of AI and IoT, Intelligence Community Studies Board, Division on Engineering and Physical Sciences, The National Academy of Sciences/Engineering, Washington, DC, February, 2019.

Tracing the Arc of Smartphone Application Security, Duke University, Durham, NC, February, 2019.

The Challenges of Machine Learning in Adversarial Settings, Department of Computer Science, University at Buffalo, Buffalo, NY, November, 2018.

The Challenges of Machine Learning in Adversarial Settings, Department of Computer Science, Purdue University, West Lafayette, Indiana, November, 2018.

The Challenges of Machine Learning in Adversarial Settings, Computer Science Department, Indiana University of Pennsylvania, Indiana, PA, October, 2018.

The Challenges of Machine Learning in Adversarial Settings, Penn State University Alumni Association, University Park, PA, September, 2018.

The Challenges of Machine Learning in Adversarial Settings, Department of Software and Information Systems, University of North Carolina at Charlotte, Charlotte, NC, February, 2018.

Tracing the Arc of Smartphone Application Security, School of Electrical and Computer Engineering, Georgia Tech University, Atlanta, GA, December, 2017.

Tracing the Arc of Smartphone Application Security, Department of Electrical Engineering and Computer Science, Ohio University, Athens, OH, October, 2017.

Attacks, Defenses, and Impacts of Machine Learning in Adversarial Settings, 2017 Conference on Security and Privacy in Communication Networks (SecureComm), Niagara Falls, Canada, October, 2017.

Attacks, Defenses, and Impacts of Machine Learning in Adversarial Settings, Celebrating 50 Years of Computer Science @ NC State, North Carolina State University, Raleigh, NC, October, 2017.

Tracing the Arc of Smartphone Application Security, Computer Science Department and the Electrical and Computer Engineering Department Seminar Series, Colorado State University, Fort Collins, CO, October, 2017.

Tracing the Arc of Smartphone Application Security, Rochester Institute of Technology, College of Computing and Information Sciences, Rochester, NY, September, 2017.

Tracing the Arc of Smartphone Application Security, University of Texas-Dallas, Department of Computer Science, Dallas, TX, May, 2017.

Tracing the Arc of Smartphone Application Security, 2017 ACM on International Workshop on Security And Privacy Analytics, Scottsdale, AZ, March, 2017.

Tracing the Arc of Smartphone Application Security, The Ohio State University, Department of Computer Science and Engineering, Columbus, OH, March, 2017.

Tracing the Arc of Smartphone Application Security, University of California-Irvine, Computer Science Department, Irvine, CA, March, 2017.

Tracing the Arc of Smartphone Application Security, Virginia Technical University, Department of Computer Science, Blacksburg, VA, March, 2017.

Tracing the Arc of Smartphone Application Security, 12th International Conference on Information Systems Security , Jaipur, India, December, 2016.

Tracing the Arc of Smartphone Application Security, University of Michigan, Ann Arbor, Ann Arbor, MI, November, 2016.

Machine Intelligence in Adversarial Settings, Developing a Normative Framework for Cyberwarfare, United States Naval Academy, Annapolis, MD, September, 2016.

Eight Years of Mobile Smartphone Security, University of Pittsburgh, Pittsburgh, PA, September, 2016.

Eight Years of Mobile Smartphone Security, New Jersey Institute of Technology, Newark, NJ, September, 2016.

Setting a Cyber-Security Baseline for Physical Systems: Terminology, Technologies, and Goals, Pacific Northwest Clean Water Association, webinar, August, 2016.

The Limitations of Machine Learning in Adversarial Settings, 25th International Conference on Computer Communication and Networks (ICCCN 2016), Waikoloa, HI, August, 2016.

Learning from Ourselves: Where are we and where can we go in mobile systems security?, Mobile Security Technologies (MOST) 2016 Workshop, IEEE Computer Society Security and Privacy Workshops, San Jose, CA, May, 2016.

Eight Years of Mobile Smartphone Security, Center for Secure and Dependable Systems (CSDS) Cybersecurity Symposium, Coeur d'Alene, April, 2016.

Eight Years of Mobile Smartphone Security, University of Idaho, Moscow, ID, April, 2016.

Army Installation 2035: Cyber Challenges and Opportunities, US Department of Defense, Arlington, VA, April, 2016.

The Limitations of Machine Learning in Adversarial Settings, Florida Institute on National Security Assured Autonomy Workshop, Fort Myers, FL, February, 2016.

SABOT: Specification-based Payload Generation for Programmable Logic Controllers, Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) , San Francisco, CA, February, 2016.

Seven Years of Mobile Smartphone Security, Computer and Information Sciences Department, Temple University, Philadelphia, PA, January, 2016.

Seven Years of Mobile Smartphone Security, Massachusetts Institute of Technology–Lincoln Labs, Lexington, MA, January, 2016.

Six Years of Mobile Smartphone Security, Information Trust Institute, University of Illinois at Urbana-Champaign, Urbana-Champaign, IL, September, 2015.

The Importance of Measurement and Decision Making to a Science of Security, 2015 IEEE Conference on Communications and Network Security, Florence, Italy, September, 2015.

The Importance of Measurement and Decision Making to a Science of Security, 3rd International Symposium on Resilient Cyber Systems, Philadelphia, PA, August, 2015.

Six Years of Mobile Smartphone Security, CISPA Distinguished Lecture Series, Max Planck Institute/Saarland University, Saarbrücken Germany, July, 2015.

Six Years of Mobile Smartphone Security, Technische Universität Darmstadt, Darmstadt Germany, July, 2015.

Estimating Attack Intent and Mission Impact From Detection Signals, Workshop on Cyber Attack Detection, Forensics and Attribution for Assessment of Mission Impact, NATO Science and Technology Organization, Information Systems Technology Panel, Istanbul, Turkey, June, 2015.

The Importance of Measurement and Decision Making to a Science of Security, 2015 Symposium And Bootcamp on the Science of Security (Hotsos), University of Illinois at Urbana-Champaign, April, 2015.

Security and Science of Agility, First ACM Workshop on Moving Target Defense (MTD 2014), Scottsdale, AZ, November, 2014.

Evaluating Mobile Smartphone Security: The First Five Years, Computer Science Colloquium Series, Harvard School of Engineering and Applied Sciences, Harvard University, Boston, MA, October, 2014.

A Secondary Internet Revolution: How the Smart Device has Changed the Information Security Landscape, IEEE New Technology Industry Seminar (NTIS '13), Everett, WA, August, 2013.

Geotargeting: Mobile Device Privacy and Security, National Academy of Sciences, Washington DC, February, 2013.

Authentication and Web Security, Security and Privacy in IT-EMTM 604 Guest Lecture, University of Pennsylvania, Philadelphia, PA, February, 2013.

The Realities of Voting: A Retrospective of Ten Years of Information Security and Electronic Voting Systems, 2012 Information Assurance Day, Computer Science Department, Indiana University of Pennsylvania, Indiana, PA, November, 2012.

Permission-based Application Governance; A Step Forward or Backward?, 26th Annual WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'12), Paris, France, July, 2012.

Evaluating Mobile Smartphone Security: The First Four Years, Carnegie Mellon University, Pittsburgh, PA, April, 2012.

Scalable Integrity-Guaranteed AJAX, The 14th Asia-Pacific Web Conference (APWeb), Kunming, China, April, 2012.

Evaluating Mobile Smartphone Application Security, Singapore Management University, Singapore, September, 2011.

Evaluating Mobile Smartphone Application Security, Computer Security Foundations Symposium, Florham Park, NJ, July, 2011.

Security Challenges and Solutions in Mobile Smartphone Applications, Computer Security Foundations Symposium, Domaine de l'Abbaye des Vaux de Cernay, France, June, 2011.

Security Challenges and Solutions in Mobile Smartphone Applications, Computer and Information Science Department, University of Oregon, Eugene, OR, April, 2011.

Identifying (and Addressing) Security and Privacy Issues in Smart Electric Meters, Center for Non-Linear Studies, Los Alamos, NM, February, 2011.

Security Challenges and Solutions in Mobile Smartphone Applications, Department of Software Information Systems College of Computing and Informatics, UNC Charlotte, Charlotte, NC, December, 2010.

Security Challenges and Solutions in Mobile Smartphone Applications, Computer Science Department, Indiana University of Pennsylvania, Indiana, PA, December, 2010.

Security Challenges and Solutions in Mobile Smartphone Applications, Computer Science Department, Georgetown University, Washington D.C., November, 2010.

Security Challenges and Solutions in Mobile Smartphone Applications, Networking and Security Research Center, Computer Science and Engineering, Pennsylvania State University, University Park, PA, October, 2010.

Security Challenges and Solutions in Mobile Smartphone Applications, Security Day Seminar, Penn State University, University Park, PA, October, 2010.

The Changing Vulnerability Landscape, Association for Computing Machinery, Penn State Student Chapter, University Park, PA, September, 2010.

The Changing Vulnerability Landscape, ExxonMobil, Falls Church, VA, March, 2010.

The Impact of Supply Chain on Information and Communications Technology Security, The 1st Workshop on Telecommunications Infrastructure Protection and Security, Honolulu, HI, December, 2000.

Energy Theft in the Advanced Metering Infrastructure, Networking and Security Research Center, Computer Science and Engineering, Pennsylvania State University, State College, PA, October, 2009.

Secure Provenance in High-End Computing Systems, NSF HECURA FSIO PI Meeting, Arlington, VA, August, 2009.

Missing Glue: Architectural Support for Security Annotations, National Science Foundation Security Driven Architecture Workshop, Arlington, VA, July, 2009.

Scalable Integrity-Justified Content Provenance, NSERC ISSNet Workshop, Ottawa, Canada, June, 2009.

Utility Grid Automation and Risk Management, Clean Technology Conference and Expo, Houston, Texas, May, 2009.

Scalable Integrity-Justified Content Provenance, Center for Applied Cybersecurity Research, Indiana University, Bloomington, IN, April, 2009.

Scalable Integrity-Justified Content Provenance, Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI, April, 2009.

What is Security, Dickenson Law School, Penn State University, State College, PA, April, 2009.

Scalable Integrity-Justified Content Provenance, Department of Computer Science and Engineering, Notre Dame University, South Bend, IN, April, 2009.

Electronic Voting: The Good, the Bad, and the Reality, Software Engineering Research Center Showcase, Muncie, IN, November, 2008.

Ohio Voting Systems Integrity: The EVEREST Report, Networking and Security Research Center, Computer Science and Engineering, Pennsylvania State University, State College, PA, October, 2008.

Data Provenance: Challenges and Technology, Cyber Physical System Security Forum, Cyber Security Research and Development Review, Washington DC, October, 2008.

System-Wide Information Flow Enforcement, NICIAR PI Meeting, Washington DC, September, 2008.

Presto: Configuration Management at Massive Scale, NSF Workshop on Assurable and Usable Security Configuration, George Mason University, Fairfax, VA, August, 2008.

Asymmetry in Performance and Security Requirements for I/O in High-end Computing, NSF HECURA FSIO PI Meeting, Arlington, VA, August, 2008.

Authentication and Web Security, Security and Privacy in IT-EMTM 604 Guest Lecture, University of Pennsylvania, Philadelphia, PA, May, 2008.

SPAM and SPAM Mitigation, Computer Science Department, St. Vincent's University, Latrobe, PA, April, 2008.

Phones, The Press, Research and Grad School ... or how to make trouble and have fun doing it, Computer Science Department, St. Vincent's University, Latrobe, PA, April, 2008.

Applications and Services in Telecommunications Networks, NSF Wireless Security Workshop, Georgia Institute of Technology, Atlanta, GA, March, 2008.

Vulnerabilities and Opportunities in SMS-Capable Cellular Networks, Computer Science Department, Carleton University, Ottawa, Canada, March, 2008.

Ohio Voting Systems Integrity: The EVEREST Report, Case-Western Reserve University, Cleveland, OH, February, 2007.

Ohio Voting Systems Integrity: The EVEREST Report, Ohio State University, Columbus, OH, February, 2007.

Ohio Voting Systems Integrity: The EVEREST Report, Ohio University, Athens, OH, February, 2007.

Ohio Voting Systems Integrity: The EVEREST Report, Miami University, Ohio, Oxford, OH, February, 2007.

Ohio Voting Systems Integrity: The EVEREST Report, Bowling Green State University, Bowling Green, OH, February, 2007.

Vulnerabilities and Opportunities in SMS-Capable Cellular Networks, Computer Science Department, Indiana University of Pennsylvania, Indiana, PA, September, 2007.

Asymmetry in Performance and Security Requirements for I/O in High-End Computing, HECIWG FSIO 2007 Workshop, NSF, Arlington, VA, August, 2007.

Toward Valley-Free Interdomain Routing, IEEE International Conference on Communications (ICC) 2007, Glasgow, Scotland, June, 2007.

Extending Developer Tools for Security-Typed Languages, Software Engineering Research Center Fall Showcase, West Lafayette, IN, June, 2007.

Open Functionality in SMS/Cellular Networks, Computer and Information Science, University of Oregon, Eugene, OR, May, 2007.

Open Functionality in SMS/Cellular Networks, Computer Security Symposium, St. Cloud State University, St. Cloud, MN, May, 2007.

Authentication and Web Security, Security and Privacy in IT-EMTM 604 Guest Lecture, University of Pennsylvania, Philadelphia, PA, April, 2007.

Grains of SANs: Building Storage Area Networks from Memory Spots, CISCO Remote Faculty Seminar, University Park, PA, April, 2007.

Grains of SANs: Building Storage Area Networks from Memory Spots, 2007 IEEE Security and Privacy Crystal Ball Workshop, Hawthorne, NY, January, 2007.

Password Exhaustion: Predicting the End of Password Usefulness, 2nd International Conference on Information Systems Security , Kolkata, India, December, 2006.

Privacy Preserving Web-based Email, 2nd International Conference on Information Systems Security, Kolkata, India, December, 2006.

Physical and Digital Convergence: Where the Internet is the Enemy, Eighth International Conference on Information and Communications Security (ICICS '06), Raleigh, NC, December, 2006.

Extending Developer Tools for Security-Typed Languages, Software Engineering Research Center Fall Showcase, Muncie, IN, November, 2006.

Open Functionality in SMS/Cellular Networks, Johns Hopkins University, Computer Science Department, Baltimore, MD, September, 2006.

Open Functionality in SMS/Cellular Networks, George Mason University, Computer Science Department, Fairfax, VA, September, 2006.

Exploiting Open Functionality in SMS-Capable Cellular Networks, Motorola Security Symposium, Itasca, IL, September, 2006.

IsleB: Testing Large Scale BGP Security in Replayable Network Environments, NSF/DETER Community Workshop, Arlington, VA, June, 2006.

BGPRV: A Library for Fast and Efficient Routing Data Manipulation, NSF/DETER Community Workshop, Arlington, VA, June, 2006.

JifClipse: Extending Developer Tools for Security-Typed Languages, Software Engineering Research Center Spring Showcase, Schaumburg, IL, June, 2006.

Trends in Security: Critical Engineering in the Large, Schlumberger InnovateIT! 2006, Cambridge, MA, May, 2006.

Information Flow Revisited: Software Engineering to Provable Security, Network Center of Excellence, Motorola Labs, Schaumburg, IL, May, 2006.

Authentication and Web Security, Security and Privacy in IT-EMTM 604 Guest Lecture, University of Pennsylvania, Philadelphia, PA, April, 2006.

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

Exploiting Open Functionality in SMS-Capable Cellular Networks, Computer Science Department, University of Virginia, Charlottesville, VA, January, 2006.

Software Engineering Tools for Security-Typed Languages: Using Eclipse to Make Secure Programming Practical, Software Engineering Research Center Showcase, Muncie, IN, November, 2005.

Exploiting Open Functionality in SMS-Capable Cellular Networks, AT&T IP Services Security Council, Middletown, NJ, October, 2005.

Exploiting Open Functionality in SMS-Capable Cellular Networks, Computer Science Department, Carnegie Mellon University, Pittsburgh, PA, October, 2005.

Exploiting Open Functionality in SMS-Capable Cellular Networks, Computer Science Department, Yale University, New Haven, CT, October, 2005.

Exploiting Open Functionality in SMS-Capable Cellular Networks, Computer Science Department, SUNY-Stony Brook, Stony Brook, NY, October, 2005.

Exploiting Open Functionality in SMS-Capable Cellular Networks, Networking and Security Research Center, Computer Science and Engineering, Pennsylvania State University, State College, PA, October, 2005.

IsleB: Trace Driven Modeling of Internet-Scale BGP Attacks and Countermeasures, 2nd Annual DETER/EMIST Workshop, Newport Beach, CA, September, 2005.

Critical Infrastructure Security through Provably Secure Network Mediation, 2nd Japan/US Workshop on Critical Information Infrastructure Protection (CIIP), Tokyo, Japan, June, 2005.

Extending Developer Tools for Security-typed Languages, Software Engineering Research Center Showcase, West Lafayette, IN, June, 2005.

Origin Authentication in Interdomain Routing, 2005 IEEE Communications Quality and Reliability (CQR) International Workshop, St. Petersburg, FL, April, 2005.

Analysis of Security Vulnerabilities in the Movie Production and Distribution Process, Messiah College, Senior Seminar Series, Grantham, PA, April, 2005.

Origin Authentication in Interdomain Routing, Intel Research, Folsom CA, April, 2005.

Key Distribution Strategies For Low-Power Wireless Networks, Network Center of Excellence, Motorola Labs, Schaumburg, IL, April, 2005.

Policy Evolution: Autonomic Environmental Security, Software Engineering Research Center Showcase, Muncie, IN, December, 2004.

Information Assurance for Enterprise Networks, BAE Systems, Networking Seminar, Reston, VA, November, 2004.

Origin Authentication in Interdomain Routing, Computer Science Department, Purdue University, West Lafayette, IN, October, 2004.

Origin Authentication in Interdomain Routing, Electrical Engineering and Computer Science Department, University of Michigan, Ann Arbor, MI, October, 2004.

Origin Authentication in Interdomain Routing, Computer Science Department, University of Wisconsin, Madison, MD, September, 2004.

Analysis of Security Vulnerabilities in the Movie Production and Distribution Process, Computer Science and Engineering Student Organization, University Park, PA, September, 2004.

Useless Metaphors? Why Specifying Policy is So Hard, Workshop on Usable Privacy and Security Software, Center for Discrete Mathematics and Theoretical Computer Science (DIMACS), New Brunswick, New Jersey, July, 2004.

Analysis of Security Vulnerabilities in the Movie Production and Distribution Process, Information Systems Research Seminar, Stern School of Business, New York University, New York, NY, April, 2004.

Analysis of Security Vulnerabilities in the MovieProduction and Distribution Process, Ball State University, Muncie, IN, April, 2004.

Origin Authentication in Interdomain Routing, Computer Science Department, University of Illinois, Champaign, IL, March, 2004.

Origin Authentication in Interdomain Routing, Computer Science and Engineering Department, University of Minnesota, Minneapolis, MN, March, 2004.

Origin Authentication in Interdomain Routing, Computer Science Department, Johns Hopkins University, Baltimore, MD, March, 2004.

Origin Authentication in Interdomain Routing, Department of Computer Science, University of Massachusetts - Amherst, Amherst, MA, March, 2004.

Origin Authentication in Interdomain Routing, Computer Science and Engineering Department, PennState University, University Park, PA, March, 2004.

Origin Authentication in Interdomain Routing, School of Electrical Engineering and Computer Science, Oregon State University, Corvallis, OR, February, 2004.

Origin Authentication in Interdomain Routing, Computer Science Department, Northwestern University, Evanston, IL, February, 2004.

Origin Authentication in Interdomain Routing, Computer Science Department, SUNY-Stony Brook, Stony Brook, NY, February, 2004.

Attack Profiling and Simulation in Interdomain Routing, P2INGS Quarterly Meeting, Tempe, AZ, February, 2004.

Analysis of Security Vulnerabilities in the MovieProduction and Distribution Process, AT&T Finance Lunch, Morristown, NJ, January, 2004.

Origin Authentication in Interdomain Routing, AT&T IP Security Conference, Middletown, NJ, November, 2003.

Origin Authentication in Interdomain Routing, 10th ACM Conference on Computer and Communications Security (CCS), Washington, DC, October, 2003.

Origin Authentication in Interdomain Routing, Computer Science Department, Stevens Institute of Technology, Hoboken, NJ, October, 2003.

Origin Authentication in Interdomain Routing, Computer Science Department, Arizona State University, Mesa, AZ, September, 2003.

Analysis of Security Vulnerabilities in the MovieProduction and Distribution Process, 31st Technology Policy Research Conference (TPRC), Arlington, VA, September, 2003.

On Context in Authorization Policy, 8th ACM Symposium on Access Control Models and Technologies, Como, Italy, June, 2003.

The Antigone Project, DARPA Principal Investigator Meeting, San Antonio, TX, January, 2003.

Methods and Limitations of Security Policy Reconciliation, 2002 IEEE Symposium on Security and Privacy, Oakland, CA, May, 2002.

Policy Management in Distributed Systems, Cigital, Washington, DC, April, 2002.

Antigone: Policy Management in Secure Group Communication, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, April, 2001.

Antigone: Policy Management in Secure Group Communication, Computer Science Department, University of Wisconsin, Madison, MD, April, 2001.

Antigone: Policy Management in Secure Group Communication, Computer Science Department, University of Maryland, College Park, MD, April, 2001.

Antigone: Policy Management in Secure Group Communication, Computer Science Department, University of North Carolina, Chapel Hill, NC, April, 2001.

Antigone: Policy Management in Secure Group Communication, Computer Science Department, Johns Hopkins University, Baltimore, MD, March, 2001.

Antigone: Policy Management in Secure Group Communication, AT&T Shannon Laboratory, Florham Park, NJ, February, 2001.

Antigone: Policy Management in Secure Group Communication, Telcordia Applied Research Laboratory, Morristown, NJ, February, 2001.

Policy Problem Area 3 - Overview and Requirements, Internet Engineering Task Force MSEC BOF, San Diego, CA, December, 2000.

Multicast Security Policy Requirements and Building Blocks, Quarterly Secure Multicast Research Group Meeting (SMuG), San Diego, CA, December, 2000.

Antigone: Implementing Policy in Secure Multiparty Communication, Systems Design and Implementation (SDI) / Laboratory for Computer Systems (LCS) seminar series, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, November, 2000.

Secure Group Communication in Antigone 2.0, 11th Annual IPoCSE Research Symposium, Ann Arbor, MI, October, 2000.

Antigone Secure Group Communication, Bi-Annual DARPA Visit, Software System Research Laboratory, Ann Arbor, MI, September, 2000.

Problem Area 3: Policy, Quarterly Secure Multicast Research Group Meeting (SMuG), Pittsburgh, PA, July, 2000.

Windowed Certificate Revocation, IEEE INFOCOM 2000, Tel Aviv, Israel, March, 2000.

A Response to 'Can We Eliminate Certificate Revocation Lists?', Financial Cryptography 2000, Anguilla, British West Indies, February, 2000.

Multicast Security Policy Definition, Quarterly Secure Multicast Research Group Meeting (SMuG), Washington, DC, November, 1999.

Antigone: A Flexible Framework for Secure Group Communication, Quarterly Secure Multicast Research Group Meeting (SMuG), NAI Labs, Baltimore, MD, September, 1999.

Antigone: A Flexible Framework for Secure Group Communication, 10th Annual IPoCSE Research Symposium, Ann Arbor, MI, September, 1999.

Antigone: A Flexible Framework for Secure Group Communication, 8th USENIX Security Symposium, Washington, DC, August, 1999.

Antigone: A Flexible Framework for Secure Group Communication, IBM Watson Security Seminar, Westchester County, NY, July, 1999.

Windowed Revocation in Public Key Infrastructures, Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI, September, 1998.

Scalable Key Distribution Hierarchy, 9th Annual IPoCSE Research Symposium, Ann Arbor, MI, March, 1998.

JavaLauncher Applet Platform, NASA, Kennedy Space Center Security Seminar, Kennedy Space Center, FL, January, 1998.

Secure High Performance Group Communication, Directed StudyDefense, Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI, September, 1997.