

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Gregory G. Raleigh
U.S. Patent No.: 8,639,811 Attorney Docket No.: 39843-0180IP1
Issue Date: January 28, 2014
Appl. Serial No.: 13/742,312
Filing Date: January 15, 2013
Title: AUTOMATED DEVICE PROVISIONING AND ACTIVATION

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: June 17, 2024

By: 
Patrick McDaniel, Ph.D.

Table of Contents

I.	ASSIGNMENT.....	4
II.	QUALIFICATIONS AND BACKGROUND INFORMATION.....	4
III.	OVERVIEW OF CONCLUSIONS FORMED	18
IV.	LEVEL OF ORDINARY SKILL IN THE ART.....	19
V.	LEGAL STANDARDS	20
	A. Terminology.....	20
	B. Legal Standards.....	21
	C. Anticipation.....	22
	D. Obviousness	22
VI.	MATERIALS CONSIDERED	28
VII.	TECHNOLOGY OVERVIEW.....	35
	A. Mobile Devices	35
	B. Policy-based Management.....	39
	C. Network Bandwidth Management.....	51
	D. Bandwidth Management Policy.....	54
VIII.	THE '811 PATENT.....	60
	A. Overview of the '811 Patent	60
	B. Prosecution History of the '811 Patent.....	61
IX.	OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES ..	62
	A. U.S. Pat. App. Pub. No. 2006/0039354 ("Rao")	63
	B. U.S. Pat. No. 8,400,491 ("Panpaliya")	71
	C. Rao-Panpaliya Combination.....	73
	D. U.S. Pat. No. 8,285,850 ("Jones")	77
	E. Rao-Jones Combination.....	81
	F. U.S. Pat. App. Pub. No. 2008/0162981 ("Jajoo")	93
	G. Rao-Jones-Jajoo Combination	95
	H. U.S. Pat. App. Pub. No. 2008/0080458 ("Cole")	100
	I. Rao-Jones-Cole Combination	103
	J. U.S. Pat. App. Pub. No. 2009/0207817 ("Montemurro")	106
	K. Rao-Montemurro Combination	108
	L. U.S. Pat. App. Pub. No. 2009/0185527 ("Akhtar").....	111
	M. Rao-Akhtar Combination.....	112
	N. U.S. Pat. App. Pub. No. 2009/0228951 ("Ramesh").....	116
	O. Rao-Ramesh Combination.....	118
	P. U.S. Pat. No. 5,987,611 ("Freund").....	121

Q. Rao-Freund Combination	124
R. U.S. Pat. App. Pub. No. 2010/0281154 (“Bedi”)	129
S. Rao-Freund-Bedi Combination	130
T. U.S. Pat. App. Pub. No 2007/0032230 (“Pregont”)	133
U. Rao-Jones-Pregont Combination	137
X. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE ‘811 CLAIMS UNPATENTABLE	141
A. Ground 1A: Rao renders claims 1, 3, 6, 8-11, 14 and 19-20 obvious .	141
B. Ground 1B: Rao-Panpaliya renders claim 2 obvious	185
C. Ground 1C: Rao-Jones renders claims 4, 13, 21, 23, 25 obvious.....	186
D. Ground 1D: Rao-Jones-Jajoo render claims 17 obvious	198
E. Ground 1E: Rao-Jones-Cole renders claim 22 obvious.....	201
F. Ground 1F: Rao-Montemurro renders claim 5 obvious	202
G. Ground 1G: Rao-Akhtar renders claim 7 obvious.....	204
H. Ground 1H: Rao-Ramesh renders 18 obvious	208
I. Ground 1I: Rao-Freund renders claims 12, 15-16, and 26-27, 29-30 obvious	211
J. Ground 1J: Rao-Freund-Bedi renders claim 28 obvious.....	217
K. Ground 2: Rao-Pregont-Jones renders claims 1, 24 obvious	218
XI. CONCLUSION.....	222

I. ASSIGNMENT

1. I have been retained on behalf of Samsung Electronics Co., Ltd. (“Samsung”) to offer technical opinions related to 8,639,811 (“the ’811 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 ’811 patent.
2. I have been asked to provide my independent analysis of the ’811 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 ’811 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 ’811 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 [INSERT]; my experience in teaching those subjects; and my experience in working with others involved in those fields. In addition, I have analyzed the following publications and materials, in addition to other materials I cite in my declaration:
18. I have reviewed the '811 patent (SAMSUNG-1001), and relevant excerpts of the prosecution history (SAMSUNG-1002) of the '811 patent. Among various textbooks, documents, and publications, I have also reviewed the following prior art references:
 - SAMSUNG-1005 U.S. Pat. App. Pub. No. 2006/0039354 ("Rao")

- SAMSUNG-1006 U.S. Pat. No. 8,285,850 (“Jones”)
- SAMSUNG-1007 U.S. Pat. No. 8,400,491 (“Panpaliya”)
- SAMSUNG-1008 U.S. Pat. App. Pub. No. 2009/0207817
 (“Montemurro”)
- SAMSUNG-1009 U.S. Pat. App. Pub. No. 2009/0185527
 (“Akhtar”)
- SAMSUNG-1010 U.S. Pat. App. Pub. No. 2008/0162981 (“Jajoo”)
- SAMSUNG-1011 U.S. Pat. App. Pub. No. 2009/0228951
 (“Ramesh”)
- SAMSUNG-1012 U.S. Pat. App. Pub. No 2007/0032230
 (“Pregont”)
- SAMSUNG-1013 U.S. Pat. No. 5,987,611 (“Freund”)
- SAMSUNG-1019 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-1020 IETF RFC 791, Internet Protocol, September 1981, downloaded from the internet at <https://www.ietf.org/rfc/rfc791.txt> on July 28, 2023
- SAMSUNG-1021 IETF RFC 5246, The Transport Layer Security (TLS) Protocol, version 1.2, August 2008, downloaded from the internet at <https://datatracker.ietf.org/doc/html/rfc5246> on May 9, 2024
- SAMSUNG-1022 Internet connection speed recommendations, downloaded from the Internet at <https://help.netflix.com/en/node/306> on April 29, 2024. (“Netflix”)
- SAMSUNG-1023 Apostolopoulos, et al., 2002. Video streaming: Concepts, algorithms, and systems. HP Laboratories, report HPL-2002-260, pp.2641-8770. (“Apostolopoulos”)
- SAMSUNG-1024 U.S. Pat. App. Pub. No. 2006/0282566 (“Virdi”)
- SAMSUNG-1025 U.S. Pat. App. Pub. No. 2005/0080904 (“Green”)

- SAMSUNG-1026 IETF RFC 793, TRANSMISSION CONTROL PROTOCOL, September 1981, downloaded from the internet at <https://datatracker.ietf.org/doc/html/rfc793> on April 24, 2024. (“TCP”)
- SAMSUNG-1027 U.S. Pat. App. Pub. No. 20070121615 (“Weill”)
- SAMSUNG-1029 U.S. Pat. App. Pub. No. 2008/0080458 (“Cole”)
- SAMSUNG-1030 U.S. Pat. App. Pub. No. 2010/0281154 (“Bedi”)
- SAMSUNG-1031 Lobo, et. al., (1999). A policy description language. AAAI/IAAI, 1999, 291-298. (“Lobo”)
- SAMSUNG-1032 Verma, et. al., (2002). Policy-based management of content distribution networks. IEEE network, 16(2), 34-39. (“Verma”)
- SAMSUNG-1034 Banchs, et. al., Distributed weighted fair queuing in 802.11 wireless LAN, 2002 IEEE International Conference on Communications, Conference Proceedings. ICC 2002 pp. 3121-3127), 2002 (“Banchs”)

- SAMSUNG-1035 Wu, et. al., 2001. Scalable video coding and transport over broadband wireless networks. Proceedings of the IEEE, 89(1), pp.6-20.
- SAMSUNG-1036 IETF RFC 2205, Resource ReSerVation Protocol (RSVP), version 1 Functional Specification, September 1997, downloaded from the internet at <https://datatracker.ietf.org/doc/html/rfc2205> on May 16, 2024
- SAMSUNG-1037 Excerpts, Computer Networks, Fourth Edition, by Andrew Tanenbaum, Prentice Hall, 2003
- SAMSUNG-1038 U.S. Pat. App. Pub. No. 2007/0258459 (“Smith”)
- SAMSUNG-1039 Agrawal, et. al., 2005. Policy-based management of networked computing systems. IEEE Communications Magazine, 43(10), pp.69-75 (“Agrawal”)
- SAMSUNG-1041 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-1042 Reeder, et. al., 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.
- SAMSUNG-1043 Mansour, et al., 2001. Jitter control in QoS networks. IEEE/ACM Transactions On Networking, 9(4), pp.492-502.
- SAMSUNG-1044 Westerinen, et al., IETF RFC 3198, Terminology for Policy-Based Management, November 2001, downloaded from the Internet on May 27, 2024.
- SAMSUNG-1045 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-1046 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-1047 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-1048 Simplified Policy Language (CIM-SPL).
Document Number DSP0231, version, 1. (“CIM-SPL”)
- SAMSUNG-1049 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-1050 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-1051 U.S. Pat. App. Pub. No. 2008/0122796 (“Jobs”)
 - SAMSUNG-1052 Grossman, Invention of the year: The iPhone.
Time Magazine Online, 1, downloaded from the internet at
https://content.time.com/time/specials/2007/article/0,28804,1677329_1678542_1677891,00.html on May 28, 2024.
 - SAMSUNG-1053 Excerpts, Telcom Dictionary, Althos Publishing, 2007.
 - SAMSUNG-1054 U.S. Pat. App. Pub. No. 2008/0002652.
 (“Gupta”)
 - SAMSUNG-1055 U.S. Pat. No. 8,019,868 (“Rao-2”)
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 ’811 patent at the time of the earliest possible priority date of the ’811 patent, and I have done so during my review of these materials. I have been informed by Counsel to use the filing date January 28, 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 '811 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 '811 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 of all of the considered materials and my personal experience. 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, 3, 6, 8, 10-11, 14, and 19-20 obvious.
- Ground 1B renders claim 2 obvious.
- Ground 1C renders claims 4, 13, 21, 23, 25 obvious.

- Ground 1D renders 17 claim obvious.
 - Ground 1E renders 22 claim obvious.
 - Ground 1F renders 5 claim obvious.
 - Ground 1G renders 7 claim obvious.
 - Ground 1H renders 18 claim obvious.
 - Ground 1I renders claims 12, 15-16, 26-27, 29-30 obvious.
 - Ground 1J renders claim 28 obvious.
 - Ground 2 renders claims 1, 24 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 ‘811 patent in Section X.

IV. LEVEL OF ORDINARY SKILL IN THE ART

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

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 be given their plain meaning unless that meaning is inconsistent with the patent specification or the patent's history of examination before the Patent Office. Counsel has also informed me, and I

understand that, the words of the claims should be interpreted as they would have been interpreted by one of ordinary skill at the time of the invention was made (not today). The '811 patent was filed January 15, 2013, and claims priority to many provisional applications, the earliest of which was filed 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 '811 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.

C. 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).

D. 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. MATERIALS CONSIDERED

45. My analysis and conclusions set forth in this declaration are based on my educational background and experiences in the field (*see* Section II). Based on my knowledge and experience, I believe that I am considered to be an expert in the field. Also, based on my knowledge and experience, I understand and know of the capabilities of persons of ordinary skill in the field around 2009, and I taught, participated in organizations, and worked closely with many such persons in the field during that time frame.
46. As part of my independent analysis for this declaration, I have considered the following: the background knowledge/technologies that were commonly known to persons of ordinary skill in this art during the time before the earliest claimed priority date for the '811 patent; my own knowledge and experiences gained from my work experience in the field of the '811 patent and related disciplines; and my experience in working with others involved in this field and related disciplines.

47. In addition, I have analyzed the following publications and materials:

- SAMSUNG-1001 U.S. Patent No. 8,639,811 to Raleigh (“the ’811 Patent”)
- SAMSUNG-1002 Excerpts from the Prosecution History of the ’811 Patent (“the Prosecution History”)
- SAMSUNG-1005 U.S. Pat. App. Pub. No. 2006/0039354 (“Rao”)
- SAMSUNG-1006 U.S. Pat. No. 8,285,850 (“Jones”)
- SAMSUNG-1007 U.S. Pat. No. 8,400,491 (“Panpaliya”)
- SAMSUNG-1008 U.S. Pat. App. Pub. No. 2009/0207817 (“Montemurro”)
- SAMSUNG-1009 U.S. Pat. App. Pub. No. 2009/0185527 (“Akhtar”)
- SAMSUNG-1010 U.S. Pat. App. Pub. No. 2008/0162981 (“Jajoo”)
- SAMSUNG-1011 U.S. Pat. App. Pub. No. 2009/0228951 (“Ramesh”)
- SAMSUNG-1012 U.S. Pat. App. Pub. No 2007/0032230 (“Pregont”)
- SAMSUNG-1013 U.S. Pat. No. 5,987,611 (“Freund”)
- SAMSUNG-1014 U.S. Pat. App. Pub. No. 2009/0116415 (“Kashima”)

- SAMSUNG-1017 First Amended Complaint, *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al.*, 2:22-cv-00422, E.D. Tex., November 30, 2022
- SAMSUNG-1019 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-1020 IETF RFC 791, Internet Protocol, September 1981, downloaded from the internet at <https://www.ietf.org/rfc/rfc791.txt> on July 28, 2023
- SAMSUNG-1021 IETF RFC 5246, The Transport Layer Security (TLS) Protocol, version 1.2, August 2008, downloaded from the internet at <https://datatracker.ietf.org/doc/html/rfc5246> on May 9, 2024
- SAMSUNG-1022 Internet connection speed recommendations, downloaded from the Internet at <https://help.netflix.com/en/node/306> on April 29, 2024. (“Netflix”)
- SAMSUNG-1023 Apostolopoulos, et al., 2002. Video streaming: Concepts, algorithms, and systems. HP Laboratories, report HPL-2002-260, pp.2641-8770. (“Apostolopoulos”)

- SAMSUNG-1024 U.S. Pat. App. Pub. No. 2006/0282566 (“Virdi”)
- SAMSUNG-1025 U.S. Pat. App. Pub. No. 2005/0080904 (“Green”)
- SAMSUNG-1026 IETF RFC 793, TRANSMISSION CONTROL
PROTOCOL, September 1981, downloaded from the internet at
<https://datatracker.ietf.org/doc/html/rfc793> on April 24, 2024.
 (“TCP”)
- SAMSUNG-1027 U.S. Pat. App. Pub. No. 20070121615 (“Weill”)
- SAMSUNG-1029 U.S. Pat. App. Pub. No. 2008/0080458 (“Cole”)
- SAMSUNG-1030 U.S. Pat. App. Pub. No. 2010/0281154 (“Bedi”)
- SAMSUNG-1031 Lobo, et. al., (1999). A policy description
language. AAAI/IAAI, 1999, 291-298. (“Lobo”)
- SAMSUNG-1032 Verma, et. al., (2002). Policy-based management
of content distribution networks. IEEE network, 16(2), 34-39.
 (“Verma”)
- SAMSUNG-1034 Banchs, et. al., Distributed weighted fair queuing
in 802.11 wireless LAN, 2002 IEEE International Conference on
Communications, Conference Proceedings. ICC 2002 pp. 3121-3127),
2002

- SAMSUNG-1035 Wu, et. al., 2001. Scalable video coding and transport over broadband wireless networks. Proceedings of the IEEE, 89(1), pp.6-20.
- SAMSUNG-1036 IETF RFC 2205, Resource ReSerVation Protocol (RSVP), version 1 Functional Specification, September 1997, downloaded from the internet at <https://datatracker.ietf.org/doc/html/rfc2205> on May 16, 2024
- SAMSUNG-1037 Excerpts, Computer Networks, Fourth Edition, by Andrew Tanenbaum, Prentice Hall, 2003
- SAMSUNG-1038 U.S. Pat. App. Pub. No. 2007/0258459 (“Smith”)
- SAMSUNG-1039 Agrawal, et. al., 2005. Policy-based management of net-worked computing systems. IEEE Communications Magazine, 43(10), pp.69-75 (“Agrawal”)
- SAMSUNG-1041 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-1042 Reeder, et. al., 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.

- SAMSUNG-1043 Mansour, et al., 2001. Jitter control in QoS networks. IEEE/ACM Transactions On Networking, 9(4), pp.492-502.
- SAMSUNG-1044 Westerinen, et al., IETF RFC 3198, Terminology for Policy-Based Management, November 2001, downloaded from the Internet on May 27, 2024.
- SAMSUNG-1045 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-1046 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-1047 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-1048 Simplified Policy Language (CIM-SPL). Document Number DSP0231, version, 1. (“CIM-SPL”)
- SAMSUNG-1049 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-1050 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-1051 U.S. Pat. App. Pub. No. 2008/0122796 (“Jobs”)
- SAMSUNG-1052 Grossman, Invention of the year: The iPhone. Time Magazine Online, 1, downloaded from the internet at https://content.time.com/time/specials/2007/article/0,28804,1677329_1678542_1677891,00.html on May 28, 2024.
- SAMSUNG-1053 Excerpts, Telcom Dictionary, Althos Publishing, 2007.
- SAMSUNG-1054 U.S. Pat. App. Pub. No. 2008/0002652. (“Gupta”)

- SAMSUNG-1055 U.S. Pat. No. 8,019,868 (“Rao-2”)

48. My analysis and conclusions set forth in this declaration are based on the perspective of a POSITA.

VII. TECHNOLOGY OVERVIEW

49. In this section I provide a broad overview of the relevant technology and state of the technical community before the priority date of the '811 patent. This description is not intended to be exhaustive, but to provide sufficient background to support and contextualize my analysis below.

A. Mobile Devices

50. 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 app¹ 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.

51. 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

¹ The “app” refers to software applications that generally run on smartphones, e.g., email, browsers, streaming, and social media applications. A app market is the application and developer infrastructure for creating and providing apps to smartphone users.

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. Devices were connected to wireless networks using WWAN (cellular) and WLAN (Wi-Fi) modems.²

52. 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)³ 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

² 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.

³ 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.

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.

53. 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.

B. Policy-based Management

54. A key challenge in 2009 was finding ways to address the rapidly increasing needs of mobile users using the resource-limited devices and networks. One approach was to use policies, often expressed as rules, to manage competing demand for resources. 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.
55. Policy for computational systems has been a part of the technical landscape since the 1970s, with a primary focus 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. 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. 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.

56. A policy can be defined as a set of rules to administer, manage, and control access to network resources.⁴ 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 device, and the action component specifies the action that is to be performed by the device in that situation.” SAMSUNG-1032, 2.

⁴ See, e.g., SAMSUNG-1044.

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-1031, 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.

57. 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-1005, [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.

58. 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-1046, 10.

59. 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.)
60. Gonçalves’s similarly describe policy conditions that are “ORed or ANDed.” SAMSUNG-1050, 4. Further, CIM-SPL defined conditions as Boolean expressions of arbitrary complexity. SAMSUNG-1047, 5; SAMSUNG-1048, 51. In summary, Boolean conditions including multiple clauses were well-known as of the Critical Date.

61. 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-1032, 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-1005, [0184].
62. The policies can be specified using many different syntaxes.⁵ Among the many examples are PDL,⁶ Ponder,⁷ and CIM-SPL,⁸

⁵ Stone provides one overview of policy languages in SAMSUNG-1046.

⁶ See, generally, SAMSUNG-1031.

⁷ See, generally, SAMSUNG-1045.

⁸ See, generally, SAMSUNG-1047, SAMSUNG-1048.

and hardware and software vendors often defined their own proprietary policy-specification languages.

63. 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-1039, 3.
64. 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.⁹

⁹ This example is merely illustrative; user interfaces of actual systems were typically far more complex.

Policy specification

Condition:

Action:

65. Ponnappan includes an example that “shows the Policy Editor developed in the system, and an example of a policy rule.”

SAMSUNG-1049, 7.

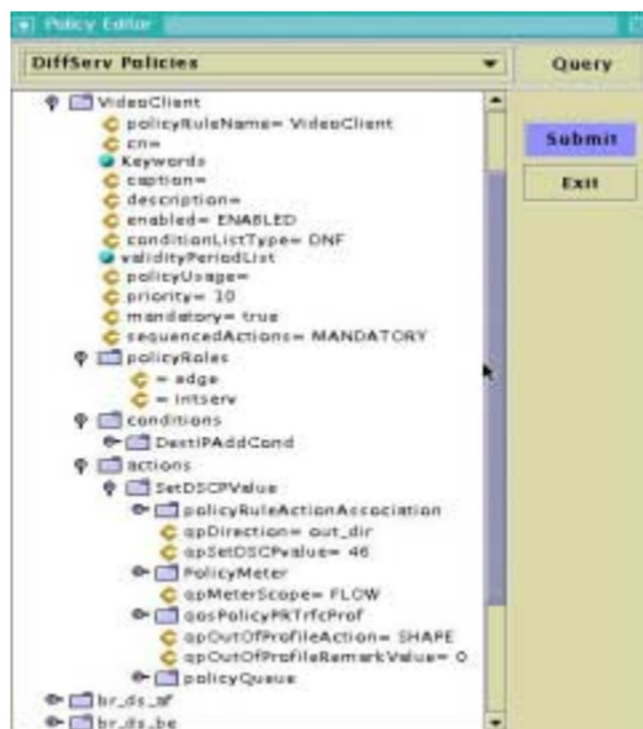


Figure 3: Policy Editor and a Policy Rule example

Id.

66. 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-1050,

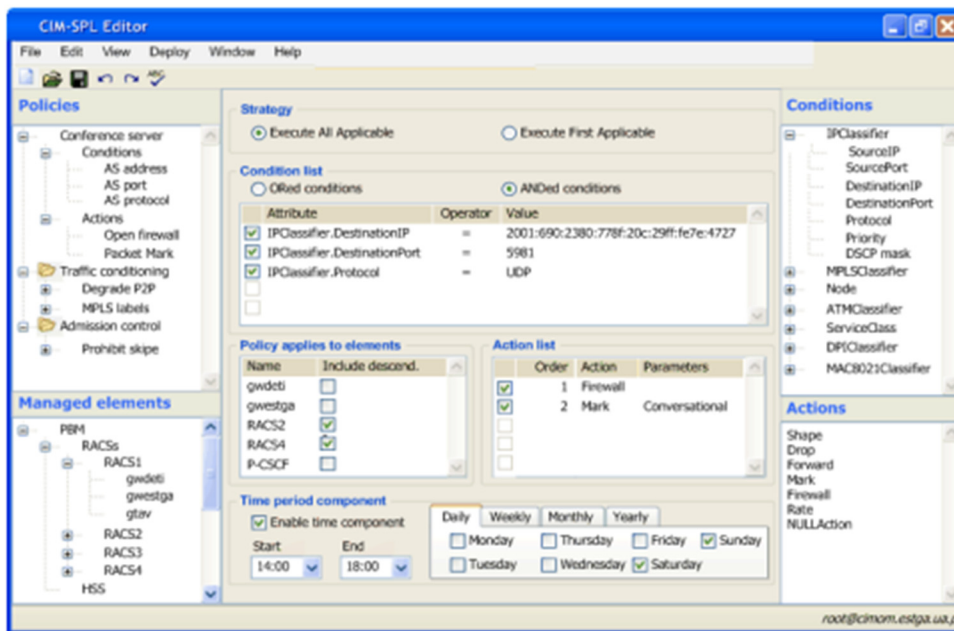


Figure 3 - Graphical editor view

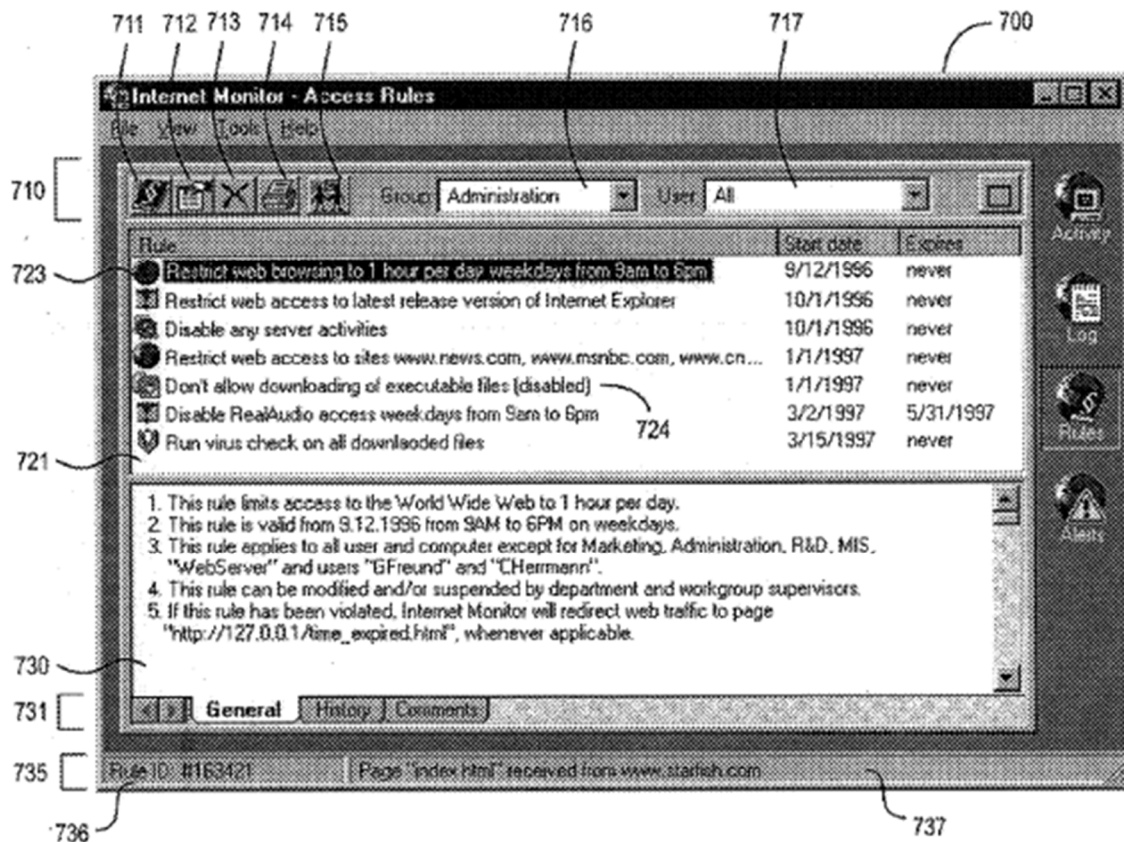
Id.

67. 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.” REEDER

1042, 5.

68. 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-1013, 24:16-24. Figure 7A (below) shows an example UI panel.



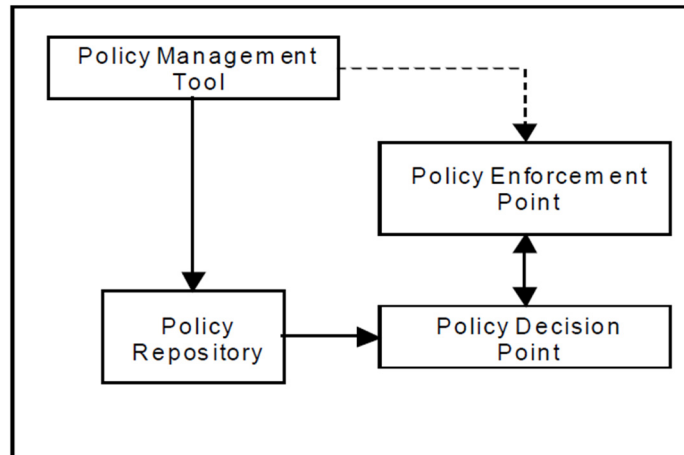
SAMSUNG-1013, FIG. 7A.

69. 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-1050, 4.

70. 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-1032, 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).

71. 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-1032, Figure 1.

72. A Policy Decision Point (PDP) and Policy Enforcement Point (PEP) are essential components in policy-based systems.¹⁰ 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.

¹⁰ SAMSUNG-1032, 1-2.

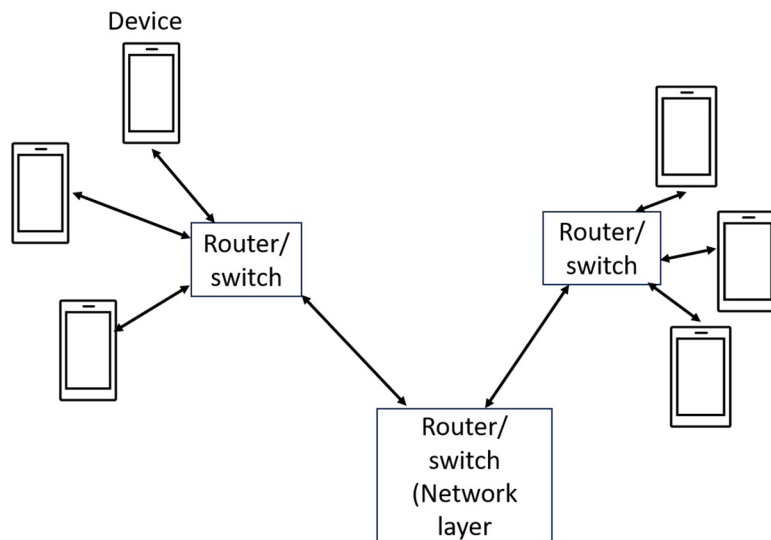
C. Network Bandwidth Management

73. 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 fair¹¹ 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-1041, 12.
74. 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

¹¹ Fair does not necessarily mean equal, as discussed below.

to support all requests—even when network failures occur that prevent serving those requests.

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

76. 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 consistent¹² 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

¹² 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.*

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.

77. Above the device layer, a network element (such as a router or switch) can enforce network-local bandwidth policies that apply to all devices connected to that network devices. The network element ensures that the bandwidth available to the network element is allocated appropriately among its connected devices. Akhtar provides some background on this approach. *See, generally, SAMSUNG-1009.*

D. Bandwidth Management Policy

78. 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 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-1041, 1.

79. Generally speaking, there are three techniques used to control bandwidth: prioritization, quotas, and adaptive application controls.
80. 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.
81. 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-1041, 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*

82. 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.

83. 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.
84. 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.

85. 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.

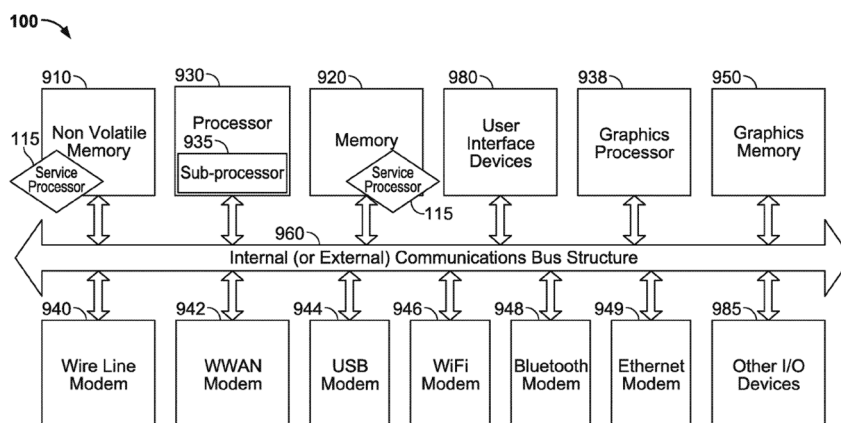
86. Bandwidth policies can also be customized based on the hardware capabilities of devices, especially when devices have multiple interfaces accessing different networks, e.g., WiFi and cellular. Each network interface offers varying performance characteristics and cost structures and thus requires 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.
87. 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.

88. 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 endpoints, relying solely on the network elements to manage bandwidth. In some cases, enforcement is performed on both devices and network elements.
89. 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 '811 PATENT

A. Overview of the '811 Patent

90. The '811 Patent is directed to a wireless device that uses policies to control access to wireless networks by applications running on the device. SAMSUNG-1001, Abstract. The device determines aspects of the policy used to control access based on user input obtained through a user interface. *Id.* A hardware diagram of the device is shown in FIG. 9, reproduced below. SAMSUNG-1001, 26:43-45.



SAMSUNG-1001, FIG. 9.

B. Prosecution History of the '811 Patent

91. Application Serial No. 13/742,312 was filed with 30 original claims, some of which were first amended responsive to a restriction requirement. SAMSUNG-1002, 249-254, 675-683. In a first prior art rejection, the Examiner rejected claims 1-30 as unpatentable over Kaminsky et al. (U.S. Patent No. 8,495,227).

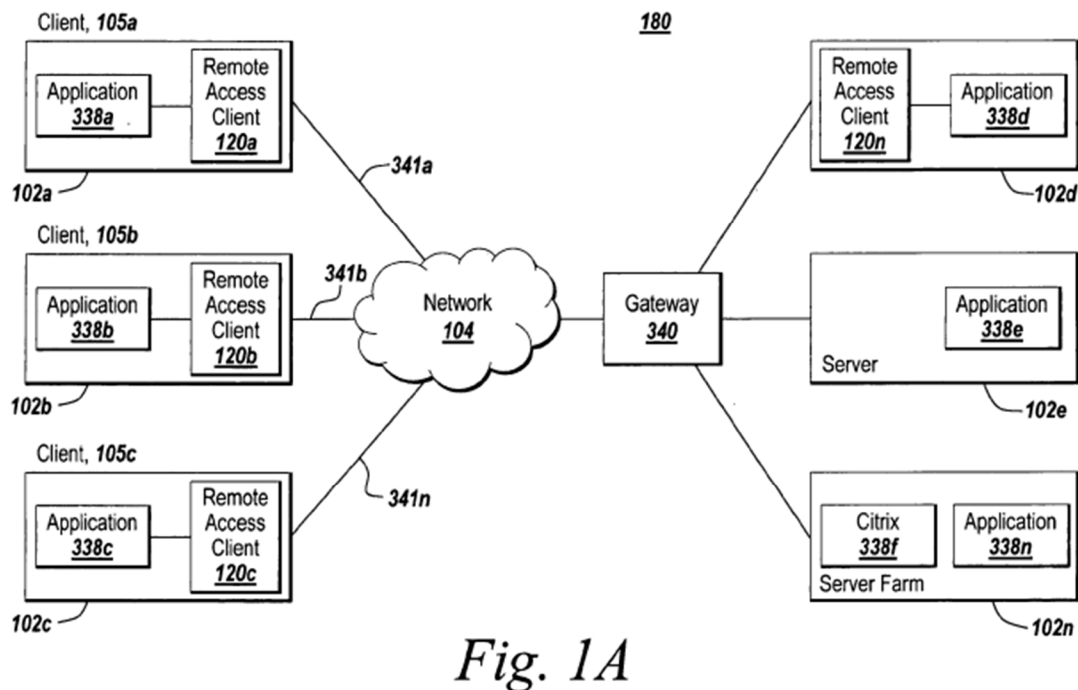
SAMSUNG-1002, 690-691. In response, Applicant amended the claims and argued against the rejection. *Id.*, 836-851. The Examiner then allowed the claims. *Id.*, 855-863. Notably, the Office never considered Rao¹³, Panpaliya, Jones, Jajoo, Cole, Kashima, Montemurro, Akhtar, Ramesh, Freund, Bedi, Jobs or Pregont. SAMSUNG-1002, 693-735; §IV.A. These references render the Challenged Claims obvious, as discussed below.

IX. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES

¹³ U.S. Patent 8,019,868 (“Rao-2”) is cited among the hundreds of references on the face of the ’811 patent. SAMSUNG-1001, 3. While the patents appear to share common inventorship (Rao, Rodriguez, and Brueggermann), I compared Rao-2 with Rao, and found that Rao-2 does not disclose many key teachings of Rao, including the Remote Access Client, relied on heavily in the Petition and in my declaration. *See, generally*, SAMSUNG-1055. In fact, while the word “queue” appears over 80 times in Rao, including in the claims, it appears to be absent from Rao-2. *See, generally*, SAMSUNG-1005; SAMSUNG-1055. Given the significance of Rao’s teaching relating to queues, this omission in Rao-2 is significant.

A. U.S. Pat. App. Pub. No. 2006/0039354 (“Rao”)

92. Rao discloses a “remote access architecture” for “peer-to-peer communications and remote access connectivity” that runs on a computing device. SAMSUNG-1005, Abstract, [0098]. The system (e.g., Figure 1A, below) includes clients 105 (e.g., computing devices 102) that communicate over a network 104 to other devices, such as servers and server farms. *Id.*, [0086]-[0096].



SAMSUNG-1005, FIG. 1A

93. 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 suffering from increased latency and reduced quality of voice communication. SAMSUNG-1005, [0003]. Such inefficiencies are most frequently noticed by a user of interactive real-time applications (such as the VoIP application discussed in Rao) and non-interactive real-time applications, such as video streaming. Regarding video streaming, Viridi explains that “if multimedia content is streamed to and not received fast enough by the client device, the user sees glitches or breaks in the presented multimedia content.” SAMSUNG-1024, [0005]. VoIP is also subject to such stuttering of audio streams, which may disrupt interactions among users.

94. Rao addresses these inefficiencies through a prioritization scheme that “provide[s] application-aware, client-specific prioritization of packet traffic.” SAMSUNG-1005, [0003]. The scheme is achieved by augmenting client 105 with remote access

client (RAC) 120 that interacts with applications 338 and network stack 310. *Id.*, [0089], [0098]-[0100].

95. Figure 1C shows an example of a system with a RAC for routing network packets from client 105 to network 104:

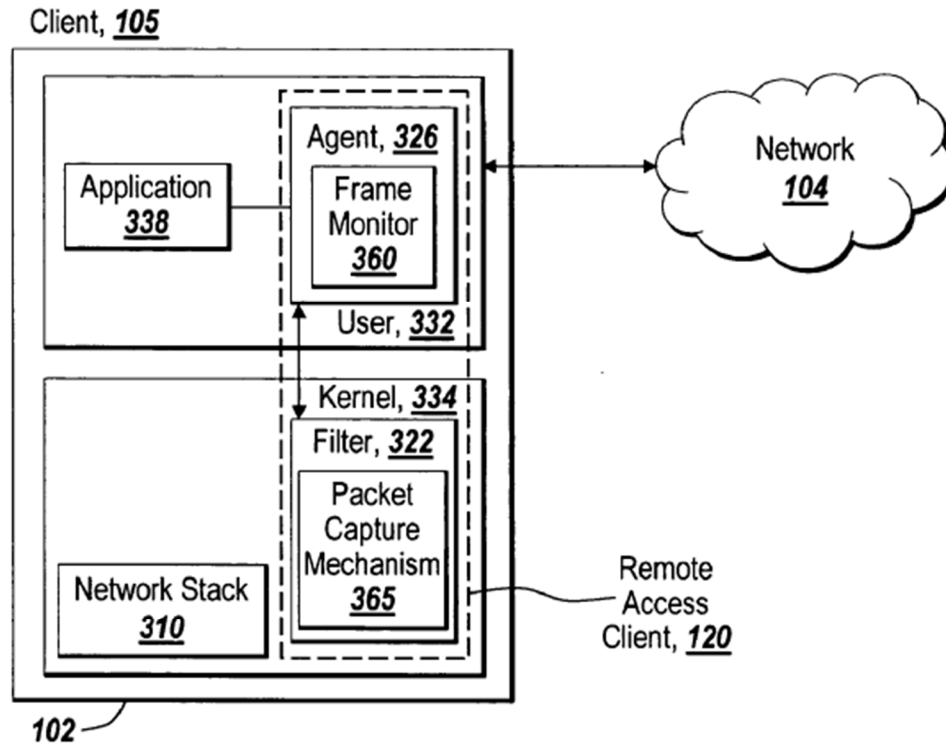


Fig. 1C

SAMSUNG-1005, FIG. 1C

96. RAC includes a filter that uses a “filtering table ... to determine what action to take against packets,” including “ensur[ing] that unwanted packets are discarded,” “deny[ing] access to particular protocols,” and/or “prevent[ing] unauthorized access from

remote computers by discarding packets to specified destination addresses.” SAMSUNG-1005, [0102]. RAC 120 can include agent 326 with frame monitor 360 that “include[s] policies and logic for applying a policy to a received packet.” *Id.*, [0108]. Frame monitor 360 “transmit[s] a packet to a gateway 340 responsive to a policy-based determination made by the frame monitor 360.” *Id.* The use of policies in RAC 120 thereby guides efficient use of network resources and enables Rao’s system to address the inefficiencies identified within Rao’s disclosure. In Rao’s example, interactive applications such as VoIP are more likely to provide satisfactory user experiences when traffic from those applications is not delayed by traffic from lower-priority and less time-sensitive applications such as file download.

97. To this end, Rao’s system enables intelligent and client-centric “prioritization of application network communications on a client based on the type and/or priority of an application.” SAMSUNG-1005, [0179], [0182]-[0184], FIG. 5A. Among Rao’s application examples are streaming video, email, collaboration, online meeting, desktop sharing and “any

application related to real-time data communications.”

SAMSUNG-1005, [0088], [0179]. In Rao, an administrator assigns priority to each of these applications such that the system uses network capacity to provide the best user experience. Rao, [0183].

98. To perform prioritization, Rao’s system “appl[ies] a policy to determine a condition of the client 105, or endpoint, at the time of transmission of the packet.” *Id.*, [0109]. Frame monitor can “identify an application 338 that generated the packet,” which, as described above, allows the device to assign priority to applications according to the network needs of each application. *Id.*, [0109].
99. Figure 5A shows an environment of a client providing client-side application-aware network communication:

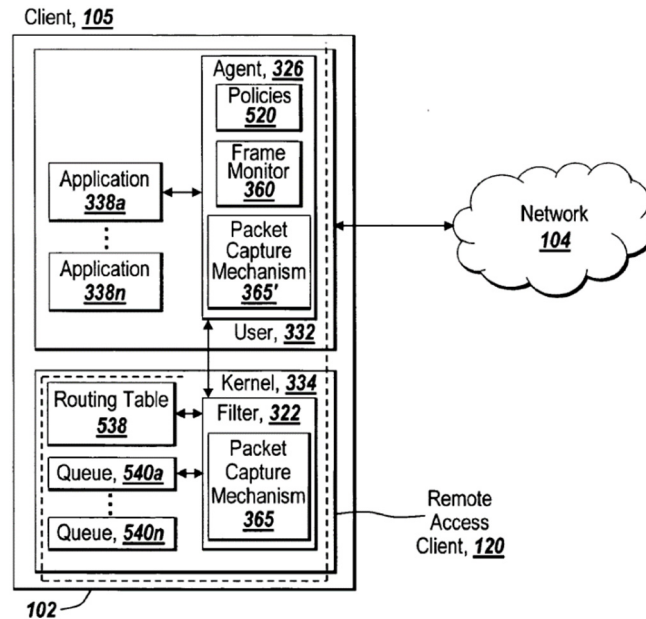


Fig. 5A

SAMSUNG-1005, FIG. 5A

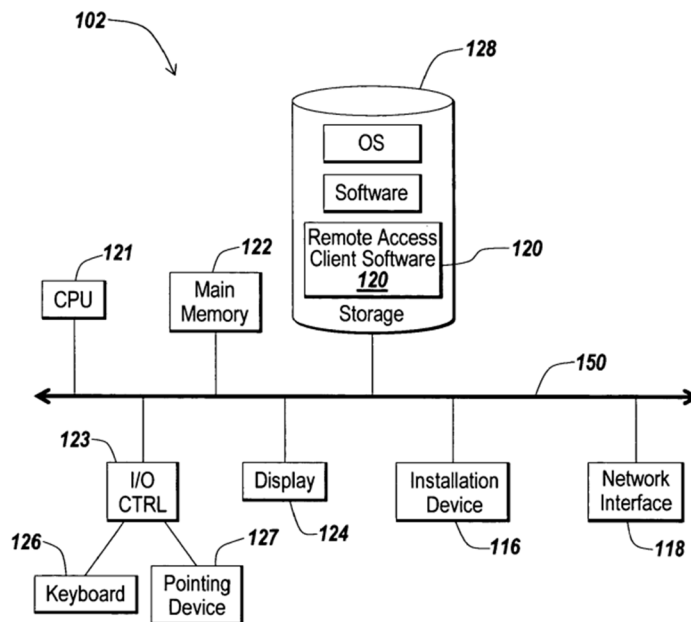
100. Rao offers non-limiting disclosure relating to policy specification and how its system leverages policies for prioritization. SAMSUNG-1005, [0182] (“any suitable means and/or mechanisms”), [0183]-[0184]. As examples, Rao describes that policies can be specified, e.g., by “name of the application,” “type of application,” and type of “protocols used by the applications.” SAMSUNG-1005, [0182]. In addition, policies “may be specified hierarchically to account for multiple applications” and “may be specified conditionally, such as if one application 338 a is running, a second application 338 b may

have a higher or lower priority.” SAMSUNG-1005, [0182]. To enable configuration of such policies, “Rao’s agent “may provide a configuration mechanism such as a user interface, graphical or otherwise, design and constructed for configuring or specifying the policies.” SAMSUNG-1005, [0183].

101. The Rao Device (RD), which is illustrated in FIG. 1D (reproduced below), includes a central processing unit (CPU) and a main memory unit, and can include a visual display device, a keyboard and/or a pointing device, such as a mouse, input/output devices, a cache memory in communication with the central processing unit 102. SAMSUNG-1005, [0118]. RD’s CPU is logic circuitry that responds to and processes instructions fetched from the main memory unit, and is therefore configured to perform or assist in performing the operations discussed in all Grounds (since all Grounds include Rao). *Id.*, [0119].

102. RD can further include a network interface to interface to networks through a variety of connections including, but not limited to, standard telephone lines, LAN or WAN links (e.g., 802.11, T1, T3, 56 kb, X.25), broadband connections (e.g.,

ISDN, Frame Relay, ATM), wireless connections, or some combination of any or all of the above. SAMSUNG-1005, [0125]. The network interface can include “a built-in network adapter, network interface card, PCMCIA network card, card bus network adapter, wireless network adapter, USB network adapter, modem or any other device suitable for interfacing the computing device 102 to any type of network capable of communication and performing the operations described herein.” *Id.*



SAMSUNG-1005, FIG. 1D.

103. As of the Critical Date, mobile devices commonly included CPU, memory, network interfaces/modems, a user interface,

etc., as shown, e.g., in Jobs. SAMSUNG-1051, [0090]-[0163] and *generally*, SAMSUNG-1051.

B. U.S. Pat. No. 8,400,491 (“Panpaliya”)

104. Panpaliya teaches adjusting “video parameters of a video communication session based on a type of use for the video communication session” which can include “applying a profile of video parameters to the session based on the use.”

SAMSUNG-1007, Abstract. Video parameters include, but are not limited to, screen size, resolution, buffer size, frames per second, color, motion, and audio quality parameters.”

SAMSUNG-1007, 4:65-67.

105. Panpaliya further explains that video parameters can be adjusted based on a detected network constraint. SAMSUNG-1007, Abstract. In Panpaliya, a “network constraint detection component” monitors and/or measures “the current network parameters associated with an existing video communication session ... to detect if a network constraint exists.” SAMSUNG-1007, 5:66-6:3.

106. When the network constraint detection component “determines that an unfavorable threshold level has been reached, a network

constraint is detected” and the system “adjusts video parameters in a manner that continues to provide an acceptable user experience.” SAMSUNG-1007, 6:7-12. Video parameters “can include, but are not limited to, screen size, resolution, buffer size, frames per second, color, motion, and audio quality parameters.” SAMSUNG-1007, 6:64-66.

107. Adapting video to meet the network constraints was known (and widely practiced) long before Panpaliya. For example, Wu writes:

Network-aware adaptation consists of two elements: network awareness and adaptation. The process of network awareness, or network monitoring, is to collect the information about the current status of underlying network resources (e.g., available bandwidth and bit error conditions) [9]. Adaptation is to adapt video streams based on network status. Hence, network-aware end systems are able to monitor relevant QoS fluctuations in wireless networks and react accordingly to achieve graceful change in perceptual quality. We describe mechanisms for network monitoring and adaptation in Sections III-A and III-B, respectively. SAMSUNG-1035, 7.

108. In fact, most of the techniques described in Wu were not even new at the time of that publication, as evidenced by Wu’s

bibliography, which includes 71 references. SAMSUNG-1035, 13-15.

C. Rao-Panpaliya Combination

109. As described above, RD prioritizes the packets according to priority. *See* §IX.A. However, a POSITA would have recognized that prioritizing packets does not address insufficient bandwidth to accommodate an application's bandwidth requirements, such as the bandwidth required for video. More broadly, flow prioritization does not address the total amount of resources requested by apps, but simply determines how much network resources to give each of the requesting apps when more is requested than can be served. Hence, apps with low priority may receive few or no resources, thus resulting in a degraded user experience.
110. That video resolution will be, in some cases, constrained by bandwidth was well-known as of the Critical Date. For example, "[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," so a network

providing less than 6 Mbps would have insufficient bandwidth to stream video at DVD quality.¹⁴ SAMSUNG-1019, 1.

111. In addition, Netflix provides the following current recommendations, “[t]o watch TV shows and movies on Netflix, we recommended having a stable internet connection with a download speed shown below in megabits per second (Mbps).”

SAMSUNG-1022, 1.

Video quality	Resolution	Recommended speed
High definition (HD)	720p	3 Mbps or higher
Full high definition (FHD)	1080p	5 Mbps or higher
Ultra high definition (UHD)	4K	15 Mbps or higher

Id.

112. While UHD did not exist (or at least was not widely deployed) in 2009, a POSITA would have recognized that for a particular

¹⁴ Mbps is megabits per second. Note that there are 8 bits in a byte, so 6 Mbps is 0.75 megabytes per second.

resolution,¹⁵ some minimum bandwidth will be required, with higher resolutions requiring more bandwidth. The Netflix reference simply provides some examples.

113. If sufficient bandwidth is not available, allowing the video application to transmit the video provides a poor user experience for that application, e.g., showing video that stutters and freezes. For example, Virdi explains that “if multimedia content is streamed to and not received fast enough by the client device, the user sees glitches or breaks in the presented multimedia content.” SAMSUNG-1024, [0005]. Green provides a similar explanation:

114. When a receiving unit runs out of data to decode (or present), it is called ‘underflow.’ Underflow occurs when the receiving unit is ready to decode (or present) the next frame, but the has not yet received (or decoded) all of the data of that frame. The practical and noticeable manifestation of an underflow is a temporal

¹⁵ The compression technique used also impacts the necessary bandwidth, with more effective compression requiring less bandwidth, but when the same compression is used, higher resolution requires more bandwidth.

interruption (i.e., ‘hiccup’ or ‘stutter’) in the presentation motion video rather than the desired effect, which is a smoothly playing motion video. For example, instead of showing a motion video at a fixed frequency (e.g., 15 frames per second), a receiving unit experiencing underflow would show a frame of the video stream followed by a noticeable delay before the next or a later frame would display. This may continue for several seconds or minutes.” SAMSUNG-1025, [0031]-[0032].

115. Therefore, to address cases where the network provides insufficient bandwidth to support a particular networking operation (e.g., streaming media at a given resolution), a POSITA would have looked to references such as Panpaliya, which teaches that the multimedia data can be adjusted to meet network constraints. Panypaliya, Abstract, 6:65-67, 5:66-6:3, 6:64-66.
116. In operation, the resulting Rao-Panpaliya device (RPD) adjusts video parameters based detected network constraints (if any exist),¹⁶ then transmits the adjusted video stream using policy-

¹⁶ If sufficient bandwidth exists, RPD need not adjust the video.

based priority queuing (per Rao). For example, a device might prioritize VoIP over streaming video, and therefore requires the complementary teachings of Rao and Panpaliya.

117. Combining Rao and Panpaliya would have involved (1) combining prior art elements according to known methods to yield predictable results; and (2) use of known techniques to improve similar devices (methods, or products) in the same way. See MPEP §2143. Such a combination would have amounted to nothing more than the use of a known technique to improve video transmission in a similar way and combining prior art elements according to known methods to yield the predictable results described above. *KSR*, 550 U.S. at 417. RPD’s processor would be configured to perform the operations discussed in this Ground. See §IX.A.

D. U.S. Pat. No. 8,285,850 (“Jones”)

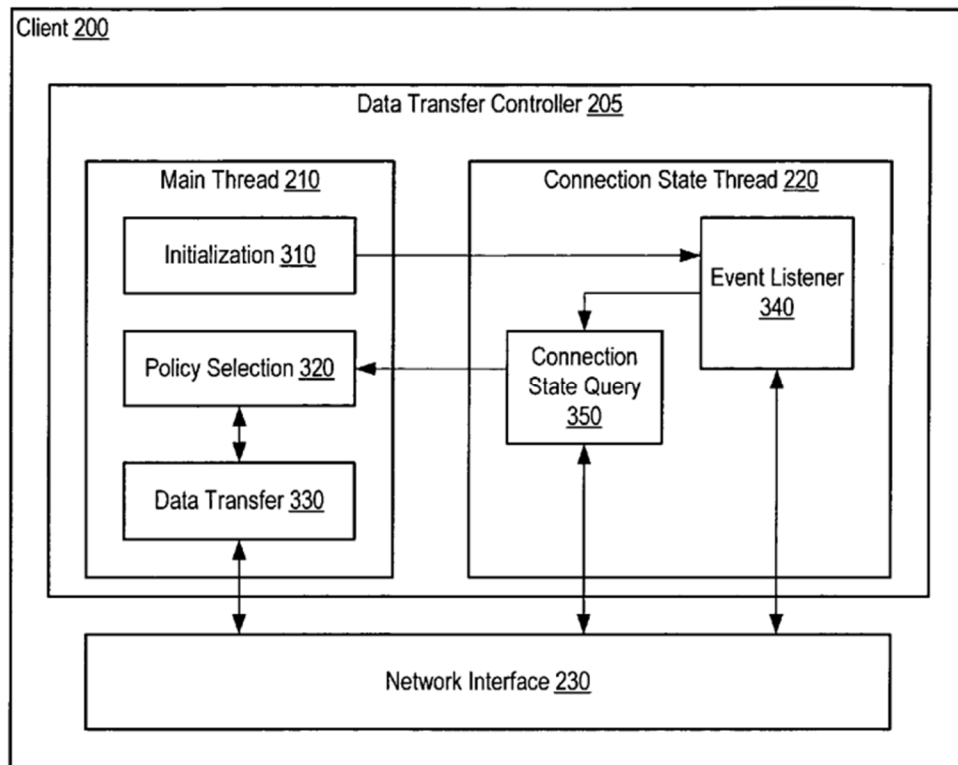
118. Jones discloses techniques for “managing data transfers between client computers and a computer network” in which client devices include a “data transfer controller” and “data transfer rules.” SAMSUNG-1006, Abstract. Jones explains that “it has become common for client computers to be

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 the mobile device can connect to multiple networks, writing that 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.

119. 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

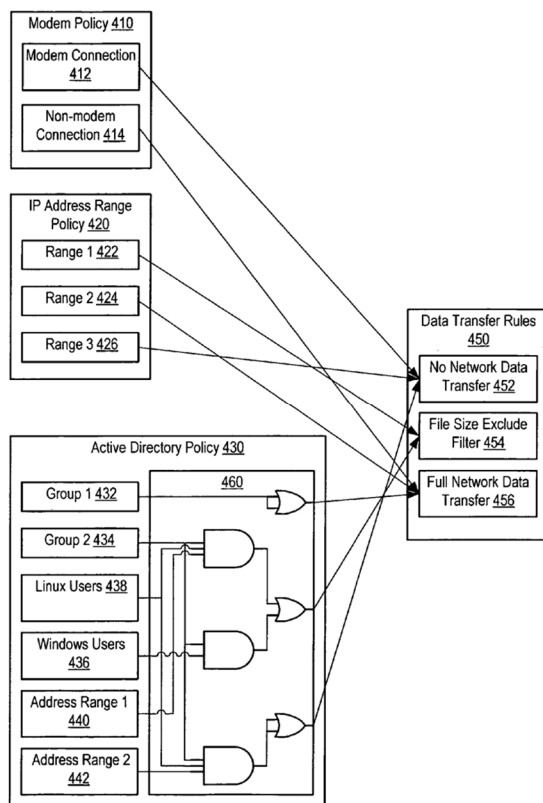
users tend to complicate any backup mechanism.” *Id.*, 3:30-32, 47-51. In one example, Jones states that, “if the connection type is slow, such as via a modem, a user who is attempting to access e-mail or browse the internet may be frustrated as the available bandwidth is consumed by backup data transfers.” *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.

120. 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.



SAMSUNG-1006, FIG. 3.

121. When event listener recognizes an event, it causes the connection state query to fetch the current state of the network interface and forwards the current connection state to policy selection component of the main thread. *Id.*, 4:40-45. In response, policy selection applies one or more rules to data transfer, and the results (policy action aspects of policies, as described in *supra* VII.B) can include “no network data transfer 452,” “file size exclude filter 454” and “full network data transfer 456,” as illustrated in FIG. 4. *Id.*, 4:45-48, FIG. 4.



SAMSUNG-1006, FIG. 4

E. Rao-Jones Combination

122. Rao “provides various techniques for optimizing peer-to-peer communications, including real-time communications such as streaming video, voice over internet protocol (VoIP) signaling and media, video, and other real-time data applications such as web collaboration, screen or desktop sharing, and instant messaging” using “application-aware prioritization of client-side network communications,” where one application is granted a

higher priority than another for access to network resources.

SAMSUNG-1005, [0004], [0088]. Rao notes that it is “desirable to provide application-aware, client-specific prioritization of packet traffic,” for example, to address situations where a client device is running both real-time and non-real-time applications. *Id.*, [0003]. Without applying the teachings of Rao, packets from the non-real-time application “may be processed ahead of the real-time network packets of the VoIP telephone call thereby increasing the latency and reducing the quality of the voice communication.” SAMSUNG-1005, [0003]. A POSITA would have recognized that Rao’s teaching applies to packets from other real-time applications, such as streaming video. For example, Rao specifically lists “desktop sharing” and “hosted service [] such as GoToMeeting.com provided by Citrix Systems, Inc. of Ft. Lauderdale, Fla., WebEx.com provided by WebEx, Inc. of Santa Clara, Calif., or LiveMeeting.com provided by Microsoft Corporation of Redmond, Wash.” SAMSUNG-1005, [0090]. A POSTIA would have recognized these as examples of real-time applications.

123. A POSITA would have known that interactive applications such as streaming media, videophones and interactive games have real-time network constraints, such as bandwidth and latency. For example, Apostolopoulos explains that:
124. Interactive applications such as videophone or interactive games have a real-time constraint. Specifically the information has a time-bounded usefulness, and if the information arrives, but is late, it is useless. This is equivalent to a maximum acceptable end-to-end latency on the transmitted information, where by end-to-end we mean: capture, encode, transmission, receive, decode, display. The maximum acceptable latency depends on the application, but often is on the order of 150 ms.
- SAMSUNG-1023, 4.
125. Rao implicitly assumes that favoring real-time traffic by delaying non-real-time traffic from these types of applications (by assigning such traffic to low-priority queues) will be sufficient to meet such requirements of real-time traffic. A POSITA, however, would have recognized that when available networks cannot meet such real-time constraints, even using queues to delay lower-priority traffic will not provide an

acceptable user experience since network capacity is simply insufficient even in the best circumstances.

126. As described in §VIII.D and §VIII.E, in some cases, in response to a network lacking bandwidth to support an application, an application can adjust its behavior (e.g., downscaling video) to sufficiently compensate for bandwidth constraints. However, other cases, sufficient bandwidth for even downscaled video will not exist, and the video will suffer from stuttering. For example, a network might have insufficient bandwidth even for lower-definition video. In another example, an application might limit the downscaling (e.g., not allowing the video to be scaled to a resolution below some minimum level), which ensures that the video maintains some minimum quality. In such cases, transmitting the video will lead to a poor user experience, and therefore Rao's techniques (even as augmented by Panpaliya) will not suffice.¹⁷

¹⁷ And, of course, downscaling can be used only by some applications. E.g., a system cannot omit a portion of data from a backup as that would result in data not being backed up, defeating the purpose of the backup.

127. In addition, the negative impact to the user experience is not confined to the video since transmitting video saps network capacity from other applications. In one example, transmitting standard-definition video signal at DVD quality requires approximately 6 Mbps, so transmitting a video on a network with 3 Mbps would not only result in stuttering video, it would also occupy at least some of the 3 Mbps of bandwidth (and perhaps the entire 3 Mbps, depending on how traffic is controlled) that would have otherwise been available to other applications. SAMSUNG-1019, 1. For example, if the user was downloading a new application, downloading an application update, synchronizing email, conducting a VoIP call, etc., any or all of those actions would be delayed by the video stream, which could be rendered unwatchable by stuttering.¹⁸ Therefore, not only does the user get poor video quality, other user application

¹⁸ The detrimental impact is not even limited to network use. Decoding the video occupies CPU cycles and memory resources, so displaying poor video can even disrupt applications that do not require the network.

- that require network access also suffer. Clearly this is undesirable, and denying access to the application is preferred.
128. In addition, contention among such applications can adversely impact the applications themselves. For example, Jones explains that while a network can possess sufficient capacity to support a particular application, it can lack capacity to simultaneously support *multiple* applications. SAMSUNG-1006, 1:54-58; For example, “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, 1:54-58. Cole provides a corroborating example: “if the connection is being used nearly to capacity and an additional application is executed that requires still more bandwidth, the connection may not be able to support the total load” so “running applications may experience increased latency for data transfers.” SAMSUNG-1029, [0073].
129. In such cases, while there can be sufficient bandwidth to serve a first application (e.g., email per Jones or other applications such as multimedia streaming), network use by other applications

limits available bandwidth such that the first application cannot provide an acceptable user experience. SAMSUNG-1006, 1:54-58. For example, if a network has exactly enough bandwidth to support video streaming at DVD quality, the network cannot support both that video streaming and VoIP (or any concurrent application that requires bandwidth). SAMSUNG-1019, 1. Therefore, a POSITA would have recognized that a lack of bandwidth can be caused both by a slow network (the network that cannot meet application constraints) and by network contention (the network cannot satisfy aggregate bandwidth demands).

130. In both cases, a POSITA would have recognized that denying an application access to a network is preferable to prioritization since the denial of use by one application both preserves device resources and improves user experience (since the non-denied applications then have sufficient bandwidth to perform effectively).
131. Therefore, a POSITA would have recognized that there are at least two complementary approaches for managing contention: (1) network prioritization (as taught by Rao) when sufficient

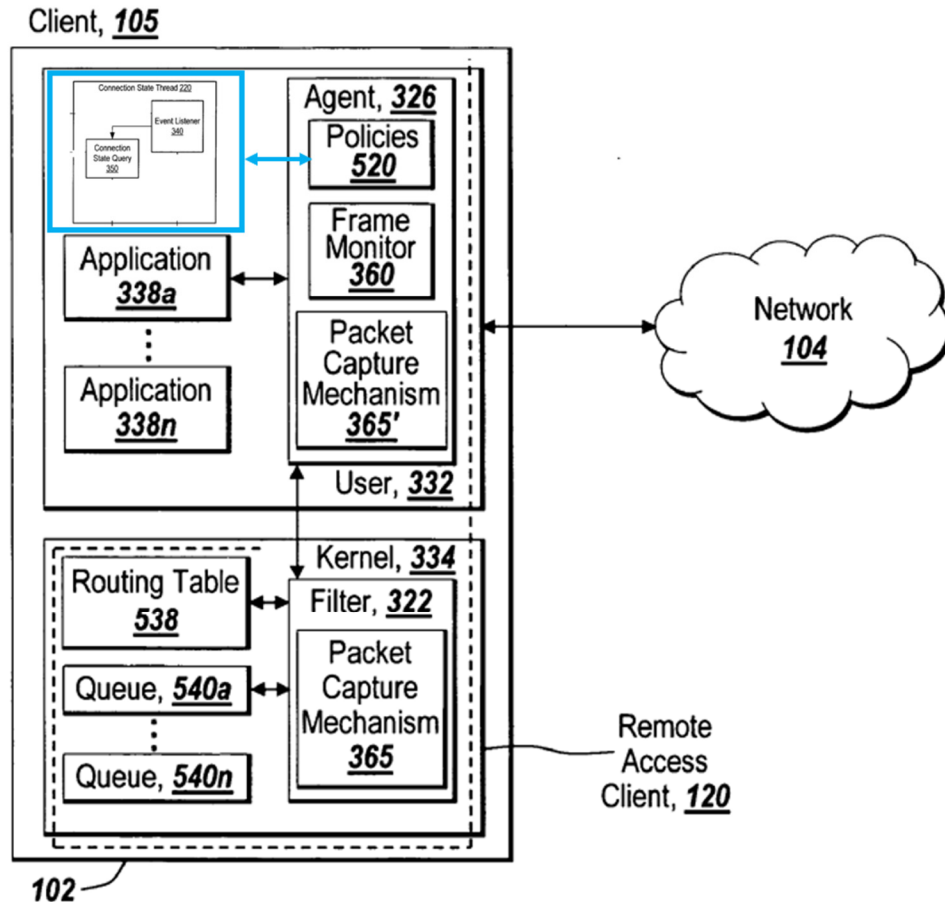
bandwidth exists and (2) denying network access to some applications (as taught by Jones) to manage insufficient bandwidth and network contention.¹⁹ SAMSUNG-1005, [0184]; SAMSUNG-1006, 5:13-32. Consequently, a POSITA would have been motivated to combine the teachings of Rao and Jones to operate in instances where bandwidth is limited and there is contention among applications for bandwidth.

132. The resulting Rao-Jones device (RJD) evaluates policies relating to a wide range of factors such as characteristics of the network (e.g., “type of connection, connection bandwidth, user priorities, etc.,” per Jones, and “the size of the payload of the network packet,” per Rao) among other factors (e.g., “the name of the application, “the type of application,” “whether an application is running in the foreground or the background.” SAMSUNG-1005, [0182], SAMSUNG-1006, 5:13-15. The

¹⁹ Panpaliya (SAMSUNG-1007) offers a third approach, reducing the amount of data transmitted, but such an approach is applicable only to a subset of application (that is, application that can send only a subset of the data) and only when network resources are sufficient to handle the reduced data transfer.

result of the policy evaluation first determines whether the transfer is allowed (per Jones), and if so, assigns the corresponding packets to a priority-based queue (per Rao). SAMSUNG-1005, [0182], [0189]; SAMSUNG-1006, 5:15-32. Therefore, RJD blocks an application's access to the network when permitting even prioritized access by an application degrades overall device performance, and for traffic that is permitted, uses the prioritization techniques of Rao.

133. RJD includes the client 105 of Rao modified to include the "Connection State Thread" of Jones, as illustrated below. SAMSUNG_1005, FIG. 5A.



Rao, FIG. 5A (modified).

134. In addition, RJD can access multiple networks, as taught by Jones, “rules may be applied to data transfers depending on the ... type of connection,” and “policies for data ... are sensitive to the type of connection.” SAMSUNG-1006, 5:13-19. Such function was common as of the Critical Date, and explained in Jobs, for example. SAMSUNG-1051, [0100].
135. Further, RJD communicates directly or via a gateway (which Rao defines as “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 network”) with various networked systems, such as other instances of RJD, servers and server farms, as illustrated below. SAMSUNG-1005, [0089]-[0092].

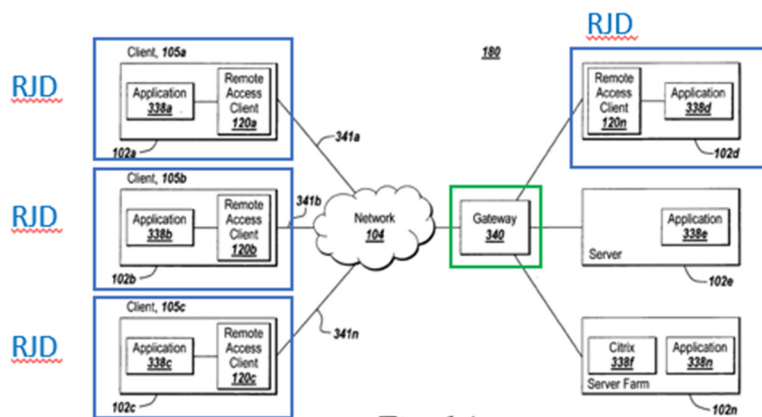


Fig. 1A

SAMSUNG-1005, FIG. 1A (modified).

136. Rao provides several specific examples, including that “any of the remote access clients 120a-120n may communicate with the remote access client 120n via the gateway 340;” “any of the clients 105a may communicate via the gateway 340 to a server 102e running an application 338e, which for example, may be an application server providing email services such as Microsoft Exchange manufactured by the Microsoft Corporation of Redmond, Wash., a web or Internet server, or a desktop sharing

server, or a collaboration server;” “any of the clients 105a may communicate via the gateway 340 to a server farm 102n or server network, which is a logical group of one or more servers that are administered as a single entity;” and “the gateway 340 may be used to provide a virtual private network connection to give a client 105a-105c access to a private network.”

SAMSUNG-1005, [0089]-[0092].

137. In operation, the RJD client monitors the connection state using the connection state thread (as taught by Jones), which provides the connection state to the policies component 520 (which is analogous to policy selection component of Jones).

SAMSUNG-1006, 4:43-45. The policy component uses the configured policies to determine whether to permit or prevent the data transfer based on the connection state. For permitted data transfers, the RJD client uses the policies to apply a priority to network packets in accordance with the configured policies and queues the packets according to the priority, restricting some packets in favor of others. SAMSUNG-1005, [0189], [0191]. The client then communicates the packets according to the priorities. SAMSUNG-1005, [0194].

138. Thus, the components of RCD each operate as they would in isolation. 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 before the Critical Date. 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. *KSR*, 550 U.S. at 417.

139. RJD's processor would be configured to perform or assist in performing the operations discussed in Grounds related to RJD.

F. U.S. Pat. App. Pub. No. 2008/0162981 ("Jajoo")

140. Jajoo describes a "method for controlling data traffic in a wireless or other communication network" in which "agents monitor the L1 (physical) and L2 (data link) layers of the network for the presence of indicators associated with network failover operations." SAMSUNG-1010, Abstract. "Based on detected indicators ... the agents determine if a failover operation has occurred" and if so, "data congestion associated with the

failover operation is controlled according to a failover congestion monitoring and recovery mode.” *Id.*

141. Jajoo “differentiates between failover congestion and actual congestion” and “[h]ow the traffic is controlled in either case can be both implementation-dependent and traffic-type dependent” such that “different traffic types can be subjected to a reduction/shredding process, and/or to a delay process, and/or to a dropping process.” SAMSUNG-1010, [0017].
142. Jajoo explains that “data packets associated with the failover congestion are controlled using the failover congestion control mode 54, which accounts for the temporary nature of the failover data congestion,” e.g., “failover congestion may be controlled according to the data source backoff model 58, which controls delays in transmission and/or re-transmission of the data packets at the transmission source(s).” SAMSUNG-1010, [0028]. As a result, “instead of dropped calls, data packets are delayed in a controlled manner,” which “is sufficient to accommodate the failover operation, wherein once the failover operation is complete, the data packets are then transmitted or re-transmitted over the newly established link.” *Id.* Jajoo

further notes that “[t]raffic patterns can be separated at the network and data link layers by adopting an alternate de-queuing algorithm while the failover congestion lasts.” SAMSUNG-1010, [0029].

143. To determine whether failover has occurred, “the L1 layer may be monitored for occurrences of physical layer alarms (e.g., DS1 alarms) generated by one or more network entities, and the L2 layer may be monitored for occurrences of data link protocol errors and/or information and signaling exchanges associated with failover operations in the data link layer.” SAMSUNG-1010, [0009].

G. Rao-Jones-Jajoo Combination

144. Jones describes applying rules based on “type of connection, connection bandwidth, [and] user priorities.” SAMSUNG-1006, 5:14-15. A POSITA would have recognized that available bandwidth typically varies over time. If there is no contention for a network, then the available bandwidth is simply the maximum bandwidth for the particular network, which is based on factors such as the physical properties of the network.

145. More commonly, some of that maximum bandwidth is consumed by systems and applications using the network, so the bandwidth available (that is, the maximum bandwidth minus any bandwidth used by the system and applications) at any given time will vary. Some applications will begin using the network, some applications will cease using the network, and demand for bandwidth by the applications will vary over time as they request to send and receive data.
146. In addition, Jajoo teaches that one source of variance in available network bandwidth occurs in response to failover. SAMSUNG-1010, [0006]. For example, Jajoo teaches that when network failover occurs, the result can be “decreased bandwidth and a perceived congestion condition.” SAMSUNG-1010, [0006]. This can occur, for example, as applications attempt to reestablish connections when they move from a failing or failed network to a new, operational network. However, the “network normally handles congestion by dropping the load at the source, failover operations may result in dropped calls,” so users can be negatively impacted. SAMSUNG-1010, [0006].

147. Instead, in Jajoo, “the source and nature of the failover congestion are taken into consideration to reduce instances of dropped calls that would otherwise occur if the failover congestion were handled according to a general purpose congestion monitoring and recovery mode of the network.” SAMSUNG-1010, [0007]. Thus, in Jajoo, “data packets associated with the failover data congestion are controlled in a manner that accounts for the temporary nature of the failover data congestion,” e.g., “data packets are delayed in a controlled manner until the failover operation is finished.” SAMSUNG-1010, [0011]. Therefore, to mask the errors and avoid unnecessary disruption (e.g., multimedia transmission failures such as dropped calls) caused by failover, a POSITA would have been motivated to modify the RJD with Jajoo’s failover monitoring. SAMSUNG-1010, [0007].
148. A POSITA would have recognized the “calls” described in Jajoo naturally include VoIP calls as described in Rao. SAMSUNG-1005, [0004]. In fact, Rao specifically discusses a “network disruption shielding technique” that addresses “temporary disruption in a network connection [that] may occur

when the mobile client roams between different access points in the same network, or when the client switches between networks” which can disrupt “the network service to the client and may drop the VoIP telephone call.” SAMSUNG-1005, [0081]. In such cases, “network communications are queued during the network disruption and transmitted once the network is available.” *Id.* A POSITA would have recognized that Jajoo’s “failover data congestion” is an example of “network disruption” as discussed in Rao. SAMSUNG-1005, [0081]; SAMSUNG-1010, [0007]. Therefore, a POSITA would have naturally combined the teachings of Jajoo with the teachings of Rao at least to provide additional stability to VoIP calls.

149. In operation, in the resulting Rao-Jones-Jajoo Device (RJJD), when the client recognizes an event, per Jones, it fetches the current state of network interface and forwards the current connection state to policy selection. SAMSUNG-1006, 4:40-48. Before determining a policy-based response, the client determines whether the condition is transient, e.g., as the result of a failover, per Jajoo. SAMSUNG-1010, [0007]-[0010], [0017], [0029]. Using both the current network condition, and a

determination as to whether the condition is transient, RJJD permits or denies access to the network (per Jones), and if access is permitted in the presence of a transient condition, “failover data congestion are controlled in a manner that accounts for the temporary nature of the failover data congestion” using the priority-based queuing of Rao, e.g., by assigning such traffic to a lower-priority queue during the temporary disruption.

SAMSUNG-1005, [0179]-[0195]; SAMSUNG-1010, [0011].

As I described above, transient surges in bandwidth requests can accompany a network failover (e.g., as applications reestablish connection), and using Rao’s priority queuing shields the network from the surge. As a result, while the multimedia session might suffer temporarily (e.g., stuttering video when its packets are queued), the session will not terminate.

SAMSUNG-1010, Abstract, [0007]-[0008]. RJJD policies are based on user input, as described in both Rao and Jones.

SAMSUNG-1005, [0183]; SAMSUNG-1006, 6:39-41; §VII.B, §IX.D.

150. Combining Rao, Jones and Jajoo would have involved (1) combining prior art elements according to known methods to

yield predictable results; and (2) use of known techniques to improve similar devices (methods, or products) in the same way. *See* MPEP §2143. Such a combination would have amounted to nothing more than the use of a known technique to improve similar smart phone devices equipped with network interfaces in a similar way and combining prior art elements according to known methods to yield the predictable results described above. *KSR v. Teleflex*, 550 U.S. 398, 417 (2007). RJJD’s processor would be configured to perform or assist in performing the operations discussed in this Ground.

H. U.S. Pat. App. Pub. No. 2008/0080458 (“Cole”)

151. Cole is directed to providing network connectivity for a mobile device with multiple “communication interfaces.” SAMSUNG-1029, Abstract. Figure 1 (below) shows mobile device 110 connected to communication networks 120 (e.g., WWAN 130, WLAN 140). SAMSUNG-1029, [0031].

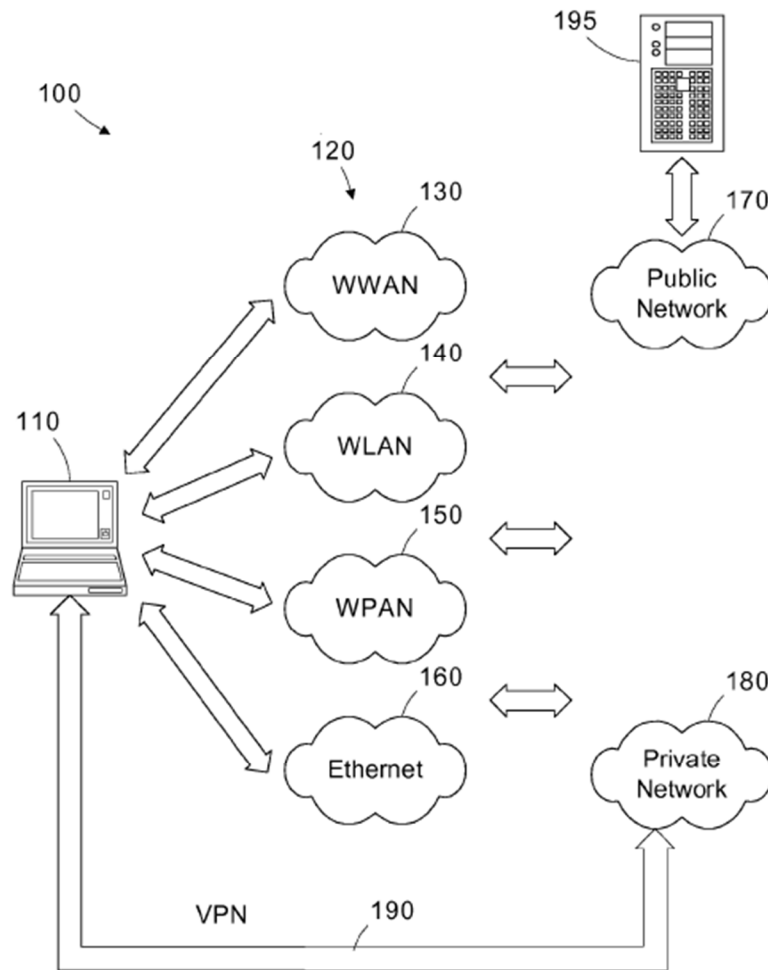


Figure 1

SAMSUNG-1029, FIG. 1

152. Cole addresses situations in which the bandwidth being used on a connection approaches a bandwidth limit, which can cause performance of the device and its applications to degrade.

SAMSUNG-1029, [0073]. In one example, “if the connection is

being used nearly to capacity and an additional application is executed that requires still more bandwidth, the connection may not be able to support the total load” so “running applications may experience increased latency for data transfers.” *Id.* In response, Cole’s connection manager “tries to proactively prevent increased latency from an overloaded connection from impacting the performance of the running applications or the efficiency of the user.” *Id.*, [0074].

153. In response, “[w]hen the monitored load exceeds a predetermined threshold (e.g., 85% of capacity),” the connection manager “may take one of several actions to manage the load” including “attempt[ing] to establish a connection with a higher bandwidth,” e.g., attempting to connect “to a visible or invisible network 120 having higher capacity.” *Id.*, [0075], [0077].
154. To determine which network interface to use, the connection manager “evaluates availability, bandwidth, user preferences, application requirements, mobile device resources, etc.” *Id.*, [0036]. The connection manager identifies “available connections and uses the default hierarchy to select a particular communication interface 225 to configure.” *Id.*, [0045]. While

an example default hierarchy can be “LAN, WLAN, WWAN, WPAN,” the user can override the default hierarchy by setting “preferences for fast connect, including disabling the function entirely or selecting particular networks that may or may not be used.” *Id.*, [0042], [0067]. Cole gives an example in which “a user may not want to use a 3G network for fast connection because the use may incur added costs per connection,” but “if the user has an unlimited usage plan, the user might want to always prefer 3G for the fast connect function.” *Id.*, [0067]. In summary, Cole’s connection manager “attempts to establish connectivity to the fastest eligible connection based on the connection time data and the user's preferences.” *Id.*

I. Rao-Jones-Cole Combination

155. Jones describes applying rules based on “type of connection, connection bandwidth, [and] user priorities.” SAMSUNG-1006, 5:14-15. Additionally, as I discussed in §VIII.I, a POSITA would have recognized that while total bandwidth of a connection is relevant, also relevant is the bandwidth available at a given time. Consequently, a POSITA would have looked to references such as Cole, which teaches determining whether

monitored load (e.g., “85% of capacity” exceeds a predetermined threshold. SAMSUNG-1029, [0075]. A POSITA would have recognized that by monitoring currently-available bandwidth, and seeking better connections when such bandwidth fails to satisfy the device’s needs, the device can ensure that the available bandwidth supports the demands of applications running on the device. SAMSUNG-1029, [0075], [0077].

156. In operation, in the resulting Rao-Jones-Cole Device (RJCD), when the device determines that available bandwidth fails to satisfy a threshold (e.g., exceeds the 85% threshold described in Cole), the device uses control policies relating to connection order (per Cole) to select a network with higher-bandwidth. SAMSUNG-1029, [0036], [0045], [0075], [0077]. At least since control policies indicate connection order, and connection order is a user preference (“a default hierarchy of connection preferences may be used”), RJCD control policies are based on user preference. SAMSUNG-1029, [0042], [0067]. Cole further states that the “mobile device 110 implements a connection manager 260 (e.g., a software application) that

manages the various communication interfaces 225 to determine which connections should be active at any given time,” and “the connection manager 260 evaluates availability, bandwidth, *user preferences*, application requirements, mobile device resources, etc. to select a particular communication interface 225.”

SAMSUNG-1029, [0036]. (See also the analysis of [1.7b], which discusses connection order.) RJCD then uses the techniques of Jones to determine whether a particular transfer is permitted over a connection, and if so, uses the priority-queueing techniques of Rao to manage use of the connection bandwidth. SAMSUNG-1005, [0184]; SAMSUNG-1006, 3:55-67. As described above, Rao’s and Jones’s policies are also based on user preference, with Rao explaining “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,” and Jones explaining, “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-1005, [0183]; SAMSUNG-1006, 6:36-41.

157. The components of RJCD each operate as they would in isolation. 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 before the Critical Date. *Id.* 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. *Id.*; *KSR*, 550 U.S. at 417.

158. RJD’s processor would be configured to perform the operations discussed in this Ground. *See* §IX.A.

J. U.S. Pat. App. Pub. No. 2009/0207817 (“Montemurro”)

159. Montemurro describes communication devices “capable of at least two communication modes,” e.g., WLAN and WWAN, that “can be configured to optimize communications using a policy-based mechanism to configure connections and routes.” SAMSUNG-1008, Abstract. A “rules engine evaluates its

policies on a state change (e.g. network availability, time of day, etc.) to configure a routing table” and “provides an appropriate connection to an application for its respective communications.”

Id. Policies can be responsive to various factors (e.g., bandwidth, cost, time of day, application type, etc.). *Id.* “Rules engine 206A configures the communication operations with a set of rules/policies.” *Id.*, [0029].

160. Montemurro describes a “natural language example of a policy” where “the MP3 download application 204D runs on the lowest cost network” available. *Id.*, [0029]. In another example, “the CRM application ... only synchronizes the sales contact database (e.g. 120B) over a WLAN network.” *Id.*
161. Figure 2 (below) shows a device configured with Montemurro’s system. *Id.*, [0025]-[0037].

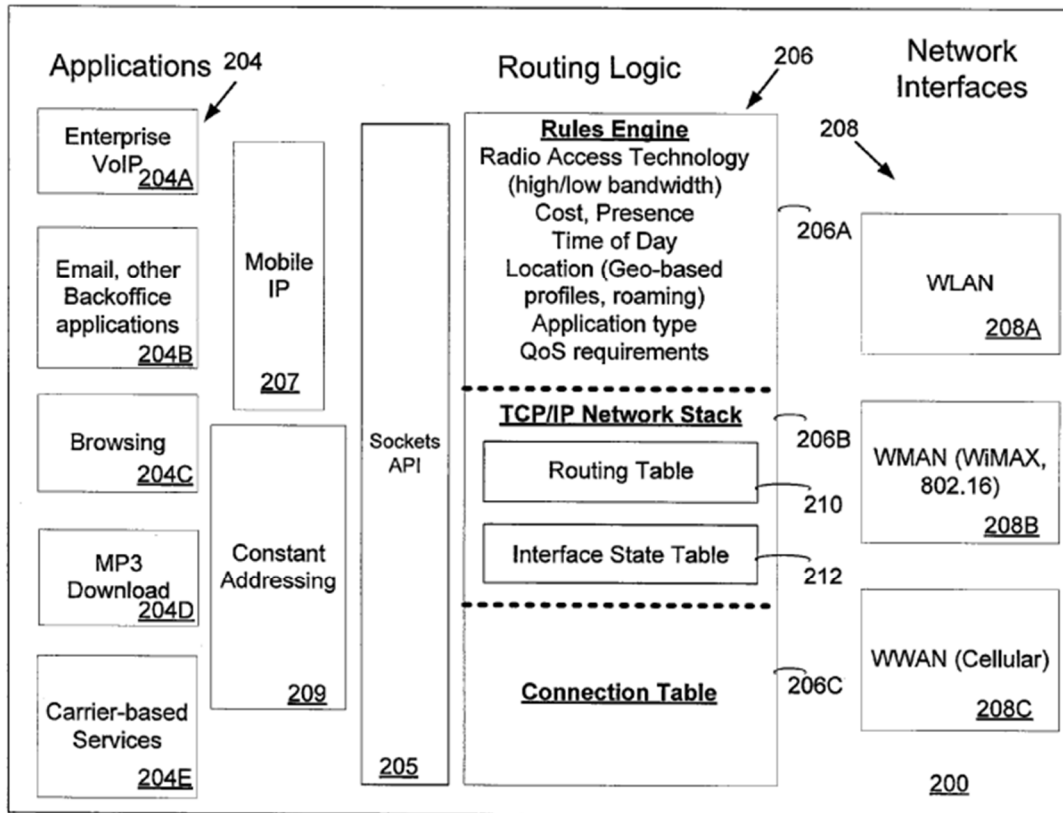


Figure 2

SAMSUNG-1008, FIG. 2

162. Montemurro explains that various applications can benefit from network selection techniques, including VoIP, email, and MP3 downloading applications. *Id.*, [0025]-[0037].

K. Rao-Montemurro Combination

163. As described above, the RD would use Rao's techniques to manage network access using priority-based queues. *See* §IX.A. However, a POSITA would have recognized that, when a device

has multiple network interfaces,²⁰ further efficiency and cost savings would be gained by assigning different applications to different networks, such as in the examples from Montemurro, where “the MP3 download application 204D runs on the lowest cost network ... available” and “the CRM application ... only synchronizes the sales contact database ... over a WLAN network.” SAMSUNG-1008, [0029]. In Montemurro’s example, the MP3 download is assigned to a low-cost network since the download is cost-sensitive, but not time-sensitive, and the CRM synchronization is assigned to a WLAN since database synchronization can require large data transfers. Thus, to improve the operation of RD and further improve efficiency, a POSITA would have looked to teachings of other references, such as Montemurro.

164. In operation, the resulting Rao-Montemurro Device (RMD) (i) uses the techniques of Montemurro to select the most

²⁰ Devices with multiple network interfaces were common as of the Critical Date. For example, Jobs’s device included GSM, EDGE, CDMA, 802.a, 802.11b, Wi-MAX, etc. SAMSUNG-1051, [0100], [0180], [0213]-[0214]

appropriate network for an application (e.g., CRM over WLAN), and (ii) uses Rao's priority queuing to manage network access. *See* §IX.A; SAMSUNG-1008, Abstract. In one example, VoIP, email and backup are assigned to a WLAN network (per Montemurro), and Rao would prioritize the real-time traffic of VoIP over the backup and email traffic.²¹ SAMSUNG-1005, [0003], [0179]-[0184].

165. RMD's processor would be configured to perform the operations in [5] for at least the reasons described above. *See* §IX.A.
166. Combining Rao and Montemurro would have involved (1) combining prior art elements according to known methods to yield predictable results; and (2) use of known techniques to improve similar devices (methods, or products) in the same way. *See* MPEP §2143. The combination would have amounted to nothing more than the use of a known technique to improve similar smart phone devices equipped with network interfaces in

²¹ If a WWAN was also available, the email application could be assigned to that network, but even without the email traffic, a backup over WLAN could disrupt real-time VoIP traffic.

a similar way and combining prior art elements according to known methods to yield the predictable results described above. *KSR*, 550 U.S. at 417.

L. U.S. Pat. App. Pub. No. 2009/0185527 (“Akhtar”)

167. Akhtar explains that “[a]pplications using wireless technology for data delivery have to explicitly reserve network resources before data can be exchanged to meet unique resource requirements for the content being transmitted.” Akhtar, [0016]. Such reservation must “be done by the originating and terminating parties for satisfactory communication since various media content have specific requirements in terms of delay and jitter tolerance,” which can be characterized as “delay sensitive, rate sensitive, time sensitive, or some other quality adversely impacting the communication.” SAMSUNG-1009, [0016].
168. In response, Akhtar teaches “a communication protocol on a wireless communication network to allocate network resources” in which a “radio network controller maintains quality of service (QoS) profiles.” SAMSUNG-1009, Abstract. Akhtar is “aimed toward reserving resources to support communications between”

access devices (“access terminals”) and “IP based network 3 specifically.” SAMSUNG-1009, [0028].

169. In Akhtar, a radio network controller (RNC) “learns the nature of the content from the requests reserved by the originator of media and sets aside resources a priori for the terminating end without waiting for a request” from the terminating access terminal. SAMSUNG-1009, [0017]. To accomplish resource reservation, “[a] serving node determines the type of application in a communication call and determines a QoS policy it transmits to the radio network” and “[t]he radio network identifies the QoS profile based on the received policy and allocates network resources before announcing the call to an access terminal.” SAMSUNG-1009, Abstract.

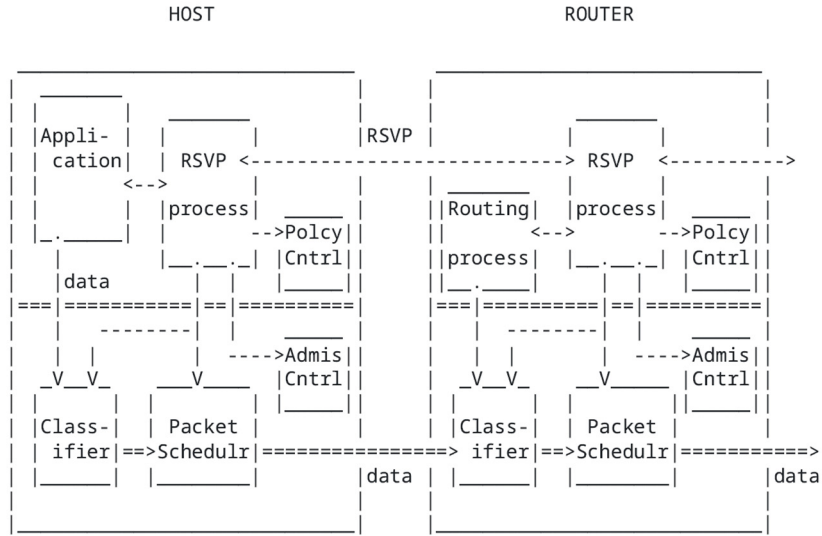
M. Rao-Akhtar Combination

170. Rao’s RAC “controls network communication prioritizations on the client” where “the prioritizations are based on priorities of the application on the client.” SAMSUNG-1005, [0080]. Such network communication is “generally described in connection with an internet protocol (IP) based protocol.” SAMSUNG-1005, [0082].

171. However, as I described in §VII.E, a POSITA would have recognized that Rao’s client-side prioritization is insufficient to achieve end-to-end communication network requirements. For example, since intermediate networking devices receive packets from multiple devices, each potentially running different applications, and only some running RAC, packets arriving at the intermediate device do not necessarily reflect intended transmission priorities. If such intermediate devices do not reserve resources to support communications between devices (per Akhtar), traffic from a high priority application might not be sufficient to meet the application’s requirements. As a result, as Akhtar explains, “[a]pplications using wireless technology for data delivery have to explicitly reserve network resources before data can be exchanged to meet unique resource requirements for the content being transmitted.” Akhtar, [0016].
172. Consider, for example, a networking device, such as a wireless access point that is providing connectivity to a large set of mobile devices. Some devices are running real-time, interactive applications, such as VoIP, while others are running non-real-time applications such as downloading new applications or

uploading photos. Absent resource reservation, traffic from the applications that do not have real-time requirements will impair operation of the higher priority, interactive applications. In one example, if a networking device receives packets from 25 devices running non-real-time applications and one device running a real-time application, if the networking device cannot tell which applications do and do not have real-time requirements, the device will process packets first-in-first-out, which results in 25 packets from non-real-time applications being transmitted for each packet from the real-time application. Note that any queuing that occurs at the device running the real-time application does not address this situation since packets are arriving from other devices, which are not running real-time applications.

173. This problem was recognized long before Akhtar. For example, IETF RFC 2205 defined the “Resource ReSerVation Protocol (RSVP),” which “is used by a host to request specific qualities of service from the network for particular application data streams or flows.” SAMSUNG-1036, 4. The RSVP architecture is illustrated in Figure 1, reproduced below.



SAMSUNG-1036, Figure 1.

174. Consequently, to ensure end-to-end priority delivery of packets (e.g., from application with real-time constraints), a POSITA would have been motivated to implement RD's RAC as a terminal device in Aktar's wireless communication network. In the resulting Rao-Akhtar Device (RAD), to attain end-to-end priority, applications reserve network resources (per Akhtar), and to ensure on-device priority, when RAD transmits data, packets are sent according to Rao's application-aware prioritization. SAMSUNG-1005, [0179]-[0195]. In the resulting system, packets leave RAD according to priority (per Rao) and are processed by the intermediate network according to the appropriate QoS profile (per Akhtar).

175. Thus, the components of RAD as modified by Akhtar each operate similarly to how they operate in isolation. A POSITA would have had a reasonable expectation of success in creating the combination, which would have required only routine programming knowledge well within the skill of a POSITA before the Critical Date. *Id.* 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. *Id.*; *KSR*, 550 U.S. at 417.
176. RAD’s processor would be configured to perform the operations discussed in this Ground. *See* §IX.A.

N. U.S. Pat. App. Pub. No. 2009/0228951 (“Ramesh”)

177. Ramesh explains that “[i]n the next-generation distributed computing environment, large scale system of systems may have a large number of roaming mobile nodes/device,” which can “carry out the intended commercial, military, or social processes.” SAMSUNG-1011, [0001]. However, “constant and rapid changes of business requirements at the application level” can require rapid re-configuration of security parameters in both

the mobile and static environments, and these roaming nodes/devices may need to comply rapidly to conform with new high level business requirement updates.” SAMSUNG-1011, [0004].

178. Ramesh’s disclosure provides “policy-managed communities of interest within which individuals may access network-connected data, computing, tooling and other assets they may need to engage.” SAMSUNG-1011, [0021]. In Ramesh’s architecture, “assets may be kept under the control of a policy manager” and “assets may be protected so that they respond only to requests from subjects based on the approval of entitlement-specifying policies.” SAMSUNG-1011, [0021].
179. In Ramesh, a policy distribution node (PDN) distributes routing security policies to policy decision points on mobile clients (MCs) via a policy exchange channel (PXC). SAMSUNG-1011, [0036]. Since not all MCs carry security policies, a PDN can distribute the appropriate set of security policies to the MCs based on their mandatory access control identities and roles. SAMSUNG-1011, [0036]. Ramesh further explains that the PXC may provide a secure security assertion protocol that

allows distribution of policies from the PDN to the policy decision point (PDP) through the policy enforcement point (PEP), e.g., using existing industry standards such as SAML (security assertion markup language), RMI (remote method invocation), TLS (transport layer security), or SSH FTP secure extension (RFC-2228). SAMSUNG-1011, [0037].

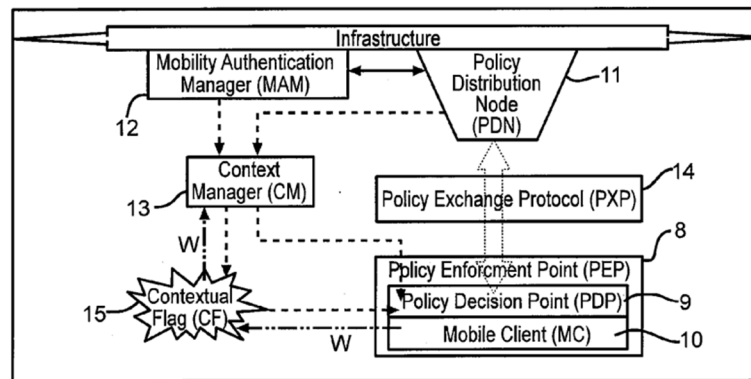


FIG. 3

Ramesh, FIG. 3.

180. As I described in §VII.B, the general policy architecture, include a PDP, PEP and a policy repository that provided policies to PDPs, was well-known as of the Critical Date.

O. Rao-Ramesh Combination

181. Rao teaches that policies “may be accessible by the agent,” “configured into the agent,” or “loaded by the agent.”

SAMSUNG-1005, [0183]. In one example, Rao explains that

the “policies may be provided by or downloaded via the gateway,” which is one example of a network element. *Id.* A POSITA would have recognized that policy distribution from Ramesh’s PDN to a mobile client (as taught by both Rao and Ramesh) is an example of a policy being “configured into the agent” and/or “loaded by the agent,” as taught by Rao. More generally, it is an instance of the policy architecture explained in Verma. SAMSUNG-1032, 1-2; *see* §VII.B. Therefore, a POSITA would have been motivated to modify the RD with Ramesh’s teaching of secure policy distribution to prevent tampering with policies during distribution, e.g., preventing hackers from intercepting the policies before they arrive at the device and making malicious alterations.

182. In the resulting Rao-Ramesh Device (RRD), secure policy distribution advantageously prevents policy tampering, e.g., in “avionic hardware/software of airplanes” where “[c]ompromised data content may potentially lead to fatal consequences.” SAMSUNG-1011, [0024]. In RRD, policies can be configured into the device (e.g., as taught by Rao) and/or downloaded from

a network element (PDN) over a secure link (as taught by Ramesh). SAMSUNG-1005, [0183].

183. Whether to configure policies through a user interface (e.g., as described in Rao at SAMSUNG-1005, [0183]) or load them from the agent will largely depend on the situation. Configuring a single device is typically done most efficiently at the device; providing a common configuration to hundreds or thousands of devices can be done at scale using network management devices (e.g., Mobile Device Management (MDM) in the context of mobile devices) by setting the policies at a server and loading them onto the devices. In fact, the two approaches are not mutually exclusive: a base set of policies can be loaded onto a set of devices, and users can be given the option to tailor the policies at their devices using a local interface, as is common in most environments with distributed network management.
184. Thus, the components of RRD each operate similarly to how they operate in isolation. A POSITA would have a reasonable expectation of success in creating the combination, which would have required only routine programming knowledge well within the skill of a POSITA before the Critical Date. *Id.* 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. *Id.*; *KSR*, 550 U.S. at 417.

185. RRD’s processor would be configured to perform the operations discussed in this Ground. *See also* §IX.A.

P. U.S. Pat. No. 5,987,611 (“Freund”)

186. Freund addresses challenges, including “hording[sic] available network bandwidth through use of bandwidth-intensive applications (e.g., real-time audio programs).” SAMSUNG-1013, 2:12-14. In one example, Freund’s system monitors “access to the Internet by individual applications” which “allows the system ... to not only track Internet traffic” but also “determine in many cases data exchanged on a per application basis.” SAMSUNG-1013, 11:9-15. Freund explains that “per application monitoring simplifies the task of tracking bandwidth utilization for a network, including providing detailed review on how the Internet access is being used” which “greatly eases planning of hardware and connection requirements.”

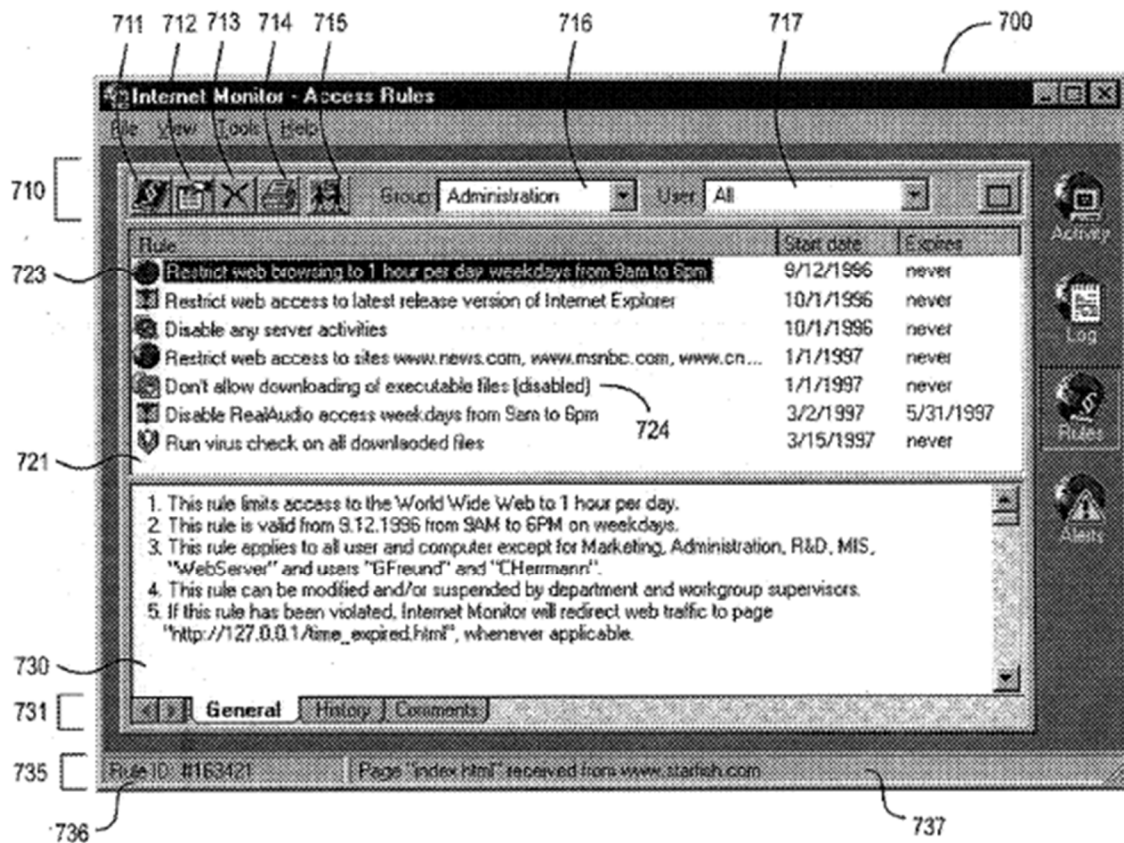
SAMSUNG-1013, 11:20-25. In addition, “[i]nadvertent disruptions of the network by individual users, such as bandwidth hording by a user using RealAudio for listening to a Web audio ‘broadcast,’ can be averted.” SAMSUNG-1013, 11:25-28.

187. To address such issues, Freund uses “access rules” for efficient use of computing resources and controlling the use of networks. SAMSUNG-1013, 3:62-67. “[A]ccess rules can include criteria such as total time a user can be connected to the Internet,” “time a user can interactively use the Internet,” and “a list of applications or application versions that a user can or cannot use in order to access the Internet,” among others. *Id.*, 4:8-19.
188. To enforce the rules, Freund includes “bandwidth and interactive use monitoring” during which a Client Monitor intercept networking calls and “[a]dds the data lengths to a DataIn or DataOut accumulator or counter of the Application's list entry and global activity record.” SAMSUNG-1013, 30:11-26. The Client Monitor then checks whether “the DataIn or DataOut fields exceed rule-based quantity either for the specific Application or the user/workstation,” and if so “the Client

Monitor disables future Internet access and/or warns the user.”

Id., 30:26-29.

189. To enable rule configuration, “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-1013, 24:16-24. Figure 7A (below) shows an example UI panel.



SAMSUNG-1013, FIG. 7A.

190. Policies are loaded from a network element (“supervisor”), and “the Supervisor filters rules appropriate for the client ... and transmits them to the Client Monitor.” SAMSUNG-1013, 28:14-18. The Client Monitor “saves a copy of the rules onto a local hard disk” where they are ready for use. SAMSUNG-1013, 28:18-19. Such a configuration is similar to the one described in Ramesh. *See* §VIII.R, §VIII.S. I also described techniques for storing and distributing policies in §VII.B.

Q. Rao-Freund Combination

191. Rao and Freund describe using policies/rules to control network traffic. For example, as described above, Rao “may apply a policy to determine a condition of the client 105 ... at the time of transmission of the packet.” SAMSUNG-1005, [0109]. Further, the frame monitor “may identify an application 338 that generated the packet,” and the frame monitor “may make a policy-based determination to transmit the packet to the gateway 340 responsive to the identified application.” *Id.* Rao explains such “*policies 520 may be specified by any suitable means and/or mechanisms,*” including the name or type of the application, “the type of one or more protocols used by the

applications 338a-338n and/or the size of the payload of the network packet,” and “whether an application is running in the foreground or the background of the client.” *Id.*, [0182]-[0184]. Rao notes that a POSITA “will recognize and appreciate the multitude of ways to define client-side application priorities.” *Id.*

192. A POSITA would have recognized that the network traffic control policies of Freund are simply additional examples of client-side policies, such as those Rao contemplates. For example, Freund includes “access rules [that] can include criteria such as total time a user can be connected to the Internet ... time a user can interactively use the Internet ... a list of applications or application versions that a user can or cannot use in order to access the Internet, a list of URLs (or WAN addresses) that a user application can (or cannot) access, a list of protocols or protocol components ... that a user application can or cannot use” and a “rule-based quantity either for the specific Application or the user/workstation” limiting network data use. SAMSUNG-1013, 4:9-19. 30-26-29. A POSITA would have naturally recognized that Freund’s policy examples are among

the “multitude of ways to define client-side application priorities” described in Rao and recognized that Freund’s policy examples could be incorporated in Rao. SAMSUNG-1005, [0182]. In fact Freund even describes a “a list of applications or application versions” and Rao lists “the name of the application 338 a-338 n and/or the type of application 338 a-338.” SAMSUNG-1005, [0182]; SAMSUNG-1013, 13:6-8.

193. Rao further teaches that policies “may be configurable by a user by any suitable means and/or mechanism ... such as a user interface, graphical or otherwise, design and constructed for configuring or specifying the policies.” SAMSUNG-1005, [0183]. For details on the UI, a POSITA would have looked to references such as Freund, which shows “bitmap screenshots illustrating a preferred user interface or ‘wizard’ dialog for configuring rules” including a preferred interface that “provides a ‘view’ of rules governing operation of the Internet access monitor, displaying all of the rules which are available for a current configuration.” SAMSUNG-1013, 6:47-49, 24:17-20, FIGS. 7A-K. Such a UI allows a user to create, edit, or delete rules. SAMSUNG-1013, 24:22-24. In fact, policy user

interfaces were well-known as of the Critical Date, as I described in §VII.B.

194. Rao explains that policies “may be accessible by the agent 326, configured into the agent 326, or loaded by the agent 326,” e.g., the policies “may be provided by or downloaded via the gateway.” SAMSUNG-1005, [0183]. For implementation details on how to obtain the policies, a POSITA would have looked to references such as Freund. As described above, Freund teaches an example of policies being loaded by an agent: “the Supervisor filters rules appropriate for the client (i.e., application, Host, and other rules), and transmits them to the Client Monitor.” SAMSUNG-1013, 28:14-18.
195. Because both Rao and Freund teach using policies/rules to control network traffic, including defining and loading policies/rules, it would have been obvious to a POSITA to combine the teachings of Rao and Cole with Freund’s teachings to achieve the benefits of Freund’s UI for configuring rules and for more detailed enumeration of network traffic control policies contemplated but not explicitly described in Rao.

196. In operation, the resulting Rao-Freund Device (RFD) would use policy-based traffic management techniques of Rao and Freund to use networks efficiently. SAMSUNG-1005, [0182]-[0183]; SAMSUNG-1013, 4:9-19. Freund's Client Monitor function is included in RFD's RAC. For example, Rao teaches that RAC "transparently intercepts network communications associated with applications executing on the client ... and determines priorities for the network communications based on a priority for the application." SAMSUNG-1005, [0080]. A POSITA would have recognized that RAC's transparent interception can be accomplished using Freund's teaching that an application calls an API (e.g., WinSock send()), and the Client Monitor intercepts the call. SAMSUNG-1013, 30:16-17. RFD adds the data lengths (measure of usage) to a counter associated with the application and uses the counter to apply rules (as described by Freund). SAMSUNG-1013, 30:24-29.
197. In addition, the policies governing the operation of RFD would be configured with the UI techniques of Freund and/or loaded from a network element using the techniques of Rao and Freund. SAMSUNG-1005, [0182]-[0183]; SAMSUNG-1013, 24:22-24.

198. The components of RFD each operate as they would in isolation.

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 before the Critical Date. *Id.* 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. *Id.*; *KSR*, 550 U.S. at 417.

199. RFD's processor would be configured to perform the operations discussed in this Ground. *See also* §IX.A.

R. U.S. Pat. App. Pub. No. 2010/0281154 (“Bedi”)

200. Bedi explains that “[i]t is impossible to maintain an adequate log file on some pervasive devices, since the required storage space may run to many megabytes and the available storage may quickly fill up.” SAMSUNG-1030, [0004]. In response, Bedi teaches a monitoring apparatus that “includes a publishing capability for transmitting log data, output by monitoring and control applications, to a publish/subscribe message broker system.” *Id.*, [0038]. Bedi's “invention makes use of

publish/subscribe mechanisms to provide access to an application's log data that conventionally would be saved to a local log file,” but that “do not have sufficient non-volatile storage capacity to store a large log file locally.” *Id.*, [0039]. A messaging program then passes the publication to a message broker system which identifies subscribers for each publication and transmits the publications across the network to the respective identified subscribers. *Id.*, [0066].

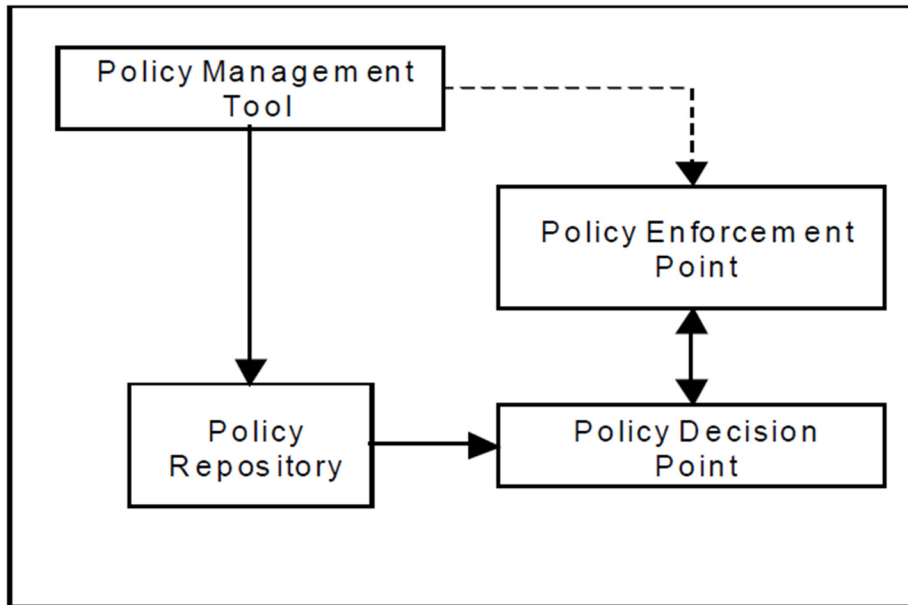
S. Rao-Freund-Bedi Combination

201. A POSITA would have recognized that RFD is a pervasive (mobile) device as taught by Bedi. In cases where RFD lacked the resources necessary to evaluate policies, e.g., lacking storage space and/or computational resources needed to accumulate the data required to evaluate policy conditions, or where such policies would be more efficiently evaluated in a centralized or remote manner, a POSITA would have looked to references such as Bedi, which teaches remote monitoring of resources-constrained devices. SAMSUNG-1030, Abstract, [0004].
202. In a system including RFD and as modified by Bedi, monitoring data are transmitted via a message broker to a subscriber tasked

with aggregating quantified monitoring data and providing the data to a policy decision point (PDP), which can be, but need not be, the RFD. (See the discussion of PEP/PDP in §VII.B) The PDP evaluates the policy and provides the decisions (e.g., whether to block the traffic, per Freund) to RFD for enforcement. As a result, the policy-based management provided by RFD can operate even when the resources (e.g., storage) of RFD are insufficient to support that function. In addition, while RFD might begin with sufficient storage resources (when first turned on), as users operate the device, adding applications and data, at some point, the resource requirement of policy-based management can exceed the *available* resources of the device. Combining RFD with Bedi addresses that issue by offloading aspects of policy-based management to a remote device.

203. The concepts of policy decisions points (PDPs) and policy enforcement points (PEPs) were well-known in the art as of the Critical Date. For example, as I described in §VII.B, Verma explains that “policy framework defined by the IETF/DMTF consists of four basic elements,” which are “the policy

management tool, the policy repository, the policy enforcement point (PEP), and the policy decision point (PDP),” as illustrated below. SAMSUNG-1032, 1.



Id.

204. Verma further states that the “logical entities that can take actions to enforce the policies are known as the policy enforcement points (PEPs)” and the “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.” *Id.*, 2.

205. Regarding the location of enforcement, in one example, “the PEP would be the function inside the router that makes QoS

decisions” and the “PDP would be a software module inside the same router (**or another router**) that decides which set of DiffServ markings are to be active at any given time.” *Id.*

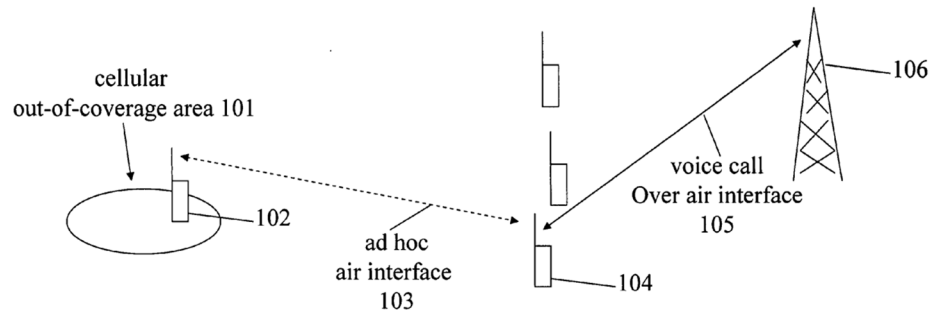
Importantly, by noting that the PDP can be a software module in a different router (“another router”), Verma confirms both that the PDP and PEP can run on different devices, and that PDPs were known to execute on routers (“network elements”).

206. The components of RFD as modified by Bedi each operate as they would in isolation. 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 before the Critical Date. 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. *Id.*; *KSR*, 550 U.S. at 417.

207. RFD’s processor would be configured to perform the operations discussed in this Ground. See §IX.A.

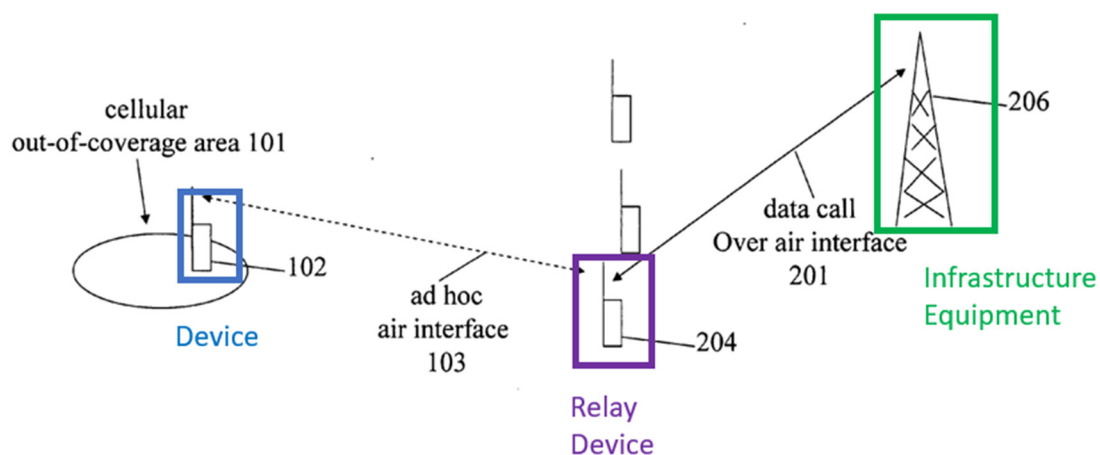
T. U.S. Pat. App. Pub. No 2007/0032230 (“Pregont”)

208. Pregont addresses situations where a “communication unit 102 existing within area 101 is unable to communicate directly with infrastructure equipment 106.” SAMSUNG-1012, [0003].



SAMSUNG-1012, FIG. 1.

209. In response, Pregont describes “a method and apparatus for relaying calls.” SAMSUNG-1012, [0011]. “By utilizing ad-hoc networking, communication unit 102 communicates with communication unit 104 (via ad-hoc air interface 103)” and “[c]ommunication unit 104 then relays the communication to infrastructure 106 via air interface 105.” SAMSUNG-1012, [0003]. In the annotated figure below, communication unit 104 is called “relay device,” since it provides relay services.



SAMSUNG-1002, FIG. 2 (annotated)

210. Pregont notes that, “[t]o be able to relay a call, communication unit 104 must be equipped to hold a simultaneous call over the ad hoc link (802.11, Blu-tooth, etc) and the cellular link (GSM, CDMA2000, etc).” Id., [0004]. The communication unit includes “cellular and ad-hoc receivers 301 and 303, respectively, cellular and ad- hoc transmitters 302 and 304,” and “the cellular air interface (utilizing a cellular over-the-air protocol) typically serves long-range communication, while the ad-hoc air interface (utilizing an ad-hoc over-the-air protocol) serves short- range communication.” SAMSUNG-1012, [0020].
211. In Pregont, “[w]hen a first communication unit (204) receives a request from a second communication unit (102) (over an ad hoc

network) to relay a call, the first communication unit will start a data call (e.g., voice over IP call) over the cellular link using the cellular phone's data capability.” SAMSUNG-1012, Abstract.

212. Pregont further notes that “a need exists for a method and apparatus for relaying calls which allows the relaying device to complete multiple simultaneous calls.” SAMSUNG-1012, [0004]. Otherwise, as Pregont explains, “[o]nce communication unit 104 is relaying the call, it is incapable of making a phone call of his own since communication units typically only have one transmitter.” *Id.* This would have limited the usefulness of the device to the device owner, and Pregont’s techniques address this potential downside by providing a mechanism for a device to relay data, providing value to other devices, while not impairing the device’s function for its primary user.
213. When, “during a relayed call, the first communication unit decided to make a phone call of its own, they would dial the number as usual,” and “[t]he phone, knowing that it is currently relaying another call, would not set up the call as a normal cellular call; instead, it would use the existing data call to piggyback a message to the infrastructure equipment,” and “the

two VoIP sessions would co-exist on the single data session between the cellular phone and the infrastructure equipment.” SAMSUNG-1012, [0012].

U. Rao-Jones-Pregont Combination

214. Rao describes a computing device with applications, e.g., IP telephony and other applications. SAMSUNG-1005, [0088], [0179]. Pregont similarly describes a communication device, enhanced with the ability to make calls and relay traffic simultaneously. SAMSUNG-1012, [0004], [0011]-[0012]. To enable Rao’s device to extend the communication range of other devices, a POSITA would have been motivated to include Pregont’s call-relay application as an additional application on Rao’s device. The resulting device both executes applications (e.g., the applications enumerated by Rao), and relays telephony traffic, as described in Pregont. SAMSUNG-1005, [0179]; [0180]; SAMSUNG-1012, [0011]-[0012].
215. However, a POSITA would have further understood that, when multiple applications use the network, as would be the case in Rao alone (e.g., running e-mail, video conferencing, etc.) and in the Rao-Pregont combination (which runs those applications and

telephony relays), network bandwidth can be exhausted. For example, Gupta gives exemplary network limits such as “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-1054, [0004]. A POSITA would have recognized that other networks will also have limits that depend on factors such as physical limits, protocol efficiency, etc.

216. When multiple applications are contending for bandwidth, network capacity can be exhausted. On lower bandwidth networks (e.g., 3GSM), this can occur quickly, and even higher-bandwidth networks can be saturated by communication-heavy applications.
217. To avoid overwhelming network capacity, adversely impacting all device applications that use the network,²² a POSITA would

²² Saturating the network can also result in adverse impact to the CPU, which is involved in network transmissions, so even applications that do not use the network can suffer.

have looked to references such as Jones,²³ which teaches that applications can be denied network access when bandwidth is insufficient. SAMSUNG-1006, 5:13-15. Denying network access to certain application preserves bandwidth for others.

218. As described above, Pregont uses VoIP to communicate between the relay station and the downstream communication infrastructure. SAMSUNG-1012, Abstract. In such cases, Jones teaches applying rules “to data transfers depending on the desired functionality, type of connection, connection bandwidth, user priorities, etc.,” and such rules “may prohibit data transfers.” SAMSUNG-1006, 5:13-26. Thus, a POSITA would have recognized that, when the device’s bandwidth is constrained, Jones teaches prohibiting data transfers, e.g., by the relay application (a type of functionality, as described in Jones). Further, since Pregont’s relay service is providing value to *other* devices, a POSITA would have recognized that the owner of the device benefits by blocking traffic from the relay application

first, preserving bandwidth for applications that benefit the device's owner, not other devices.

219. The resulting Rao-Pregont-Jones Device (RPJD) is a conventional mobile computing device (per Jobs) that provides relay services to other devices (per Pregont). SAMSUNG-1005, [0086]-[0096]; SAMSUNG-1012, [0004], [0011]-[0012].

When a different communication device is outside cell coverage, it connects to RPJD, which provides relay services (using VoIP) between that device and the infrastructure equipment, as taught by Pregont. SAMSUNG-1012, [0004], [0011]-[0012].

Additionally, per Jones, RPJD determines whether sufficient bandwidth exists for the relay application; if bandwidth is insufficient, RPJD denies network access to the relay application. SAMSUNG-1006, 5:13-26. In essence, RPJD donates excess bandwidth to other devices via the relay service, but when no excess bandwidth exists, RPJD blocks traffic from the relay application.

220. Per Jones, RPJD presents "a graphical user interface," enabling policies to be "configured by a user such as a system administrator." SAMSUNG-1006, 6:36-41. As described in

§VII.B, user interfaces for specifying policy were well-known before the Critical Date.

221. The components of RPJD each operate similarly to how they operate in isolation. A POSITA would have a reasonable expectation of success in creating the combination, which would have required only routine programming knowledge well within the skill of a POSITA before the Critical Date. 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. *Id.*; KSR, 550 U.S. at 417.

222. RPJD's processor would be configured to perform the operations discussed in this Ground.

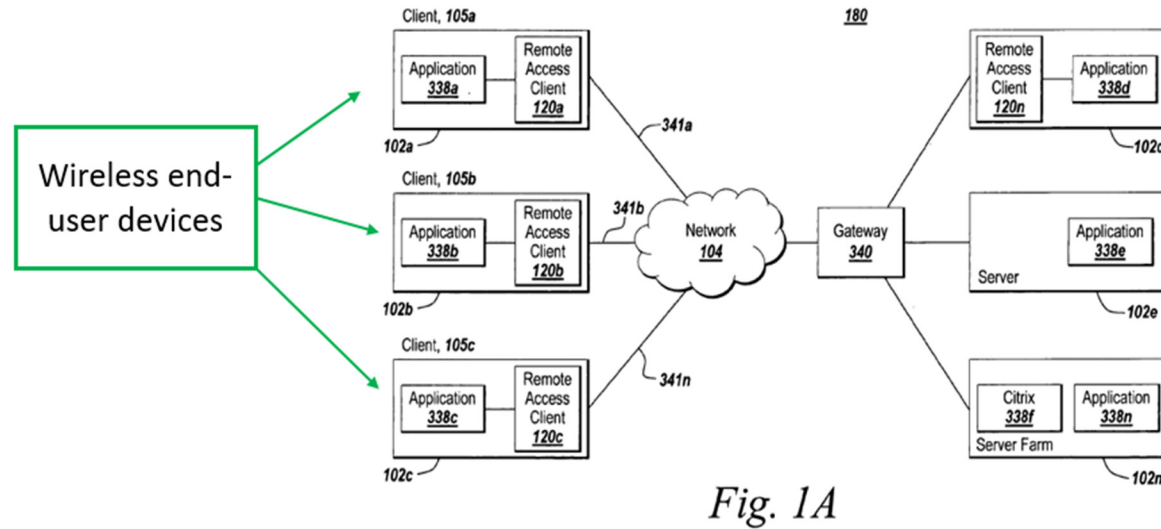
X. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '811 CLAIMS UNPATENTABLE

A. Ground 1A: Rao renders claims 1, 3, 6, 8-11, 14 and 19-20 obvious

[1.1] A wireless device, comprising:

223. To the extent the preamble is limiting, Rao teaches or renders it obvious.

224. Rao teaches a client (Rao Device or RD) that is a “wireless end-user device,” shown in Figure 1A:



SAMSUNG-1005, FIG. 1A (annotated), [0086]-[0093]

225. Rao discloses an environment that “includes multiple computing devices 102a-102c (also referred to as clients 105a-105c) connected to a network.” SAMSUNG-1005, [0086]. The computing device can be any number of devices, including a “**handheld computer**,” “**mobile telephone**,” “**smart phone**,” or “other form of computing or telecommunications device.”

SAMSUNG-1005, [0130], [0198].

[1.2] one or more modems for enabling the wireless device to communicate over at least a first wireless network;

226. Rao teaches or renders [1.2] obvious. SAMSUNG-1005, [0095], [0125], [0172], [0198].
227. Rao explains that the client “may be ... a smart phone” and includes teachings regarding a wireless modem to communicate data for Internet service activity, e.g., the computing device includes a network interface, which can comprise a “modem.” SAMSUNG-1005, [0125], [0198]. The network interfaces to the Internet through connections, including wireless connections which can use 802.11 wireless protocols. SAMSUNG-1005, [0095], [0125]. Therefore, a POSITA would have understood or found obvious that Rao’s device includes a modem to communicate over a wireless network.
228. More generally, a POSITA would have known that wireless devices commonly included wireless modems as of the Critical Date. For example, the first iPhone was shown in Time Magazine’s Invention of the Year in 2007 and included wireless data capabilities.²⁴ Similarly, as demonstrated by at least Jobs (in a patent application assigned to Apple Inc, maker of the

²⁴ See, e.g., SAMSUNG-1052.

iPhone), wireless devices were known by the Critical Data to include modem circuitry and communicate over wireless networks. SAMSUNG-1051, [0100].

[1.3] a user interface;

229. Rao teaches or renders [1.3] obvious. SAMSUNG-1005, [0095], [0125], [0172], [0198]; *supra*, §IX.A.
230. Rao’s agent “may provide a configuration mechanism such as a user interface, graphical or otherwise, design and constructed for configuring or specifying the policies.” SAMSUNG-1005, [0183]. Rao further states that “policies 520 may be configurable by a user by any suitable means or mechanism.” In fact, techniques for users configuring or specifying the policies as described in Rao were well known by the Critical Date and would have been obvious to include for permitting user configurability based on Rao’s disclosure and a POSITA’s general knowledge of user interface technology, as I described in §VII.B, citing examples from Gonçalves (SAMSUNG-1050), Ponnappan (SAMSUNG-1049) and Freund (SAMSUNG-1013).
231. In addition, Rao explains that “[t]he client 105 can be any type and/or form of computing device 102 that can run one or more

applications 338 that access a network, such as network 104” and “[t]he application 338 can be any type and/or form of application such as any type and/or form of web browser, web-based client, client-server application, a thin-client computing client, an ActiveX control, or a Java applet, or any other type and/or form of executable instructions capable of executing on client 105 or communicating via a network 104.” SAMSUNG-1005, [0088]. A POSITA would have recognized that web browsers, web-based clients, client-server applications, etc. all conventionally includes graphical user interfaces. Therefore, since Rao’s client can run such applications, a POSITA would have understood that Rao’ device necessarily includes a user interface.

232. In addition, a POSITA would have recognized that Rao’s user interface would have included panels provided by multiple applications. Since the device can run “one or more applications 338,” each of which can have its own user interface panels, a POSITA would have recognized that RD’s interface includes multiple panels. SAMSUNG-1005, [0088]. For example, Jobs includes illustrates that a user interface can include panels for

applications such as chat, email, photo browsing, etc., and each application can display one or more panels. SAMSUNG-1051, FIGS. 5-46. A POSITA would have further recognized that, depending on the size of the screen and the capabilities of the device, such screens might be displayed one at a time or multiple at a time, potentially overlapping.

233. Further, as described above, Rao's agent "may provide a configuration mechanism such as a user interface, graphical or otherwise, design and constructed for configuring or specifying the policies." SAMSUNG-1005, [0183]. Therefore, a POSITA would have recognized that Rao's user interface includes panels from applications and panels for administrative tasks such as configuration. Including configuration panels for a mobile device was also known as of the Critical Date, as shown, for example, in Jobs FIGS. 62A-62G and accompanying descriptions (entitled "Settings"). SAMSUNG-1051, [1326]-[1347], FIGS. 62A-62G

[1.4] memory configured to store a control policy associated with a first application on the wireless device, the first application at least enabling the wireless device to access at least a first data service over the first wireless network; and

234. Rao teaches or renders [1.4] obvious.

235. Rao's remote access client "may have one or more policies 520 for specifying client-side prioritization of network communications related to applications." SAMSUNG-1005, [0182]. Examples of Rao's applications include email, collaboration, online meeting, desktop sharing, and VoIP. SAMSUNG-1005, [0090], [0179], [0184]. Because Rao teaches "policies 520 for specifying client-side prioritization of network communications related to applications," and the client can be any type of computing device "that can run one or more applications 338 that access a network" including a "web browser, web-based client [or] client-server application," a POSITA would have recognized or found obvious that such applications enable the device to access data services, such as server-based services coupled to those applications, over a wired or wireless network. SAMSUNG-1005, [0088], [0090].
236. For example, Rao explains that its client may communicate to a server running an application such as "an application server providing email services such as Microsoft Exchange manufactured by the Microsoft Corporation of Redmond, Wash., a web or Internet server, or a desktop sharing server, or a

collaboration server” and that any of the applications “may comprise any type of hosted service.” SAMSUNG-1005, [0090]. A POSITA would have recognized that these applications enable the device to access data services, such as server-based services supporting those applications, over a wired or wireless network. For example, email was typically maintained from an email server (e.g., a POP server defined in IETF RFC 1939 and/or and IMAP server defined in IETF RFC 1730) and manipulated by a user device. Therefore, the local email application running on RD would access a data service (email server) over a network, which in RD is a wireless network. Rao provides examples, explaining that “any of the clients 105 a may communicate via the gateway 340 to a server 102 e running an application 338 e, which for example, may be an application server providing email services such as Microsoft Exchange manufactured by the Microsoft Corporation of Redmond, Wash., a web or Internet server, or a desktop sharing server, or a collaboration server” and that “any of the application 338 e may comprise any type of hosted service, such as GoToMeeting.com provided by Citrix Systems, Inc. of Ft.

Lauderdale, Fla., WebEx.com provided by WebEx, Inc. of Santa Clara, Calif., or LiveMeeting.com provided by Microsoft Corporation of Redmond, Wash.” SAMSUNG-1005, [0090]. A POSITA would have recognized or found obvious that Rao’s applications enable RD to access data services over the Rao’s wireless network based on Rao’s disclosure of these various data services. For example, the first iPhone was shown in Time Magazine’s Invention of the Year in 2007 and included the capability of accessing email over its modem (i.e., wireless network). SAMSUNG-1052. In additions, Jobs’s device includes email, with Jobs explaining that its device includes “a protocol for email (e.g., Internet message access protocol (IMAP) and/or post office protocol (POP))”. SAMSUNG-1051, [0100].

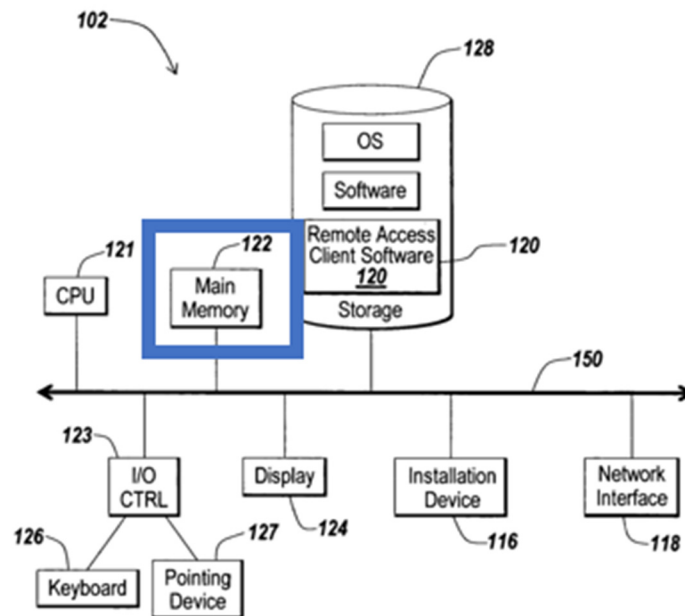
237. Therefore, a POSITA would have recognized or found obvious that Rao’s applications enable RD to access data services over Rao’s wireless network based on Rao’s disclosure of these various data services.
238. Rao further teaches that policies are associated with applications. SAMSUNG-1005, [0042], [0182]. For example,

Rao's method includes "associating a priority with the first application." SAMSUNG-1005, [0042]. Rao teaches that this association is created via policies, explaining that policies "may be specified by the name of the application," thus associating a particular policy with the named application. SAMSUNG-1005, [0182]. When policies are defined as condition/action pairs (as described in §VII.B), a POSITA would have recognized when a policy includes the condition aspect "ApplicationName equals MyApp," that condition aspects associates the policy with the application named "MyApp." Therefore, since Rao's policies "may be specified by the name of the application" (e.g., "ApplicationName equals MyApp"), Rao teaches that policies are associated with applications.

239. Rao further discloses policies that "may be accessible by the agent" component of Rao's RAC, "configured into the agent 326, or loaded by the agent 326." SAMSUNG-1005, [0183]. A POSITA would have recognized or found obvious that such policies would be stored in memory on RD, e.g., Rao's "main memory unit 122" and/or "storage device 128" which are

coupled to Rao's RAC, as illustrated in Fig. 1D. SAMSUNG-1005, [0118], Fig. 1D.

240. A POSITA would have further recognized that policies that are “configure into the agent” must be stored somewhere, and the options in RD are storage and/or memory. *Id.* However, since the CPU is “is any logic circuitry that responds to and processes instructions fetched from the main memory unit,” when evaluated, even policies stored in RD's storage must be transferred from storage to memory to the CPU and therefore are stored, at least temporarily in main memory. SAMSUNG-1005, [0119].



Rao, Fig. 1D (annotated).

241. In addition, as described with reference the [1.7a], RD policies consist of conditions and actions. (*See also supra* §VII.B.)
- When RD evaluates the condition to TRUE, it performs the actions, e.g., assigning a packet to a particular queue. Rao states that “[t]he central processing unit 102 is any logic circuitry that responds to and processes instructions fetched from the main memory unit 104.” SAMSUNG-1005, [0119]. A POSITA would have recognized that at least the condition portion of a policy is the instructions needed to evaluate the condition and/or data used in the evaluation of the condition, and both instructions and data are stored in memory.

[1.5] one or more processors configured to execute one or more machine-executable instructions that, when executed by the one or more processors, cause the one or more processors to:

242. Rao teaches or renders [1.5] obvious. RD includes a processor (e.g., Rao’s “CPU 121”), which is configured to “process[] instructions fetched from the main memory unit.” SAMSUNG-1005, [0119], Fig. 1D; §IX.A. As discussed above in §IX.A, the processor executes instructions to perform the operations

described in Rao including the operations mapped to the claim limitations addressed below.

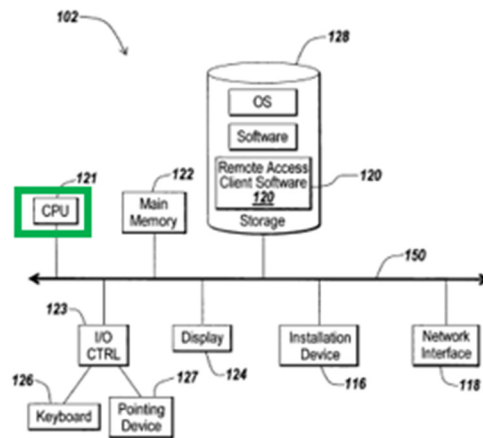


Fig. 1D

SAMSUNG-1005, FIG. 1D (annotated)

[1.6] assist in obtaining a user input through the user interface,

243. Rao teaches or renders [1.6] obvious.

244. Rao teaches a processor that assists in obtaining user input through a user interface, where such input is used to configure policies, as I discussed in reference to [1.3] and in §VII.B.

245. For example, Rao explains that policies “may be configurable by a user by any suitable means and/or mechanism.” SAMSUNG-1005, [0183]. Rao notes that the agent “may provide a configuration mechanism such as a user interface, graphical or

otherwise, design[ed] and constructed for configuring or specifying the policies 520.” *Id.*

246. A POSITA would have recognized or found obvious that policy user interfaces that provide input used to create and modify policies were well known by the Critical Date and would have been obvious to include for permitting user configurability based on Rao’s disclosure and a POSITA’s general knowledge of user interface technology. For example, in §VII.B, I provided examples from Freund (SAMSUNG-1013), Agrawal (SAMSUNG-1039), Ponnapan (SAMSUNG-1049) and Gonçalves (SAMSUNG-1050).

[1.7a] determine at least an aspect of the control policy based on the user input,

247. Rao teaches or renders [1.7a] obvious.
248. As background, I described in §VII.B that a common approach to specifying policies is a condition aspect and a corresponding action aspect.
249. Rao teaches that “policies” are “configurable by a user by any suitable means and/or mechanism,” including by using “a user interface ... for configuring or specifying the policies.” SAMSUNG-1005, [0183]. In view of Rao’s teachings, a

POSITA would have recognized or found obvious that policy user interfaces accept user input used to create and modify policies. *See* [1.6], §VII.B. In one example, Agrawal explains that “[a] policy definition tool (PDT) is a user interface by which policy authors create and modify policies.” SAMSUNG-1039, 3.

250. Rao’s policies are “specified conditionally” and are configured using user input from the user interface as discussed above. SAMSUNG-1005, [0182]-[0184]. A POSITA would have understood Rao’s policies, therefore, to include a condition aspect comprised of one or more clauses of a Boolean expression, as I explained at length in §VII.B. For example, a condition aspect includes clauses that specify the circumstances under which the policy applies, e.g., ***based on the name*** and/or ***based on type of the application***, and can include other Boolean clauses. SAMSUNG-1005, [0182]. From Rao’s teaching and a POSITA’s knowledge of policy, including conditions and actions, a POSITA would have understood that the condition aspect can include: “((ApplicationName **EQUALS** ‘TheStreamingApp’) **OR** (ApplicationType **EQUALS**

VOIP_TYPE)))” indicating that the condition aspect is satisfied if either the application name is “TheStreamingApp” or the type of the application is defined as the VOIP_TYPE. In addition, the condition aspect expressed as the Boolean expression can include fewer clauses (e.g., simply “(ApplicationName **EQUALS** ‘TheStreamingApp’)), additional clauses or a different set of clauses. An action aspect defines the corresponding action if the Boolean condition is met and includes, for example, queue priority for packets from the application that determines queue assignment. SAMSUNG-1005, [0184].

251. Since Rao’s policies are configurable by a user interface, a POSITA would have recognized or found obvious that Rao’s user interface obtains user input that indicates the condition aspect of a policy. SAMSUNG-1005, [0182]-[0184]. As I explained in §VII.B, determining aspects of policies (conditions and actions) based on user input from a user interface was well known by the Critical Date, and it would have been obvious to use user inputs in determining aspects of Rao’s policies based on

Rao's disclosure and a POSITA's general knowledge of policy determination and user interface technology.

[1.7b] the at least an aspect of the control policy for at least assisting in restricting or preventing a first access to the first wireless network by the first application when the first application is executing,

252. Rao teaches or renders [1.7b] obvious.

253. Rao teaches determining, from user input, a condition aspect of a control policy that includes one or more Boolean expressions, e.g., based on the name of the application and/or type of the application. SAMSUNG-1005, [0182]; see [1.7a], §VII.B.

254. Rao further teaches that control policies assist in restricting access to a wireless network by an executing application. For example, Rao teaches policy-based queuing to provide “client-side application-aware network communication prioritization.” SAMSUNG-1005, [0131]. In Rao, “priorities for applications” are used to “place, arrange, or coordinate 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-1005, [0191], [0194]. As a result, “real-time data

communications of [an] application” are prioritized ahead of other applications. SAMSUNG-1005, [0184].

255. Rao teaches policy-based queuing to provide “client-side application-aware network communication prioritization.” SAMSUNG-1005, [0131]. In Rao, “priorities for applications” are used to “place, arrange, or coordinate 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-1005, [0191], [0194]. As a result, “real-time data communications of application” are prioritized ahead of other applications. SAMSUNG-1005, [0184]. Rao further teaches that the queues “may be organized by levels of priority, such as high, medium, low, or numerically such as priority 1 . . . 10,” which enables prioritization of real-time data communications applications ahead of non-real-time data communications applications. SAMSUNG-1005, [0180], [0184]. Packets in a higher priority queue “are communicated from the queues” before packets in a lower priority queue, and the remote access client “will communicate the network packets from the queues

in a manner according to or consistent with the determined priorities.” *Id.*, [0194].

256. Specifically regarding “restricting or preventing access,” a POSITA would have recognized Rao’s system to be an example of weighted (priority) queuing. In weighted queuing systems, “the bandwidth received by a flow in a shared link is in proportion to the flow’s weight.” SAMSUNG-1034, 1. For example, a system could have three queues with high, medium and low priority, which are assigned weights of 10, 5 and 1, respectively.²⁵ A system using these weighting would send 10 packets from the high priority queue, 5 from the medium priority

²⁵ Systems are not limited to three queues or to this weighting. Depending on the system’s objectives, virtually any number of queues and priorities can be used. Rao notes that “[o]ne ordinarily skilled in the art will recognize and appreciate that number of queues 540a-540n may be based on any desired granularity of prioritization, such as 3, 5 or 10 levels of priority.” SAMSUNG-1005, [0180].

queue, and 1 from the low priority queue, then return to the high priority queue.²⁶

257. In contrast, systems that do not use weighted queuing typically transmit packets in the order that they arrive. Rao explains that “[c]ommunications over a network between two computers are typically processed in the order generated by the activity of a user and applications of the client and incoming network communications are processed in the order they are received.” SAMSUNG-1005, [0003]. Rao notes that this approach can be undesirable since packets from non-real-time applications “may be processed ahead of the real-time network packets of the VoIP telephone call thereby increasing the latency and reducing the quality of the voice communication” and therefore “[i]t is desirable to provide application-aware, client-specific prioritization of packet traffic.” SAMSUNG-1005, [0003].
258. In contrast to systems that lack weighted queuing (where packets are processed in the order they arrive), as a result of using Rao’s weighted queuing, traffic from some applications is restricted

²⁶ If a particular queue is empty, the system simply skips it.

from using the network, e.g., traffic from applications that have packets assigned to the medium- and low-priority queues in the example above, which are transmitted less frequently than packets assigned to the high-priority queue. In addition, in Rao, since packets are queued and handled in priority order, such applications have degraded (restricted) access as compared to traffic handled by a system that does not use priority queuing (which handles packet in the order they arrive). When there exists traffic in higher priority queues (such as the high-priority queue of the example), lower-priority traffic (that is, in lower-priority queues) is also delayed (since it is sent after high priority packets) and throttled (since the rate of transmission of such packets is limited by the queue weighting).

259. Note that Rao's priority queuing could, in theory, be used to prevent access to a network by assigning a particular queue zero priority. However, a POSITA would have recognized this approach to be impractical in many cases. First, as noted above, if there is no traffic in a higher-priority queue, traffic from lower-priority queues is sent. Therefore, at times of low use, even a zero-priority queue could have packets transmitted,

therefore not preventing access. Depending on the design goal, this might or might not be an acceptable outcome. In addition, if the queue literally received zero priority – that is, its packets were never transmitted, even at time of no competing use – a POSITA would have recognized that maintaining the queue itself would simply be a waste of system resources. Therefore, to block traffic completely, a POSITA would have looked to alternative approaches, e.g., as discussed in reference to [4].

260. Returning to Rao, Rao explains that its teachings apply to a broad range of applications, including streaming video, email, collaboration, online meeting, desktop sharing, and “any application related to real-time data communications.”

SAMSUNG-1005, [0088], [0179]; §IX.A. Rao further teaches that application priority is relative, e.g., by “associating a priority with the first application higher than a priority associated with the second application.” SAMSUNG-1005, [0042]. As a result, Rao prevents “network packet[s] of [an] application from being communicated ... ahead of ... network packets of [another] application.” SAMSUNG-1005, [0040].

261. Rao provides an example in which “secure real-time data communications can be communicated from the client at higher priorities than other applications of the client to improve the quality of the real-time experience, such as VoIP.” SAMSUNG-1005, [0218]. A POSITA would have recognized that, among Rao’s “other applications” it is beneficial to provide real-time, non-interactive applications (e.g., streaming video) priority over non-real-time, non-interactive applications (email), e.g., to avoid video stuttering. For example, as I explain in §IX.C, when real-time applications do not receive sufficient bandwidth, they can fail to operate correctly, as described in Verdi and Green. SAMSUNG-1024, [0005]; SAMSUNG-1025, [0031]-[0032].
262. A POSITA also would have thus recognized the benefits of prioritizing interactive real-time traffic (e.g., VoIP) over non-interactive real-time traffic (e.g., streaming video), and prioritizing both over non-real-time traffic. SAMSUNG-1005, [0042], [0218]. Moreover, a POSITA would have recognized or found obvious that the name of an application is used to determine the particular priority of an application. In the discussion of [1.4], I provided one example of

“ApplicationName equals MyApp.” This aligns with Rao’s teaching that the control policy would specifies application priority based on the name of an application, and the priority is based (at least in part) on whether the application provides real-time data communications or is instead non-real-time.

SAMSUNG-1005, [0184].

263. Therefore, a POSITA would have known that, in Rao, priority-based queuing is applied such that lower-priority applications are restricted from using the network at least when contention for the network exists, e.g., when multiple applications request transmission. SAMSUNG-1005, [0042], [0179], [0184], [0218].
- In such cases, “packets are communicated according to the determined priority,” which is an example of weighted queuing. SAMSUNG-1005, [0184]. For example, when video streaming (a non-interactive application) is executing as a first application, Rao’s priority-based queuing restricts its network access by placing its packets in a lower-priority queue as compared to packets from higher-priority applications (e.g., an active application such as VoIP). SAMSUNG-1005, [0184], [0218].

264. Since the condition aspect of a policy determines when to apply the action aspect of a policy, a POSITA would have recognized that the condition aspect of a policy (which can include a Boolean clause specifying application name) at least assists in restricting access (of lower priority application) to the network. *See* [1.7a]; §VII.B.

265. In addition, a POSITA would have recognized that priorities assigned to applications, or classes of application, are determined by systems administrators.²⁷ In one example, interactive applications (e.g., VoIP) can be the highest priority, since any lag will influence both sides of the communication. For example, if there is a 5-second lag, one party will be hearing what the other party said 5 seconds ago, so the user impact is high. For multiparty interactive applications, the results would be even worse since multiple participants could speak over one another. Real-time, non-interactive applications (e.g., streaming

²⁷ A POSITA would have recognized that a system administrator administers the system, and configuring queue priority is generally a systems administration task.

video) can be the next highest since, as described above, delays can cause stuttering and lag. Other non-real-time, non-interactive applications (email) might be lower still since users are less likely to perceive delay. Applications such as critical software updates might be assigned a priority between real-time and non-real-time applications since momentary delays are unlikely to cause harm, although a systems administrator might choose to assign such updates the highest priority to reduce security risks. Regardless of the relative order selected by the systems administrator, as Rao teaches, “priorities for applications” are used to “place, arrange, or coordinate 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-1005, [0191], [0194]. As a result, network bandwidth is allocated according to the priorities set by the administrators. A POSITA would have known that, in Rao, priority-based queuing is applied such that lower-priority applications are restricted from using the network at least when contention for the network exists, e.g., when multiple

applications request transmission. SAMSUNG-1005, [0179], [0184]. In such cases, “packets are communicated according to the determined priority.” SAMSUNG-1005, [0184]. For example, when video streaming is a first application, Rao’s priority-based queuing restricts its network access by placing its packets in a lower-priority queue as compared to packets from higher-priority applications (e.g., VoIP). SAMSUNG-1005, [0184].

266. Therefore, in summary, a POSITA would have recognized or found obvious that at least an aspect of the control policy (condition aspect) at least assists in restricting access to the first wireless network by the first application (by assigning its packets to a lower-priority queue). SAMSUNG-1005, [0179], [0184].

[1.7c] the at least an aspect of the control policy enabling a first control of the first access to the first wireless network by the first application when the first application is executing that differs from a second control of a second access to the first wireless network by a second application on the wireless device, and

267. Rao teaches or renders [1.7c] obvious.

268. Rao teaches or renders obvious that policies include aspects, such as condition aspects and action aspects, which are determined based on user input, and that restrict access to the

wireless network and that differ for different applications (e.g., since the conditions are based, at least in part, on application name). See [1.7a]-[1.7b]; §VII.B. Thus, Rao teaches or renders obvious that the aspect of the control policy enables a first control of access to the wireless network by the first application that differs from a second control of access to the wireless network by a second application (e.g., by determining a priority for the first application that differs from a priority for the second application, thereby resulting in access to wireless network being controlled differently for the first and second applications). *Id.*

269. For example, Rao teaches that, based on the condition aspect ((“at least an aspect”), which includes “*the name of the application*”, RAC assigns packet priority, explaining that RAC “determines the association of network packets with applications” to “determine priorities and apply any priority based policies.” SAMSUNG-1005, [0182]-[0184], [0187]. Then, “[b]ased on the indicated priorities for applications,” the filter “may place, arrange, or coordinate network packets into queues” in support of the priorities and “the network packets are

communicated from the queues 540a-540n according to the determined priorities.” SAMSUNG-1005, [0191], [0194].

270. Since Rao teaches a condition aspect (e.g., based at least in part on an application’s name) can determine the queue for the application’s packets, and the queue determines the order of transmission, a POSITA would have recognized or found obvious that the condition aspect enables a first control (e.g., the order of the application’s packet transmission). SAMSUNG-1005, [0182]-[0184], [0187], [0191], [0194]. As I described above, this is simply weighted queuing based on application name.

271. A POSITA would have further recognized or found obvious that, for a second application with a different name, at least in some cases, Rao assigns packets to a different queue.

SAMSUNG-1005, [0182]-[0184], [0187], [0191], [0194].

Extending the example I gave above, instead of

“ApplicationName equals MyApp”), a first policy might have a condition aspect that states “ApplicationName equals MyApp1” and a second policy might have a condition aspect that states “ApplicationName equals MyApp2”. The first policy might

have an action aspect that assigns “medium” priority, while the second policy might assign “high” priority. MyApp1 might be the name of a streaming video application and MyApp2 might be the name of a VoIP application, although they could be names of any applications. In this example, two applications with different names are assigned different priorities.

272. Rao provides a specific example in which an application “generate[s] real-time data of VoIP communications” and the client, “using the techniques of the present invention, may prioritize the real-time data communications of [the] application ... ahead of other applications, such as non-real-time data communication applications.” SAMSUNG-1005, [0184]. As I explained immediately above, a POSITA would have known or found obvious that the VoIP application would have a different name than “other applications,” and the packets of the two applications are assigned to different queues.

273. Since queues determine the order of transmission, a POSITA would have recognized that the second application’s name enables, at least in part, a second control (e.g., the order of the second application’s packet transmission), which differs from

the first control. These are “medium” and “high” priorities in the example above.

274. In the example, since the second application (VoIP) is interactive and the first application (video streaming) is not, it would be natural for a systems administrator to assign the VoIP traffic to a higher-priority queue. Therefore, the control of the two applications (video streaming and VoIP) differs since their traffic is assigned to queues of differing priority.

[1.8] apply the control policy, thereby at least assisting in restricting or preventing the first access to the first wireless network by the first application when the first application is executing.

275. Rao teaches or renders [1.8] obvious. SAMSUNG-1005, [0182]-[0184]; [0187], [0191], [0194].
276. Rao applies control policies that restrict access to the first wireless network by the first application (e.g., non-interactive video streaming) when the first application is executing by assigning packets from the application to a queue that is not the highest priority. SAMSUNG-1005, [0182]-[0184], [0187], [0191], [0194]; *see* [1.7b], [1.7c]. Application of the control policy is evidenced by Rao explaining that “a priority for the intercepted and queued network packet is determined based on

the type and/or priority of the application” and “the network packets are communicated according to the determined priority.”

SAMSUNG-1005, [0184], as discussed in detail above.

[3] The wireless device recited in claim 1, wherein restricting or preventing the first access to the first wireless network by the first application when the first application is executing comprises restricting communication associated with the first application over the first wireless network when the first application runs as a background process.

277. Rao teaches or renders [3] obvious.

278. Rao teaches restricting access to the first wireless network by the first application, and further teaches that the restriction can be “based on whether an application is running in the foreground or the background of the client.” *See* [1.7b]-[1.8]; SAMSUNG-1005, [0182]. A POSITA would have therefore found it obvious to restrict the first access to the first network by assigning packets from the first application (e.g., video streaming) when it is running as a background application to lower-priority queues, thus restricting its communication. SAMSUNG-1005, [0182], [0184]; *see* [1.7b]; *see also* SAMSUNG-1005, [0179]-[0195]. A POSITA would have recognized that, in most case, background applications are receiving less focus from the user (as compared to foreground applications), and therefore merit lower priority.

[6] The wireless device recited in claim 1, wherein apply the control policy comprises at least assist in routing or directing at least a portion of traffic associated with the first application over the first wireless network to a particular network communication end point, route, or tunnel.

279. Rao teaches or renders [6] obvious.

280. Rao's "remote access client 120 may also have, access, or use a routing table" that includes "information about a source computing device and a destination computing device to identify a communication path or connection between a source and destination communication points." SAMSUNG-1005, [0181]. A POSITA would have recognized or found obvious that "a communication path" is a route and "destination communication point" is an endpoint, and therefore Rao teaches or renders obvious routing or directing traffic to a communication endpoint. *Id.*

281. In addition, Rao teaches that traffic is assigned to priority queues based on policy. SAMSUNG-1005, [0184]; *see* [1.7b]-[1.7c]. For example, Rao explains that the remote access client includes policies for "specifying client-side prioritization of network communications related to applications," and policies can "indicate prioritization based on the destination network address, such as host name or IP address, and/or destination port

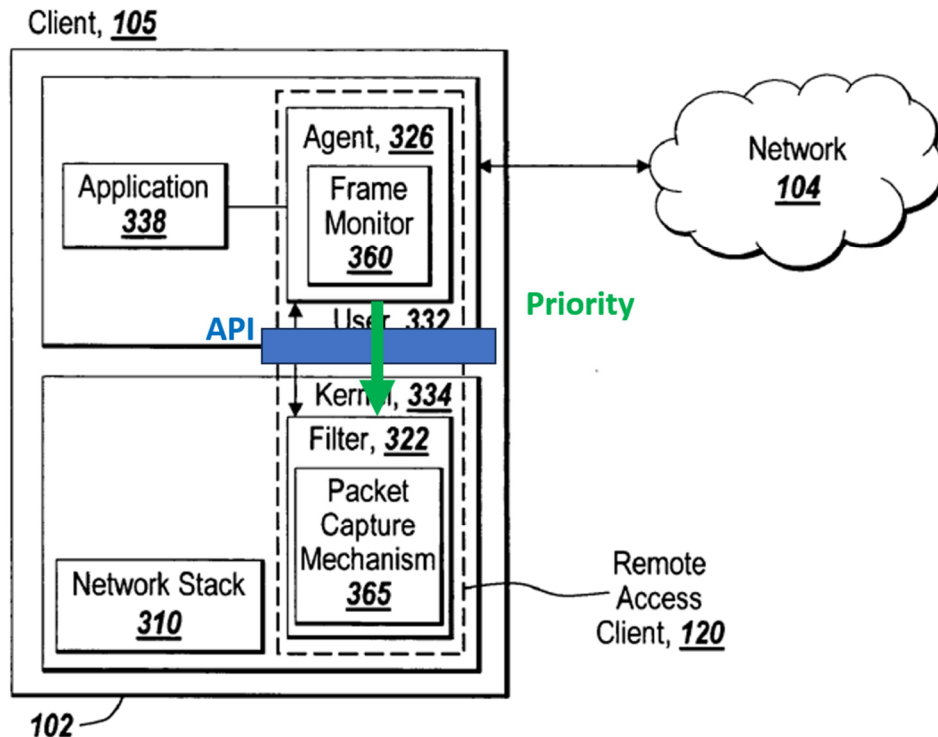
number.” SAMSUNG-1005, [0182]. A POSITA would have recognized or found obvious that when an application (e.g., video streaming) transmits data to a destination network address, the destination’s network address identifies a particular endpoint, and therefore Rao’s prioritizing communication based on the endpoint’s network address assists in routing and directing traffic from the application and to the endpoint at that network address. SAMSUNG-1005, [0088], [0181]-[0182]. Specifically, as routing traffic involves transferring data between endpoints, RD would assist routing video streaming application traffic, for example, by ensuring such traffic is sent ahead of other, low-priority, application traffic.

[8] The wireless device recited in claim 1, wherein apply the control policy comprises use an application programming interface to communicate with a software component that at least assists in restricting or preventing the first access to the first wireless network by the first application when the first application is executing.

282. Rao teaches or renders [8] obvious. RD includes an agent and filter that restrict and prevent access to networks by executing applications, including video streaming. §IX.A.

283. In Rao, the client “runs a filter,” and the agent “may communicate the priority of network packets to the filter 322 by

any suitable means and/or mechanism such as *via an application programming interface (API)*.” SAMSUNG-1005, [0099, [0190]. An example of such an API is illustrated below. The agent uses the API (drawn in blue) to pass the priority (drawn in green) to the filter. Note that the API can run in user space (322), kernel space (334) or have components in each. This is a simple design choice.



284. SAMSUNG-1005, FIG. 1C, annotated.

285. The filter “may place, arrange, or coordinate network packets into queues 540a-540n in support of the priorities.” SAMSUNG-1005, [0191].
286. A POSITA would have recognized of found obvious that Rao’s filter is a software component that assists in restricting access to the network (using packet priority) by an application, including a first application (video streaming), that is executing. *See* [1.7b].
287. As described above, systems that do not use Rao’s priority queuing typically process communication in the order generated. SAMSUNG-1005, [0003]. In contrast, Rao assigns traffic to priority queues, and for lower-priority applications (for which traffic is assigned to lower-priority queues), results in an access restriction since its traffic is allocated a smaller share of the bandwidth as compared to the highest-priority applications.

[9] The wireless device recited in claim 1, wherein apply the control policy comprises use an application programming interface to communicate information to a software component that at least assists in restricting or preventing the first access to the first wireless network by the first application when the first application is executing, the information being associated with: (a) the first wireless network, (b) a cost associated with the first wireless network, (c) a connection state of the first wireless network, (d) a user preference, or (e) a combination of these.

288. Rao teaches or renders [9] obvious.

289. Rao “communicates the priority of network packets to the filter” using “any suitable means and/or mechanism such as via an application programming interface (API).” SAMSUNG-1005, [0190]. Rao’s policies, which include packet priorities, are “configurable by a user,” thereby reflecting a user preference. SAMSUNG-1005, [0183]. (See also the discussion of policy user interfaces in ¶VII.B.)
290. The filter is a software component that assists in restricting access to the network by “plac[ing], arrang[ing], or coordinat[ing] network packets into queues,” including packets from the first application (video streaming). SAMSUNG-1005, [0099], [0191]. Rao states that the filter can be a software component, noting that “*any portion of the remote access client 120*, such as the agent 326, frame monitor 360, the filter 322, and packet capture mechanism 365, or any portion thereof *may comprise software*, hardware, such as an ASIC or an FPGA, or any combination of software and/or hardware. In some embodiments, portions of the remote access client 120 may be provided via one or more blades on the client 105.” SAMSUNG-1005, [0114].

291. As discussed in [8], in Rao, the client “runs a filter,” and the agent “may communicate the priority of network packets to the filter 322 by any suitable means and/or mechanism such as *via an application programming interface (API)*.” SAMSUNG-1005, [0099, [0190].
292. Thus, the information communicated through the API (as discussed in [8]) can include information associated with a user preference (e.g., the priority of an application) expressed in a policy that was configured “by a user,” and is therefore associated with a user preference. SAMSUNG-1005, [0183].

[10] The wireless device recited in claim 1, wherein apply the control policy comprises use an application programming interface to communicate with a software component that at least assists in controlling an e-mail transfer option, a media content resolution, or a compression level.

293. Rao teaches or renders [10] obvious.
294. Rao teaches an API to communicate with a software component (filter) that assists in restricting application access. *See [8]*.
295. Rao further teaches that the software component (filter) assists in controlling an email transfer option. For example, Rao teaches that “all networks [sic] packets for a type of application” such as an email or voice application may be “placed in a queue” used to prioritize “networks [sic] packets for one or more

applications,” e.g., “online collaboration related applications” can “be placed and prioritized in a first queue 540a for collaboration related applications” and a “second queue 540b may be used for email related applications.” SAMSUNG-1005, [0192]. A POSITA would have recognized that placing email packets in a particular priority queue is controlling an e-mail transfer option. For example, a POSITA would have recognized that placing email packets in a particular priority queue is controlling an e-mail transfer option – e.g., the rate at which email messages are sent, e.g., to a POP or IMAP server (See discussion of [1.4]).

[11] The wireless device recited in claim 1, wherein apply the control policy comprises use an application programming interface to communicate with a software component that at least assists in controlling a background access.

- 296. Rao teaches or renders [11] obvious.
- 297. Rao teaches an API to communicate with a software component that assists in restricting application access. *See [8].*
- 298. Rao further teaches assisting in controlling background access using the API, explaining that the agent may use characteristics of the application “such as running in the foreground or background, to indicate priority for a network packet of the

application.” SAMSUNG-1005, [0182]; *see also discussion of* [3]. For example, when the condition aspect indicates that an application is running in the foreground, its traffic is assigned to a higher-priority queue (since the user is more aware of application responsiveness), and when the condition aspect indicates that the application is running in the background, its traffic is assigned to a lower-priority queue (since the user is less sensitive to delays incurred by background applications).

[14] The wireless device recited in claim 1, wherein the user input comprises a directive to restrict, block, disable, turn off, throttle, delay, quarantine, or shape at least a portion of traffic over the first wireless network associated with the first application.

299. Rao teaches or renders [14] obvious.

300. As discussed above, in RD, user input determines policies. *See* [1.6], [1.7a]-[1.7c]; §IX.A.

301. As background, at least in systems using priority queuing, there is little practical distinction between restricting, delaying and throttling traffic. As described in reference to [1.7b], when traffic is assigned to one of Rao’s lower-priority queues, such traffic is restricted, delayed (while higher priority traffic is transmitted) and throttled (limited to its weighted allocation) as higher priority traffic is transmitted.

302. Thus, Rao's policies are directives to restrict, throttle and/or delay at least a portion of the traffic by assigning such traffic to priority-based queues. For example, "the filter 322 may place, arrange, or coordinate 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-1005, [0191], [0194]. A POSITA would have recognized that priority queues throttle, restrict, and delay traffic based on priority assigned to the traffic. SAMSUNG-1005, [0184]; *see* §VII.C, §VII.D. For example, low-priority queues are restrict and delay traffic as compared to higher-priority queues.

[19] The wireless device recited in claim 1, wherein the control policy at least assists in controlling the second access to the first wireless network by the second application on the wireless device, and wherein the user input is a first user input, and wherein the at least an aspect of the control policy is a first aspect of the control policy, and wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to: assist in obtaining a second user input through the user interface, and determine at least a second aspect of the control policy based on the second user input, the at least a second aspect of the control policy for at least assisting in controlling the second access to the first wireless network by the second application on the wireless device.

303. Rao teaches or renders [19] obvious.

304. Rao renders obvious the wireless device of claim 1, wherein the control policy at least assists in controlling the second access to the first wireless network by the second application on the wireless device. *See discussion of* [1.7c].
305. Rao renders obvious user input that is a first user input, and wherein the at least an aspect of the control policy is a first aspect of the control policy. *See* [1.6], [1.7a]-[1.7c]; §VII.B.
306. For similar reasons, Rao renders obvious user input that is a second user input, and that the second user input determines a second aspect of the control policy (action aspect) that controls access to the wireless network for a second application (e.g., assigning different priorities to different applications). *See* [1.6], [1.7a]-[1.7c]; §VII.B. For example, Rao renders obvious machine-executable instructions that are executed by RD'S processors that cause the processor to assist in obtaining a second user input through the user interface. *Id.* Rao's policies include conditions (first aspects, including, e.g., the name of the application, type of application, foreground/background status, etc.), and actions (second aspects), which indicate priority. SAMSUNG-1005, [0182]-[0193]; *see* VII.B. Further, Rao

explains that the agent can “provide a configuration mechanism such as a user interface, graphical or otherwise, design[ed] and constructed for configuring or specifying the policies.”

SAMSUNG-1005, [0183]. Therefore, a POSITA would have recognized that policies, including conditions (first aspect of the policy) and actions (second aspect of the policy), are obtained as user input from a user interface and determined from that input.

See [1.6], [1.7a]; §VII.B.

307. Rao renders obvious determining at least a second aspect of the control policy based on the second user input (the action element of the policy, as I described in §VII.B) that assists in controlling the second access to the first wireless network by the second application on the wireless device. For example, Rao teaches policies where the action aspect of the policy controls application access to the wireless network by assigning packets to priority queues, including a second access by a second application (e.g., VoIP). SAMSUNG-1005, [0004], [0184].

[20] The wireless device recited in claim 1, wherein the control policy assists in controlling a third access to a second wireless network by the first application.

308. Rao teaches or renders [20] obvious.

309. Rao's policies assist in controlling access to all networks (including a second wireless network) by all applications (including the first application, video streaming). See [1.7b], [1.7c]. For example, Rao teaches accessing multiple networks, e.g., "the 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, standard telephone lines, LAN or WAN links (e.g., 802.11, T1, T3, 56 kb, X.25), broadband connections (e.g., ISDN, Frame Relay, ATM), wireless connections, or some combination of any or all of the above.' SAMSUNG-1005, [0125]. Rao explains that the network interface can include "a built-in network adapter, network interface card, PCMCIA network card, card bus network adapter, wireless network adapter, USB network adapter, modem or any other device suitable for interfacing the computing device 102 to any type of network capable of communication." *Id.* As I described in §VII.A, such function was common in mobile devices as of the Critical Date.

310. A POSITA would have recognized that when RD is connected to a first network (e.g., a home wireless network) the control policy assists in controlling access, and when RD is connected to a second network (e.g., a work wireless network), the control policies assists in controlling access. For example, the control policy could throttle video traffic in a home network (e.g., by placing it in a low priority queue), while such traffic could be prioritized in a work network (e.g., for teleconferences). In another example, when RD is connected to a home network, policies can be used to deprioritize security updates (if the home user finds them annoying), while an enterprise might insist that such traffic be prioritize relatively highly.

B. Ground 1B: Rao-Panpaliya renders claim 2 obvious

[2] The wireless device recited in claim 1, wherein the first application is configured to at least assist in restricting or preventing the first access to the first wireless network by the first application when the first application is executing.

311. RPD renders [2] obvious.

312. In Panpaliya, a “network constraint detection component” monitors and/or measures “the current network parameters associated with an existing video communication session ... to detect if a network constraint exists,” and when it “determines

that an unfavorable threshold level has been reached, a network constraint is detected” and the system “adjusts video parameters in a manner that continues to provide an acceptable user experience.” SAMSUNG-1007, 5:66-6:12. As I described in §IX.B, such video adaptation techniques were known as of the Critical Date, e.g., as explained in Wu. SAMSUNG-1035, 7.

313. When RPD runs a first application (e.g., the video streaming application of Rao, which instantiates a video communication session of Panpaliya), it detects a network constraint (e.g., insufficient bandwidth) and restricts access to the wireless network by “adjusting one or more video parameters of a video communication session,” such as the frame rate, which reduces (restricts) the bandwidth demand. SAMSUNG-1005, [0088]; SAMSUNG-1007, Abstract, 4:62-67, 5:27-35. A POSITA would have known the lower frame rates require less data to be transmitted, and thus reduces the bandwidth required by the application. Of course, the lower frame rate results in lower-quality video, so the restriction comes with a cost.

C. Ground 1C: Rao-Jones renders claims 4, 13, 21, 23, 25 obvious

[4] The wireless device recited in claim 1, wherein restricting or preventing the first access to the first wireless network by the first application comprises

preventing communication associated with the first application over the first wireless network when the first application runs as a background process.

314. RJD renders [4] obvious.

315. RJD evaluates policies relating to a wide range of factors including “whether an application is running in the foreground or the background.” SAMSUNG-1005, [0182]; §III.A.c. The first application can be a non-interactive application such as video streaming (Rao) or backup (Jones). SAMSUNG-1005, [0088], [0179]; SAMSUNG-1006, 5:13-32. The result of RJD’s policy evaluation first determines if the transfer is allowed, or conversely, “a first rule may prohibit data transfers over a modem connection.” SAMSUNG-1006, 5:25-26; §IX.A. For example, for example, RJD uses foreground/background conditions of Rao, and disallows network traffic of background traffic using the action (prohibit transfer) of Jones. A POSITA would have recognized that foreground applications are more likely to have user attention, and therefore preserving bandwidth for foreground application by disallowing traffic of background application is preferred. Thus, RJD prevents network access when the application runs as a background process.

SAMSUNG-1005, [0182]; SAMSUNG-1006, 5:25-26; §IX.A.

316. For example, Jones teaches that “data protection software ... may execute in the background to perform data backups” and the “[b]ackup frequency ... may depend on ... enterprise policies.” SAMSUNG-1006, 3:45-51. A POSITA would have recognized that restricting network access for the backup process running (in the background) by assigning its packets lower priority leaves additional bandwidth for other applications, avoiding cases where background packets are “processed ahead of the real-time network packets of the VoIP telephone call thereby increasing the latency and reducing the quality of the voice communication,” as described in Rao. SAMSUNG-1005, [0003].
317. In a second example, if a user is streaming a video, then opens a video call (which moves the streaming video to the background), a POSITA would have recognized that it is preferable for RJD to block the video stream to prevent the video stream from competing for device resources with the video call (which is an interactive application). Since video streams contain large amounts of data (as described in §IX.E), if RJD used priority queuing to hold the data instead of blocking it, RJD would

expend considerable resources to store the data in the queue, especially if the video call lasted for more than a few seconds. Such an approach quickly becomes impractical. Therefore, it is preferable for RJD to block the transmission rather than expend device resources to queue what can be a large amount of data.

[13] The wireless device recited in claim 1, wherein the control policy is further based on a network administrator input.

318. RJD renders [13] obvious.

319. Rao teaches that policies “may be configurable by a user by any suitable means and/or mechanism,” e.g., “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-1005, [0183]. Jones similarly 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.” SAMSUNG-1006, 5:15-29. Therefore, in view of the teachings of Rao and Jones, a POSITA would have recognized that RJD’s configuration mechanism for specifying policies is an instance of systems administrator input, as explained in both Rao and Jones.

SAMSUNG-1005, [0183]; SAMSUNG-1006, 5:15-29.

Particularly relevant for work networks, systems administrators would have unique vantage points into the efficient operation of the network involving, potentially, thousands of endpoints, and thus, would be uniquely qualified specify policies pertinent to minimizing network congestion within a work environment.

[21] The wireless device recited in claim 20, wherein the at least an aspect of the control policy is further based on a characteristic of the first wireless network or the second wireless network.

320. RJD renders [21] obvious.

321. RJD policies are based on user input, as described in both Rao and Jones. SAMSUNG-1005, [0183]; SAMSUNG-1006, 6:39-41 (“a user may be presented with a graphical user interface through which each policy may be selected and configured in successive operations”); *see* [1.7a]. In addition, policies were commonly based in user input, as I explained in §VII.B

322. Further, in RJD, the aspect of a control policy (e.g., a clause in the condition) is based, at least in part, on a characteristic of the first or second wireless network. For example, Jones teaches that policies may be applied to data transfers based on connection bandwidth, explaining that “[a] variety of rules 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 recognized bandwidth to be a characteristic of a network. For example, Smith explains that “applications in a tactical data network are unaware of and/or do not account for the particular characteristics of the network,” e.g., “an application may simply assume it has as much bandwidth available to it as it needs.” SAMSUNG-1038, [0015].

323. A POSITA would have recognized or found obvious that the condition aspect can depend on multiple factors, e.g., the application name and connection bandwidth, each of which at least assists in restricting or preventing network access. As I explained in §VII.B, condition aspects with multiple Boolean clauses were common as of the Critical Date.

324. RJD policies restrict (per Rao) or prevent (per Jones) access to the network. SAMSUNG-1005, [0184]; SAMSUNG-1006, 5:13-32; §IX.E.

[23] The wireless device recited in claim 1, wherein the control policy is a first control policy, and wherein the memory is further configured to store a second control policy associated with the first application, the second control policy for at least assisting in controlling a third access to a second wireless network by the

first application when the first application is executing, and wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to apply the second control policy.

325. RJD renders [23] obvious.

326. RJD supports multiple policies relating to an application. For example, Rao explains that the remote access client “may have one or more policies 520 for specifying client-side prioritization of network communications related to applications.”

SAMSUNG-1005, [0182]. Rao teaches that policies can be “based on application, name, protocol, etc.” SAMSUNG-1005, [0182]. Jones further teaches that policies can depend on “the desired functionality, type of connection, connection bandwidth, user priorities, etc.,” and that “a system administrator may configure policies for data transfers such as backups, updates.”

SAMSUNG-1006, 5:13-19. A POSITA would have recognized that applications (e.g., video streaming, backup and update) would be subject both to rules specified based on “based on application, name, protocol, etc.” and to rules based on “the desired functionality, type of connection, connection bandwidth, user priorities, etc.,” and therefore to a first and second control policy. SAMSUNG-1005, [0182]; SAMSUNG-1006, 5:13-19.

For example, a video streaming application would be associated with policies that specify the application's name (e.g., "MyVideoApp") and policies that specify a protocol used by the application ("based on ... protocol", per Rao). SAMSUNG-1005, [0182].

327. In Rao, such policies control access to networks (including a third access to a second wireless network) by applications (including the first application, video streaming), e.g., by prioritizing access. *See* [1.7b], [1.8], [20]. In fact, a purpose of Rao is to control access to networks, with Rao writing that "the remote access client of the present invention manages and controls network communication prioritizations on the client." SAMSUNG-1005, [0080]. RJD can access multiple networks, as taught by Jones, "rules may be applied to data transfers depending on the ... type of connection," and "policies for data ... are sensitive to the type of connection." SAMSUNG-1006, 5:13-19; §IX.D.

328. In RJD, memory stores policies (including a second control policy associated with the first application) and machine-executable instructions executed by processors cause the

processor to apply policies (including the second control policy).

See §IX.A; [1.4]-[1.5].

[25] The wireless device recited in claim 1, wherein the wireless device is capable of being communicatively coupled to an intermediate networking device over the first wireless network, the intermediate networking device providing a forwarding service for forwarding traffic between the wireless device and a network system communicatively coupled to the intermediate networking device over a second wireless network, and wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to determine the at least an aspect of the control policy based on a characteristic of the second wireless network.

329. RJD renders [25] obvious.

330. RJD is capable of being communicatively coupled to a gateway (intermediate networking device) over the first wireless network, as taught by Rao, such that the gateway provides a connection between clients (e.g., RJD) and computing devices.

SAMSUNG-1005, [0087], [0095]; §IX.E.

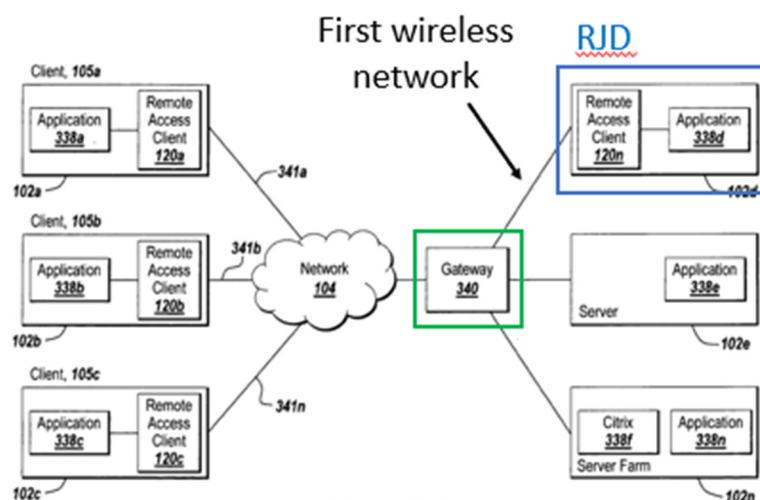
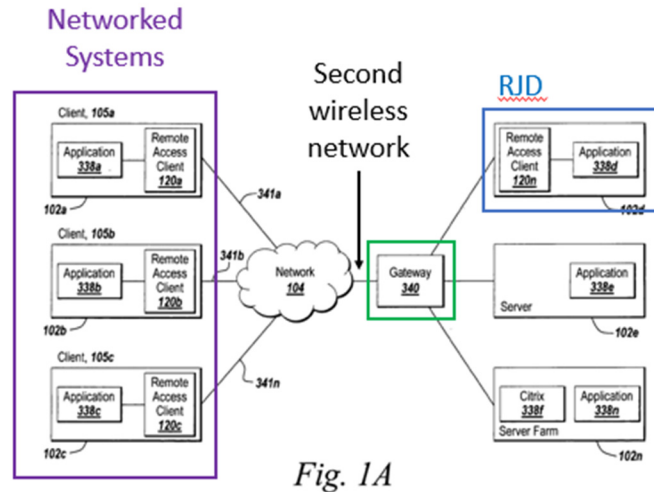


Fig. 1A

SAMSUNG-1005, FIG. 1A (annotated).

331. For example, Rao's FIG. 1A illustrates clients connected to the Gateway 340, which is connected to Network 104, which then connects to other clients. A POSITA would have known that the Network 104 could connect to other types of computing devices since networks commonly connected virtually any type of networked device to virtually any other type of network device. Thus, the Gateway 304 is providing a forwarding service that forwards traffic from RJD to other computing devices, including through Network 104.
332. The gateway provides a forwarding service for forwarding traffic between the wireless device and network systems coupled

to gateway over a second wireless network. SAMSUNG-1005, [0089]-[0092], as illustrated below.



SAMSUNG-1005, FIG. 1A (annotated).

333. Rao teaches that networks can be wired, wireless or any combination thereof. SAMSUNG-1005, [0095], [0100] (“The client 105 may also have a network stack 310” and “network stack 310 may comprise one or more protocols, such as the TCP/IP protocol over Ethernet or a wireless protocol”). Therefore, a POSITA would have recognized that the connections to and from the Gateway 340 can be wired, wireless or any combination thereof. SAMSUNG-1005, [0095].
334. RJD determines an aspect of the control policy (e.g., a clause in the condition) based on a characteristic (bandwidth) of the

second wireless network. For example, Jones explains that “rules may be applied to data transfers depending on ... connection bandwidth.” SAMSUNG-1006, 5:13-15.

335. A POSITA would have recognized that the bandwidth available to RJD is the minimum bandwidth of any network between RJD and the communication endpoint with which it is communicating. Consider the case where the JKD is connected to the gateway using a high-speed interface that provides 10 Mbps, and the gateway is connected to the network (or another computing device) using a lower-speed interface, e.g., 5 Mbps.²⁸ In this case, since the link between the gateway and the network is only 5 Mbps, the bandwidth available to RJD is only 5 Mbps even though the link between RJD and the gateway supports 10 Mbps. The second network (gateway to network) limits the bandwidth available to RJD. More generally, the effective

²⁸ It is also possible that the gateway is serving numerous devices, so while its connection to the network and other device uses a faster interface, the gateway allocates RJD only a portion of the bandwidth, e.g., 5 Mbps. This configuration does not change my analysis.

bandwidth available to RJD cannot be larger than the bandwidth of the lowest-bandwidth link along the path between RJD and the endpoint.

336. Therefore, at least when the second wireless network has lower bandwidth than the first wireless network (and therefore limits the end-to-end bandwidth), RJD determines at least an aspect of the control policy based on a characteristic of the second wireless network (bandwidth).

D. Ground 1D: Rao-Jones-Jajoo render claims 17 obvious

[17] The wireless device recited in claim 1, wherein the user input comprises a directive to restrict, block, throttle, delay, quarantine, or shape at least a portion of traffic over the first wireless network associated with the first application when a quality of a second wireless network satisfies a condition relative to a threshold.

337. RJJJ renders [17] obvious.

338. RJJJ policies contain a condition aspect and an action aspect.

See [1.7a]. RJJJ policies are based on user input, as described in both Rao and Jones. SAMSUNG-1005, [0183]; SAMSUNG-1006, 6:39-41; §IX.G. Therefore, it would have been obvious to a POSITA that since policy includes condition and action aspects, the condition aspect and the action aspect of a policy are based on user input. For example, Verma writes that “the

conditional part describes a specific situation that can be encountered by a network device, and the action component specifies the action that is to be performed by the device in that situation.”) SAMSUNG-1032, 2. Similarly, Agrawal writes that “[a] policy definition tool (PDT) is a user interface by which policy authors create and modify policies.” SAMSUNG-1039, 3. More generally, I discussed policy condition and action aspects and policy user interfaces in §VII.B.

339. In the case where a second network fails over to a first network, RJD policies evaluate the behavior of networks (e.g., a second wireless network), e.g., using “the L1 (physical) and L2 (data link) layers of the network for the presence of indicators associated with network failover operations.” SAMSUNG-1010, Abstract, [0009].
340. Jajoo teaches determining failover from the second network to the first network by evaluating metrics of the second network. SAMSUNG-1010, [0025]. Jajoo’s techniques include filters comparing failover indicators to one another and to “conditions, criteria, or thresholds associated with failover operations in the network.” *Id.* Jajoo explains that a failover is indicated “if the

failover indicators, relative to one another in terms of the time scale 112, etc., meet certain criteria suggesting the likely occurrence of a failover operation.”

341. Thus, it would have been obvious to a POSITA to include, in RJJD policies, conditions that compare “the failover indicators 102a-102c to one another, and to one or more empirically determined conditions, criteria, or thresholds associated with failover operations in the network.” SAMSUNG-1010, [0025].
342. When a failover from a second network to a first network is detected, the conditions of an RJJD policy evaluate to TRUE, and a corresponding action is selected. As I explained in §VII.B, policies operating as condition-action pairs was known as of the Critical Date. The selected policy action controls traffic using a “delay process” (per Jajoo) for traffic from the first application (video streaming, per Rao). SAMSUNG-1005, [0088]; SAMSUNG-1010, [0017]. RJJD implements the delay using Rao’s priority queues, e.g., via policy actions that assign a lower priority to the packets, which results in the packets being placed in lower-priority queues, thereby delaying packet transmission. SAMSUNG-1005, [0179]-[0195].

E. Ground 1E: Rao-Jones-Cole renders claim 22 obvious

[22] The wireless device recited in claim 20, wherein the at least an aspect of the control policy is further based on a user preference comprising a directive to allow access to the second wireless network by the first application based on a characteristic of the first wireless network.

343. RJCD renders [22] obvious.

344. RJCD policies, which include packet priorities, are

“configurable by a user,” and thus by definition reflect a user preference. SAMSUNG-1005, [0183]. (See also, §VII.B.)

Similarly, Cole teaches control policies for selecting connections that direct RJCD to attempt “to establish connectivity to the fastest eligible connection based on the connection time data and *the user's preferences*.” SAMSUNG-1029, [0067]. Such control policies alter the default connection order, e.g., when a user “select[s] particular networks that may or may not be used.” *Id.*

345. Cole further teaches that policies, which are based on user preferences (as described immediately above and in §VII.B), are directives to allow access to a second wireless network based on a characteristic of the first network. Cole provides a first example in which the device “is connected to the remote network through the first communication interface” (first

network), but in response to a “loss of connectivity” characteristic of that network, a “second one of the communication interfaces is selected for establishing a second connection to a remote network” (second network).

SAMSUNG- 1029, Abstract. In this case, the condition aspect includes a “loss of connectivity” clause in the condition’s Boolean expression. (As I discussed in §VII.B, condition aspects can include multiple Boolean clauses.)

346. Cole provides a second example in which “the monitored load [characteristic of the first network] exceeds a predetermined threshold (e.g., 85% of capacity),” and in response, the connection manager attempts “to establish a connection [to a second network] with a higher bandwidth.” SAMSUNG-1029, [0075], [0077]. Here the condition aspect includes a bandwidth threshold (of the first network) clause in the condition’s Boolean expression.

F. Ground 1F: Rao-Montemurro renders claim 5 obvious

[5] The wireless device recited in claim 1, wherein the first wireless network comprises a cellular network, a roaming network, or an access network associated with a cost.

347. RMD renders [5] obvious.

348. RMD can access a first wireless network that is a cellular network. For example, Rao states that “The network 104 as illustrated in FIG. 1A can be any type of network.” SAMSUNG-1005, [0095]. Rao also discloses that, “The client 105 may be a mobile client, such as a notebook, personal digital assistant (PDA), a smart phone, or any type of mobile computing or telecommunications device.” SAMSUNG-1005, [0198]. Thus, a POSITA would have observed that at least one the networks disclosed in Rao can be a cellular network—if for no other reason that Rao applies to smartphones. E.g., as noted in the discussion of [1.2], the iPhone 1 was released in 2007 and accessed cellular networks, as did the Jobs device. SAMSUNG-0151, SAMUNG-1052.
349. Moreover, Montemurro explains that “[i]n the example network 100, mobile device 102 is capable of wireless communication in accordance with WLAN or WMAN (e.g. Wi-Fi or WiMAX) and WWAN (e.g. *GSM Cellular*) standards”, and “[a]s such, it may communicate through cellular network 104 and a representative base station 108 coupled to the Internet 112 and/or through

WLAN or WMAN network 106 and its access point 110 also coupled to Internet 112.)” SAMSUNG-1008, [0013].

G. Ground 1G: Rao-Akhtar renders claim 7 obvious

[7] The wireless device recited in claim 1, wherein apply the control policy comprises identify or insert a flow tag in a traffic flow associated with the first application, the flow tag configured to assist in preserving the association of the traffic flow with the first application when the traffic flow is processed by one or more functions of the wireless device that operate on the traffic flow:

350. RAD renders [7] obvious.

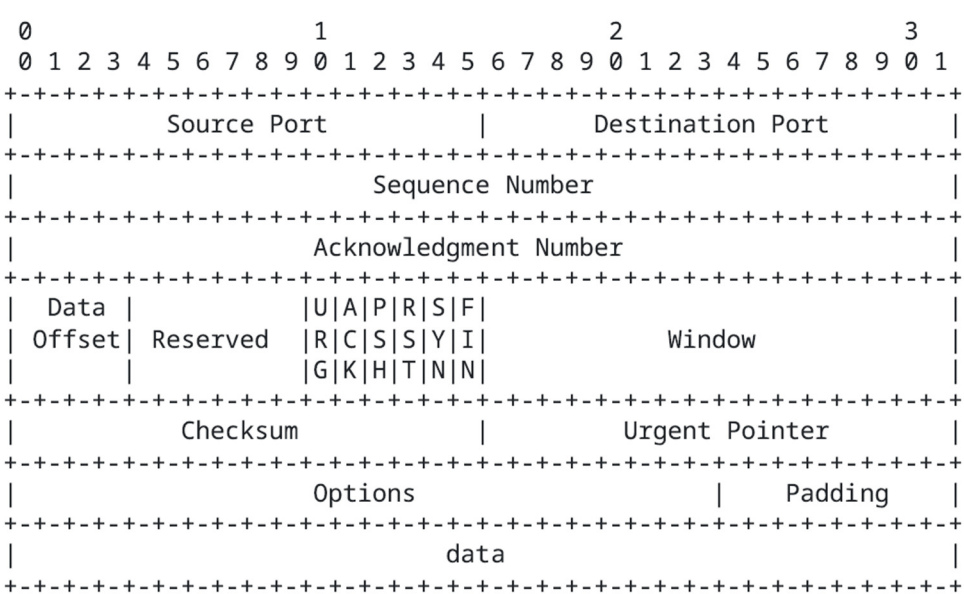
351. Rao teaches using TCP/IP. For example, Rao states that “[t]he network 104 as illustrated in FIG. 1A can be any type of network” and “[c]onnections can be established using a variety of communication protocols (e.g., **TCP/IP**, IPX, SPX, NetBIOS, Ethernet, ARCNET, Fiber Distributed Data Interface (FDDI), RS232, IEEE 802.11, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, and direct asynchronous connections).” SAMSUNG-1005, [0095].

352. A POSITA would have known that TCP packets include a source port in the header. For example, IETF RFC 793, which defines the Transmission Control Protocol (TCP) states that: TCP segments are sent as internet datagrams. The Internet Protocol header carries several information fields, including the source and

destination host addresses. A TCP header follows the internet header, supplying information specific to the TCP protocol. This division allows for the existence of host level protocols other than TCP.

SAMSUNG-1026, 34,

353. RFC 793 illustrates the header:



SAMSUNG-1026, Figure 3.

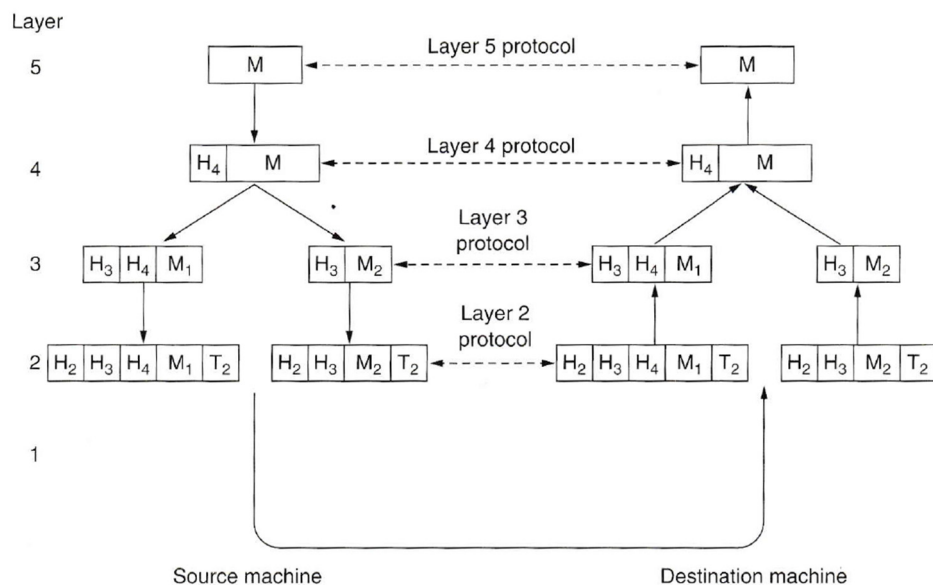
354. The “source port” is 16 bits and is defined as “[t]he source port number.” SAMSUNG-1026, 34.

355. A POSITA would have further known that TCP source ports are associated with applications. For example, Weill explains that the TCP header “provides information for ensuring that the packet is reliably transmitted from the source node to the

destination node,” and “typically includes, among other things, source and destination port numbers that respectively identify particular software applications executing in the source and destination nodes.”. SAMSUNG-1027, [0006].

356. A POSITA would have known that the TCP header, including the source port, is preserved until it reaches its destination, and thus preserves the association of the traffic flow (packet) with the first application when the traffic flow is processed by the wireless device. Generally speaking, network protocol headers are preserved until the packet reaches the destination served by the protocol.

357. For example, Tanenbaum provides this illustration:



SAMSUNG-1037, 3.

358. In this illustration, a message (M) is passed from “source machine” to “destination machine.” Layer 4 adds a layer 4 header (H₄), creating a packet that contains the layer 4 header and the message.²⁹ Layer 3 then adds a Layer 3 header (H₃) at the front, and layer 2 adds a layer 2 header (H₂). At the destination, protocol layers are traversed in the reverse direction, each layer stripping its respective header. (At transmission, headers are added sequentially to the front of the packet, easing removal at the destination.) Importantly, as shown in this example, the headers are preserved until they are received and removed by protocol layers at the destination machine.
359. With that background, in RAD, “[t]he first step is to identify the application (such as VoIP, PTT, and VT etc.) associated with the transmitted data.” Ahktar, [0028]. Ahktar “identifies the application (such as VoIP, PTT, and VT etc.) based on various characteristics of the incoming data packets,” including “the source IP address, the destination IP address, the IP flow

²⁹ In Tanenbaum’s example, M is too large to fit in one layer 3 packet, so it is split into two pieces. Such detail is beyond the scope of this discussion.

identification, the Differentiated Services Code Point (DSCP) values in the packet header (which specifies a per-hop behavior applied to the packet), source port number, destination port number, and other packet/policy attributes.” *Id.*

360. Thus, in RAD, applying a policy includes identifying a flow tag associated with the application (source port), where the flow tag preserves the association of the traffic flow with the first application when the traffic flow is processed by functions of the wireless device that operate on the traffic flow (the TCP network stack in RAD), which is required for Akhbar’s QoS.

SAMSUNG-1009, Abstract, [0028]; §IX.L.

H. Ground 1H: Rao-Ramesh renders 18 obvious

[18] The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to: assist in establishing a secure control link between the wireless device and a network element, the secure control link secured by an encryption protocol and configured to support control-plane communications between the wireless device and the network element, and obtain at least a portion of the control policy from the network element over the secure control link.

361. RRD Ramesh renders [18] obvious.

362. Ramesh includes a “policy distribution node” (PDN) that distributes policies to devices “via a policy exchange channel” (PXC). SAMSUNG-1011, [0036]. Since the PDN distributes

policies to devices, RD as modified by Ramesh obtains policies from the PDN. Further, since Rao teaches that “the policies may be provided by or downloaded via the gateway,” a POSITA would have recognized that Rao’s gateway (which is a network element) is serving as a PDN. SAMSUNG-1005, [0183]. More generally, since PDNs are connected to RDs over a network, a POSITA would have recognized that Ramesh’s policy distribution node is a network element.

363. In RRD, the control link (PXC) is secured by an encryption protocol, e.g., Transport Layer Security (TLS). SAMSUNG-1011, [0037]. Ramesh explains that the Policy Exchange Channel (PXC)³⁰ can “provide a secure security assertion protocol that may allow distribution of policies from the PDN 11 to the PDP 9 through the PEP 8,” e.g., using encrypted protocols

³⁰ Ramesh’s (SAMSUNG-1011) FIG. 3 labels the PXC as “Policy Exchange Protocol (PXP) 14”, which the specification at [0036] refers to it as “policy exchange channel (PXC) 14.” Since PXP does not appear in the specification, a POSITA would have recognized that these refer to the same component, which I call the PXC.

such as TLS and SSH FTP secure extension. SAMSUNG-1011, [0037]. A POSITA would have recognized that control links using encrypted protocols (e.g., TLS) are secured by an encryption protocol. For example, the TLS Protocol specification states that the TLS “connection is private” and that “[s]ymmetric cryptography is used for data encryption (e.g., AES [AES], RC4 [SCH], etc.).” SAMSUNG-1021, 3.

364. In addition, a POSITA would have recognized that since the control link “allow[s] the distribution of policies,” and policies are used to manage communication sessions, the control link supports control-plane communications between the wireless device and the network element. SAMSUNG-1011, [0037]. A “control plane” is defined as “the portions of a network system that are involved in the setup, *management* and termination of communication sessions and services”) (emphasis added). SAMSUNG-1053, 3.

365. Further, a POSITA would have known that clients (e.g., RRD) assist in establishing TLS links using a handshake protocol. The TLS protocol specification states that “the TLS Handshake Protocol, allows the server and client to authenticate each other

and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data.” SAMSUNG-1021, 3. Since the client and server “authenticate each other” and “negotiate,” a POSITA would have recognized that the client assists. *Id.*

366. Therefore, RRD assists in establishing a secure control link (e.g., TLS handshake) secured by an encryption protocol and obtaining control policies from the network element over the secure control link (from Ramesh’s PDN). SAMSUNG-1011, [0036]-[0037].

367. Machine-executable instructions cause RD’s processor to perform the operations. §IX.A.

I. Ground 11: Rao-Freund renders claims 12, 15-16, and 26-27, 29-30 obvious

[12] The wireless device recited in claim 1, wherein the control policy is further based on a relationship between a usage limit and a measure of usage of the first wireless network associated with the first application.

368. RFD renders [12] obvious.

369. As taught by Freund, in RFD, to send data, an application (e.g., a video streaming of Rao) calls an API (e.g., WinSock send()), and the Client Monitor intercepts the call. SAMSUNG-1005, [0088]; SAMSUNG-1013, 30:16-17. RFD adds the data

lengths (measure of usage) to a counter associated with the application. SAMSUNG-1013, 30:24-26. RFD then determines whether the counter exceeds a “rule-based quantity” (control policy specifying a usage limit) for the application, and if so, disables future Internet access and/or warns the user.

SAMSUNG-1013, 30:26-29. This approach address one of the problems noted by Freund: “hording[sic] available network bandwidth through use of bandwidth-intensive applications (e.g., real-time audio programs).” SAMSUNG-1013, 2:12-14. In most cases, video streaming requires even more bandwidth than the “real-time audio” described in Freund, further motivating the use of Freund’s techniques.

[15] The wireless device recited in claim 1, wherein the user input comprises a directive to restrict, block, throttle, delay, quarantine, or shape at least a portion of traffic over the first wireless network associated with the first application when an amount or cost of usage of the first wireless network associated with the first application satisfies a condition relative to a threshold.

370. RFD renders [15] obvious.

371. As taught by Freund, RFD adds the data lengths (amount of usage) to a counter associated with the application (e.g., Rao’s video streaming). SAMSUNG-1005, [0088]; SAMSUNG-1013, 30:24-26. RFD then determines whether the counter exceeds a

“rule-based quantity” (control policy specifying condition related to a usage limit threshold) for the application, and if so, disables (blocks) future Internet access and/or warns the user. SAMSUNG-1013, 30:26-29. (I discuss conditions in §VII.B.)

372. This approach aligns with Freund’s teaching that a system should restrict “ho[a]rding available network bandwidth through use of bandwidth-intensive applications (e.g., real-time audio programs).” SAMSUNG-1013, 2:12-14. In response, Freund’s system monitors “access to the Internet by individual applications” which “allows the system ... to not only track Internet traffic” but also “determine in many cases data exchanged on a per application basis.” *Id.*, 11:9-15.
373. In RFD, control policies result from user input. *See* [1.6], [1.7a]; *see also*, §VII.B. In addition, Freund teaches a “rule wizard interface” that “allows [a] user (e.g., administrator)” to configure “rules which govern use of the protocols monitored by the system.” SAMSUNG-1013, 23:65-24:1. A POSITA would have recognized that wizards collect user input, which is then used to create RFD policies.

[16] The wireless device recited in claim 15, wherein the user input further comprises an indication of the threshold or information associated with the threshold.

374. RFD renders [16] obvious.

375. For example, Freund's wizard dialog (which obtains the user input) "asks the user what kind or type of new rule should be created." SAMSUNG-1013, 25:1-3. Freund's rules are combinations of "access rights granted on the basis of available applications, permitted time limits, permitted user activities, permitted protocols, and the like," which can include an indication of a threshold that defines the permitted data use by an application (as accumulated in the DataOut counter).
SAMSUNG-1013, 25:3-6, 30:24-29.

[26] The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to obtain a measure quantifying at least the first access to the first wireless network by the first application.

376. RFD renders [26] obvious.

377. As taught by Freund, in RFD, to send data, an application (e.g., video streaming of Rao) calls an API (e.g., WinSock send()), and the Client Monitor intercepts the call. SAMSUNG-1005, [0088]; SAMSUNG-1013, 30:16-17. RFD adds the data

lengths of the send (measure quantifying an access) to a counter associated with the application. SAMSUNG-1013, 30:24-26.

[27] The wireless device recited in claim 26, wherein obtain a measure quantifying at least the first access to the first wireless network by the first application comprises determine the measure quantifying at least the first access to the first wireless network by the first application.

378. RFD renders [27] obvious.

379. As taught by Freund, RFD determines the measure (amount of data sent) quantifying network access by the first application.

See [26]; SAMSUNG-1013, 30:16-26.

[29] The wireless device recited in claim 26, wherein the measure quantifying at least the first access to the first wireless network by the first application comprises an amount of data, a cost, or a time.

380. RFD renders [29] obvious.

381. As taught by Freund, RFD includes a measure of an amount of data sent (e.g., during a Winsock send()) by the first application (e.g., Rao's video streaming). SAMSUNG-1005, [0088]; SAMSUNG-1013, 30:16-26.

382. Freund further teaches a time measure, explaining that "monitoring the total time particular applications access the Internet provides enhanced control." SAMSUNG-1013, 10:45-45. Freund's monitoring "can track Internet access on a per application basis -- that is, access broken down by the

application or applications used for the access,” which “affords much better tracking and regulating of Internet activities, and “by monitoring total time users/workstations access the Internet, an organization can better determine the overall Internet access requirements and loads.” SAMSUNG-1013, 10:47-54.

383. Thus, per Freund, RFD measures both an amount of data and a time (total time the Internet is accessed, which can be per application).

[30] The wireless device recited in claim 26, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to assist in presenting, through the user interface, information based on the measure quantifying at least the first access to the first wireless network by the first application.

384. RFD renders [30] obvious.

385. RFD determines whether the counter exceeds a “rule-based quantity” (control policy specifying condition related to a usage limit threshold) for the application (e.g., Rao’s video streaming), and if so, disables (blocks) future Internet access and/or **warns the user**. SAMSUNG-1005, [0088]; SAMSUNG-1013, 30:26-29. A POSITA would have known that warning a user was conventionally done in a user interface.

386. In addition, the claimed “user interface,” does not appear to be limited to graphical user interface. Thus, to the extent Freund’s warning the user includes non-graphical components (sounds, vibrations, etc.), a POSITA would understand these to be presenting such information in the user interface. However, a POSITA would have understood “warn the user” to indicate, at least in some cases, a graphical warning.

J. Ground 1J: Rao-Freund-Bedi renders claim 28 obvious

[28] The wireless device recited in claim 26, wherein obtain a measure quantifying at least the first access to the first wireless network by the first application comprises obtain, from a network element, the measure quantifying at least the first access to the first wireless network by the first application.

387. RFD as modified by Bedi renders [28] obvious.

388. As described in §IX.S, when RFD lacks sufficient storage or computational resources to collect measures quantifying access to the network, RFD provide such data via a message broker to a data aggregator (network element). SAMSUNG-1030, [0004]; §XI.R, §IX.S. To enforce policies on applications, including the first application, RFD, obtains a measure quantifying network access by the first application, and uses that value to enforce the policy. *See* §XI.R, §IX.S.

389. Additionally, Bedi provides a second motivation for storing measures on external devices, explaining that “any data saved in volatile RAM will not survive a device or application failure—only log records saved to non-volatile storage will be available for analysis of the failure.” SAMSUNG-1030, [0004]. A POSITA would have recognized that if data are accumulated only on the device, and limits on aggregate behavior are enforced, a user could defeat the limit by restarting the device periodically. Such shenanigans are not possible when data are stored external to the device, e.g., on a network element.

K. Ground 2: Rao-Pregont-Jones renders claims 1, 24 obvious

[1.1]-[1.7a]

390. RPJD renders [1.1]-[1.7a] obvious. *See* §X.A.[1.1]-[1.7a].

[1.7b] the at least an aspect of the control policy for at least assisting in restricting or preventing a first access to the first wireless network by the first application when the first application is executing,

391. RPJD renders [1.7b] obvious.

392. Jones teaches that rules include a condition aspect that can depend on “the desired functionality, type of connection, connection bandwidth, user priorities, etc.” SAMSUNG-1006, 5:13-15. The condition aspect assists in determining whether to apply the action aspect, which “may prohibit data transfers.”

SAMSUNG-1006, 5:25-26. (I discuss policy conditions and actions in §VII.B.) Thus, a POSITA would have recognized that the condition aspect of RPJD’s control policy assists in preventing access by the first application (Pregont’s telephony relay). §IX.T, §IX.U. As I discuss in §VII.B, conditions determine whether to perform actions, in this case, blocking access.

393. Blocking access would occur, for example, when bandwidth is constrained. As I describe in §IX.U, Pregont’s relay service is providing value to *other* devices, so a POSITA would have recognized that the owner of the device benefits by blocking traffic from the relay application first, preserving bandwidth for applications that benefit the device’s owner, not other devices.

[1.7c] the at least an aspect of the control policy enabling a first control of the first access to the first wireless network by the first application when the first application is executing that differs from a second control of a second access to the first wireless network by a second application on the wireless device, and

394. RPJD teaches or renders [1.7c] obvious.

395. The condition aspects in Jones’s policies can depend on “the desired functionality, type of connection, connection bandwidth, user priorities, etc.” SAMSUNG-1006, 5:13-15. Pregont’s telephony relay application “passes through the cellular link as

data in the form of a data call (e.g., VoIP call).” SAMSUNG-1012, Abstract. Other RPJD applications (e.g., video conferencing) provide different functionality and use different connection types, so conditions that evaluate to TRUE for Pregont’s telephony relay application will evaluate to FALSE for other RPJD applications. For example, the functionality of email obviously differs from that of a forwarding service, and will use different protocols (e.g., POP or IMAP).

396. Thus, a first control (blocking network access) applied to the first application (telephony relay) will differ from a second control (allowing access) by a second application (e.g., video conferencing). As discussed in §IX.U and [1.7b] of this Ground, RPJD will prefer its own applications over the relay application.

[1.8] apply the control policy, thereby at least assisting in restricting or preventing the first access to the first wireless network by the first application when the first application is executing.

397. RPJD renders [1.8] obvious.

398. For example, Jones teaches that applying the policy “may prohibit data transfers,” which a POSITA would have recognized as preventing access. SAMSUNG-1006, 5:25-26.

[24] The wireless device recited in claim 1, wherein the first application is configured to assist in providing a forwarding service, the forwarding service for

forwarding traffic between (a) one or more other devices communicatively coupled to the wireless device over a second network and (b) a network system communicatively coupled to the wireless device over the first wireless network, and wherein the at least an aspect of the control policy at least assists in determining whether the forwarding service is available to one or more of the one of more other devices.

399. RPJD renders [24] obvious.

400. RPJD's telephony relay provides a forwarding service between a device coupled to RPJD and a network system. For example, Pregont teaches that, when the device "receives a request from" another device "(over an ad hoc network) to relay a call," it "start[s] a data call (e.g., voice over IP call) over the cellular link using the cellular phone's data capability." SAMSUNG-1012, Abstract.

401. Further, the condition aspect of RPJD's control policy at least assists in determining whether the telephony forwarding service is available to a second communication unit, e.g., based on available bandwidth. Conditions determine whether to execution actions, as I discuss in §VII.B.

402. For example, Jones teaches that policies can depend on "connection bandwidth," so if sufficient connection bandwidth is unavailable, RPJD prohibits data transfer from the telephony relay application, thereby making the forwarding service

unavailable to other devices. SAMSUNG-1006, 5:13-26;

§IX.X. As discussed in §IX.U and [1.7b] of this Ground, RPJD will prefer its own applications over the relay application.

XI. CONCLUSION

403. For all the reasons I have noted in the foregoing paragraphs, claims 1-30 of the '811 Patent are obvious in view of the references discussed above.

404. 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 Uhlott*, 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 Octeau 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 Neamtiu 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. Niagra 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. Tucson, 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 Miadzezhanka 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, CISP A 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.

Iseb: 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.