

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Gregory G. Raleigh, et al.
U.S. Patent No.: 9,137,701 Attorney Docket No.: 39843-0155IP1
Issue Date: September 15, 2015
Appl. Serial No.: 14/675,113
Filing Date: March 31, 2015
Title: WIRELESS END-USER DEVICE WITH DIFFERENTIATED
NETWORK ACCESS FOR BACKGROUND AND
FOREGROUND DEVICE APPLICATIONS

DECLARATION OF DR. PATRICK McDANIEL

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

Dated: August 25, 2023


By: _____
Patrick McDaniel, Ph.D.

TABLE OF CONTENTS

I.	ASSIGNMENT.....	4
II.	QUALIFICATIONS.....	4
III.	SUMMARY OF CONCLUSIONS FORMED.....	8
IV.	LEVEL OF ORDINARY SKILL IN THE ART.....	9
V.	LEGAL PRINCIPLES.....	10
	A. Terminology	10
	B. Legal Standards	11
	C. Anticipation	11
	D. Obviousness.....	12
VI.	MATERIALS CONSIDERED	16
VII.	TECHNOLOGY OVERVIEW.....	19
	A. Mobile Devices.....	19
	B. Resource Management in Mobile Devices	22
VIII.	OVERVIEW OF THE '701 PATENT	24
	A. Specification.....	24
	B. Claims.....	26
	C. Prosecution History	34
IX.	INTERPRETATION OF THE '701 PATENT CLAIMS	34
X.	SUMMARY OF RELEVANT PRIOR ART	35
	A. Rao (U.S. Pat. App. Pub. No. 2006/0039354)	35
	B. Oestvall (U.S. Pat. App. Pub. No. 2007/0038763)	40
	C. Montemurro (U.S. Pat. App. Pub. No. 2009/0207817)	43
	D. Araujo (U.S. Pat. App. Pub. No. 2009/0217065).....	46
XI.	GROUND 1A: Rao in view of Oestvall renders obvious claims 1-4, 9, 10, 13, 14, 16, 19, 20, and 25	52
	A. Combination of Rao and Oestvall	52
	B. Analysis of the Claims	56

XII.	GROUND 1B: Rao in view of Oestvall and Montemurro renders obvious claims 5-8, 11, 17, 18, 23, and 24	108
A.	Combination of Rao, Oestvall, and Montemurro.....	108
B.	Analysis of the Claims	111
XIII.	GROUND 1C: Rao in view of Oestvall and Araujo renders obvious claims 12, 15, 21 and 22	134
A.	Combination of Rao, Oestvall, and Araujo.....	134
B.	Analysis of the Claims	137
XIV.	CONCLUSION.....	145

I, Patrick McDaniel of Verona, Wisconsin, declare that:

I. ASSIGNMENT

1. I have been retained on behalf of Samsung Electronics Co., Ltd. (“Samsung”) to offer technical opinions related to 9,137,701 (“the ’701 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 ’701 patent.

2. I have been asked to provide my independent analysis of the ’701 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 ’701 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 ’701 patent.

II. QUALIFICATIONS

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 the 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 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, 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.

III. SUMMARY OF CONCLUSIONS FORMED

16. This Declaration explains the conclusions that I have formed based on my analysis. Based on my review, claims 1-25 (“the Challenged Claims”) of the ’701 patent are unpatentable. To summarize those conclusions:

- **Ground 1A:** Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claims 1-4, 9, 10, 13, 14, 16, 19, 20, and 25 are obvious in view of the Rao and Oestvall references.
- **Ground 1B:** Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claims 5-8, 11, 17, 18, 23, and 24 are obvious in view of the Rao, Oestvall, and Montemurro references.
- **Ground 1C:** Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claims 12, 15, 21, and 22 are obvious in view of the Rao, Oestvall, and Araujo references.

IV. LEVEL OF ORDINARY SKILL IN THE ART

17. I have been informed that a person of ordinary skill in the art (“POSITA”) is a hypothetical person who is presumed to have the skill and experience of an ordinary worker in the field at the time of the alleged invention. The ’701 patent was filed March 31, 2015, 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 ’701

patent as the point in time for claim interpretation purposes. My opinion does not change if the invention date is earlier.

18. Based on my knowledge and experience in the field and my review of the '701 patent and file history, I believe that a person of ordinary skill in the art in this matter would have had (1) at least a bachelor's degree in computer science, electrical engineering, or a related field, and (2) three to five years of experience with networking, power consumption of networked computing devices, and/or wireless digital communications systems. Additional graduate education could substitute for professional experience, and *vice versa*. Based on my experiences, I have a good understanding of the capabilities of a POSITA. Indeed, I have taught, mentored, advised, and collaborated closely with many such individuals over the course of my career.

V. LEGAL PRINCIPLES

A. Terminology

19. I have been informed by Counsel and understand that the best indicator of claim meaning is its usage in the context of the patent specification as understood by one of ordinary skill. I further understand that the words of the claims should be given their plain meaning unless that meaning is inconsistent with the patent specification or the patent's history of examination before the Patent Office. Counsel has also informed me, and I understand that, the words of the

claims should be interpreted as they would have been interpreted by one of ordinary skill at the time of the invention was made (not today). I have been informed by Counsel that I should use January 28, 2009 as the point in time for claim interpretation purposes.

B. Legal Standards

20. 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. 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

21. 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. 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. 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

22. 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. 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.

23. 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.

24. 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." 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.

25. 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. 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.

26. 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.

27. 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. 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.

28. 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. 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. 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

29. 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.

30. 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 '701 patent; my own knowledge and experiences gained from my work experience in the field of the '701 patent and related disciplines; and my experience in working with others involved in this field and related disciplines.

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

- SAMSUNG-1001 U.S. Patent No. 9,137,701 to Raleigh, et al. (“the ‘701 Patent”)
- SAMSUNG-1002 Excerpts from the Prosecution History of the ‘701 Patent (“the Prosecution History”)
- SAMSUNG-1004 Complaint, *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al.*, 2:22-cv-00422, E.D. Tex., October 26, 2022
- SAMSUNG-1005 U.S. Pat. App. Pub. No. 2006/0039354 (“Rao”)
- SAMSUNG-1006 U.S. Pat. App. Pub. No. 2007/0038763 (“Oestvall”)
- SAMSUNG-1007 U.S. Pat. App. Pub. No. 2009/0207817 (“Montemurro”)
- SAMSUNG-1009 U.S. Pat. App. Pub. No. 2008/0080458 (“Cole”)
- SAMSUNG-1010 U.S. Pat. No. 5,987,611 (“Freund”)
- SAMSUNG-1011 U.S. Pat. App. Pub. No. 2009/0217065 (“Araujo”)
- SAMSUNG-1013 U.S. Pat. No. 8,381,127 (“Singh”)
- SAMSUNG-1014 U.S. Pat. App. Pub. No. 2007/0173283A1 (“Livet”)
- SAMSUNG-1015 U.S. Pat. No. 8,413,172 (“Sng”)
- SAMSUNG-1016 Flinn, Jason, et al. “The case for intentional networking,” Proceedings of the 10th Workshop on Mobile Computing Systems and Applications, 2009 (“Flinn”)
- SAMSUNG-1017 Carter, Casey et al., “Contact networking: a localized mobility system,” Proceedings of the 1st International

Conference on Mobile systems, Applications and Services, 2003
("Carter")

- SAMSUNG-1019 U.S. Pat. App. Pub. No. 2009/0019022
("Schallert")
- SAMSUNG-1020 David Flanagan, O'Reilly & Associates, Inc.,
"Java in a Nutshell," 1996, ISBN: I-56592-183-6
- SAMSUNG-1021 W. Richard Stevens, et. al, "UNIX Network
Programming Volume 1, Third Edition: The Sockets Networking API,"
2004, ISBN: 0-13-141155-1
- SAMSUNG-1022 U.S. Pat. App. Pub. No. 2009/0093247
("Srinivasan")
- SAMSUNG-1023 U.S. Pat. App. Pub. No. 2008/0311897 ("Segal")
- SAMSUNG-1024 Buxton, B., "Integrating the Periphery and
Context: A New Model of Telematics," in Proceedings of Graphics
Interface '95, 1995
- SAMSUNG-1025 Hinckley et. al, "Foreground and background
interaction with sensor-enhanced mobile devices," ACM Trans. Comput.
Hum. Interact., vol. 12, no. 1, pp. 31–52, Mar. 2005
- SAMSUNG-1026 International Publication No. WO 03/100581
("Dive-Reclus")
- SAMSUNG-1027 U.S. Pat. No. 7,757,185 ("Paquette")
- SAMSUNG-1028 Westerinen, et al., IETF RFC 3198, Terminology
for Policy-Based Management, November 2001, *available at*
<https://www.ietf.org/rfc/rfc3198.txt>
- SAMSUNG-1029 Durham, et. al., IETF RFC 2748, "The COPS
(Common Open Policy Service) Protocol," January 2000, downloaded

from the internet at <https://www.rfc-editor.org/rfc/rfc2748.html> on August 1, 2023

- SAMSUNG-1034 W. Richard Stevens, UNIX Network Programming, Prentice Hall, 1990
- SAMSUNG-1035 A. Freier, et al., The Secure Sockets Layer (SSL) Protocol Version 3.0, Internet Engineering Task Force (IETF), Request for Comments: 6101, ISSN: 2070-1721, August 2011

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

VII. TECHNOLOGY OVERVIEW

33. In this section I provide a broad overview of the relevant technology and state of the technical community at the priority date of the '701 patent. This description is not intended to be exhaustive, but to provide sufficient background to support and contextualize my analysis below.

A. Mobile Devices

34. 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 app 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.

35. 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, (non-transitory¹) memory capacities in smartphones of 2009 were generally limited, typically ranging from 128 MB to 512 MB. Long term storage was also limited, consisting of between 4 to 16GB of space. Devices were

¹ In patents, the term “non-transitory” can refer to computer-readable media (CRM) that stores data for short periods or in the presence of power such as a memory device or Random Access Memory (RAM).

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

36. 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 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

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.

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.

37. At the same time, battery technology had not yet seen significant advancements, leading to smartphones with relatively short battery life. The computational requirements and increased user engagement (using the phone for longer periods) led to increased demand for energy. Here, the combination of power-hungry processors, smaller batteries, and less optimized software meant that users often had to charge their phones frequently.

B. Resource Management in Mobile Devices

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

39. 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.

40. A Policy Decision Point (PDP)⁴ and Policy Enforcement Point (PEP)⁵ are essential components in policy-based systems.⁶ 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.

⁴ A PDP is “[a] logical entity that makes policy decisions for itself or for other network elements that request such decisions.” SAMSUNG-1028, 8.

⁵ A PEP is “[a] logical entity that enforces policy decisions.” SAMSUNG-1028, 8.

⁶ SAMSUNG-1029, 3-6.

The PEP communicates with the PDP to obtain the relevant policy decisions and then enacts them by controlling access to resources. 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).

VIII. OVERVIEW OF THE '701 PATENT

A. Specification

41. The '701 Patent relates to “a wireless end-user device that has wireless wide-area network (WWAN) and wireless local-area network (WLAN) modems.” SAMSUNG-1001, Abstract. For example, the system “analyzes traffic from [a] network service consuming application,” and “categorize[s] the traffic” based on various criteria, such as “network type, time of day, connection cost, whether home or roaming, network busy state, QoS, and whether the particular service usage activity is in foreground of user interaction or in the background of user interaction.” *Id.*, 100:56-101:39.

42. Further, the system uses one or more policies to “determine an appropriate prioritization for traffic to and/or from the network service consuming application.” *Id.*, 101:47-57. For example, in accordance with one or more policies, the system can selectively (i) “cause[] the network service consuming application

... traffic to be queued in [an] application traffic cache” for transmission over a network or (ii) “restrict network access of a particular service usage activity.” *Id.*, 101:63-102:37).

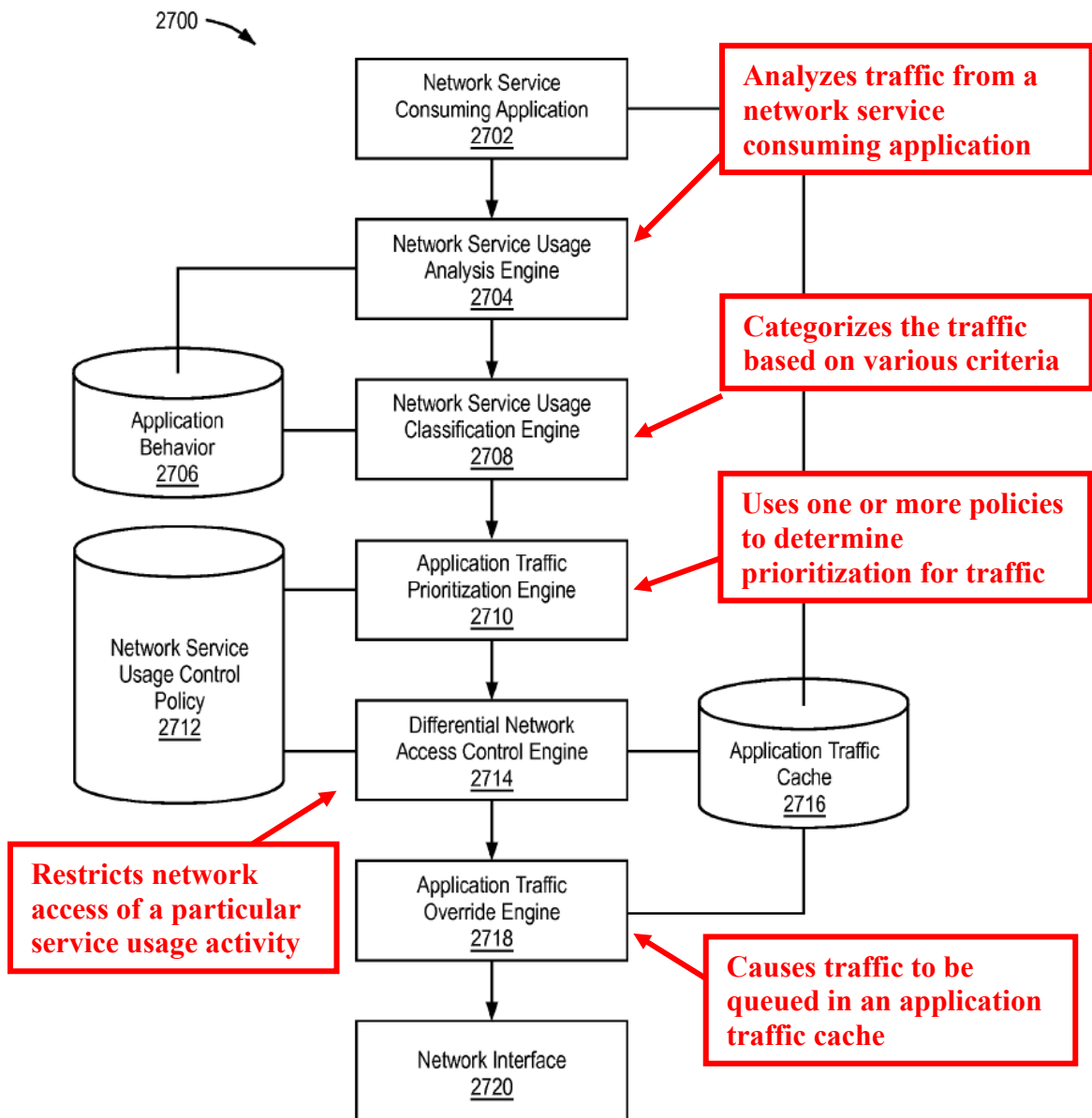


FIG. 27

SAMSUNG-1001, Figure 27

B. Claims

43. The table below includes identifiers for the '701 patent claims and limitations, which are referenced throughout.

Claim 1	
[1pre]	A wireless end-user device, comprising:
[1a]	a wireless wide area network (WWAN) modem to communicate data for Internet service activities between the device and at least one WWAN, when configured for and connected to the WWAN;
[1b]	a wireless local area network (WLAN) modem to communicate data for Internet service activities between the device and at least one WLAN, when configured for and connected to the WLAN;
[1c]	one or more processors configured to
[1d]	determine, for a first end-user application capable of running in a background state and capable of running as a foreground application, whether the application is running in a background state or as a foreground application, and
[1e]	control, via an application program interface (API), application access for Internet service activities provided through the WWAN modem and the WLAN modem, to, based on a first differential traffic control policy, selectively block and allow access by the first

	end-user application to the WWAN modem at a time when data for Internet service activities is communicated through a WWAN modem connection to the at least one WWAN,
[1f], [1g]	wherein the access is selectively blocked based on a determination that the first end-user application is running in a background state, and wherein the access is selectively allowed based on a determination that the first end-user application is running as a foreground application.
Claim 2	
[2]	The wireless end-user device of claim 1, wherein the one or more processors are configured to determine that the first end-user application is running in a background state when a user of the device is not directly interacting with that application or perceiving any benefit from that application.
Claim 3	
[3]	The wireless end-user device of claim 1, further comprising a user interface to provide a user of the device with information regarding why the first differential traffic control policy is applied to the first end-user application.
Claim 4	

[4]	The wireless end-user device of claim 1, further comprising a user interface to inform a user of the device when there are options to set, control, override, or modify service usage controls that affect the first differential traffic control policy.
Claim 5	
[5]	The wireless end-user device of claim 1, wherein the first differential traffic control policy is part of a multimode profile having different policies for different networks.
Claim 6	
[6]	The wireless end-user device of claim 5, wherein the one or more processors are further configured to select a traffic control policy from the multimode profile based at least in part on the type of network connection currently in use by the device.
Claim 7	
[7]	The wireless end-user device of claim 6, wherein the one or more processors are further configured to, when the type of network connection is at least one type of WLAN connection, select a traffic control policy from the multimode profile based at least in part on a type of network connection from the WLAN to the Internet.

Claim 8	
[8a]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to determine whether a second end-user application is running in a background state or as a foreground application, and
[8b]	control application access for Internet service activities by the second end-user application similar to the control of application access for the first end-user application, except the control of application access for Internet service activities by the second end-user application is based on a second differential traffic control policy that can be set different from the first differential traffic control policy.
Claim 9	
[9]	The wireless end-user device of claim 1, further comprising a network stack interface integrated with the API.
Claim 10	
[10]	The wireless end-user device of claim 1, further comprising a networking stack, wherein the one or more processors are further configured to, at an application service interface layer, identify application traffic flows prior to the flows entering the networking stack.

Claim 11	
[11]	The wireless end-user device of claim 1, wherein the one or more processors control of application access based on a first differential traffic control policy is applied to one of but not both of a connection to a roaming WWAN network and a connection to a home WWAN network.
Claim 12	
[12]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the first differential traffic control policy based on a power state of the device.
Claim 13	
[13]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the first differential traffic control policy based on a device usage state.
Claim 14	
[14]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the

	application of the first differential traffic control policy based on monitoring of user interaction with the device.
Claim 15	
[15]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the first differential traffic control policy based on power control state changes for one or more of the modems.
Claim 16	
[16]	The wireless end-user device of claim 1, wherein the one or more processors are configured to associate the first end-user application with the differential traffic control policy based on an application behavior.
Claim 17	
[17]	The wireless end-user device of claim 1, wherein the differential traffic control policy defines that applications to which the policy applies can only have WWAN network access events during particular time windows.
Claim 18	

[18]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to update the first differential traffic control policy based on information received from a network element.
Claim 19	
[19]	The wireless end-user device of claim 1, further comprising an agent to block, modify, remove, or replace user interface messages generated by the first end-user application based on the applied differential traffic control policy.
Claim 20	
[20]	The wireless end-user device of claim 1, wherein the one or more processors configured to control application access are configured to selectively block access by the first end-user application by intercepting open, connect, and/or write requests by the first end-user application to a network stack.
Claim 21	
[21]	The wireless end-user device of claim 20, wherein the API responds to an intercepted request by the first end-user application by emulating network messaging.

Claim 22	
[22]	The wireless end-user device of claim 21, wherein emulating network messaging comprises responding to a network request from the particular application by blocking the request from passing to a network stack and returning to the particular application a message indicating the network request was not successful.
Claim 23	
[23]	The wireless end-user device of claim 1, the first differential traffic control policy comprising first and second sub-policies applicable respectively to Internet data service provided using the WWAN modem to connect to a home WWAN and a roaming WWAN, wherein the one or more processors are further configured to apply the first sub-policy when Internet data service is provided through a home WWAN and to apply the second sub-policy when Internet data service is provided through a roaming WWAN.
Claim 24	
[24]	The wireless end-user device of claim 1, the first differential traffic control policy comprising first, second, and third sub-policies applicable respectively to Internet data service provided using the

	WWAN modem and three different network types from the network types consisting of 2G, 3G, 4G, home, and roaming.
Claim 25	
[25]	The wireless end-user device of claim 1, wherein the one or more processors are configured to determine when the first end-user application is running in a background state or as a foreground application based on a state of user interface priority for the application.

C. Prosecution History

44. The '701 patent was allowed on the first action, and no prior art rejection was made. SAMSUNG-1002, 317-324. During prosecution, the Patent Office did not consider any of Rao, Oestvall, Montemurro, and Araujo. As explained in more detail below, these references in various combinations render the Challenged Claims obvious.

IX. INTERPRETATION OF THE ' 701 PATENT CLAIMS

45. I understand that, for purposes of my analysis in this *inter partes* review proceeding, the terms appearing in a patent claim should be interpreted according to their ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. In that regard, I understand that the best indicator of claim meaning is its usage in

the context of the patent specification as understood by a POSITA. 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. I also understand that the words of the claims should be interpreted as they would have been interpreted by a POSITA at the time the invention was made (not today). Because I do not know at what date the invention as claimed was made, if ever, I have used the Critical Date of the '701 patent as the point in time for claim interpretation purposes. My opinion does not change if the invention date is earlier.

X. SUMMARY OF RELEVANT PRIOR ART

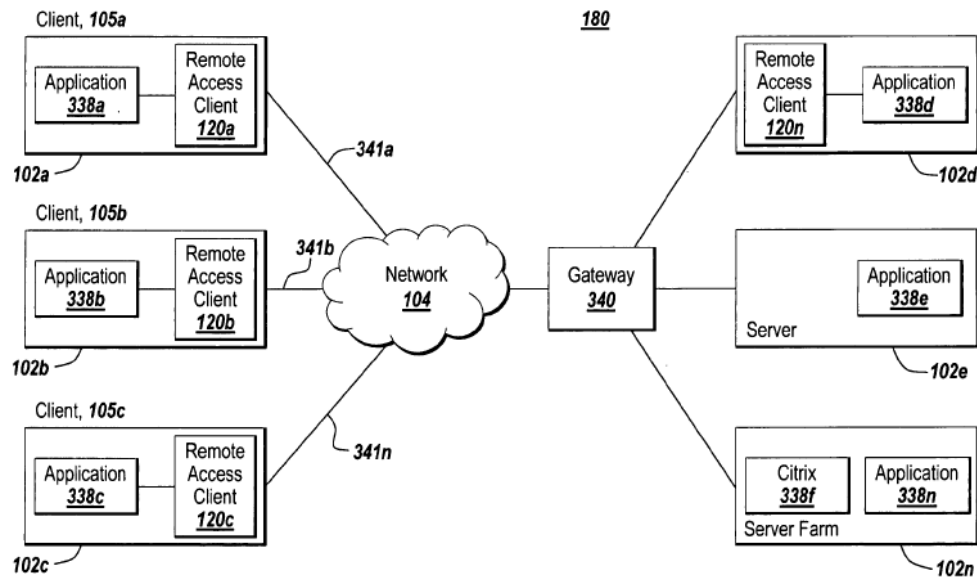
A. Rao (U.S. Pat. App. Pub. No. 2006/0039354)

46. Rao relates to a "remote access architecture" for a system that provides "peer-to-peer communications and remote access connectivity." SAMSUNG-1005, Abstract. The system includes clients 105 (instances of computing devices 102) that communicate with each other over a network 104 (and optionally through a gateway 340) and with other types of computing devices, such as servers 102e and server farms 102n. *Id.*, [0086]-[0096].

47. Rao is analogous art to the '701 patent since, like the '701 patent, Rao describes techniques for using policies to regulate network-related activity and/or adjust the operation of applications running on a device. SAMSUNG-1001, 104:8-

18. Additionally, Rao describes techniques reasonably pertinent to the problem allegedly solved by the '701 patent. For example, as discussed below, Rao describes techniques for analyzing traffic from an application, categorizing the traffic, and classifying an interaction state of an application based on whether the application is running in the background or the foreground. *Id.*, 103:16-103:67.

48. Figure 1A shows an example of the Rao system:



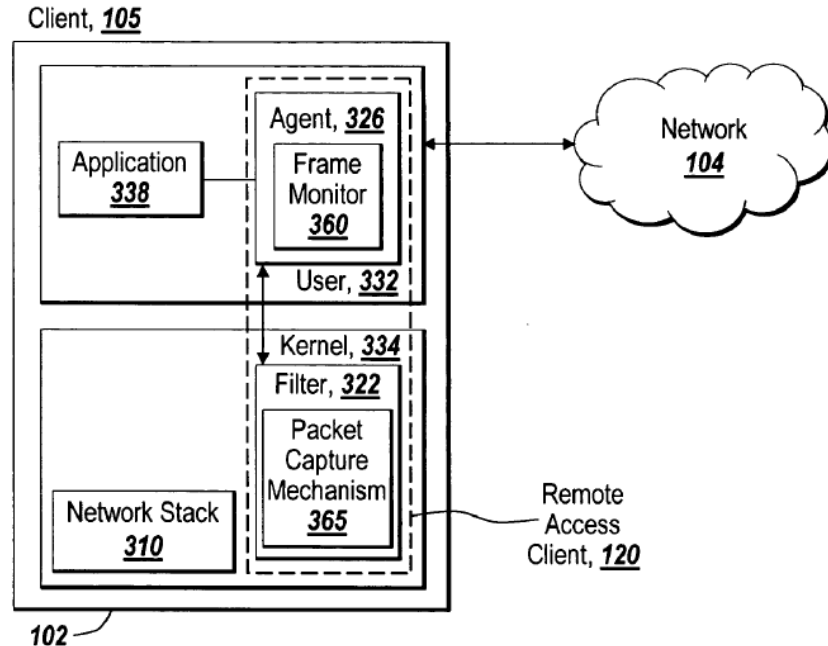
SAMSUNG-1005, Figure 1A

49. Rao's system is designed to address 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" since "a network packet generated or received for an application running in the background may be processed ahead of a network packet

generated or received for the application running in the foreground.” SAMSUNG-1005, [0001]. This results in applications suffering from increased latency and reduced the quality of voice communication. *Id.*

50. In Rao these network inefficiencies are addressed through a prioritizations scheme that “provide[s] application-aware, client-specific prioritization of packet traffic.” SAMSUNG-1005, [0003]. The prioritization scheme is achieved by augmenting client 105 with a remote access client 120 that interacts with applications 338 and network stack 310. SAMSUNG-1005, [0100].

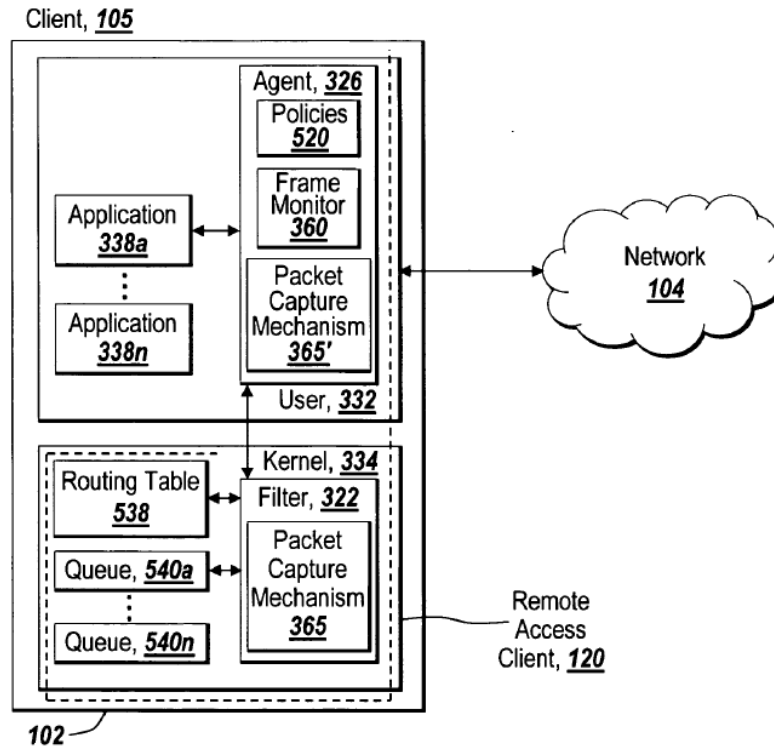
51. Figure 1C shows an example of a system with a remote access client for routing network packets from client 105 to network 104.



SAMSUNG-1005, Figure 1C

52. The remote access client 120 includes a filter 322 that uses a filtering table “to determine what action to take against packets,” including “ensur[ing] that unwanted packets are discarded” and “deny[ing] access to particular protocols or to prevent unauthorized access from remote computers by discarding packets to specified destination addresses.” SAMSUNG-1005, [0102]. An agent 326 with a frame monitor 360 “include[s] policies and logic for applying a policy to a received packet.” *Id.*, [0108]. Frame monitor 360 also “transmit[s] a packet to a gateway 340 responsive to a policy-based determination made by the frame monitor 360.” *Id.* Use of policies through remote access client 120 guides efficient use of network resources and thereby enables the Rao system to address the deficiencies identified within Rao’s disclosure.

53. Further, Rao’s client-side application-aware network communication system enables “intelligent and client centric prioritization of application network communications on a client based on the type and/or priority of an application.” *Id.*, [0179], Figure 5A (reproduced below). To perform this prioritization, the Rao system “appl[ies] a policy to determine a condition of the client 105, or endpoint, at the time of transmission of the packet.” SAMSUNG-1005, [0109].



SAMSUNG-1005, Figure 5A

54. Rao offers non-limiting disclosure relating to the specification of policies 520 and how its system leverages each of these policies 520 for prioritization. SAMSUNG-1005, [0182] (“policies 520 may be specified by any suitable means and/or mechanisms”). As examples, Rao describes that policies 520 can be specified by “name of the application 338a-338n,” “type of application 338a-338n,” or “type of one or more protocols used by the applications 338a-338n.” SAMSUNG-1005, [0182]. Further, policies 520 can “define prioritization based on whether an application is running in the foreground or the background of the client 105,” “indicate prioritization based on the destination network address, such as host name or IP address, and/or destination port number,” and be

“specified conditionally, such as if one application 338a is running, a second application 338b may have a higher or lower priority.” *Id.* Indeed, “[o]ne ordinarily skilled in the art will recognize and appreciate the multitude of ways to define client-side application priorities.” *Id.* Further, policies 520 can be used to “determine which packets to queue and/or discard.” *Id.*, [0207]. Thus, policies 520 can “apply a priority to network packets of applications 338a-338n in accordance with the prioritization rules specified or indicated by the policies 520.” *Id.*

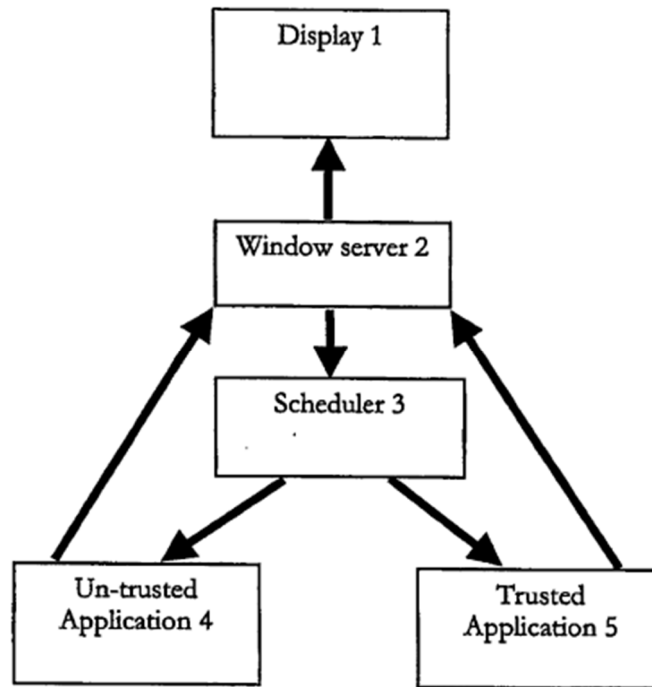
B. Oestvall (U.S. Pat. App. Pub. No. 2007/0038763)

55. Oestvall relates to techniques to “preserve or conserve resources, such as battery power” on mobile devices. SAMSUNG-1006, [0002]. Oestvall emphasizes that battery consumption is “very important,” particularly in devices that “consume high power levels by virtue of connecting to always-on GPRS or 3G cellular networks.” *Id.*, [0004]. This problem is “especially acute for multi-tasking devices, i.e., devices with an operating system that can run several applications at the same time.” *Id.*, [0007]. This occurs since conventional schedulers used for multitasking may be configured such that “applications will continue to run even when not actually in active use,” which results in the applications continuing to “use some system resources, even when residing in the ‘background.’” *Id.*, [0006].

56. Oestvall is analogous art to the ’701 patent since, like the ’701 patent, Oestvall describes techniques for regulating network-related activity and of

applications running on a device. SAMSUNG-1001, 104:8-18. Additionally, Oestvall describes techniques reasonably pertinent to the problem allegedly solved by the '701 patent. For example, as discussed below, Rao describes techniques for classifying an interaction state of an application based on whether the application is running in the background or the foreground and adjusting an application's access to device resources based on the classification. *Id.*, 104:40-65.

57. In Oestvall these power consumption challenges are addressed using techniques that “deny[] system resources and services to background applications that do not meet predefined ‘trust’ or certification criteria,” which it refers to as “untrusted” applications. SAMSUNG-1006, [0010], Figure 1 (below). Examples of untrusted applications include those that are “not able to access certain predefined protected resources,” from third-party sources and thereby “loaded from RAM”, or have not been validated using a “predefined validation or certification process. *Id.*, [0011]-[0013].



SAMSUNG-1006, Figure 1

58. In Oestvall, a window server component 2 determines “if an application is in the background or foreground on display 1.” SAMSUNG-1006, [0023]. If the application is an untrusted application 4 and is running in the background, then the window server component 2 “sen[ds] a control signal to the scheduler 3” that prevents untrusted application 4 from “running, e.g., being given any services or consuming any resources.” *Id.* Oestvall offers several non-limiting examples for how scheduler 3 may regulate access to resources by a background untrusted application 4. *Id.* As examples, scheduler 3 may “never allocate any services or resources,” or “place any interrupts from [the application] to the back of its queue and never allow them to be executed.” *Id.* As another example,

scheduler 3 may prevent background untrusted applications 4 from “‘polling’ for data over a wireless network” or “prevent[ed] from running.” *Id.*, [0024]. Further, when an application is in the foreground, then the application may be permitted to “run again—e.g., to be provided with resources and services.” *Id.*, [0025].

C. Montemurro (U.S. Pat. App. Pub. No. 2009/0207817)

59. Montemurro relates to “policy-based routing of communications among two or more modes of wireless communication.” SAMSUNG-1007, [0001]. Devices with such connectivity capabilities are “dual or multi-mode devices,” with “radio access technologies that provide access to” multiple network types, including WLAN, WWAN, another others. *Id.*, [0003]. But “[t]here are costs associated with application access from these different network[,]” and thus, “[i]t is therefore desirable to have a mechanism that seeks to optimize communications for multi-mode capable devices.” *Id.*, [0004].

60. Montemurro is analogous art to the ’701 patent since, like the ’701 patent, Montemurro describes techniques for enabling network access to different types of wireless networks. SAMSUNG-1001, Abstract. Additionally, Montemurro describes techniques reasonably pertinent to the problem allegedly solved by the ’701 patent. For example, as discussed below, Montemurro describes techniques for identifying the types of wireless networks that are available for connection and routing techniques for establishing a connection to the most suitable network. *Id.*

61. Montemurro's mechanism broadly relies on policies to "configure connections and routes." SAMSUNG-1007, [0011]. The configuration is accomplished using a "rules engine" that "evaluates [the] policies on a status change (e.g., network availability, time of day, etc.) to configure a routing table." *Id.* Together, the rules engine and the routing table "provides an appropriate connection to an application for its respective communications." *Id.* Figure 2 (below) shows "policy-based data routing for multi-mode operations of device 102 for communicating with network infrastructure." SAMSUNG-1007, [0024].

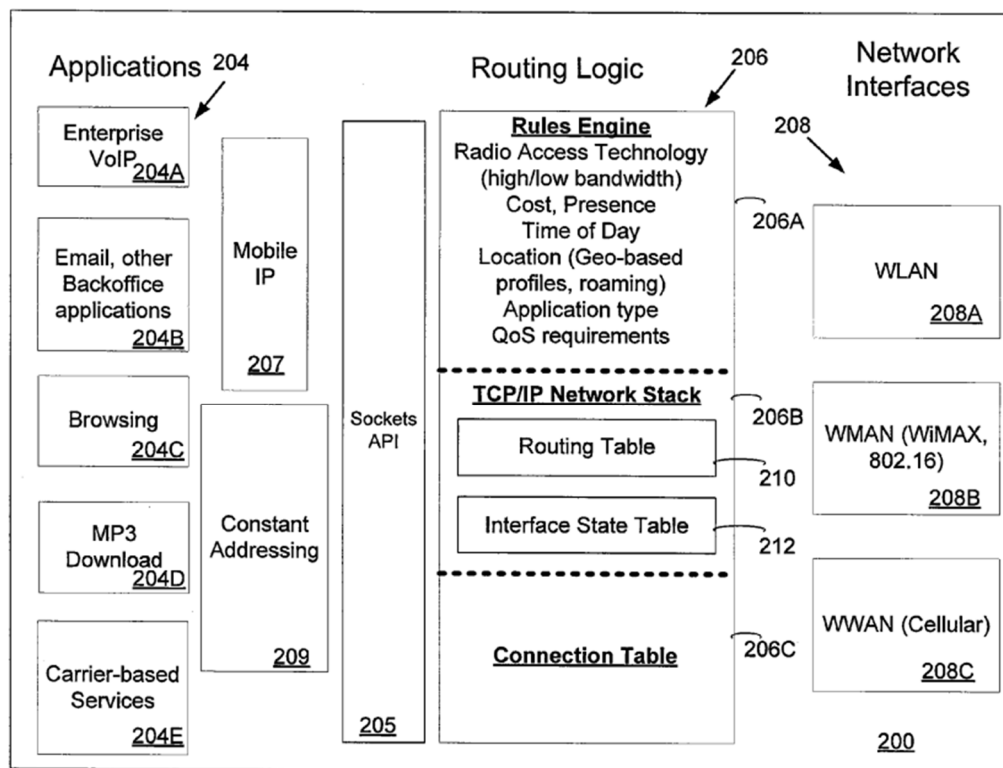


Figure 2

SAMSUNG-1007, Figure 2

62. In Montemurro, the device 102 includes “a plurality of applications 204, routing logic 206, and network interfaces 208.” SAMSUNG-1007, [0025]. Routing logic 206 further includes rules engine 206A as a “policy-based mechanism using rules to configure TCP/IP network stack 206B and connection table 206C to coordinate communications for applications 204 using communications interfaces [208].” *Id.*, [0027]. For example, “a rule is a specific policy that is entered in the ‘rules engine’ for carrying out the policy.” *Id.*

63. Network interfaces 208 include “an interface for each of WLAN 208A, WMAN 208B and WWAN 208C network communications,” and optionally, “short-range wireless interfaces (e.g., Bluetooth wireless) and interface(s) for wired network communications (e.g., serial interfaces such as USB, RS 232, etc.).” SAMSUNG-1007, [0028]. Rules engine 206A “configures the communication operations with a set of rules/policies” for “various factors such as radio access technology (e.g., for high/low bandwidth properties), cost, presence, time of day, location (e.g., geo-based policies, network roaming), destination IP address, application type, and Quality of Service (QoS) requirements, among others.” *Id.*, [0029].

64. Further, rules engine 206A “configures (i.e. modifies, periodically in response to changes of state and the evaluation of its rules) connection table 207C and routing table 210 to optimize the flow of communications over multiple

communications modes (e.g., interfaces 208 and respective networks 104 and 106).” SAMSUNG-1007, [0033]. On a state change, e.g., “time of day,” “connecting/disconnecting of device 102 with a specific network 104 and 106,” rules engine 206A executes and modifies “routing table 210 to ensure that data goes out to the most appropriate network (via respective network interface 208).” *Id.*, [0035]. Rules engine 206A further “determine[s] which interface would be best to service a particular application.” *Id.*

D. Araujo (U.S. Pat. App. Pub. No. 2009/0217065)

65. Araujo describes “a power-management policy” for managing a “machine's power usage.” SAMSUNG-1011, Abstract. Araujo’s policy can be implemented on “[e]lectronic devices,” such as “computers, wireless telephones, audio/video equipment, etc.)” *Id.*, [0014]. The policy is applied to “justify [a program] consuming power, depending on what the program is doing.” *Id.*, [0004]. By implementing this policy, a device can better “use the energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge.” *Id.*, [0001].

66. Araujo is analogous art to the ’701 patent since, like the ’701 patent, Araujo describes techniques for allowing or blocking an application’s access to device resources based on a classification of the application. SAMSUNG-1001, 100:56-101:39. Additionally, Araujo describes techniques reasonably pertinent to

the problem allegedly solved by the '976 patent. For example, as discussed below, Araujo describes mechanisms to allow or prevent an application from performing actions based on a power consumption associated with performing those actions. *Id.*, 89:8-43.

67. Araujo also teaches that a device can classify programs with respect to various criteria, and selectively provide resources to the programs based on their classifications. SAMSUNG-1011, [0027]. As an example, Araujo describes that programs “may have a status that reflects its worthiness to consume power.” *Id.* In particular, a program “may have a ‘VIP’ status that allows them to consume power in situations where other programs would not be permitted to consume power,” where “VIP” typically stands for “very important person,” but in this context may be applied to a program in this sense of denoting one program's relative merit or justification to consume energy.” *Id.* As Araujo explains, “[w]hether a program is permitted to consume power could be based on a finding as to whether the program's status justifies the consumption of power under the circumstances that are present.” *Id.*

68. Araujo teaches that the device can provide resources to the applications differently, based on whether the applications are “worthy” to consume power. SAMSUNG-1011, [0024]. For example, Araujo describes that a program can generate “a request to perform an action using a particular device,

such as “a request to send data over a wireless network” using a “wireless network card.” *Id.*, [0020], [0024].

69. In response, the device can selectively perform various operations with respect to the request, including:

- “Allow[ing]” the request if the power management policy “allows the device’s power state to be changed,” such as powering-on a device that is in an “off state” or send the request to a device that is “already powered on” (SAMSUNG-1011, [0035]; Figure 3, 302), or
- “Block[ing]” the request if the power management policy “does not allow the device's power state to be changed,” either permanently or temporarily, such as by queuing the request, blocking the request, dropping the request, delaying the request, and/or referring the request to another device (*Id.*, [0035], [0050]; Figure 4, 406).

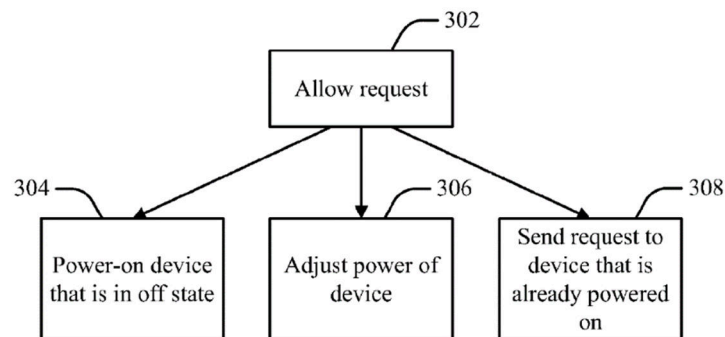
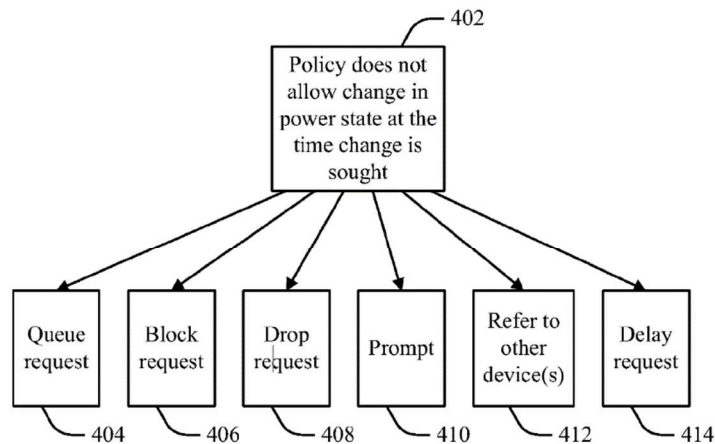


FIG. 3

SAMSUNG-1011, Figure 3

**FIG. 4**

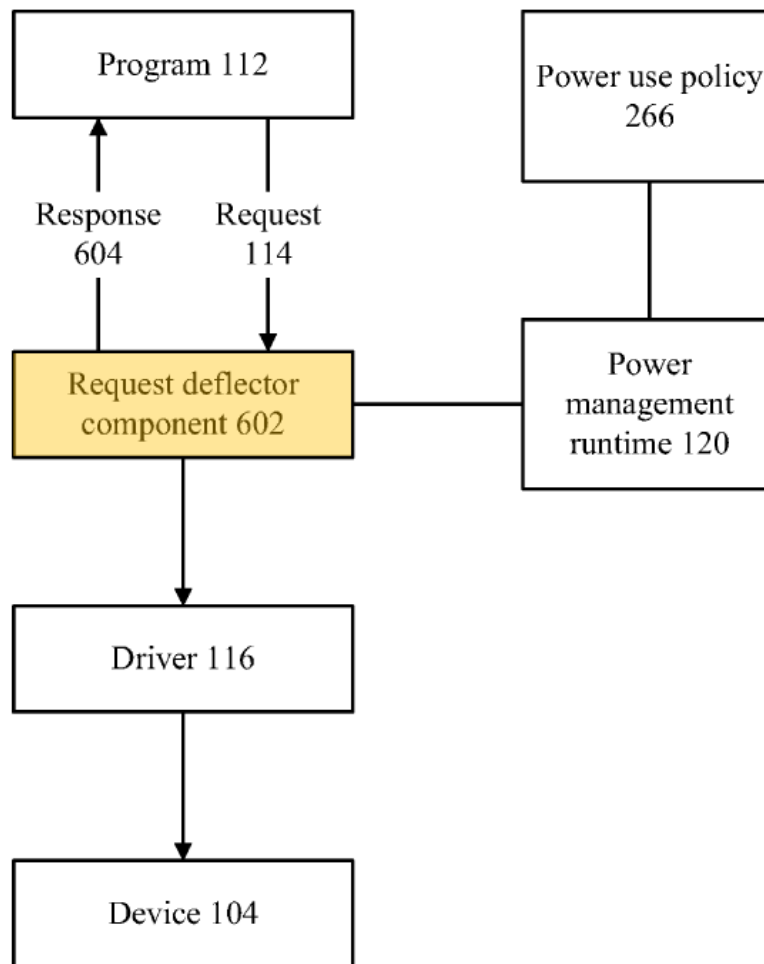
SAMSUNG-1011, Figure 4

70. Specifically, Araujo describes selectively allowing or blocking a request using a “request deflector component” that is “interposed” between a “program” and a “driver” of a “device,” and configured to “intercept[] requests and respond[] to the requests based on power management considerations before the request reach a device driver.” SAMSUNG-1011, [0024], [0050]. As Araujo explains:

Request deflector component 602 is a component that is interposed between program 112 and driver 116. Request deflector component receives requests before the requests are conveyed to drivers. When request deflector component 602 detects that a request (such as request 114) has been made, it interacts with power management runtime 120 to determine what the ambient policy (e.g., power use policy 266) says about

whether the request may be carried out at the expense of power use. *If power management runtime 120 determines that request 114 may be carried out under the power policy, then request deflector component 602 passes the request along to driver 116. Otherwise, request deflector component may permanently or temporarily deflect the request from reaching driver 116.*”

Id. (emphasis added).



SAMSUNG-1011, Figure 6 (annotated)

71. Araujo describes that the “request deflector component” can be used to mediate a program’s request to any of several different types of devices. As one example, Araujo describes that “device 104 may be machine 102’s wireless network card, and request 114 may be a request [by the program 112] to send data over a wireless network.” *Id.*, [0020]. Based on the program 112’s “worthiness” to consume power (*e.g.*, whether the program is “VIP” or “non-VIP”), the request deflector 602 can selectively:

- Power on the network card “in order to allow the device to service the request” (*Id.*, [0037]; Figure 3, 304),
- Use the “already-powered” network card “to service the program’s request” (*Id.*, [0037]; Figure 3, 308), and/or
- “Block the request” for usage of the network card (*Id.*, [0040]; Figure 4, 406).

That is, Araujo’s device selectively allows a program’s request when it deems that the program is sufficiently important to consume resources (*e.g.*, “worthy” programs, such as “VIP” programs), while selectively denying the program’s request when it deems that the program is not sufficiently important to consume resources (*e.g.*, programs that are not “worthy,” such as “non-VIP programs).

XI. GROUND 1A: Rao in view of Oestvall renders obvious claims 1-4, 9, 10, 13, 14, 16, 19, 20, and 25

A. Combination of Rao and Oestvall

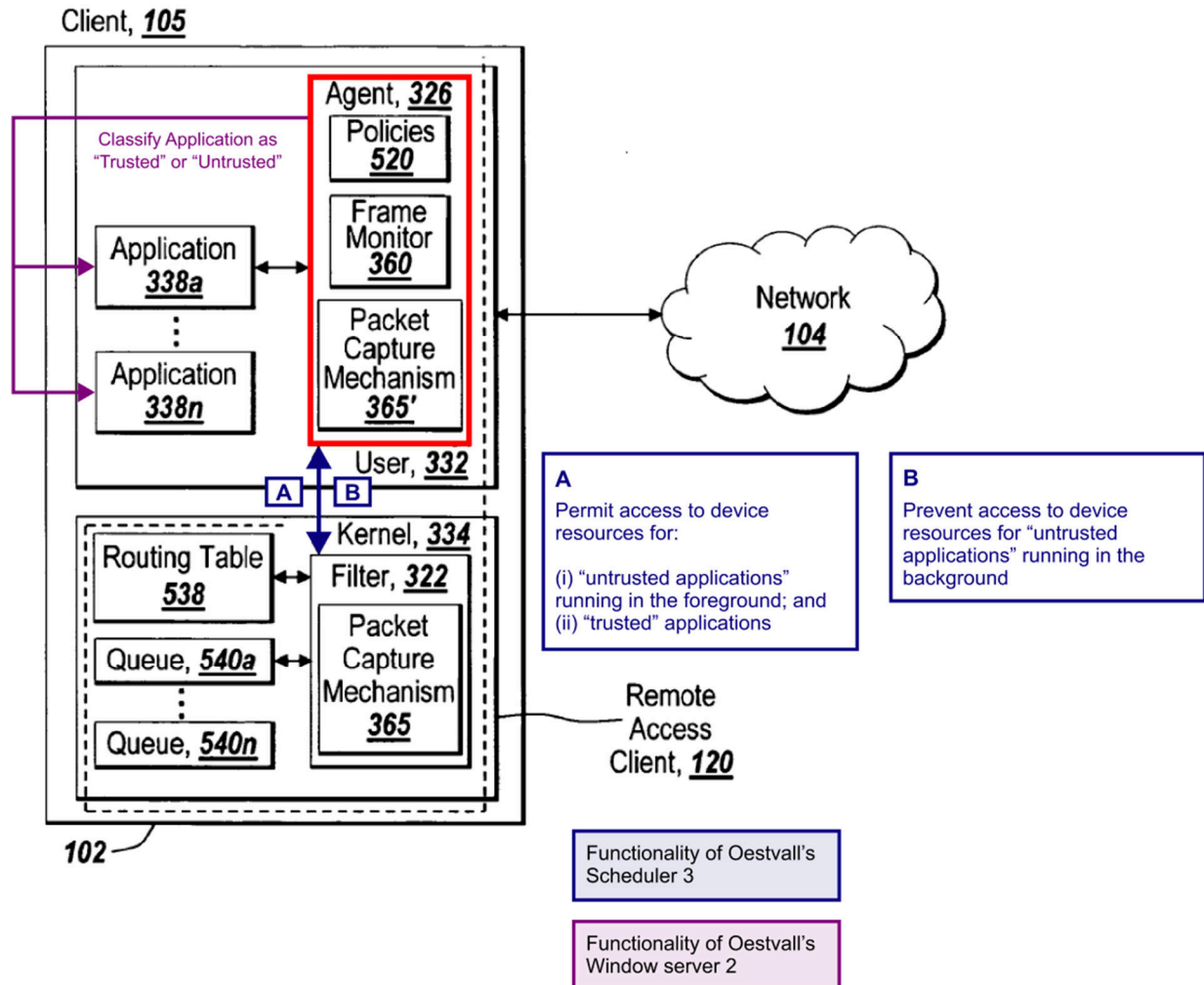
72. As described above, Rao describes applying policies to prioritize transmission of certain higher-priority network packets over other lower-priority network packets. SAMSUNG-1005, [0179]-[0195], Figure 5A. While Rao teaches that such prioritization techniques would have improved the efficient utilization of network resources, a POSITA would have further understood that the prioritization techniques may have implications not specifically addressed within Rao's disclosure. For instance, by the Critical Date, a POSITA would have recognized that Rao's prioritization techniques reduce congestion and improved packet throughput. SAMSUNG-1005, [0195]. But Rao does not expressly discuss implementation of using application states in its prioritization techniques, and by the Critical Date, a POSITA would have understood that application states similarly impact the problems addressed in Rao, such as network usage efficiency. A POSITA looking to implement Rao would have therefore been motivated to look to solutions to improve Rao's packet-based prioritization techniques.

73. In seeking solutions, a POSITA would have identified Oestvall, which, like Rao, is broadly focused on achieving efficiencies associated with mobile device operation. SAMSUNG-1006, [0002]. Oestvall further offers techniques to "preserve[] system resources by denying system resources and

services” to certain applications. SAMSUNG-1006, [0010]. A POSITA would have found obvious integration of Oestvall’s resource conservation techniques into the Rao system to promote more efficient peer-to-peer communications and network access connectivity that also reduces power consumption on a mobile device. As explained below, the resulting Rao-Oestvall device would have performed various types of prioritizations regulating access to device resources by applications, such as those based on network packet transmission (“application-aware, client-specific prioritization of packet traffic” as described in Rao) and others based on the classification of an application (described in Oestvall). Given Oestvall’s focus on battery conservation, Rao-Oestvall would have therefore enabled prioritization in a manner that conserves battery power. *Id.*

74. For example, in the Rao-Oestvall device (shown below), a POSITA would have improved the agent 326 (red) to incorporate functionality associated with Oestvall’s window server 2 (purple) and functionality associated with scheduler 3 (blue). SAMSUNG-1006, [0023]. Such a configuration would have enabled an improved agent to classify applications 338a-n (for which packet transmissions are prioritized) as an “trusted” or “untrusted” application. *Id.* The configuration would have also enabled the improved agent to prevent an untrusted application from running or being given access to a service that consumes

resources. *Id.* Below is a visual diagram of the Rao-Oestvall combination discussed above.



SAMSUNG-1005, Figure 5A (illustrating the Rao-Oestvall combination)

75. As illustrated above, a POSITA would have found obvious that the Rao-Oestvall combination enables policies that provide various types of prioritizations, consistent with Rao. SAMSUNG-1005, [0182]. This would have improved the use of policies in certain network scenarios contemplated in Rao

since policies can be used to prevent network packet transmissions of applications that would have otherwise contributed to additional power consumption.

76. To implement the functionality discussed above, a POSITA would have also modified Rao's policies 520 to include logic relating to a classification of an application. Such a modification is consistent with Rao, which specifies that the policies already "may be specified by the name of the application 338a-338n and/or the type of application 338a-338n." SAMSUNG-1005, [0182]. Further, Rao describes that policies "define prioritization based on whether an application is running in the foreground or the background of the client 105." *Id.* Thus, a POSITA would have found it natural to implement the Rao-Oestvall device such that the policies used by the device indicate information for both packet-based and application-based prioritizations.

77. Finally, configuring Rao's client to leverage Oestvall's teachings would have required only routine programming knowledge well within the skill of a POSITA prior to the earliest effective filing date. Indeed, the change would have amounted to nothing more than the use of a known technique to improve similar devices – in each instance a smart phone equipped with software to regulate device activity based on monitoring user-device interactions – in a similar way, and combining prior art elements according to known methods to yield the predictable results described above.

78. Furthermore, the elements of the resulting Rao-Oestvall system would each perform functions they had been known to perform prior to the combination—client 105 would perform the same functions to prioritize higher-priority messages over lower-priority messages through the use of policies 520, as taught in Rao, but would leverage functionality offered by Oestvall’s window server 2 and scheduler 3 to identify a classification of an application (trusted, untrusted) and the application’s interaction state (foreground, background). Accordingly, a POSITA would have naturally expected success when incorporating Oestvall’s teachings into the Rao system, as described above.

B. Analysis of the Claims

1. Claim 1

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

79. Even if the preamble were considered to be limiting, the Rao-Oestvall combination renders obvious a ***wireless end-user device***. For example, Rao describes “multiple computing devices 102a-102c” (also referred to as “clients 105a-105c”), which connect to a network using one or more network connections. SAMSUNG-1005, [0086]. Client 105 can be “any type and/or form of computing device 102 that can run one or more applications 338,” such as a “web browser, web-based client, client-server application, a thin-client computing client, an ActiveX control, or a Java applet.” *Id.*, [0088]. Client 105 can also be a “mobile

client,” such as a “notebook, personal digital assistant (PDA), a smart phone” or “telecommunication device.” *Id.*, [0198].

[1a] a wireless wide area network (WWAN) modem to communicate data for Internet service activities between the device and at least one WWAN, when configured for and connected to the WWAN;

80. The Rao-Oestvall combination renders this limitation obvious because the device in the combination would have included network connectivity features that Rao describes for device 102 (client 105). For example, Rao describes a device including a “network interface 118 to interface to ... Wide Area Network (WAN) through a variety of connections,” such as “standard telephone lines, LAN or WAN links,” “broadband connections,” “wireless connections,” or “some combination of any or all of the above.” SAMSUNG-1005, [0095], [0125]. Rao’s “network interface” includes “a built-in network adapter, network interface card, PCMCIA network card, card bus 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.* A POSITA would have therefore understood and found obvious to implement network interface 118 to enable multiple types of network connectivity such that network interface 118 includes, among others, a “***WWAN modem***” to permit Rao-Oestvall to communicate with network 104 as a WWAN (“***at least one WWAN***”) for accessing services

associated with a remote access client (“*communicate data for Internet service activities*”). SAMSUNG-1005, [0172], [0198], [0090].

81. Network configurations for mobile devices that enabled WLAN and WWAN connectivity and techniques for alternating connectivity between such configurations were conventional by the Critical Date. For example, Cole (SAMSUNG-1009) describes a mobile device 110 that includes one or more “communication interfaces 225,” including, for example, “a *WWAN modem 230*, a WLAN modem 235, a LAN device 240, a WPAN device 245, and a voice band modem 250 (e.g., V90).” SAMSUNG-1009, [0035], Figure 2. As another example, Montemurro (SAMSUNG-1007) describes that “if both the WLAN and WWAN radios...of [a] device [] *are connected* to their respective networks 104 and 106, there will be a route associated with each network 104 and 106...” *Id.*, [0030].

[1b] a wireless local area network (WLAN) modem to communicate data for Internet service activities between the device and at least one WLAN, when configured for and connected to the WLAN;

82. The Rao-Oestvall combination provides [1b]. For example, as discussed in [1a], Rao provides non-limiting disclosure relating to network connectivity features provided by network interface 118, which would have been included in Rao-Oestvall. SAMSUNG-1005, [0095], [0125]. Rao’s network interface 118 enables connectivity “through a variety of connections,” such as “standard telephone lines, LAN or WAN links,” “broadband connections,”

“wireless connections,” or “some combination of any or all of the above.”

SAMSUNG-1005, [0125]. A POSITA would have therefore understood and found obvious to implement network interface 118 to enable multiple types of network connectivity such that network interface 118 includes, among others, a “**WLAN modem**” to permit Rao-Oestvall to communicate with network 104 as a wireless LAN (“**at least one WLAN**”) for accessing services associated with a remote access client (“**communicate data for Internet service activities**”). SAMSUNG-1005, [0172], [0198], [0090]. Further, as noted above, network configurations for mobile devices that enabled WLAN and WWAN connectivity and techniques for alternating connectivity between such configurations were conventional by the Critical Date. SAMSUNG-1007, [0030]; SAMSUNG-1009, [0035], Figure 2.

[1c] one or more processors configured to

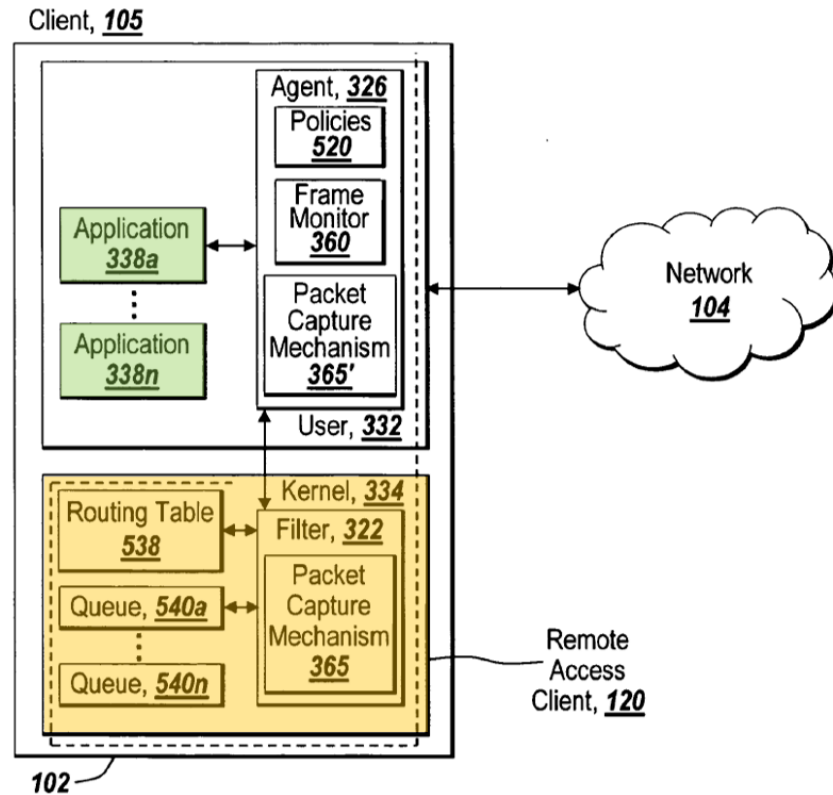
83. The Rao-Oestvall device renders obvious [1c]. Rao’s device 102 includes “central processing unit” (“**one or more processors**”), which can be “any logic circuitry that responds to and processes instructions fetched from the main memory unit 104.” SAMSUNG-1005, [0118]-[0119]; *see also id.*, [0121] (“main processor”). For example, device 102 includes “central processing unit [112]” (or “CPU 112” as depicted in Figure 1D), which may be “any logic circuitry that responds to and processes instructions from the main memory 104.” *Id.*, [0119].

Further, it would have been obvious for the processor(s) in the Rao-Oestvall device to perform the operations required in the Challenged Claims.

[1d] determine, for a first end-user application capable of running in a background state and capable of running as a foreground application, whether the application is running in a background state or as a foreground application, and

84. The Rao-Oestvall device renders obvious ***determining ... whether the application is running in a background state or as a foreground application.*** For example, Rao's device 102 (i.e., "client 105") includes "remote access client 120" that "determine[s] whether the application 338a-338n associated with the network packet is running in the foreground or the background of the client 105."

SAMSUNG-1005, [0188], [0182] ("the remote access client 120 may have one or more policies 520 for specifying client-side prioritization of network communications related to applications 338a-338n running on application. ... the policies 520 define prioritization based on whether an application is running in the foreground or the background of the client 105."); *see also id.*, [0189] ("the agent 326 may use characteristics of the application 338a-338n, such as running in the foreground or background, to indicate priority for a network packet of the application 338a-338n.").



SAMSUNG-1005, Figure 5A (annotated)

85. The Rao-Oestvall device further renders obvious *a first end-user application capable of running in a background state and capable of running as a foreground application*. For example, Rao's device 102/client 105 "execute[s] one or more applications 338a-338n, which access the network 104 via the agent 326 and filter 322 of the remote access client 120." SAMSUNG-1005, [0179]. Rao's applications 338a-338n provide services for end-users, such as "real-time data communications, such as VoIP," "email, collaboration, online meeting, and/or desktop sharing related services or functionality," thereby describing a *first end-user application*. *Id.*; see also *id.*, [0088]. Rao further describes that the

applications 338a-338n can “run[] in the foreground or the background.”

SAMSUNG-1005, [0188], [0189] (“characteristics of the application 338a-338n, such as running in the foreground or background”), [0182] (“whether an application is running in the foreground or the background of the client 105”).

86. Indeed, a POSITA would have understood and found obvious that an application can selectively run in background or foreground states. For example, a VoIP application, as discussed in Rao, can run in a foreground state when a user actively interacts with the application during a call (e.g., speaking via a microphone, listening via a speaker, dialing via a keypad, etc.), and can also run in a background state when the call is put on hold or when the VoIP is not in use (e.g., a stand-by mode). A POSITA would have understood that Rao would not contemplate the VoIP application as always running in the foreground state even if when a caller was put on hold or the application was not in active use, which would directly contradict the purposes of Rao, “improv[ing] or increas[ing] the performance, operational characteristics, and user experience on the client based on the applications running on the client.” SAMSUNG-1005, [0080]. Notably, Rao does not describe the notions of foreground and background running as mutually exclusive. Rao’s techniques (e.g., “client-side application-aware prioritization”) are applicable to an application capable of selectively running in foreground and background states, similarly to a situation where two applications are categorically

distinctive from each other as foreground and background applications.

SAMSUNG-1005, [0185] (“In this manner, the techniques of the present invention support any type of application 338a-338n on the client 105.”).

87. To the extent that Rao is not explicit as to whether a single application is capable of running selectively in foreground and background states, it would have been obvious that an application can run either of the states as needed, as evidenced in Oestvall. For example, Oestvall describes that its device is “capable of determining if an untrusted application is in the background or foreground.” SAMSUNG-1006, [0016], [0017], [0021] (describing that the “untrusted application” is switched between the background and the foreground for the purpose of preserving system resources and battery power). Therefore, in the combination, Rao’s device would have been modified such that an application (e.g., “untrusted application”) executed at the device can selectively run in foreground and background states, as taught by Oestvall. A POSITA would have been motivated to make such modification for several known benefits described above.

[1e] control, via an application program interface (API), application access for Internet service activities provided through the WWAN modem and the WLAN modem, to, based on a first differential traffic control policy, selectively block and allow access by the first end-user application to the WWAN modem at a time when data for Internet service activities is communicated through a WWAN modem connection to the at least one WWAN,

88. The Rao-Oestvall device renders obvious [1e], as discussed below.

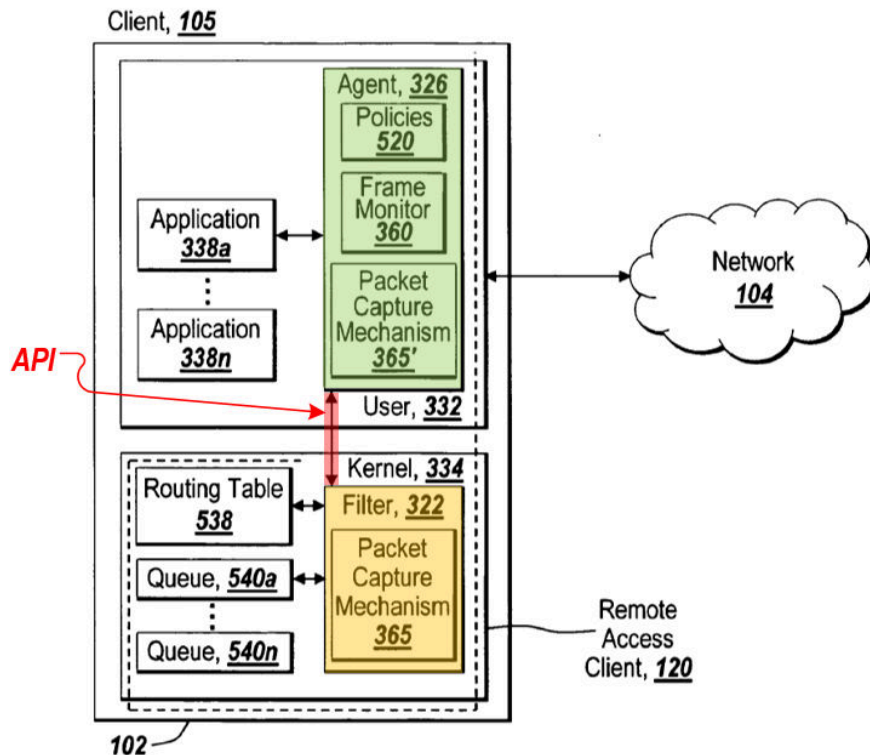
89. **First**, with respect to “*control ... application access for Internet service activities provided through the WWAN modem and the WLAN modem,*” Rao’s device 102 “execute[s] one or more applications 338a-338n, which access the network 104 via the agent 326 and filter 322 of the remote access client 120.” SAMSUNG-1005, [0179]. Such access to the network 104 is to communicate data for *Internet service activities*, such as “one or more real-time data communications, such as VoIP” and “email, collaboration, online meeting, and/or desktop sharing related services or functionality.” *Id.*, [0178], [0090], [0082] (“the illustrative embodiments of the present invention may be generally described in connection with an internet protocol (IP) based protocol”). As described in [1a] and [1b], such *Internet service activities* are *provided through the WWAN modem and the WLAN modem*.

90. Rao’s device 102 generally controls access by those applications 338a-338n (*application access*) to the network 104 by, for example, “intercepting network traffic of any of the applications 338a-338n” and “queuing and prioritizing network communications” for the applications. SAMSUNG-1005, [0179]-[0195]. In particular, Rao’s device 102 controls each application’s access to the network by (i) “intercept[ing] one or more networks packets associated with an application 338a-338n,” which then are “stored to a queue 540a-540n,” (ii) determining “a priority for the intercepted and queued network packet ... based on the type and/or

priority of the application 338a-338n,” and (iii) communicating “the network packets ... according to the determined priority.” SAMSUNG-1005, [0184]-[0190], Figure 5B.

91. **Second**, with respect to “*via an application program interface (API)*,” the Rao-Oestvall device implements various APIs. SAMSUNG-1005, [0106], [0110], [0166], [0190], [0205]. Rao describes that its “policies 520 may be accessible by the agent 326, configured into the agent 326, or loaded by the agent 326.” SAMSUNG-1005, [0183], Figure 5A (reproduced below). Further, referring to Figure 5A below, Rao’s device 102 includes “agent 326” that “indicates the priority to the filter 322 for management of network packet queues 540a-540n to apply the indicated priorities.” SAMSUNG-1005, [0190]. “The agent 326 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)*, such an IOCTL interface, or any other type and/or form of interface known to those ordinarily skilled in the art.” *Id.*; *see also id.*, [0106]. As such, Rao’s device 102 controls application access to the network 104 *via API*. The ioctl() API (input/output control) is used in computer systems to specify or change the policy associated with a network connection. SAMSUNG-1034, 43, 322-325. In the case of Rao-Oestvall, this would be used to set or modify the priority of the traffic associated with an application or network connection.

92. Below is Rao's Figure 5A that illustrates an example implementation of API.



SAMSUNG-1005, Figure 5A (annotated)

93. Similarly, Oestvall incorporates by reference Dive-Reclus (SAMSUNG-1026), which teaches using APIs in accessing a network. SAMSUNG-1006, [0020]; SAMSUNG-1026, 16:23-17:28, 20:1-12 (table).

94. As such, based on disclosure of API usage in Rao and Oestvall, the improved agent in Rao-Oestvall-Montemurro would have leveraged several types of APIs in regulating applications. *See also* SAMSUNG-1005, [0110] (“hooking application programming interface (API)”), [0166]. For example, Rao contemplates using an IOCTL API for interfacing with device drivers

(SAMSUNG-1005, [0106], [0190]) and a hooking API for intercepting and/or hooking network traffic of applications (*id.*, [0166]). Rao also describes leveraging any suitable “means” or “mechanism” to implement functionality relating to prioritization (interception). *Id.*, [0106]. Likewise, Oestvall incorporates by reference Dive-Reclus, which teaches permissions regulating network access by a third-party application that uses an API call, and a POSITA would have found obvious that a permission decision (grant, deny) is communicated to the third-party application through a corresponding API. SAMSUNG-1006, [0020]; SAMSUNG-1026, 16:23-17:28, 20:1-12 (table). Given these disclosures, a POSITA would have understood and found obvious that APIs leveraged by the improved agent of Rao-Oestvall-Montemurro includes those described in Rao and Oestvall, as well as conventional APIs known by the Critical Date, to support application operations in mobile devices.

95. One example is Java sockets API through which an application communicates data over a network. SAMSUNG-1020, 149-50. Rao describes that its device can run the Java operating system, and thus, a POSITA would have understood and found obvious that in some implementations of the Rao-Oestvall-Montemurro device, applications running on the device would access the network using Java sockets API. *Id.*; SAMSUNG-1005, [0088], [0128]. For example, when a network access condition is used to prevent an application from accessing the

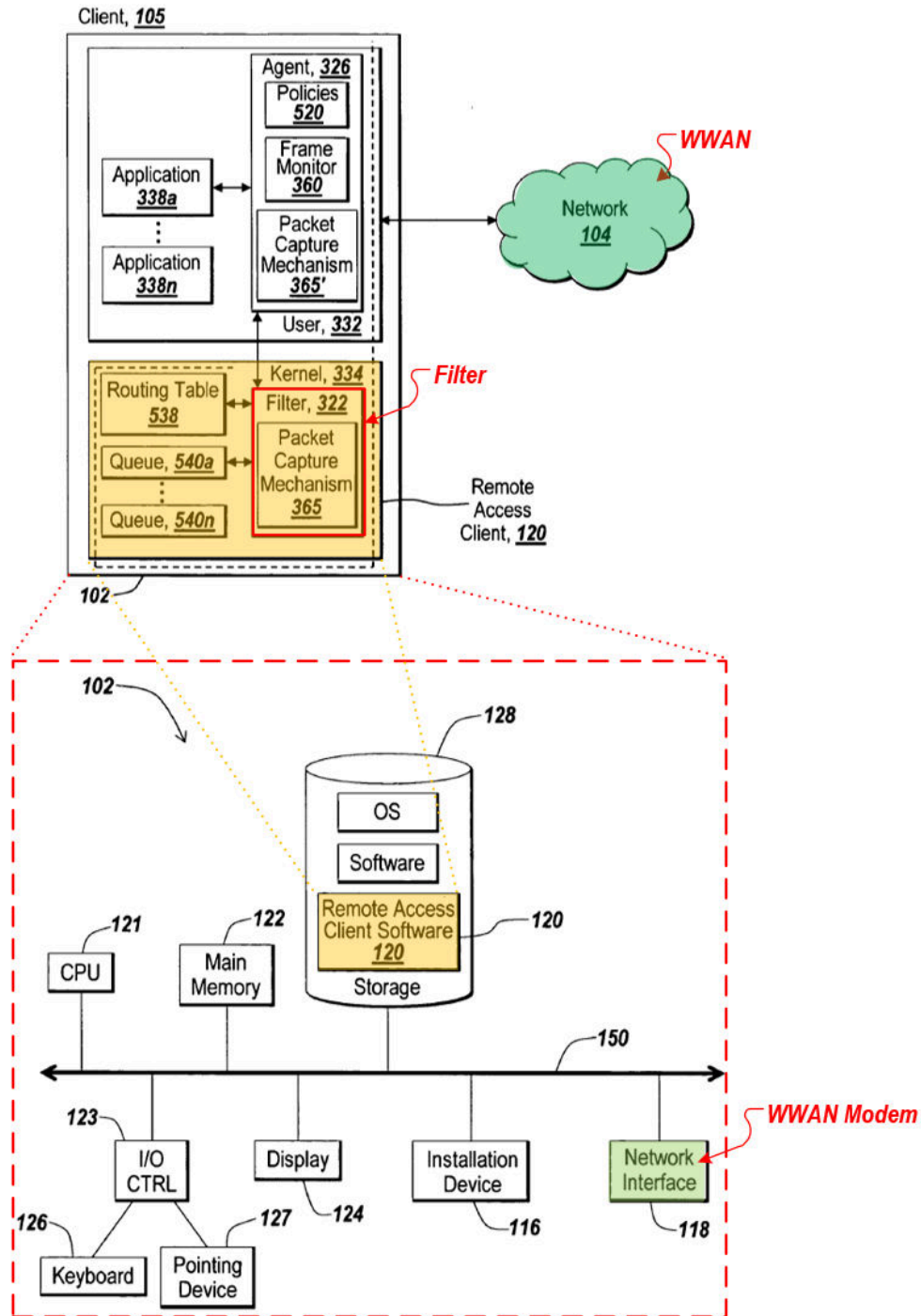
network, a POSITA would have understood and found obvious that the application would have received an indication, via the Java sockets API, of the network access condition. Note that Java sockets are a programming language specific implementation of the more general POSIX (Portable Operating System Interface) sockets interface. Socket interfaces are implemented among many programming languages and used to allow applications to connect, transmit and receive data across data networks. SAMSUNG-1034, 258-341.

96. Indeed, use of APIs to provide indications to applications was well-known by the Critical Date and a POSITA would have found it obvious to use well-known APIs to provide communications to applications in Rao-Oestvall. For example, Schallert (SAMSUNG-1019) describes providing an “API” to “allow[] [a] computer program to execute queries and integrate the results of these queries into the computer program’s internal system.” SAMSUNG-1019, Abstract. As another example, a conference publication by Flinn et al. (SAMSUNG-1016) described an “API” that “offers both blocking and event-based interfaces...” SAMSUNG-1016, 1. Flinn further indicates existence of “API features to the normal socket interface[,]” including application regulation mechanisms, such as “block[ing] [a] message until the network is available, with an optional timeout,” which is “more useful to threaded applications.” *Id.*, 3.

97. **Third**, with respect to “*based on a first differential traffic control*

policy,” Rao’s remote access client 120 in the device 102 has “one or more policies 520 for specifying client-side prioritization of network communications related to applications 338a-338n running on application.” SAMSUNG-1005, [0182]-[0183], [0187], [0189], [0193]-[0194], [0207] (“The remote access client 120 may use the policies 520 to determine which network packets to queue and/or discard.”); *see also id.*, [0108]-[0109] (The agent in Rao’s client device “provides functionality for applying a policy to a received packet.”). Because Rao’s policies are designed to prioritize, queue, and discard network packets, they offer different controls for different network traffics (network packets), thereby teaching *a first differential traffic control policy*.

98. **Fourth**, with respect to “*to ... selectively block and allow access by the first end-user application to the WWAN modem*,” Rao’s device can *allow* network packets to be transmitted to the network through the modem using filter 322 that can “place, arrange, or coordinate network packets into queues 540a-540n in support of the priorities,” which are defined by the policies 520. SAMSUNG-1005, [0191], [0182], [0179]-[0180], [0189]. According to the priorities, the device 102 communicates network packets to the network 104 (e.g., WWAN) through the network interface 118 (e.g., *WWAN modem*). *Id.*, [0184], [0191]-[0194]; *see supra* [1a]; Figures 1D and 5A (below).



SAMSUNG-1005, Figures 1D and 5A (annotated)

99. Further, Rao's device can **block** network packets from being transmitted to the network through the modem by using the same filter 322, which

can “discard[]” the network packets. SAMSUNG-1005, [0207]; *see also id.*, [0102] (“In some embodiments, the filter 322 may drop or accept the network packets depending on their content. In other embodiments, the filter 322 may route the network packets to the agent 326 based on the packets content and/or the filtering table. The filter table may also be used to ensure that unwanted packets are discarded. The filter 322 may be used to deny access to particular protocols or to prevent unauthorized access from remote computers by discarding packets to specified destination addresses.”).

100. The remote access client 120 in Rao’s device 102 includes filter 322 that can “place, arrange, or coordinate network packets into queues 540a-540n in support of the priorities,” which are defined by the policies 520. SAMSUNG-1005, [0191], [0182], [0179]-[0180], [0189]. Then, client 120 can “use the policies 520 to determine which network packets to queue and/or discard,” so that certain network packets are blocked from being transmitted to the network. SAMSUNG-1005, [0207], [0102].

101. Although Rao’s description regarding the use of “policies 520” in this context is set forth in the context of “a network disruption shielding technique” (*see, e.g.*, SAMSUNG-1005, [0199]), a POSITA would have found it obvious to also use policies 520 to discard low priority packets in other circumstances where the network is not disrupted but there exists a similar desire to, nevertheless,

reduce communications over the network (e.g., due to reductions in bandwidth of the network, or a surge in higher priority packets to be sent over the network).

Doing so would have achieved the benefit of ensuring that communication resources are selectively freed up for higher priority packets/communications. For instance, a POSITA would have understood or found it obvious to configure Rao's device to prioritize the captured packets by selectively "drop[ping] or accept[ing] the network packets depending on their content" (e.g., effectively deprioritizing those captured packets entirely) SAMSUNG-1005, [0102]. As an example, Rao's filter 322 can be used to "discard[] packets" having the lowest priority (e.g., "unwanted packets") such that the packets are not transmitted to the network. SAMSUNG-1005, [0102].

102. Notably, Rao's filter 322's packet capturing mechanism 356 can be implemented at "any layer, or portion thereof, of a network stack 310 of the client 105," so that the interception of network packets can occur at any layer or portion of the network stack in the client 105. SAMSUNG-1005, [0101]. Therefore, a POSITA would have understood and found obvious that, in Rao, the network packets generated by an application can be dropped or discarded before reaching to Rao's network interface 118 (*WWAN modem*), which means that the application's access to the network interface 118 (*access by the first end-user application to the*

WWAN modem) is ***blocked***. SAMSUNG-1005, [0207], Figures 1D and 5A (above).

103. Similar to Rao, Oestvall describes that its scheduler regulates access to resources by an untrusted application depending on whether the application runs in the background or foreground. SAMSUNG-1006, [0023]. For example, when an untrusted application is running in the background, Oestvall’s device prevents the application from “being given any services or consuming any resources,” and therefore a POSITA would have understood and found obvious that such prevention would block the application’s access to network resources (e.g., WWAN modem). *Id.*, [0023]-[0024]. When the untrusted application is running in the foreground, the application is permitted to “run again—e.g., to be provided with resources and services,” and thus a POSITA would have understood and found obvious that such permission would allow the application to access network resources (e.g., WWAN modem). *Id.*, [0025].

104. **Fifth**, with respect to “*at a time when data for Internet service activities is communicated through a WWAN modem connection to the at least one WWAN*,” as described in [1a] and [1b], Rao describes WLAN and WWAN as example network types to which network packets generated by an application can be transmitted via the network interface, such as a wireless network adapter or modem. SAMSUNG-1005, [0125]. Therefore, a POSITA would have understood

and found obvious that there would be *a time when Rao's device operates to communicate data for Internet service activities to the WWAN through the WWAN modem.*

105. Additionally, Rao describes that the network packets generated by an application are prioritized or dropped based on the policies 520, which define various criteria including (i) the name of the application, (ii) the type of the application, (iii) the type of *protocol* used by the application, (iv) the priority of the application, (v) whether the application is running in the foreground or in the background, (vi) “any other characteristics or statistics of the application” such as “size, memory usage, total execution time, and/or frequency of use,” (vii) the size of the network packet, (viii) the time the network packet is intercepted, (ix) “*other network factors, such as congestion,*” and (x) “*any network statistics and other factors occurring on the network.*” SAMSUNG-1005, [0182]-[0184], [0188]-[0189], [0192]-[0193], [0195]; *see also id.*, [0102]. In particular, Rao’s “policies 520 may be specified hierarchically to account for multiple applications 338a-338n and/or *multiple protocols* that may be executed on the client 105 at any point.” *Id.*, [0182]. Therefore, a POSITA would have understood and found obvious that WLAN and WWAN are associated with different “protocols” and that Rao’s policies can be tailored for an application capable of communicating to a specific “protocol,” such as WWAN. Accordingly, Rao teaches that *access by the first end-*

user application to the WWAN modem is selectively blocked and allowed *at a time when data for Internet service activities is communicated through a WWAN modem connection to the at least one WWAN*, as required in 1[e].

106. For example, a POSITA would have found it obvious to configure policy use by Rao-Oestvall to increase device efficiency in scenarios where device operation increases battery consumption, such as when the device is engaged in network activity over a WWAN network. Indeed, in Oestvall, “battery conservation in battery operated computing devices is very important, particularly in devices such as smartphones that consume high power levels by virtue of connecting to always-on GPRS or 3G cellular networks.” SAMSUNG-1006, [0004]. A POSITA would have found it advantageous to implement Rao-Oestvall to apply policies 520 to regulate application activity (“*control ... application access for Internet service activities ... to, based on a first differential traffic control policy, selectively block and allow access by the first end-user application*”) to reduce battery consumption during time periods when its device is connected to “always-on GPRS or 3G cellular networks” (“*at a time period when data for Internet service activities is communicated through a WWAN modem connection to the at least one WWAN*”). For example, in some scenarios where Rao-Oestvall is communicating over a WWAN network, its device would have leveraged Rao’s technique to intercept lower-priority network packets, by

leveraging Oestvall's technique of denying access to services or resources, each of which would have reduced battery consumption.

107. Moreover, the plain meaning of this limitation does not require any mobile device configuration in which policy application exclusively occurs when Internet service activities of a mobile device is communicated through a WWAN mode. Rather, as explained above, the limitation is met by any mobile device configuration in which policy application occurs on a mobile device configured to communicate over either a WWAN or WLAN. The Rao-Oestvall device is configured to communicate over either a WWAN or WLAN, and further has functionality to apply policies in either network scenario. This configuration of Rao-Oestvall renders this limitation obvious.

108. Indeed, it was well-known to implement Rao-Oestvall's techniques in the context of different networks (e.g., WWAN or WLAN) so that the device in the combination can selectively work for one or more of the networks based on various factors, as evidenced in Montemurro. For example, Montemurro describes that a device can selectively operate in multiple communication modes (e.g., WLAN or WWAN) based on rules/policies. SAMSUNG-1007, Abstract. Such rules/policies "include various factors such as radio access technology (e.g., for high/low bandwidth properties), cost, presence, time of day, location (e.g. geo-based policies, network roaming), destination IP address, *application type*, and Quality of

Service (QoS) requirements, among others.” *Id.*, [0029]. Therefore, a POSITA would have found it obvious to implement Rao-Oestvall’s device to selectively operate in one of the modes (e.g., WWAN) as taught by Montemurro, so that it can have *a time when data for Internet service activities is communicated through a WWAN modem connection to the at least one WWAN*.

109. Rao describes using policy 520 to enable application-aware prioritization, suggesting to a POSITA that policy 520 is applied “*when*” application 338 is classified as not running in the foreground. This interpretation is consistent with Rao’s disclosures that policies 520 “specify[] client-side prioritization of network communications related to applications 338a-338n” (SAMSUNG-1005, [0182]) and its motivation to address a scenario in which “a network packet generated or received for an application running in the background [is] processed ahead of a network packet generated or received for the application running in the foreground” (*id.*, [0003]). A POSITA would have found obvious that the evaluation of policies by Rao-Oestvall to prioritize network transmissions of an application given its interaction state to satisfy any temporal requirement between the use of a policy and classification of an interaction state of an application recited by this limitation.

110. As such, the Rao-Oestvall combination would have modified Rao’s device to control access by the applications 338a-338n to communicate data for

various Internet service activities (e.g., VoIP, email, collaboration, online meeting, or desktop sharing) through the WWAN and WLAN modems, via “any suitable means and/or mechanism such as via an application programming interface (API).” SAMSUNG-1005, [0179]-[0195]. Further, in the combined device, such control would have been performed, based on the policies taught by Rao, to selectively allow and block transmission of network packets to the network through the modem using filter 322 (as taught by Rao), at a time when data for Internet service activities is communicated through a WWAN modem connection to the at least one WWAN (as taught by Rao and Oestvall). SAMSUNG-1005, [0102], [0179]-[0180], [0182]-[0184], [0188]-[0189], [0191]-[0195], [0125], [0207]; SAMSUNG-1006, [0004].

[1f]-[1g] wherein the access is selectively blocked based on a determination that the first end-user application is running in a background state, and wherein the access is selectively allowed based on a determination that the first end-user application is running as a foreground application.

111. As described in [1e], Rao’s device can ***selectively block and allow access*** based on the policies 520. SAMSUNG-1005, [0191], [0179]-[0180], [0182], [0184], [0189]-[0199], [0207], [0102]. Further, the policies 520 include determining “whether an application is running in the foreground or the background of the client 105.” SAMSUNG-1005, [0182], [0184]-[0185], [0188]-[0189], [0193]-[0194]. Accordingly, a POSITA would have understood and found obvious that, in Rao, ***the access is selectively blocked or allowed based on***

determining whether the application is running in a background or foreground state because, as described in [1e], Rao's device determines whether a network packet generated by an application is allowed to be transmitted to a network or dropped at the device based on the policies including whether the application is running in the foreground or the background of the device.

112. Oestvall supplements Rao's disclosure. Particularly, Oestvall's system determines if an application (e.g., "untrusted" application) is in the background or foreground, and runs the application differently based on the determination. SAMSUNG-1006, [0022]-[0025]. For example, Oestvall's device selectively allows "untrusted application 4" to run if it is in the foreground, and, if it is in the background, "prevent[s] background untrusted applications from 'polling' for data over a wireless network." SAMSUNG-1006, [0024]. Therefore, in the Rao-Oestvall combination, Oestvall would have modified Rao's device to selectively *allow the access* by an application (e.g., "untrusted application" as taught in Oestvall) to Rao's network interface (*WWAN modem*), or *block the access, based on a determination whether the application is running in the background or foreground*, as taught in Oestvall.

2. Claim 2

[2] The wireless end-user device of claim 1, wherein the one or more processors are configured to determine that the first end-user application is running in a background state when a user of the device is not directly interacting with that application or perceiving any benefit from that application.

113. As discussed for [1d] and [1f], the Rao-Oestvall device would have incorporated functionality to determine whether an application is presently running in the background. Because Rao’s policies “define prioritization based on whether an application is running in the foreground or the background of the client 105[,]” Rao’s disclosure suggests existence of the capability to detect when an application is not in the foreground. SAMSUNG-1005, [0182], [0188], [0189]. Moreover, because Rao attributes an application “in the foreground” as one that is “currently in active use by the user,” a POSITA would have recognized that an application in the background is one that is not currently in active use by the user (“*when a user of the device is not directly interacting with that application or perceiving any benefit from that application*”). SAMSUNG-1005, [0003].

114. Oestvall offers similar disclosure regarding regulating application operation based on whether an application is running in the foreground or the background. SAMSUNG-1006, [0021]-[0023]. Further, a POSITA would have found obvious that differentiated use of “foreground” and “background” in Rao and Oestvall indicates examples of applications in the background are those where the user is not presently interacting with the application through a user interface. Further, because of Rao-Oestvall’s repeated differentiated treatment of foreground and background applications, a POSITA would have readily understood and found obvious that Rao’s device determines which state an application is running (e.g.,

determine that the first end-user application is running in a background state) to provide an intended treatment for that application. *Id.*

115. Indeed, techniques for adapting the prioritization for an application or otherwise impacts its operation based on the application's direct user interaction were well-known by the Critical Date. For example, Singh (SAMSUNG-1013) teaches that "when a user interacts with a window, the window becomes the highest priority window." SAMSUNG-1013, 9:33-35. A POSITA would have understood and found obvious that, in response to user interaction, a processor makes an application's window the highest priority (as described by Singh), and, since that application's window is displayed with highest priority, is therefore classifying the application as high priority according to the user interaction. *Id.* Here again, the application with the highest priority is the one with focus, which is what the user is interacting with. Because it is the application the user is paying immediate attention to, it is natural and appropriate for it to have priority over others.

116. As another example, Freund (SAMSUNG-1010) teaches "monitoring of time spent by an employee for 'actively' interacting with the Internet," and notes that "[a]ctive use occurs when a user directly interacts with an Internet application (e.g., Web browser) while that application accesses the Internet." SAMSUNG-1010, 10:16-24. A POSITA would have known that directly

interacting with a Web browser requires the Web browser to be in the UI foreground because user interfaces must be in the foreground to receive input. Freund further explains that “[a] given application itself can be examined for determining whether it is ‘active’ by determining whether the application receives ‘focus’ and/or receives user input (e.g., mouse clicks or keystrokes).” SAMSUNG-1010, 10:40-44. A POSITA would have known the mouse clicks and keystrokes are instances of direct interaction with an application. Freund differentiates such mouse or keyboard use from “background use which occurs when an application or process executing in the background (i.e., does not have “focus”) accesses the Internet, such as a mail client which intermittently polls an Internet-based mail server.” *Id.*, 10:20:24. In this way, Freund teaches classifying whether an application is executing in the background or foreground. *Id.* Freund teaches classifying that the first end-user application is interacting with the user in the user interface foreground when the user of the device is directly interacting with that application. *Id.*, 10:40-44.

3. Claim 3

[3] The wireless end-user device of claim 1, further comprising a user interface to provide a user of the device with information regarding why the first differential traffic control policy is applied to the first end-user application.

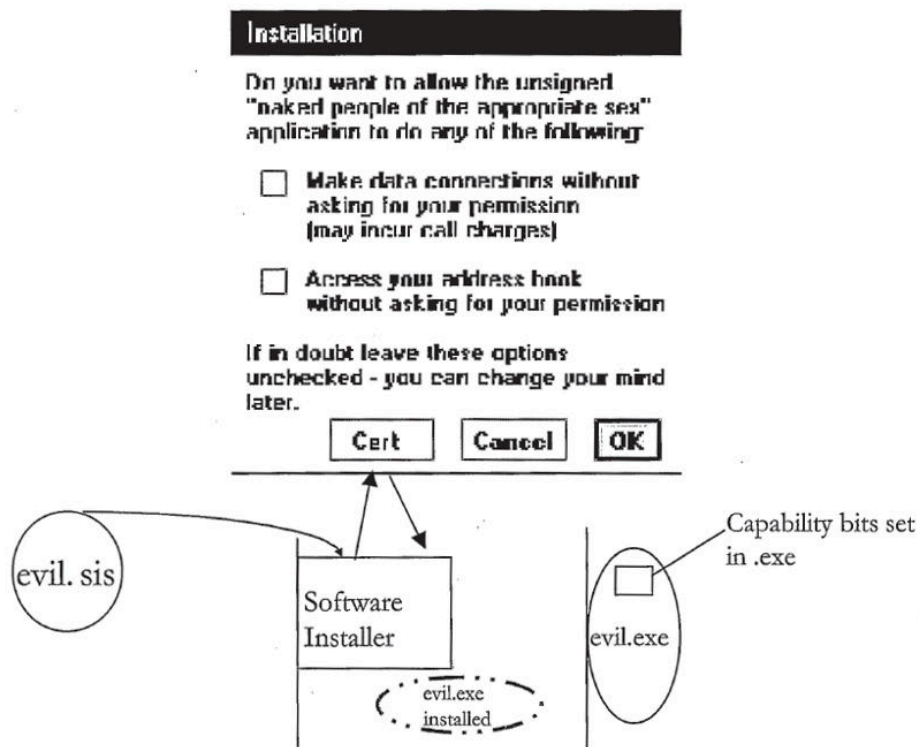
117. The Rao-Oestvall device includes a ***user interface***. Rao describes “[t]he policies 520 may be configurable by a user by any suitable means and/or

mechanism. For example, the agent 326 may provide a configuration mechanism such as *a user interface*, graphical or otherwise, design and constructed for configuring or specifying the policies 520.” SAMSUNG-1005, [0183].

118. Rao-Oestvall would have incorporated functionality to output a user interface relating to various aspects of policies used for prioritization (*“user interface to provide a user of the device with information regarding why the first differential traffic control policy is applied to the first end-user application”*).

Rao’s “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]. Based on this disclosure, POSITA would have found it obvious to configure the agent 326 in the Rao-Oestvall-Montemurro device to similarly provide a user interface to provide information regarding various aspects of applying of policies for prioritization, which would include information regarding why the differential traffic control policy is applied to the particular application. For example, in the case of normal socket communications, the connect() call would fail and return an error code indicating that network communications to the addressed endpoint would be unavailable. In addition, the failure of the connect call will be accompanied with the error code indicating *why* the connection failed, i.e., in the instance where an applied policy would indicate accessing the network was blocked. SAMSUNG-1034, 258-341.

119. Moreover, Oestvall incorporates by reference Dive-Reclus, which teaches blocking an “unsigned” application and provides an interface requesting a user to confirm whether the application should be blocked. SAMSUNG-1026, 19:17-25, Figure 2. As shown in Figure 2 (below), a user interface provides a user with information relating to whether an unsigned application should be granted network access without permission by the user.

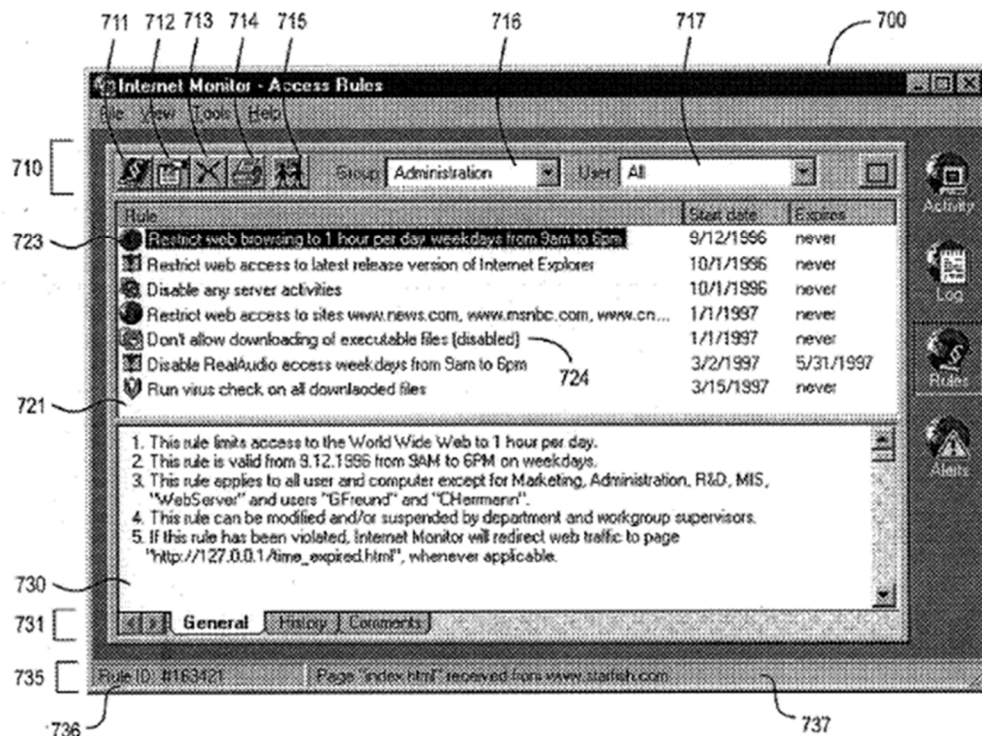


SAMSUNG-1026, Figure 2

120. Notably, user interfaces for providing information regarding policy evaluation were well-known by the Critical Date. SAMSUNG-1010, Figure 7A, 24:16-20, 25:1-13; SAMSUNG-1007, [0030]; *see also*, SAMSUNG-1009, [0116] (“The connection manager 260 is also able to report to the user why it has not used

a particular connection at a given time and indicate that the connection does work if activated.”).

121. For example, Freund (SAMSUNG-1010) includes Figure 7A illustrating an example user interface:



SAMSUNG-1010, Figure 7A

122. Freund further states, “FIGS. 7A-K illustrate a preferred user interface or ‘wizard’ dialogs for configuring rules, and “in Figure 7A, a preferred interface 700 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-1010, 24:16-20. Freund further teaches that the policies (rules) can be

associated with applications using the “wizard dialog 740 [that] asks the user what kind or type of new rule should be created.” *Id.*, 25:1-3, FIGS. 7A-K. Freund further teaches that “any given rule is a combination of access rights granted on the basis of available applications, permitted time limits, permitted user activities, permitted protocols, and the like.” *Id.*, 25:3-6. “[T]he user can select type 742 for limiting what applications (including individual applications) can do on the Internet.” *Id.*, 25:10-13. A POSITA would have recognized such access rights are examples of features enabled through the types of policy evaluation described in Rao.

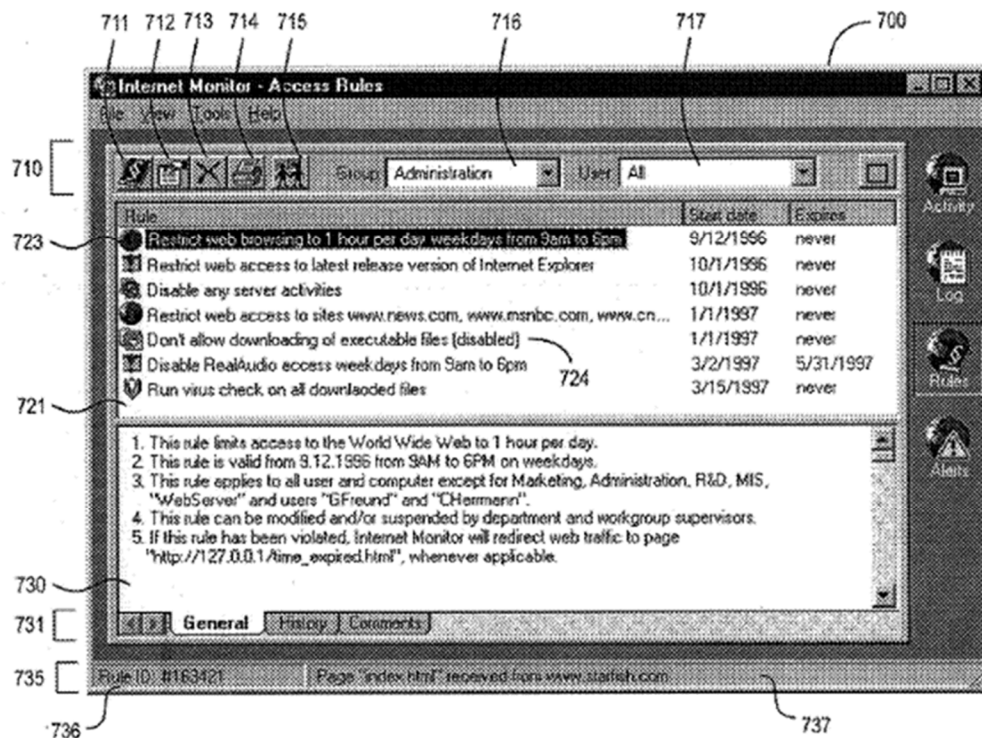
4. Claim 4

[4] The wireless end-user device of claim 1, further comprising a user interface to inform a user of the device when there are options to set, control, override, or modify service usage controls that affect the first differential traffic control policy.

123. As discussed for [3], the Rao-Oestvall device would have incorporated the functionality to output a user interface relating to policies used for prioritization, including options for setting how policies are used for prioritization (“***options to set, control override, or modify service usage controls***”). Rao’s “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]. Based on this disclosure, a POSITA would have found it obvious to configure agent 326 in the Rao-Oestvall device to

similarly provide a user interface for “configuring or specifying” policies for prioritization. A POSITA would have also found obvious that the configuration or specification of policies represent “*service usage controls*” because they can be customized and/or modified to affect the application of policies (“*affect the first differential traffic control policy*”).

124. Indeed, user interfaces for configuring the types of policies described in Rao were well-known before the Critical Date. For example, Freund (SAMSUNG-1010) includes Figure 7A illustrating an example user interface:

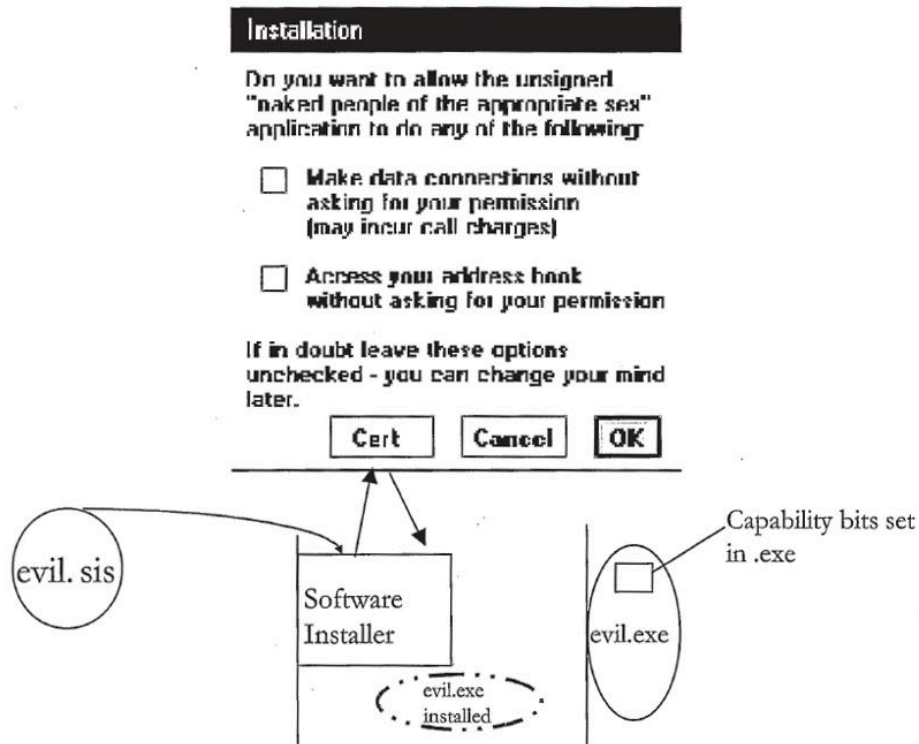


SAMSUNG-1010, Figure 7A

125. Freund further states, “FIGS. 7A-K illustrate a preferred user interface or ‘wizard’ dialogs for configuring rules, and “in FIG. 7A, a preferred interface 700 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-1010, 24:16-20. Freund further teaches that the policies (rules) can be associated with applications using the “wizard dialog 740 [that] asks the user what kind or type of new rule should be created.” *Id.*, 25:1-3, FIGS. 7A-K. Freund further teaches that “any given rule is a combination of access rights granted on the basis of available applications, permitted time limits, permitted user activities, permitted protocols, and the like.” *Id.*, 25:3-6. “[T]he user can select type 742 for limiting what applications (including individual applications) can do on the Internet.” *Id.*, 25:10-13. A POSITA would have recognized such access rights are examples of features enabled through the types of policy evaluation described in Rao.

126. As another example, as noted above, Oestvall incorporates by reference Dive-Reclus, which teaches blocking an “unsigned” and provides an interface requesting a user to confirmation whether the application should be blocked. SAMSUNG-1026, 19:17-25, Figures 2. As shown in Figure 2 (below), a user interface provides a user with information relating to whether an unsigned application should be granted network access without permission by the user.



SAMSUNG-1026, Figure 2

5. Claim 9

[9] The wireless end-user device of claim 1, further comprising a network stack interface integrated with the API.

127. As discussed for [1e], in the Rao-Oestvall combination, an improved agent would have leveraged several types of APIs (including the recited “**API**”) in regulating applications. SAMSUNG-1005, [0110], [0166], [0190], [0205]. Rao’s agent 326 is part of a “network stack” (“**networking stack**”) with “network layers,” including “applications 338a-338n,” “gateway 340,” “peer computing device,” and “remote access client 120.” *Id.*, [0185]. For example, “stacks 310a and 310b” “represent network stacks of computing devices 102a-120b or gateway 340, such

as any of the computing devices 102 and the gateway 340 illustrated in FIGS. 1A-1C, 2A, or 5A.” *Id.*, [0196]. Through these disclosures, a POSITA would have understood and found obvious that the improved agent in Rao-Oestvall (an element of Rao’s Figure 5A environment) is part of the network stacks, as described in Rao (“***network stack interface***”). Further, Rao’s agent 326 is configured to communicate via an API, and the improved agent would leverage one or more of the APIs described in Rao. A POSITA would have understood and found obvious that a network stack including the agent 326 is “***integrated with***” the API. SAMSUNG-1005, [0106], [0166], [0190], [0203].

128. For example, in Rao, “[an] application hooking is implemented via an application programming interface (API),” so that “the hooking of network packets occurs at the network layer of the network stack 310a-310n.” SAMSUNG-1005, [0166]. Rao also discusses a network architecture of a “network stack.” *Id.*, [0100]. In Rao, the “network stack” includes (1) one or more network layers, such as any networks layers of the Open Systems Interconnection (OSI) communications model as those skilled in the art will recognize and appreciate,” (2) “one or more protocols, such as the TCP/IP protocol over Ethernet or a wireless protocol, such as IEEE 802.11, as those skilled in the art will recognize and appreciate,” and (3) “one or more network drivers supporting the one or more layers, such as a TCP driver or a network layer driver.” SAMSUNG-1005, [0100]. The network drives

“may be included as part of the operating system of the computing device 102 or as part of any network interface cards or other network access components of the computing device 102,” and “may be customized, modified or adapted to provide a custom or modified portion of the network stack 310 in support of any of the techniques of the present invention described herein.” *Id.* From these disclosures, a POSITA would have understood and found obvious that Rao-Oestvall-Montemurro’s device includes a “***network stack interface integrated with the API.***”

129. Indeed, network configurations similar to those described in Rao in which an API is “***integrated with***” a networking stack were conventional by the Critical Date. For example, “Portable Operating System Interface” (POSIX) is a family of standards specified by the IEEE to maintain compatibility between operating systems which was implemented in all operating commercial systems at the critical date, e.g., implemented within the UNIX, Microsoft Windows, and Apple OSX operating systems. POSIX defines the application programming interface (API), along with command line shells and utility interfaces, for software compatibility with variants of Unix and other operating systems. SAMSUNG-1021, 104. A POSITA would have understood that a network stack is implemented within the kernel and the stacks interface for making connections and sending and receiving data is made available through systems calls (e.g., connect, send, receive

socket calls). System calls are the APIs by which applications access operating system functions. Hence, system calls represent a network stack interface integrated with an API. *Id.*, 69, 104.

6. Claim 10

[10] The wireless end-user device of claim 1, further comprising a networking stack, wherein the one or more processors are further configured to, at an application service interface layer, identify application traffic flows prior to the flows entering the networking stack.

130. As described for [9], the Rao-Oestvall device would have been configured to operate within one of Rao's network stack ("***networking stack***"). SAMSUNG-1005, [0185], [0190], [0196], Figure 3A. The network stacks include at least an "application layer" ("***application service interface layer***") that, for example, allows applications 338a-338n to establish "an application level session." SAMSUNG-1005, [0203]; *see also id.*, [0100], [0133], [0198].

131. A POSITA would have understood and found obvious that packet interception, as provided by Rao-Oestvall, involves identifying the traffic of data generated by applications ("***identify[ing] application traffic flows***") because a processor identifies a packet in the process of determining that the identified packet should be intercepted. Rao describes several examples of packet intercepting techniques, each of which a POSITA would have understood and found obvious involves identifying packets (examples of application traffic flows). *See, e.g.*, SAMSUNG-1005, [0110], [0111], [0137], [0143], [0158].

132. A POSITA would have also found obvious that the Rao-Oestvall device is configured to “*identify application traffic flows prior to flows entering the network stack*” through Rao’s disclosure of a filter process 322 intercepting a network packet “before [the packet] reaches the network stack 310a-310b.” SAMSUNG-1005, [0166]. Further, by the Critical Date, a POSITA would have understood and found obvious that, based on the architectures disclosed in Rao (e.g., Figures 3A, 6A), packet interception (and packet identification) occurs at the “application layer” (“*an application service interface layer*”), which sits at a general network layer architecture.

7. *Claim 13*

[13] The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the first differential traffic control policy based on a device usage state.

133. As described in §XI.A, a POSITA would have configured Rao-Oestvall to apply policies based on monitoring a state and classification of an application, such as an application’s present interaction state (foreground, background). A POSITA would have understood and found obvious that the present interaction state represents an example of “*device usage state*” as it indicates whether the application is currently made available for display on a mobile device, and therefore, available for active use by a user. A POSITA would have known that device usage state can include which applications are executing,

including whether each application is executing in the foreground or background.

A POSITA would have known that systems routinely monitored which application were running.

134. For example, in Rao, an application is not in the background if it is “currently in active use by the user.” SAMSUNG-1005, [0003]. A POSITA would have recognized that the Rao device performs ongoing monitoring of which applications are running, and which are running in the foreground and background, so it can dynamically determine whether to apply policies. SAMSUNG-1005, [0182], [0188]. Rao teaches that “the policies 520 define prioritization based on whether an application is running in the foreground or the background of the client 105.” SAMSUNG-1005, [0182]. Rao additionally teaches “the remote access client 120 may have one or more policies 520 for specifying client-side prioritization of network communications related to applications 338a-338n running on application” and “may determine whether the application 338a-338n associated with the network packet is running in the foreground or the background of the client 105.” SAMSUNG-1005, [0182], [0188]. A POSITA would have recognized that the Rao device performs ongoing monitoring of which applications are running, and which are running in the foreground and background, so it can dynamically determine whether to apply policies. For example, “the remote access client 120 may determine whether the application 338a–338n associated with the

network packet is running in the foreground or the background of the client 105.”

Here, detecting (and reacting to the detection by applying policy) is necessarily a dynamic operation. Note that the enforcement of policies using ongoing monitoring was a common practice in 2009 (and before). For example, it was common for operating systems to recover disk space by removing unused or unimportant files when it determined disk space was running low.

135. Rao also includes as examples other device usage states relating to the network such as congestion state. SAMSUNG-1005, [0195]. For example, Rao explains that the device performs ongoing monitoring of the device state, e.g., “the remote access client 120 may receive an indication of network congestion, such as receiving a window size of zero for a TCP connection related to an application 338a-338n,” “the remote access client 120 may recognize a high number of retransmits to a particular destination,” and “the client 105 controls and manages the prioritization of network communications of the client 105 on an application 338 a-338 n basis and in accordance with any policies 520 for the client 105 and in further view of any network statistics and other factors occurring on the network. SAMSUNG-1005, [0195].

136. Likewise, in Oestvall, an untrusted application is deemed to be in the background if “the display shows a screen saver or is actually turned off.” SAMSUNG-1006, [0024]. Oestvall also describes preventing an untrusted

application from “being given any services or consuming any resources” based on whether the application is “in the background or foreground on display.” *Id.*, [0023].

137. Based on these disclosures, Rao-Oestvall would have been configured to adjust policy evaluation relating to application-related prioritization (“*dynamically change the application of the first differential traffic control policy*”) based on the application’s present interaction state (“*device usage state*”).

8. Claim 14

[14] The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the first differential traffic control policy based on monitoring of user interaction with the device.

138. As described in §XI.A, a POSITA would have configured Rao-Oestvall to apply policies based on monitoring a state and classification of an application, such as an application’s present interaction state (foreground, background). A POSITA would have understood and found obvious that the present interaction state represents an example of “*user interaction with the device*” as it indicates whether the application is currently made available for a display on a mobile device, and therefore, available for active use by a user (“*user interaction with the device*”). A POSITA would have known that monitoring user interaction with the device can include monitoring which applications are executing, including whether each application is executing in the foreground or

background. A POSITA would have known that systems routinely monitored which application were running.

139. For example, in Rao, an application is not in the background if it is “currently in active use by the user.” SAMSUNG-1005, [0003]. A POSITA would have recognized that the Rao device performs ongoing monitoring of which applications are running, and which are running in the foreground to permit *user interaction with the device*, so it can dynamically determine whether to apply policies. SAMSUNG-1005, [0182], [0188]. Rao teaches that “the policies 520 define prioritization based on whether an application is running in the foreground or the background of the client 105.” SAMSUNG-1005, [0182]. Rao additionally teaches “the remote access client 120 may have one or more policies 520 for specifying client-side prioritization of network communications related to applications 338a-338n running on application” and “may determine whether the application 338a-338n associated with the network packet is running in the foreground or the background of the client 105.” SAMSUNG-1005, [0182], [0188]. A POSITA would have recognized that the Rao device performs ongoing monitoring of which applications are running, and which are running in the foreground and background, so it can dynamically determine whether to apply policies. For example, “the remote access client 120 may determine whether the application 338a–338n associated with the network packet is running in the

foreground or the background of the client 105.” Here, detecting (and reacting to the detection by applying policy) is necessarily a dynamic operation. Note that the enforcement of policies using ongoing monitoring was a common practice in 2009 (and before). For example, it was common for operating systems to recover disk space by removing unused or important files when it determined disk space was running low.

140. Rao also includes examples of user interaction with the device. SAMSUNG-1005, [0140], [0210], [0133]. Rao contemplates that an application can be “running in the foreground and currently in active use by the user.” SAMSUNG-1005, [0003]. For example, Rao’s device can “initiat[e] any type and/or form of communication session, real-time or otherwise, such as an *interactive user session* that involves multimedia elements such as video, voice, chat, gaming, and virtual reality.” SAMSUNG-1005, [0140]. Rao’s “remote access client 120 may re-authenticate the client and/or user of the client 105 at multiple levels, such as for network access and/or TCP connection, SSL or SSL VPN session, and/or any application level sessions, such as a media interactive user session, for example, a VoIP telephone session.” *Id.*, [0210]; *see also id.*, [0133] (“an Internet Engineering Task Force (IETF) standard protocol for initiating an interactive user session that involves multimedia elements such as video, voice, chat, gaming, and virtual reality”). Therefore, a POSITA would have understood

and found obvious that the processor(s) in the Rao-Oestvall device would ***monitor user interaction with the device*** based at least on whether the user initiates an “interactive user session” such as a VoIP telephone session or a session involving multimedia elements. SAMSUNG-1005, [0133], [0140], [0210]. A POSITA would have understood and found obvious that, based on the monitored user interaction state, the device would ***dynamically change the application of the first differential traffic control policy*** to accommodate the current operation of the device in that particular session (“interactive user session”).

141. Likewise, Oestvall describes a ***foreground*** application as “present[ing] a user interface with which a user can interact” and provides a “scheme” that “knows which application is in foreground and which ones are in background.” SAMSUNG-1006, [0006], [0022].

142. Based on these disclosures, Rao-Oestvall would have been configured to adjust policy evaluation relating to application-related prioritization (***“dynamically change the application of the first differential traffic control policy”***) based on monitoring whether the application is “currently in active use by the user” (as taught by Rao) or “present[ing] a user interface with which a user can interact” (as taught by Oestvall) (***“based on monitoring of user interaction with the device”***).

9. Claim 16

[16] The wireless end-user device of claim 1, wherein the one or more processors are configured to associate the first end-user application with the differential traffic control policy based on an application behavior.

143. As described in §XI.A, a POSITA would have configured Rao-Oestvall to apply policies based on an application's present interaction state (foreground, background). For example, Oestvall describes preventing an untrusted application from "being given any services or consuming any resources" based on whether the application is "in the background or foreground on display." SAMSUNG-1006, [0023]. A POSITA would have understood and found obvious that a present interaction state of an application (foreground, background) represents an example of "***application behavior.***" In addition, a POSITA would have understood that the application's change between its states is an example of the application behavior. Further, an application's present interaction state can indicate whether the application is currently made available for display on a mobile device.

144. The '701 patent's specification would support this because it describes "application behavior" of an application, such as "conference meeting services, video streaming, content update, software update," and "running in the background and continuing to consume potentially." SAMSUNG-1001, 8:15-22.

145. Further, in Oestvall, an untrusted application is deemed to be in the background if "the display shows a screen saver or is actually turned off."

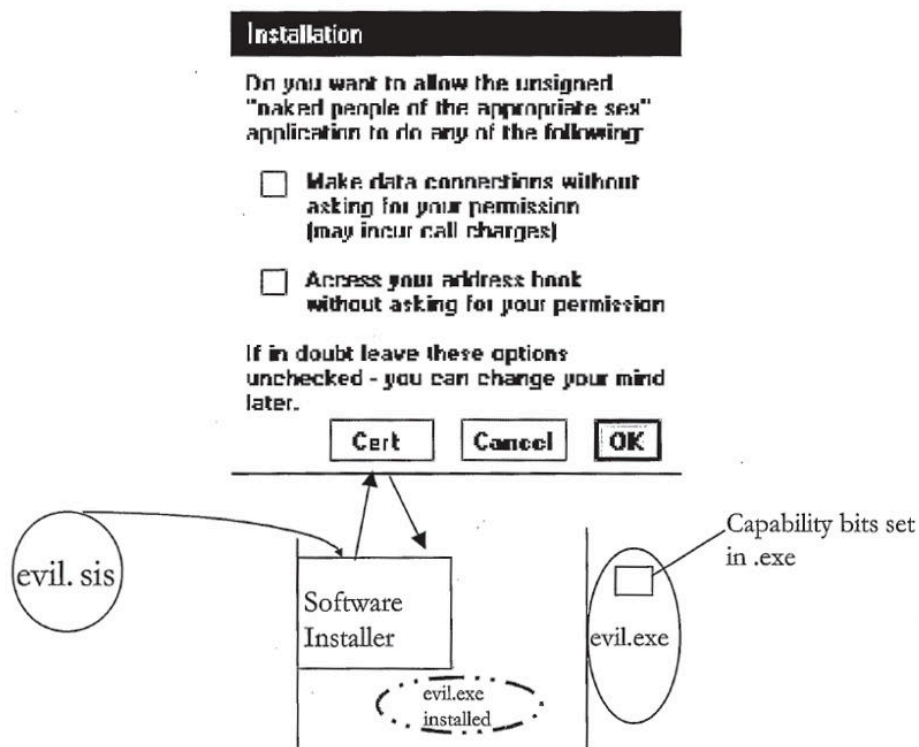
SAMSUNG-1006, [0024]. Likewise, in Rao, an application is in the background if it is “currently in active use by the user.” SAMSUNG-1005, [0003]. Further, the Rao-Oestvall device would have been configured to apply a policy to perform application-related prioritization based on the application’s present interaction state (*“configured to associate the first end-user application with the first differential traffic control policy based on an application behavior”*).

10. Claim 19

[19] The wireless end-user device of claim 1, further comprising an agent to block, modify, remove, or replace user interface messages generated by the first end-user application based on the applied differential traffic control policy.

146. Rao-Oestvall would have included an improved agent 326 (*“agent”*) for performing various management operations for applying policies for packet-related and application-related prioritization (*“based on the applied differential traffic policy”*). SAMSUNG-1005, [0182]; SAMSUNG-1006, [0023]. As discussed above, a POSITA would have configured the improved agent 326 to prevent an untrusted application from running or being given access to a service that consumes resources. SAMSUNG-1005, [0182]; SAMSUNG-1006, [0023]. In Oestvall, this is accomplished by sending a “control signal” that results in application functionality being prevented. SAMSUNG-1006, [0023]. A POSITA would have understood and found obvious that such restriction would have precluded an application from sending user interface messages (e.g., *“block,*

modify, remove, or replace...user interface messages generated by the first end-user application”). For example, as Oestvall describes, the restriction denies “system resources” and “CPU activity” that would have been necessary for an application to generate and output user interface messages. SAMSUNG-1006, [0021]. As another example, Oestvall incorporates by reference Dive-Reclus, which teaches blocking an “unsigned” application and provides an interface over the blocked application asking whether it should be blocked. SAMSUNG-1026, 19:17-25, Figure 2.



SAMSUNG-1026, Figure 2

11. Claim 20

[20] The wireless end-user device of claim 1, wherein the one or more processors configured to control application access are configured to selectively block access by the first end-user application by intercepting open, connect, and/or write requests by the first end-user application to a network stack.

147. As discussed in [1e] and [1f], the processor(s) in Rao-Oestvall's device is configured to control application access and configured to selectively block access by the first end-user application.

148. Further, Rao's device includes a "network stack 310" having "one or more protocols, such as the TCP/IP protocol over Ethernet or a wireless protocol, such as IEEE 802.11," and further having "one or more network drivers supporting the one or more layers, such as a TCP driver or a network layer driver."

SAMSUNG-1005, [0100], Figure 1C. Rao describes that network packets can be communicated "via a secure socket layer." SAMSUNG-1005, [0035].

149. Rao's device "may intercept network packets of one or more applications 338a-338n transparently to the application 338a-338n, the gateway 340, a peer computing device, ***and any of the network layers of a network stack.***" SAMSUNG-1005, [0185]. Such a blocking technique in Rao is beneficial because it allows the prioritization technique to "support any type of application 338a-338n on the client 105." SAMSUNG-1005, [0185].

150. Therefore, a POSITA would have understood and found obvious that the Rao-Oestvall device enables applications to transmit network packets to a remote server on the Internet by transmitting requests to a network stack. Further, a

POSITA would have understood and found obvious that such requests include requests to the network stack to open a socket (e.g., using the “secure socket layer”), connect to the socket, and/or write data to the socket (***“open, connect, and/or write requests by the particular application to a network stack”***). Network communication is implemented nearly universally using the socket interface, and augmented with the Secure Sockets Layer (SSL) protocol. *See, generally*, SAMSUNG, 1035. The sockets layer includes a suite of function calls that implement various network functions, e.g., open() create a network connection context, connect() implements connections over the network, and write() implements sending data over the network. SAMSUNG-1034, 258-341. Further, in view of Rao, a POSITA would have understood or found it obvious to selectively block such requests to the network stack (***“selectively block access by intercepting open, connect, and/or write requests by the first end-user application to a network stack”***), as performing such an operation would allowing Rao’s prioritization technique to “support any type of application” on a device, as taught by Rao. SAMSUNG-1005, [0024]-[0031], [0106], [0166], [0180], [0184], [0185], [0190], [0196], [0203]; *see supra* [9].

12. Claim 25

[25] The wireless end-user device of claim 1, wherein the one or more processors are configured to determine when the first end-user application is running in a background state or as a foreground application based on a state of user interface priority for the application.

151. As described in [1d], the processor(s) in the Rao-Oestvall device are configured to determine when the first end-user application is running in a background state or as a foreground application.

152. Further, as discussed in §XI.A, Rao-Oestvall would have applied policies based on an application's present interaction state (foreground, background). A POSITA would have understood and found obvious that the present interaction state represents an example of a “*state of user interface priority*” as it indicates whether the application is prioritized for display on a mobile device. Further, a POSITA would have understood and found obvious that the priority states of applications relative to each other in a user interface (“*state of user interface priority for the application*”) are associated with, or represent, present interaction states of the applications (foreground, background).

SAMSUNG-1027, 6:31-41 (“‘Foreground application,’ as used herein, may refer to an application that is currently configured to receive certain input, such as input from a keyboard. ... Moreover, a foreground application may be an application whose corresponding window is displayed on top (i.e., in the ‘foreground’) of other application windows.”), 6:42-49 (“background application, as used herein, may refer to an active application that has a corresponding window on the screen 116 but that is not the foreground application. ... Windows associated with background

applications may be physically behind (i.e., in the background) a window associated with the foreground application.”).

153. Oestvall recognizes that, “[i]n conventional multi-tasking computers running several different applications at the same time, an application will issue a software interrupt to the operating system,” and “interrupts from different applications are prioritised and queued by an interrupt handler.” SAMSUNG-1006, [0005]. Oestvall also teaches prioritization based on a “trust” classification of an application, which a POSITA would have understood and found obvious is another example of a “*state of user interface priority*.” *Id.*, [0015].

154. Similarly, Rao describes that policies “define prioritization based on whether an application is running in the foreground or the background of the client 105,” and thus, a POSITA would have found obvious that applying a policy involves a classification based on a user interface priority. SAMSUNG-1005, [0182]. Thus, a POSITA would have found obvious that Rao-Oestvall applies policies to perform application-related prioritization based on the various examples of the application’s present interaction state (e.g., foreground, background), as taught in Rao and Oestvall (“*determine when the first end-user application is running in a background state or as a foreground application*”). For example, an application in the foreground is one that is “currently in active use by the user,” which a POSITA would have understood and found obvious indicates a user

interface priority in that the application is prioritized over other applications that are running in the background. SAMSUNG-1005, [0182].

155. Moreover, the use of states of user interface priority in coordinating application operation was well-known before the Critical Date. For example, Singh (SAMSUNG-1013) describes a “window management function [that] determine[s] a relationship of windows with one another.” SAMSUNG-1013, 9:19-21. Singh teaches that “when a user interacts with a window, the window becomes the highest priority window.” *Id.*, 9:33-35. A POSITA would have known that users interact with foreground windows, and in Singh, users only interact with the highest priority window (because any interaction causes the window to be assigned the highest priority). A POSITA would have understood or found obvious that Singh’s window management function uses a state of user interface priority (e.g., the highest priority, which is defined to be the one the user is interacting with, also known as having interface focus) to classify that the application is interacting with the user in the UI foreground.

156. In addition, the difference between foreground and background states has been well established within the academic literature. For example, in 1995, a publication by Buxton described foreground as “activities which are in the fore of human consciousness”, such as “speaking on the telephone, or typing into a computer,” SAMSUNG-1024, 1. In contrast, background activities are “tasks that

take place in the periphery, ‘behind those in the foreground’.” *Id.* Activities in the “fore of human consciousness” would indicate user interface priority. *Id.* As another example, a publication by Hinckley built on this model in 2005 to further define foreground concerns as “deliberate user activity where the user is attending to the device” and background as “the realm of inattention or split attention,” which makes the user interface priority with regards to foreground actions even more explicit. SAMSUNG-1025, 1.

157. Therefore, a POSITA would have found obvious the use of states of user interface priority for classification in Rao-Oestvall.

XII. GROUND 1B: Rao in view of Oestvall and Montemurro renders obvious claims 5-8, 11, 17, 18, 23, and 24

A. Combination of Rao, Oestvall, and Montemurro

158. As described above, a POSITA would have configured Rao-Oestvall to apply policies to prioritize packet transmission and application functionality to achieve several types of operational efficiencies. SAMSUNG-1005, [0179]-[0195], Figure 5A. In implementing this combination, a POSITA would have recognized opportunities to provide additional efficiencies in scenarios where the Rao-Oestvall device has access to multiple networks. *Id.* This would have motivated a POSITA to seek solutions beyond Rao and Oestvall to achieve such additional efficiencies. *Id.*

159. Given Montemurro’s broad focus to “optimize communications using a policy-based mechanism to configure connections and routes,” a POSITA would have found Montemurro’s teachings to be reasonably pertinent to the policies applied by Rao-Oestvall for prioritization. SAMSUNG-1007, Abstract. Indeed, like Oestvall, Montemurro describes embodiments where its policies are used to “disable or enable an application for a user.” SAMSUNG-1007, [0027]. This would have led a POSITA to consider Montemurro’s broader teachings in Figure 2 relating to “policy-based data routing for multimode operations.” *Id.*, [0024]. Incorporation of such teachings into Rao-Oestvall would have yielded several improvements described in Montemurro, such as the ability to “offer different usage models depending on the mode of wireless operation selected.” *Id.*, [0003]. This configuration would have improved the Rao-Oestvall device by enabling prioritization to further account for several considerations, such as “bandwidth, range, cost, and power consumption.” *Id.* Further, policies applied by Rao-Oestvall-Montemurro would have been “responsive to various factors such as Radio Access Technology (high/low bandwidth), cost, presence, time of day, location, application type and quality of service (QoS) requirements among others to optimize communications,” as described in Montemurro. *Id.*, [0011].

160. A POSITA would have had a reasonable expectation of success in combining Rao-Oestvall and Montemurro, as discussed above. For example, Rao

provides non-limiting disclosure of the types of networks to which device 102 may connect to using network interface 118. SAMSUNG-1005, [0095], [0125].

Montemurro's use of routing tables would have thereby advanced Rao's motivation to enable multiple types of network connectivity. SAMSUNG-1007, [0024]. Additionally, both Rao and Montemurro expressly teach use of policies to regulate device functions (e.g., prioritizing network traffic in Rao, connecting to a suitable available network in Montemurro). SAMSUNG-1005, [0182];

SAMSUNG-1007, [0011]. A POSITA would have understood these disclosures to both be generally focused on improving network performance on a mobile device, making the combination of their teachings a natural option to achieve the advantages discussed above. Additionally, configuring Rao-Oestvall to leverage Montemurro's teachings would have required only routine programming knowledge well within the skill of a POSITA prior to the earliest effective filing date. The change would have involved (1) combining prior art elements according to known methods to yield predictable results; and (2) use of a known technique to improve similar devices (methods, or products) in the same way. For example, Rao-Oestvall-Montemurro would have provided a device that uses a set of policies to generally regulate applications, including policies used to prioritize network packet transmissions (as described in Rao) and policies used to select the most suitable network connection (as described in Montemurro).

B. Analysis of the Claims

1. Claim 5

[5] The wireless end-user device of claim 1, wherein the first differential traffic control policy is part of a multimode profile having different policies for different networks.

161. Rao-Oestvall-Montemurro would have incorporated the functionality described in Montemurro to apply a rules engine to coordinate connectivity for applications. SAMSUNG-1007, [0027].

162. Notably, in certain scenarios, a rules engine would have applied an instance of a routing table (“***multimode profile***”) with information for multiple networks available for selection. SAMSUNG-1007, [0030]. For example, “if both the WLAN and WWAN radios...of [a] device [] are connected to their respective networks 104 and 106, there will be a route associated with each network 104 and 106...” *Id.* The rules engine “executes” the instance of the routing table “to ensure that data goes out to the most appropriate network” , as well as “determine which interface would be best used to service a particular application.” *Id.*, [0035].

163. Further, in scenarios where multiple networks are available for selection, a POSITA would have understood and found obvious that the information specified by the instance of the routing table includes policies for each available network. In Montemurro, policies are “responsive to various factors such as Radio Access Technology, high/low bandwidth, cost, presence, time of day,

location, application type and quality of service (QoS) requirements.”

SAMSUNG-1007, [0011], [0024], [0027], [0029]. Thus, a POSITA would have understood and found obvious that an instance of the routing table with information for multiple network available for selection includes “*different policies for different networks.*” SAMSUNG-1007, [0011], [0024], [0027], [0029].

164. Moreover, the use of different policies for enabling capabilities for different networks (e.g., phone network, local network) was conventional by the Critical Date. SAMSUNG-1026, 12:13-13:9. For example, Dive-Reclus (SAMSUNG-1026) includes a table showing different permission decisions for applications submitting API calls to request network access.

Installed	PhoneNetwork	ReadUserData	WriteUserData	LocalNetwork	Certificate
Good.exe	Not granted	Granted	Not granted	Granted	Checked OK – click to view root signing cert
Bad.exe	Not granted	Not granted	Not granted	Not granted	Unsigned

SAMSUNG-1026, 20

2. Claim 6

[6] The wireless end-user device of claim 5, wherein the one or more processors are further configured to select a traffic control policy from the

multimode profile based at least in part on the type of network connection currently in use by the device.

165. As described for [5], a POSITA would have also understood and found obvious that, in some scenarios, information specified by an instance of the routing table (“***multimode profile***”) includes “***different policies for different networks.***” SAMSUNG-1007, [0011], [0024], [0027], [0029]. The rules engine “executes” the routing table “to ensure that data goes out to the most appropriate network” and also to “determine which interface would be best used to service a particular application.” SAMSUNG-1007, [0035]. For example, “if both the WLAN and WWAN radios...of [a] device [] ***are connected*** to their respective networks 104 and 106, there will be a route associated with each network 104 and 106...” *Id.*, [0030]. Thus, in this example, a POSITA would have understood and found obvious that the rules engine within Rao-Oestvall-Montemurro would have executed the instance of the routing table (“***select a traffic control policy from the multimode profile***”) based on the type of network connections of wireless radios (WLAN, WWAN), and thus, when a routing option is selected from the routing table instance, the selection (“***select a traffic control policy***”) is based on the types of current network connections of the device (“***type of network connection currently in use by the device***”). In addition, Montemurro describes performance criteria based on the type of network connection currently used by the device, and if these criteria are not maintained, “alternatives for the present access technology

or different instance of the same type of access technology (e.g., a different WLAN or subnetwork via an alternative access point, PPP connection or GSM APN) can be evaluated.” *Id.*, [0044].

166. Additionally, as noted above, Oestvall incorporates by reference Dive-Reclus, which teaches permission decisions regulating network access by third-party applications that use API calls. SAMSUNG-1006, [0020]; SAMSUNG-1026, 16:23-17:28, 20:1-12 (table).

167. Moreover, Montemurro describes a “time-based rule and/or a location-based rule” that determines where the device is located at a given time and which network is available in that location at the time and then changes the traffic route depending on the determination. SAMSUNG-1007, [0039] (“However once work hours end, a rule could be triggered, for example, by a calendar application, to change the default route so that traffic is routed across the local LAN rather than the corporate network. If the user is at work, there could be another rule to disable this default route change.”). As such, Montemurro’s policies are based on the *network currently* available or *currently in use by the device*.

3. Claim 7

[7] The wireless end-user device of claim 6, wherein the one or more processors are further configured to, when the type of network connection is at least one type of WLAN connection, select a traffic control policy from the multimode profile based at least in part on a type of network connection from the WLAN to the Internet.

168. *See supra* [6]. Montemurro offers an example in which “if both the WLAN and WWAN radios...of [a] device [] are connected to their respective networks 104 and 106, there will be a route associated with each network 104 and 106...” SAMSUNG-1007, [0030]. Thus, in this example, a POSITA would have understood and found obvious that the rules engine within Rao-Oestvall-Montemurro would have executed the routing table (“*select a traffic control policy from the multimode profile*”) when the device is connected to a WLAN connection (“*when the type of network connection is at least one type of WLAN connection*”). Additionally, as described above, Montemurro describes performance criteria based on the type of network connection currently used by the device and specifically considers when the device is connected to a WLAN connection. If the performance criteria are not maintained, “alternatives for the present access technology or different instance of the same type of access technology (e.g., *a different WLAN or subnetwork via an alternative access point*, PPP connection or GSM APN) can be evaluated.” *Id.*, [0044].

169. Montemurro also describes that “once work hours end, a rule could be triggered, for example, by a calendar application, to change the default route so that traffic is routed across the local LAN rather than the corporate network” and that “[i]f the user is at work, there could be another rule to disable this default route change.” SAMSUNG-1007, [0039]. From this disclosure, a POSITA would have

understood and found obvious that the “local LAN” is a type of “***network connection from the WLAN to the Internet.***” See also SAMSUNG-1009, [0032] (“Each of the communication networks 120 [including WLAN] may interface directly or indirectly with a public network 170 (e.g., the Internet).”).

170. For example, Montemurro describes that its device “is capable of wireless communication in accordance with WLAN” and “communicate[s] 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-1007, [0013]. A POSITA would have understood and found obvious that there would be several types of network connections implemented by various network components (e.g., base station, various WLAN components, access points, etc.) between the WLAN and the Internet, and that Rao-Oestvall-Montemurro’s device would consider a ***type*** of such network connection in ***selecting a traffic control policy from the multimode profile***, as discussed above.

4. Claim 8

[8a] The wireless end-user device of claim 1, wherein the one or more processors are further configured to determine whether a second end-user application is running in a background state or as a foreground application, and

171. See *supra* [1d]. The analysis for the “first end-user application” applies similarly for the “second end-user application.”

172. Notably, none of Rao, Oestvall, and Montemurro indicates that its respective techniques are limited to any specific application (or any specific type of application). *See, generally*, SAMSUNG-1005, SAMSUNG-1006, SAMSUNG-1007. Additionally, Rao teaches that policies “may be specified hierarchically to account for multiple applications 338a-338n and/or multiple protocols that may be executed on the client 105 at any point.” SAMSUNG-1005, [0182]. Thus, because Rao-Oestvall-Montemurro would have been configured to apply prioritization to multiple applications, a POSITA would have found obvious that the combination renders elements of claim 8 obvious in the same manner as explained above for the “*first end-user application*” based on the disclosures identified in the corresponding claim 1 limitations.

[8b] control application access for Internet service activities by the second end-user application similar to the control of application access for the first end-user application, except the control of application access for Internet service activities by the second end-user application is based on a second differential traffic control policy that can be set different from the first differential traffic control policy.

173. *See supra* [1e] as to “*control application access for Internet service activities by the second end-user application similar to the control of application access for the first end-user application.*” The analysis for the “first end-user application” applies similarly for the “second end-user application.”

174. *See supra* [5] as to “*except the control of application access for Internet service activities by the second end-user application is based on a*

second differential traffic control policy that can be set different from the first differential traffic control policy.” As discussed in [5], Montemurro describes multiple policies for different applications—“first end-user application” and “second end-user application.”

5. Claim 11

[11] The wireless end-user device of claim 1, wherein the one or more processors control of application access based on a first differential traffic control policy is applied to one of but not both of a connection to a roaming WWAN network and a connection to a home WWAN network.

175. As described for [5], in Rao-Oestvall-Montemurro, a rules engine, in certain scenarios, applies an instance of a routing table (“*multimode profile*”) with information for multiple networks available for selection. SAMSUNG-1007, [0011], [0024], [0027], [0029]. For example, “if both the WLAN and WWAN radios...are connected to their respective networks 104 and 106, there will be a route associated with each network 104 and 106,” as shown in the table below. SAMSUNG-1007, [0030].

Source IP	Destination IP	Device Interface (208)
192.168.1.20	0.0.0.0	WLAN (208A)
67.69.20.142	0.0.0.0	WWAN (208C)

176. In Montemurro, a device “has mobile IP capabilities” to “permit the device to attach to the Internet (IP network) via a home and one or more foreign

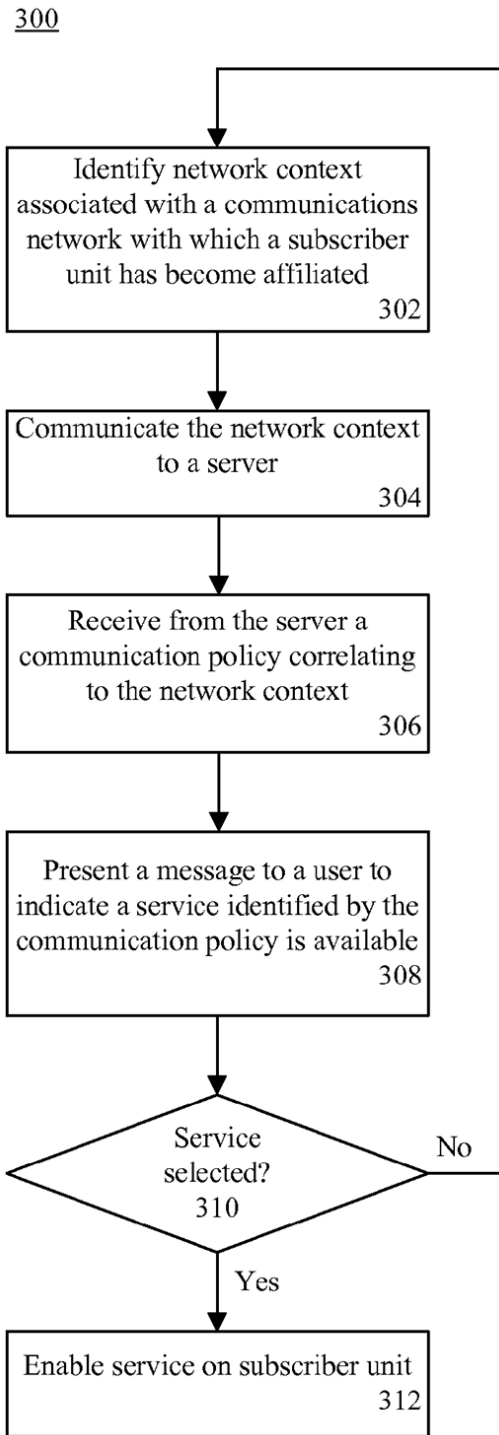
networks.” SAMSUNG-1007, [0037]. Since Montemurro contemplates devices with capabilities to connect to both home and foreign networks, a POSITA would have found obvious that the routing table may be similarly configured to provide routing options for various types of networks, including a “*home WWAN*” and “*roaming WWAN*.” *Id.*

177. Moreover, since Montemurro’s device is operable on various networks (including WWAN), a POSITA would have understood or found it obvious that the routing table is similarly configured to provide routing options for WWAN for a home network (“*home WWAN*”) and WWAN for roaming to a foreign network (“*roaming WWAN*”). SAMSUNG-1007, [0030], [0037]. Indeed, by the Critical Date, WWAN was well-known for being implemented for different settings, such as a home WWAN and a roaming WWAN. Montemurro further offers non-limiting disclosure of WWAN, e.g., “cellular technologies like GSM/GPRS EDGE, UTMS, HSPA, CDMA, WCDMA, etc.,” which a POSITA would have understood and found obvious includes roaming WWAN networks and home WWAN networks. A POSITA would have perceived network selection in Rao-Oestvall-Montemurro to provide connectivity to one of several available WWAN networks (“*connection to a roaming WWAN network and a connection to a home WWAN network*”) to represent an obvious configuration as this reduces costs and complexity, consistent with Montemurro. SAMSUNG-1007, [0029]-

[0038]. For example, it was well-known and obvious by the Critical Date to use and make selective connection to a home network (e.g., “*home WWAN*”) and a roaming network (e.g., “*roaming WWAN*”). SAMSUNG-1022, [0003] (“A wireless device is typically associated with a home network operator and, when available, uses the *home network* for wireless communications. The home network operator may have partner network operators that provide roaming service to the wireless device. That is, the roaming network operators permit the wireless device to connect to the home network via the *roaming network* when the wireless device is outside of the device's home network's coverage area. A user may desire certain information (such as cost) as an aid to deciding whether to connect to a roaming network, and/or as an aid to deciding to which roaming network to connect.”), [0004] (“Typically, to establish a data connection with a *home WWAN*, a wireless device needs to have certain information.”).

178. Systems and techniques for enabling policy-based connectivity to roaming and home networks were also conventional by the Critical Date. For example, U.S. Pat. App. No. 2008/0311897 to Segal (SAMSUNG-1023) describes a system that can activate international roaming services using an availability policy. SAMSUNG-1023, Abstract, Figure 3, [0043]. The system also communicates with a subscriber to update network communication services, which

allows a subscriber to roam internationally. *Id.* As shown in Figure 3, a user may select a policy when presented with it such an option:



SAMSUNG-1023, Figure 3

179. In Rao-Oestvall-Montemurro, policies are “responsive to various factors,” including “cost, presence, time of day, location, e.g., geo-based policies, network roaming).” SAMSUNG-1007, Abstract, [0029]. Montemurro also offers non-limiting disclosure of WWAN, including examples of “cellular technologies,” which a POSITA would have understood and found obvious includes roaming WWAN networks and home WWAN networks. SAMSUNG-1007, [0011], [0024], [0027], [0029]. A POSITA would have perceived selection of a policy by the rules engine in Rao-Oestvall-Montemurro to provide connectivity to one of several available WWAN networks while not connecting to another of the WWAN networks (“*apply the first differential policy to one of but not both of a connection to a roaming WWAN network and a connection to a home WWAN network*”) to represent an obvious configuration as this reduces costs and complexity, consistent with Montemurro’s teachings. SAMSUNG-1007, [0029]-[0038].

6. Claim 17

[17] The wireless end-user device of claim 1, wherein the differential traffic control policy defines that applications to which the policy applies can only have WWAN network access events during particular time windows.

180. As discussed for [5], Rao-Oestvall-Montemurro would have incorporated functionality for applying a rules engine to coordinate connectivity for applications by applying a routing table (“*multimode profile*”) specifying

policies for different networks. SAMSUNG-1007, [0011], [0024], [0027], [0029].

In other words, in Rao-Oestvall-Montemurro, a rules engine, in certain scenarios, applies an instance of a routing table with information for multiple networks available for selection. Policies are “responsive to various factors,” including “cost, presence, *time of day*, location, e.g., geo-based policies, network roaming).” *Id.*, Abstract, [0029]. Further, the rules engine “executes” the routing table to “ensure that data goes out to the most appropriate network (via respective network interface)” and “interacts with the connection API’s to determine which interface would be best used to service a particular application.” *Id.*, [0035]. Thus, a POSITA would have understood and found obvious that Rao-Oestvall-Montemurro regulates access to connection events to several networks, including a WWAN network (“*WWAN network access events*”).

181. Further, as noted discussed above, Rao-Oestvall-Montemurro would have regulated network access by applications through use of policies. In Montemurro, “[p]olicies may be responsive to various factors,” including “time of day.” SAMSUNG-1007, Abstract. A POSITA would have understood and found obvious that a policy applied by Rao-Oestvall-Montemurro regulates both the type of network access and the circumstances during which an application can have access to network services such that Rao-Oestvall-Montemurro “*can only have WWAN network access during particular time windows*” (e.g., time windows

during which a policy specifies network connectivity). SAMSUNG-1006, [0023]; SAMSUNG-1007, [0035].

182. Use of policies to limit network access during particular time windows was conventional by the Critical Date. For example, Freund describes “access rules can be qualified by optionally specifying: ... *time of day* when the rule should be applied (for example from 9 am to 5 pm).” SAMSUNG-1010, 10:13-17. A POSITA would have understood and found obvious the “access rules” are examples of policies since they can, e.g., “[d]elay Internet access for non-critical Applications or Protocols” and “[d]isable Internet Access for non-critical or Protocols.” *Id.*, 30:59-67. In Freund, access rules define when access to the Internet is allowed, and therefore represents, an example of a policy that limits Internet access during a particular time window (e.g., between 9 am and 5 pm).

7. Claim 18

[18] The wireless end-user device of claim 1, wherein the one or more processors are further configured to update the first differential traffic control policy based on information received from a network element.

183. As discussed above, policies applied by Rao-Oestvall-Montemurro (including the “*first differential traffic control policy*”) would have been “responsive to various factors such as Radio Access Technology (high/low bandwidth), cost, presence, time of day, location, application type and quality of

service (QoS) requirements among others to optimize communications,” as described in Montemurro. SAMSUNG-1007, [0011].

184. In Montemurro, “network infrastructure” provides support for services provided to a wireless device. SAMSUNG-1007, [0014]. Examples of “network infrastructure” include “a gateway server, a provisioning server, a discovery, and an application repository,” each of which are examples of a “*network element*.” Services provided by the network infrastructure include “Administrative and Management Service dealing with policies, such as those specifying allowed applications for users, services available to applications and more.” SAMSUNG-1007, [0015]-[0016]. Moreover, in Rao, remote access client 120 may “receive an indication of network congestion” and thereby “control[] and manage[] the prioritization of network communications,” which would have adjusted policy evaluation by the device. SAMSUNG-1005, [0195]. Based on these disclosures, a POSITA would have understood and found obvious, as an example of the services provided by Montemurro’s network infrastructure, a server (“*network element*”) provides an update for a service dealing with policies, and accordingly the Rao-Oestvall-Montemurro device would have been configured to update policies relating to application operation (“*update the differential traffic control policy*”) based on the update from the server (“*information received from [the] network element*”). For example, the update may specify a new allowed application, and

Rao-Oestvall-Montemurro would have updated policies to reference a name of the new allowed application and thereby permit regulation of the newly allowed application, consistent with Rao. SAMSUNG-1005, [0182] (“the policies 520 may be specified by the name of the applications 338a-338n and/or the type of application 338a-338n”).

185. Moreover, techniques for adapting policy configurations based on information received from network elements were conventional by the Critical Date. For example, Freund (SAMSUNG-1010) describes a network element in the form of a “supervisor” that “maintains access rules for the client-based filtering and verifies the existence and proper operation of the client-based filter application.” SAMSUNG-1010, Abstract. “The supervisor monitors whether a client has the filter application loaded and *provides the filter application with the rules for the specific user or workstation.*” *Id.*, 5:9-12. In Freund, “Client Monitor sends a login request to the Supervisor,” and in response, “the Supervisor checks if the Client Monitor (computer/user) has any Internet access rights; also, the Supervisor determines the department or workgroup for the Client Monitor, as indicated at step 805.” *Id.*, 28:6-14. Based on these determinations, “the Supervisor filters rules appropriate for the client (i.e., application, Host, and other rules), and transmits them to the Client Monitor, at step 806.” *Id.*, 28:14-16. A POSITA would have recognized that the Supervisor is a network element (a service controller) and

“the network service activity control policy set” is updated based on information received from the Supervisor.

186. Freund also describes the “centralized supervisor application is installed on a computer on the LAN that can be reached from all workstations that need access to the Internet; this is typically (although not necessarily) a server computer.” SAMSUNG-1010, 5:6-9. In this example, Freund’s server represents an example of a network element. This is consistent with the ’578 patent specification, which describes an example of a “network element” as “a service controller or another network element/function).” SAMSUNG-1001, 11:31-46.

8. Claim 23

[23] The wireless end-user device of claim 1, the first differential traffic control policy comprising first and second sub-policies applicable respectively to Internet data service provided using the WWAN modem to connect to a home WWAN and a roaming WWAN, wherein the one or more processors are further configured to apply the first sub-policy when Internet data service is provided through a home WWAN and to apply the second sub-policy when Internet data service is provided through a roaming WWAN.

187. As discussed for [5] and [11], in Rao-Oestvall-Montemurro, a rules engine, in certain scenarios, applies an instance of a routing table (“***multimode profile***”) with information for multiple networks available for selection.

SAMSUNG-1007, [0011], [0024], [0027], [0029]. For example, “if both the WLAN and WWAN radios...are connected to their respective networks 104 and

106, there will be a route associated with each network 104 and 106,” as shown in the table below. SAMSUNG-1007, [0030].

Source IP	Destination IP	Device Interface (208)
192.168.1.20	0.0.0.0	WLAN (208A)
67.69.20.142	0.0.0.0	WWAN (208C)

188. In Montemurro, a device “has mobile IP capabilities” to “permit the device to attach to the Internet (IP network) via a home and one or more foreign networks.” SAMSUNG-1007, [0037]. Montemurro contemplates devices with capabilities to connect to both home and foreign networks. A POSITA would have found obvious that the routing table may be similarly configured to provide routing options for various types of networks, including a “*home WWAN*” and “*roaming WWAN*.” SAMSUNG-1007, [0037].

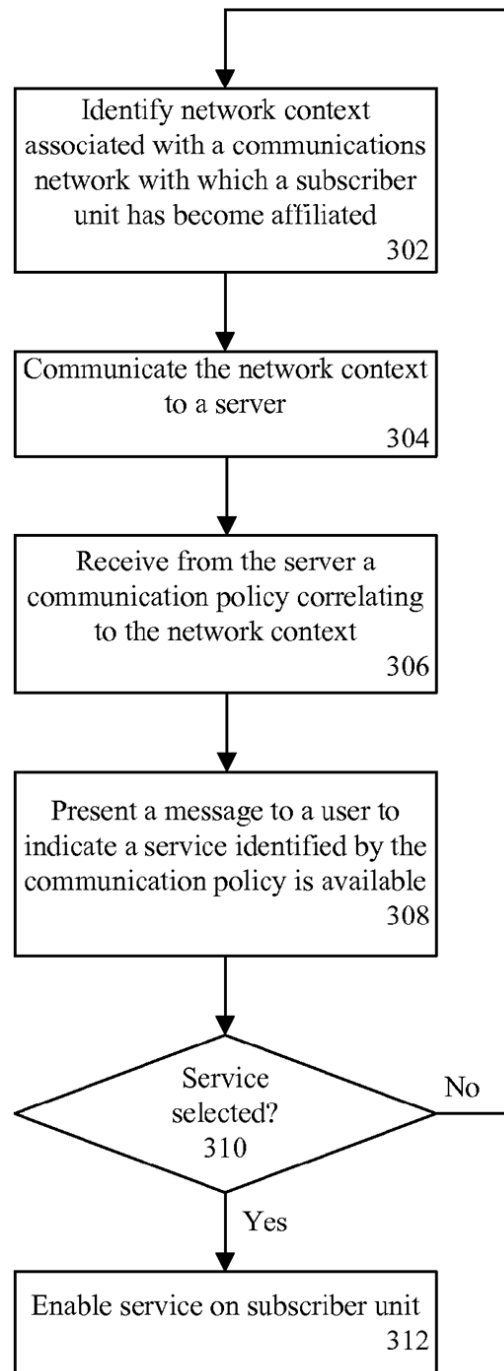
189. Moreover, Montemurro’s device is operable on various networks (including WWAN). A POSITA would have understood and found it obvious that the routing table is similarly configured to provide routing options for WWAN for a home network (“*home WWAN*”) and WWAN for roaming to a foreign network (“*roaming WWAN*”). SAMSUNG-1007, [0030], [0037]. Indeed, by the Critical Date, WWAN was well-known for being implemented for different settings, such as a home WWAN and a roaming WWAN. Montemurro further also offers non-

limiting disclosure of WWAN, e.g., “cellular technologies like GSM/GPRS EDGE, UTMS, HSPA, CDMA, WCDMA, etc.,” which a POSITA would have understood and found obvious includes roaming WWAN networks and home WWAN networks. SAMSUNG-1007, [0029]-[0038]. A POSITA would have perceived network selection in Rao-Oestvall-Montemurro to provide connectivity to one of several available WWAN networks (“*connect to a home WWAN and a roaming WWAN*”) to represent an obvious configuration as this reduces costs and complexity, consistent with Montemurro.

190. For example, it was well-known and obvious by the Critical Date to use and make selective connection to a home network (e.g., “*home WWAN*”) and a roaming network (e.g., “*roaming WWAN*”). For example, U.S. Pat. App. No. 2009/0093247 (“Srinivasan”) describes a system in which “[a] wireless device is typically associated with a home network operator and, when available, uses the home network for wireless communications[,]” where “[the] operator may have partner network operators that provide roaming service to the wireless device.” SAMSUNG-1022, [0003]. In this configuration, “the roaming network operators permit[s] the wireless device to connect to the home network via the roaming network when the wireless device is outside of the device's home network's coverage area.” *Id.* Further, “[a] user may desire certain information (such as cost) as an aid to deciding whether to connect to a roaming network, and/or as an aid to

deciding to which roaming network to connect” and “[i]n many cases, the wireless device may be programmed with the identity of one or more voice roaming partner operators of its home operator so that a partner voice roaming network operator can be located when the wireless device is outside of the home network's coverage. *Id.*

191. Systems and techniques for enabling policy-based connectivity to roaming and home networks were also conventional by the Critical Date. For example, U.S. Pat. App. No. 2008/0311897 to Segal (SAMSUNG-1023) describes a system that can activate international roaming services using an availability policy. SAMSUNG-1023, Abstract, Figure 3, [0043]. The system also communicates with a subscriber to update network communication services, which allows a subscriber to roam internationally. *Id.* As shown in Figure 3, a user may select a policy when presented with it such an option:

300

SAMSUNG-1023, Figure 3

192. Further, in Montemurro, each policy specifies a set of connection factors, such as “Radio Access Technology, high/low bandwidth, cost, presence,

time of day, location, application type and quality of service (QoS) requirements.” SAMSUNG-1007, [0011]. A POSITA would have understood and found obvious that a set of connection factors specified within a policy represents a “*sub-policy*” in that they permit connectivity to an associated network, and thereby enables Montemurro’s “policy-based mechanism to configure connections and routes.” *Id.*, Abstract. Thus, in an instance of the routing table with routing options for a home network and a foreign network, the routing table includes a first set of connection factors for the home network (“*first sub-policy when Internet data service is provided through a home WWAN*”) and a second set of connection factors for the foreign network (“*second sub-policy when Internet data service is provided through a roaming WWAN*”). SAMSUNG-1007, [0011], [0024], [0027], [0029]. Further, in Rao, policies may be “specified hierarchically to account for multiple applications” and/or “multiple protocols that may be executed on [a] client [] at any point,” demonstrating that hierarchical policy structures for adjusting the types of device functionality provided by Rao-Oestvall-Montemurro was conventional by the Critical Date. SAMSUNG-1005, [0182].

9. Claim 24

[24] The wireless end-user device of claim 1, the first differential traffic control policy comprising first, second, and third sub-policies applicable respectively to Internet data service provided using the WWAN modem and three different network types from the network types consisting of 2G, 3G, 4G, home, and roaming.

193. As discussed for [23], a POSITA would have understood and found obvious that a routing table applied by the rules engine of Rao-Oestvall-Montemurro is configured to provide routing options for various types of networks described in Montemurro. As noted above, a POSITA would have understood and found obvious that a set of connection factors specified within a policy represents a “*sub-policy*” in that they permit connectivity to an associated network, and thereby enables Montemurro’s “policy-based mechanism to configure connections and routes.” SAMSUNG-1007, [0011], Abstract. Thus, in an instance of the routing table with routing options for different networks, the routing table includes different sets of connection factors for different networks (“*first, second, and third sub-policies applicable respectively to Internet data service provided using the WWAN modem and three different network types from the network types*”). SAMSUNG-1007, [0011], [0024], [0027], [0029].

194. Montemurro identifies several non-limiting example types of WWAN, including “cellular technologies like GSM/GPRS EDGE, UTMS, HSPA, CDMA, WCDMA, etc.” SAMSUNG-1007, [0003]. It was well-known that GSM and CDMA were used for 2G standards, and WCDMA was used for a 3G standard. Also, LTE (4G) was well known and standardized before the Critical Date, and a POSITA would have considered LTE (4G) as other example cellular technologies. Given this non-limiting disclosure and the types of examples identified, a POSITA

would have understood and found obvious that the routing table is configured to accommodate “*three different network types from the network types consisting of 2G, 3G, 4G, home, and roaming.*” SAMSUNG-1007, [0022], [0029], [0037]; SAMSUNG-1009, [0031]; SAMSUNG-1022, [0003]-[0004]; SAMSUNG-1023, [0043], Figure 3.

XIII. GROUND 1C: Rao in view of Oestvall and Araujo renders obvious claims 12, 15, 21 and 22

A. Combination of Rao, Oestvall, and Araujo

195. A POSITA would have found it obvious to modify Rao-Oestvall to include Araujo’s “request deflector component” to allow the Rao-Oestvall-Araujo system to better “use the energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge.” SAMSUNG-1011, [0001].

196. As discussed in §XI.A, Rao-Oestvall provides functionality to control an application’s network access by intercepting network packets, determining the packet prioritization based on the application, and selectively communicating packets to the network based on the packet prioritization. In Rao, these prioritization operations can be performed by one or more “network drivers of a network stack 310” (e.g., by “customiz[ing], modif[ying] or adapt[ing]” the network drivers “to provide a custom or modified portion of the network stack 310 in support of any of the techniques”). SAMSUNG-1005, [0100]. For example, the Rao-Oestvall system includes “[a] filter 322 [to] place, arrange, or coordinate

network packets into queues 540 a-540 n in support of the priorities,” and these “queues 540a-540n may be included in a network driver, such as an NDIS driver for the filter 322.” *Id.*, [0143], [0180], [0191].

197. In implementing such functionality, a POSITA would have perceived opportunities for improving the interception capabilities already present in Rao to impart additional advantages, such as increasing energy efficiency. To this aspect, a POSITA would have understood and found obvious that well-known monitoring capabilities may be useful to reduce power consumption and thereby increase the longevity of techniques provided by the Rao-Oestvall device while its device operates on battery power. *Id.* A POSITA would have thereby looked to Araujo for a known monitoring technique, particularly Araujo’s “request deflector component,” which is “interposed” between each application and network driver, to selectively allow or block an application from transmitting data to the network. SAMSUNG-1011, [0050]. Incorporation of Araujo’s “request deflector component” into Rao-Oestvall would have enabled assignment of a “status” to an application, use of that status to determine if allowing an application request “justifies the consumption of power under the circumstances that are present,” and regulation (e.g., blocking, allowing) of the request based on that determination. SAMSUNG-1011, [0027]. Such a configuration would have enjoyed the benefits

of better “use the energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge.” SAMSUNG-1011, [0001].

198. In modifying Rao-Oestvall to incorporate Araujo’s teachings, a POSITA would have “interposed” Araujo’s “request deflector component” between applications and the network driver implementing Rao’s packet prioritization functionality (e.g., a network driver implementing the packet capture mechanism 364, filter 322, and queues 540a-540n). For example, a POSITA would have arranged the Araujo’s “request deflector component” to process network packets after an application providing the network packets for transmission has otherwise been deemed by Oestvall’s window server component to be running in the foreground (and thereby having access to device resources). SAMSUNG-1006, [0025]. This configuration would have enabled further assessment of whether the application can access the network (e.g., in addition to considering whether an application has exceeded application-specific data limitations) in order to further enhance the efficiency of the Rao-Oestvall-Araujo combination.

199. Further, a POSITA would have configured the “request deflector component” to determine whether each of the applications has a “status [that] justifies the consumption of power under the circumstances that are present,” and selectively allow or block the network packets from proceeding to the network driver based on the determination. For example, upon determining that the

application's status justifies the consumption of power, the "request deflector component" would allow the network packets to proceed to the network driver for prioritization. Alternatively, upon determining that the application's status does not justify the consumption of power, the "request deflector component" would block the network packets from reaching the network driver, either permanently or temporarily. The "request deflector component" would have thereby provided an additional layer of control for regulating each of the applications' access to the network (e.g., to supplement the regulation techniques already present in Rao-Oestvall).

200. Finally, a POSITA would have had a reasonable expectation of success in modifying Rao-Oestvall to incorporate Araujo. The combination would have involved (1) combining prior art elements according to known methods to yield predictable results; and (2) use of a known technique to improve similar devices (methods, or products) in the same way.

B. Analysis of the Claims

1. Claim 12

[12] The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the first differential traffic control policy based on a power state of the device.

201. As discussed in Section X.D, Araujo describes power management techniques for managing a "machine's power usage." SAMSUNG-1011, Abstract.

This occurs through use of power management policies, which account for factors, such as “current power consumption, the amount of energy stored in a battery, predictions about future power usage, or any other factor.” *Id.*, [0004]. Thus, in Rao-Oestvall-Araujo, power management is based on monitoring, for example, power consumption (“***power state***”). Rao-Oestvall-Araujo would have enabled changes to the way applications operate based on monitoring a power state, which a POSITA would have understood and found obvious involves, in some instances, adjusting a policy enforcement by Rao-Oestvall-Araujo for prioritization (“***dynamically change the application of the first differential traffic control policy***”). SAMSUNG-1011, [0031], [0046].

202. For example, “[a] power state change may be sought in order to turn on a device, or to raise the power state of a device, in order to allow the device to service a request from an application.” SAMSUNG-1011, [0038]. In response, the Rao-Oestvall-Araujo device would respond by “block[ing] the request” and the “program may receive an error code or result code.” *Id.*, [0040]. One type of request is a network packet transmission request described in Rao, and a POSITA would have understood and found obvious that blockage of the request would have resulted in the Rao-Oestvall-Araujo device selecting and/or applying a different policy for prioritization (e.g., selecting a policy that prioritizes packet

transmissions of another application that would not necessitate a power state change). SAMSUNG-1005, [0182].

2. Claim 15

[15] The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the first differential traffic control policy based on power control state changes for one or more of the modems.

203. As discussed for [12], a POSITA would have understood and found obvious that Rao-Oestvall-Araujo adjusts policy enforcement for prioritization in certain circumstances involving a power state change. Araujo further describes that “power may be controlled for devices,” such as “disks, ***network adapters***, processors, monitors.” SAMSUNG-1011, [0018]. A POSITA would have understood and found obvious that a modem is an example of network adapter, and thus, Rao-Oestvall-Araujo would have provided power management for “***one or more modems***.” A POSITA would have therefore understood and found obvious that, in some instances, Rao-Oestvall-Araujo adjusts a policy enforcement by Rao-Oestvall-Araujo for prioritization based on a power state change for a modem (“***dynamically change the application of the first differential traffic control policy***”). SAMSUNG-1011, [0031], [0046]. For example, a POSITA would have understood that a modem is a type of network adapter that serves the purpose of enabling communication between a computer and a network.

204. A POSITA would have further found obvious that the monitored power state includes “***power control state changes***,” which would then be used as to trigger a configuration change. For example, Cole offers examples of “communication load monitoring and deferred action functions” that a POSITA would have understood and found obvious to be improved by policy application by Rao-Oestvall-Araujo. SAMSUNG-1009, [0088]-[0091]. Cole further recognizes that “[a] lengthy transfer [that] is conducted using [a] WWAN modem 230 (e.g., a 3G channel)” “consumes significant battery power” and, in response, the connection manager “asks the user to find a better connection.” SAMSUNG-1009, [0088]. From this example, a POSITA would have recognized that, since modem usage impacts power consumption, changes in a connectivity state of a modem represent changes in the modem’s power control state.

3. Claim 21

[21] The wireless end-user device of claim 20, wherein the API responds to an intercepted request by the first end-user application by emulating network messaging.

205. As noted above, Rao-Oestvall-Araujo would have provided an improved agent that uses one or more APIs as a “means” or “mechanism” to provide communications relating to prioritization” for at least the same reasons as discussed for [1e]. SAMSUNG-1005, [0110], [0166], [0190], [0205]. Further, in Rao, communications related to prioritization may be accomplished using any

“form or interface known to those ordinarily skilled in the art.” SAMSUNG-1005, [0190]. Thus, based on these non-limiting disclosures in Rao, a POSITA would have found obvious that, in incorporating Araujo’s “request deflector component” into Rao-Oestvall (as discussed in §XIII.A), certain exemplary configurations involve the “request deflector component” being implemented to provide communications functionality as an API. In such configurations of Rao-Oestvall-Araujo, the “request deflector component” renders the “*API*” recited in claim 21 obvious because the “request deflector component” in Rao-Oestvall-Araujo would have provided the functionality recited in the claim (e.g., emulating network messaging) as being performed by the API, as further addressed below.

206. Indeed, APIs that were configured to provide emulating network messaging functionality between applications and drivers were well-known as of the Critical Date. For example, Sng (U.S. Pat. No. 8,413,172) describes a “socket API 220” with an emulation module for “socket API call emulation.” SAMSUNG-1015, Abstract, Figure 2. Like Araujo’s “request deflector component” being “interposed” between applications and drivers, Sng’s socket API 220 is similarly interposed between applications (e.g., application 210) and drivers (e.g., non-networked I/O device driver 240, networked I/O device driver 250). *See id.*, 3:46-5:10; *see also* SAMSUNG-1011, [0050]. As another example, as discussed for [1.8(a)], Flinn described an “API” that “offers both blocking and event-based

interfaces...” SAMSUNG-1016, 1. Flinn further indicates the existence of “API features to the normal socket interface[,]” including application regulation mechanisms, such as “block[ing] [a] message until the network is available, with an optional timeout,” which is “more useful to threaded applications.” *Id.*, 3. These disclosures relate to interception and blocking (concepts similarly contemplated in Rao and Araujo) and would have been pertinent to in implementing Rao-Oestvall-Araujo, as discussed in Section XIV.A. SAMSUNG-1005, [0143], [0100], [0180], [0191]; SAMSUNG-1011, [0001], [0027], [0050]. Moreover, the use of APIs to regulate network communications within a layered computing architecture was similarly well-known before the Critical Date. SAMSUNG-1017, 11. These disclosures similarly coincide with relevant disclosure in the ’701 patent relating to APIs that provide emulating network messaging. *See, e.g.*, SAMSUNG-1001, 91:30-36 (“For example, an emulated network API can intercept, modify, block, remove, and/or replace network socket application interface messages and/or EtherType messages[.]”).

207. Further as discussed in Section XIII.A, in Rao-Oestvall-Araujo, “if the power state change is not allowable under [a] policy,” the device can “block the request” and “notif[y] [the program] that the request will not be processed.” SAMSUNG-1011, [0038], [0041]. Further, “[t]he program may also be notified that the reason for the request is that the device is off[,]” e.g., “the program may

receive an error code or result code indicating that the request calls for a device that is not turned on.” *Id.*; *see also id.*, [0017] (“Thus, a program could be notified that a request to use a device is not being put through to the device because the request would be contrary to power-usage policy.”). Based on these disclosures, a POSITA would have understood and found obvious that the Rao-Oestvall-Araujo would have responded to an intercepted request by an application by notifying the application that the request will not be processed and/or transmitting an error code or result code to the application (“***respond[] to an intercepted request by the first end-user application by emulating network messaging***”). In doing so, the combined device would have provided the application with a greater degree of information regarding its attempt to access a network, as taught by Araujo.

208. Moreover, Araujo’s use of an “error code or result code” is consistent with the ’701 patent’s disclosure of an “emulated network API” that blocks an application’s connection attempt and sends “a message...back to the application” regarding the blocking, such as a message that “the application will understand and can interpret to indicate that the network access attempt was not allowed/blocked, that the network is not available, and/or to try again later for the requested network access.” SAMSUNG-1001, 91:25-49.

4. Claim 22

[22] The wireless end-user device of claim 21, wherein emulating network messaging comprises responding to a network request from the particular

application by blocking the request from passing to a network stack and returning to the particular application a message indicating the network request was not successful.

209. As discussed for [21], a POSITA would have configured Rao-Oestvall-Araujo to respond to an intercepted request by an application by notifying the application that the request will not be processed and/or transmitting an error code or result code to the application (“***emulating network messaging***

210. A POSITA would have also understood and found obvious to configure Rao-Oestvall-Araujo such that, in blocking a request from reaching the network driver, the request is prevented from being provided to Rao’s “network stack” (which includes “one or more network drivers supporting the one or more layers” of the network stack) (“***responding to a network request from the particular application by blocking the request from passing to a network stack***

211. Further, in Rao-Oestvall-Araujo, “if the power state change is not allowable under the policy,” the device can “block the request” and “notif[y] [the program] that the request will not be processed.” SAMSUNG-1011, [0038],

[0041]. Further, “[t]he program may also be notified that the reason for the request is that the device is off,” e.g., “the program may receive an error code or result code indicating that the request calls for a device that is not turned on” (“*...and returning to the particular application a message indicating the network request was not successful*”). *Id.*; see also *id.*, [0017] (“Thus, a program could be notified that a request to use a device is not being put through to the device because the request would be contrary to power-usage policy.”).

XIV. CONCLUSION

212. The findings and opinions set forth in this declaration are based on my work and examinations to date.

213. I may continue my examinations. I may also receive additional documentation and other factual evidence over the course of this IPR that will allow me to supplement and/or refine my opinions. I reserve the right to add to, alter, or delete my opinions and my declaration upon discovery of any additional information. I reserve the right to make such changes as may be deemed necessary.

214. In signing this declaration, I recognize that the declaration will be filed as evidence in an IPR before the PTAB. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-

examination within the United States during the time allotted for cross-examination.

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

- *Kunyang Li*, University of Wisconsin, Spring 2026
- *Rachel King*, University of Wisconsin, Spring 2026
- *Yohan Beugin*, University of Wisconsin, Spring 2025
- *Quinn Burke*, University of Wisconsin, Spring 2025
- *Eric Pauley*, University of Wisconsin, Spring 2024
- *Blaine Hoak*, University of Wisconsin, Spring 2025
- *Ryan Sheatsley*, University of Wisconsin, Fall 2023

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 Miadzezhanka*, 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 Oceau*, 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. Computer Science Department, Temple University, Philadelphia, PA, February, 2022.
2. The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective. Computer Science Department, University of Wisconsin-Madison, Madison, WI, February, 2020.
3. Shutterstock Distinguished Lecture: The Challenges of Machine Learning in Adversarial Settings. Computer Science Department, Stonybrook University, Stonybrook, NY, December, 2019.
4. Distinguished Blockchain Lecture: The Challenges of Machine Learning in Adversarial Settings. Cylab Security and Privacy Institute, Carnegie Mellon University, Pittsburgh, PA, December, 2019.
5. Distinguished Speaker Series: The Challenges of Machine Learning in Adversarial Settings. Department of Computer Science, University at Buffalo, Buffalo, NY, November, 2018.
6. 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.
7. The Challenges of Machine Learning in Adversarial Settings. Department of Software and Information Systems, University of North Carolina at Charlotte, Charlotte, NC, February, 2018.
8. Tracing the Arc of Smartphone Application Security. Celebrating 50 Years of Computer Science @ NC State, North Carolina State University, Raleigh, NC, October, 2017.
9. 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.
10. Tracing the Arc of Smartphone Application Security. Rochester Institute of Technology, College of Computing and Information Sciences, Rochester, NY, September, 2017.
11. Tracing the Arc of Smartphone Application Security, University of Texas-Dallas Department of Computer Science, Dallas, TX, May 2017.
12. Tracing the Arc of Smartphone Application Security. Rochester Institute of Technology, College of Computing and Information Sciences, Rochester, NY, May 2017.
13. Tracing the Arc of Smartphone Application Security. University of California-Irvine, Computer Science Department, Irvine CA, March, 2017.
14. Tracing the Arc of Smartphone Application Security. The Ohio State University, Department of Computer Science and Engineering, Columbus, OH, March, 2017.
15. Tracing the Arc of Smartphone Application Security. Virginia Technical University, Department of Computer Science, Blacksburg, VA, March, 2017.

-
16. Six Years of Mobile Smartphone Security, CISPA Distinguished Lecture Series, Max Planck Institute/Saarland University, Saarbrücken Germany, July, 2015.
 17. Six Years of Mobile Smartphone Security. Technische Universität Darmstadt, Darmstadt Germany, July, 2015.
 18. Security Challenges and Solutions in Mobile Smartphone Applications. Computer and Information Science Department, University of Oregon, Eugene, OR, April, 2011.
 19. 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, Abbas Acar, Stefan Achleitner, Hidayet Aksu, Leonardo Babun, Yohan Beugin, Hoak, Blaine, Dan Boneh, Christopher Burchard, Quinn Burke, Kevin Butler, Z. Berkay Celik, Kamalika Chaudhuri, Adrien Cosson, Kyle Denney, Genannt Dohmann, Kyle Domico, Matthew Durbin, Pauley, Eric, David Evans, Felix Freiling, Anshul Gandhi, Rahul George, Kanad Ghose, Kartik Gopalan, Andrew J. Grotto, Amy Hasan, Ting He, Blaine Hoak, Thorsten Holz, Syed Rafiul Hussain, Trent Jaeger, Somesh Jha, Rachel King, Engin Kirda, Srikanth V. Krishnamurthy, Daniel E. Krych, Domico, Kyle, Thomas La Porta, John Launchbury, Dongyoon Lee, Azaree Lintereur, Zhenhua Liu, David 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, Sayed M. Saghaian, Alejandro Andrade Salazar, Ryan Sheatlsey,

Ryan Sheatsley, Tyler Shipp, Sushrut Shringarputale, Amit Kumar Sikder, Simone Silvestri, Anand Sivasubramaniam, Wenjia Song, Indra Spiecker, Gang Tan, Sanchal Thakkar, Selcuk Uluagac, Prasanna Venkatesh, Gunjan Verma, Bimal Viswanath, Michael J. Weisman, Ya Xiao, Tian Xie, Danfeng Yao, Beugin, Yohan, 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 Applied Innovation, Inc., Columbus, OH	1994-1995
Project Manager Primary Access Corporation, San Diego, CA	1993-1994
Software Developer Primary Access Corporation, San Diego, CA	1991-1993
Software Developer Integrated Technologies, Inc., Muncie, IN	1989

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

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 Computing 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 Net-

work 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 Deep-fakes 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 Earlece 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 Nadji 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, February, 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

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), IEE, 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 Nadjji 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 Oceau 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 Ocateau 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 Ocateau 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 Ocateau 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 Epicc: 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 (AC-SAC), 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 Ocateau 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 Monrose, *Toward Valley-Free Inter-domain Routing*, Proceedings of 2007 IEEE International Conference on Communications (ICC 2007), June, 2007. Glasgow, Scotland.

Sunam Ryu and Kevin Butler and Patrick Traynor and Patrick McDaniel, *Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems*, Proceedings of the 3rd IEEE International Symposium on Security in Networks and Distributed Systems (SSNDS-07), June, 2007. Niagara Falls, Canada.

Hosam Rowaihy and William Enck and Patrick McDaniel and Thomas La Porta, *Limiting Sybil Attacks in Structured Peer-to-Peer Networks*, Proceedings of IEEE INFOCOM 2007 MiniSymposium, May, 2007. Anchorage, AK.

Boniface Hicks and Kiyan Ahmadizadeh and Patrick McDaniel, *Understanding Practical Application Development in Security-Typed Languages*, 22st Annual Computer Security Applications Conference (ACSAC), 153–164, December, 2006. Miami, Fl. (**best student paper**)

Luke St. Clair and Lisa Johansen and William Enck and Matthew Pirretti and Patrick Traynor and Patrick McDaniel and Trent Jaeger, *Password Exhaustion: Predicting the End of Password Usefulness*, Proceedings of 2nd International Conference on Information Systems Security (ICISS), 37–55, December, 2006. Kolkata, India.

Kevin Butler and William Enck and Jennifer Plasterr and Patrick Traynor and Patrick McDaniel, *Privacy-Preserving Web-Based Email*, Proceedings of 2nd International Conference on Information Systems Security (ICISS), 116–131, December, 2006. Kolkata, India.

Matthew Pirretti and Patrick Traynor and Patrick McDaniel and Brent Waters, *Secure Attribute-Based Systems*, Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS), 99–112, November, 2006. Alexandria, VA.

Kevin Butler and William Aiello and Patrick McDaniel, *Optimizing BGP Security by Exploiting Path Stability*, Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS), 298–310, November, 2006. Alexandria, VA.

Patrick Traynor and William Enck and Patrick McDaniel and Thomas La Porta, *Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks*, Proceedings of the Twelfth Annual International Conference on Mobile Computing and Networking (MobiCom), 182–193, September, 2006. Los Angeles, CA.

Patrick Traynor and Michael Chien and Scott Weaver and Boniface Hicks and Patrick McDaniel, *Non-Invasive Methods for Host Certification*, Proceedings of the Second IEEE Communications Society/CreateNet International Conference on Security and Privacy in Communication Networks (SecureComm), August, 2006. Baltimore, MD.

Sophie Qiu and Patrick McDaniel and Fabian Monrose and Avi Rubin, *Characterizing Address Use Structure and Stability of Origin Advertisement in Interdomain Routing*, 11th IEEE Symposium on Computers and Communications, 489–496, June, 2006. Pula-Cagliari, Sardinia, Italy.

Patrick McDaniel and Shubho Sen and Oliver Spatscheck and Jacobus Van der Merwe and William Aiello and Charles Kalmanek, *Enterprise Security: A Community of Interest Based Approach*, Proceedings of Network and Distributed Systems Security 2006 (NDSS), February, 2006. San Diego, CA.

Kevin Butler and Patrick McDaniel, *Understanding Mutable Internet Pathogens, or How I Learned to Stop Worrying and Love Parasitic Behavior*, Proceedings of 1st International Conference on Information Systems Security (ICISS), Springer-Verlag Lecture Notes in Computer Science, volume 3803, 36–48, December, 2005. Kolkata, India. (*Invited Paper*)

Wesam Lootah and William Enck and Patrick McDaniel, *TARP: Ticket-Based Address Resolution Protocol*, 21st Annual Computer Security Applications Conference (ACSAC), 95–103, December, 2005. Tuscon, AZ.

William Enck and Patrick Traynor and Patrick McDaniel and Thomas La Porta, *Exploiting Open Functionality in SMS-Capable Cellular Networks*, Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS), 393–404, May, 2005. Alexandria, VA.

Matthew Pirretti and Sencun Zhu and Vijaykrishnan Narayanan and Patrick McDaniel and Mahmut Kandemir and Richard Brooks, *The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense*, Proceedings of the Innovations and Commercial Applications of Distributed Sensor Networks Symposium, October, 2005. Bethesda, Maryland. (**best paper**)

Louis Kruger and Somesh Jha and Patrick McDaniel, *Privacy Preserving Clustering*, 10th European Symposium on Research in Computer Security (ESORICS '05), September, 2005. Milan, Italy.

Heesook Choi and William Enck and Jaesheung Shin and Patrick McDaniel and Thomas La Porta, *Secure Reporting of Traffic Forwarding Activity in Mobile AdHoc Networks*, MobiQuitous 2005, July, 2005. San Diego, CA.

Simon Byers and Lorrie Cranor and Eric Cronin and Dave Kormann and Patrick McDaniel, *Exposing Digital Content Piracy: Approaches, Issues and Experiences*, Thirty-Eighth Conference on Signals, Systems, and Computers, 45-50, Nov, 2004. Monterey, CA. (*Invited paper*)

William Aiello and John Ioannidis and Patrick McDaniel, *Origin Authentication in Interdomain Routing*, Proceedings of 10th ACM Conference on Computer and Communications Security (CCS), ACM, 165-178, October, 2003. Washington, DC.

Eric Cronin and Sugih Jamin and Tal Malkin and Patrick McDaniel, *On the Performance, Feasibility, and Use of Forward Secure Signatures*, Proceedings of 10th ACM Conference on Computer and Communications Security (CCS), ACM, 131-144, October, 2003. Washington, DC.

Patrick McDaniel, *On Context in Authorization Policy*, 8th ACM Symposium on Access Control Models and Technologies (SACMAT), ACM, 80-8, June, 2003. Como, Italy.

Geoff Goodell and William Aiello and Tim Griffin and John Ioannidis and Patrick McDaniel and Avi Rubin, *Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing*, Proceedings of Network and Distributed Systems Security 2003 (NDSS), Internet Society, 75-8, February, 2003. San Diego, CA.

Patrick McDaniel and Atul Prakash, *Methods and Limitations of Security Policy Reconciliation*, 2002 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, 73-87, May, 2002. Oakland, CA.

Patrick McDaniel and Atul Prakash and Jim Irrer and Sharad Mittal and Thai-Chuin Thuang, *Flexibly Constructing Secure Groups in Antigone 2.0*, Proceedings of DARPA Information Survivability Conference and Exposition II, IEEE Computer Society Press, 55-67, June, 2001. Los Angeles, CA.

Hugh Harney and Andrea Colegrove and Patrick McDaniel, *Principles of Policy in Secure Groups*, Proceedings of Network and Distributed Systems Security 2001 (NDSS), Internet Society, 125-13, February, 2001. San Diego, CA.

Patrick McDaniel and Sugih Jamin, *Windowed Certificate Revocation*, Proceedings of IEEE INFOCOM 2000, IEEE, 1406-1414, March, 2000. Tel Aviv, Israel.

Patrick McDaniel and Avi Rubin, *A Response to 'Can We Eliminate Certificate Revocation Lists?'*, Proceedings of Financial Cryptography 2000, International Financial Cryptography Association (IFCA), February, 2000. Anguilla, British West Indies.

Andrew Adamson and Charles J. Antonelli and Kevin Coffman and Patrick McDaniel and Jim Rees, *Secure Distributed Virtual Conferencing*, Proceedings of Communications and Multimedia Security (CMS '99), 176-190, September, 1999. Katholieke Universiteit, Leuven, Belgium.

Patrick McDaniel and Atul Prakash and Peter Honeyman, *Antigone: A Flexible Framework for Secure Group Communication*, Proceedings of the 8th USENIX Security Symposium, 99-114, August, 1999. Washington, DC.

Workshop Papers

Eric Pauley and Patrick McDaniel, *Understanding the Ethical Frameworks of Internet Measurement Studies*, The 2nd International Workshop on Ethics in Computer Security (EthiCS 2023), February, 2023. San Diego, CA. **(best paper award)**

Anshul Gandhi and Kanad Ghose and Kartik Gopalan and Syed Rafiul Hussain and Dongyoon Lee and David Liu and Zhenhua Liu and Patrick McDaniel and Shuai Mu and Erez Zadok, *Metrics for Sustainability in Data Centers*, Proceedings of the 1st Workshop on Sustainable Computer Systems Design and Implementation (Hot-Carbon'22), USENIX, July, 2022. San Diego, CA.

Leonardo Babun and Z. Berkay Celik and Patrick McDaniel and Selcuk Uluagac, *Real-time Analysis of Privacy-(un)aware IoT Applications*, Privacy Enhancing Technologies Symposium (PETS), 2021.

Sushrut Shringarputale and Patrick McDaniel and Kevin Butler and Thomas La Porta, *Co-residency Attacks on Containers are Real*, The ACM Cloud Computing Security Workshop (CCSW 2020), 2020.

Z. Berkay Celik and Patrick McDaniel, *Extending Detection with Privileged Information via Generalized Distillation*, IEEE Security & Privacy Workshop on Deep Learning and Security (IEEE S&P DLS), 2018.

Alexander Alexeev and Diane Henshel and Karl Levitt and Patrick McDaniel and Brian Rivera and Steve Templeton and Michael J. Weisma, *Constructing a Science of Cyber-Resilience for Military Systems*, Information Systems and Technology (IST) Panel, IST-153/RWS-21, CEUR Workshop Proceeding, 30-42, October, 2017.

Z. Berkay Celik and Patrick McDaniel and Rauf Izmailov, *Feature Cultivation in Privileged Information-augmented Detection*, Proceedings of the International Workshop on Security And Privacy Analytics (IWSPA 2017), 2017. *(Invited Paper)*

Stefan Achleitner and Thomas La Porta and Patrick McDaniel and Shridatt Sugrim and Srikanth V. Krishnamurthy and Ritu Chadha, *Cyber Deception: Virtual Networks to Defend Insider Reconnaissance*, Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats, ACM, 2016.

Patrick McDaniel and Robert Walls, *Estimating Attack Intent and Mission Impact from Detection Signals*, Proceedings of the NATO IST-128 Workshop: Assessing Mission Impact of Cyberattacks, Army Research Laboratory, July, 2015.

Patrick McDaniel and Trent Jaeger and Thomas La Porta and Nicolas Papernot and Robert Walls and Alexander Kott and Lisa Marvel and Ananthram Swami and Prasant Mohapatra and Srikanth V. Krishnamurthy and Iulian Neamtiu, *Security and Science of Agility*, First ACM Workshop on Moving Target Defense (MTD 2014), November, 2014. Scottsdale, AZ.

Joshua Schiffman and Thomas Moyer and Hayawardh Vijayakumar and Trent Jaeger and Patrick McDaniel, *Seeding Clouds with Trust Anchors*, Proceedings of CCSW 2010: The ACM Cloud Computing Security Workshop, October, 2010. Chicago, IL.

Stephen McLaughlin and Dmitry Podkuiko and Adam Delozier and Sergei Miadzvezhanka and Patrick McDaniel, *Embedded Firmware Diversity for Smart Electric Meters*, Proceedings of the 5th Workshop on Hot Topics in Security (HotSec '10), August, 2010. Washington, DC.

Patrick McDaniel and Kevin Butler and Stephen McLaughlin and Radu Sion and Erez Zadok and Marianne Winslett, *Towards a Secure and Efficient System for End-to-End Provenance*, the 2nd USENIX Workshop on the Theory and Practice of Provenance, February, 2010. San Jose, CA.

Thomas La Porta and Patrick McDaniel and Karl Rauscher and Jun Shu, *The Impact of Supply Chain on Information and Communications Technology Security*, In the 1st Workshop on Workshop on Telecommunications

Infrastructure Protection and Security, December, 2009. Honolulu, Hawaii.

Stephen McLaughlin and Dmitry Podkuiko and Patrick McDaniel, *Energy Theft in the Advanced Metering Infrastructure*, In the 4th International Workshop on Critical Information Infrastructure Security, September, 2009. Bonn, Germany.

Matthew Blaze and Patrick McDaniel, *Below the Salt: The Dangers of Unfulfilled Physical Media Assumptions*, In Proceedings of Seventeenth International Workshop on Security Protocols, April, 2009. Cambridge, England.

Kevin Butler and William Enck and Harri Hursti and StephenMcLaughlin and Patrick Traynor and Patrick McDaniel, *Systemic Issues in the Hart InterCivic and Premier VotingSystems: Reflections Following Project EVEREST*, In Proceedings of the 3rd USENIX/ACCURATE ElectronicVoting Technology Workshop (EVT '08), July, 2008.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Non-Volatile Memory and Disks: Avenues for Policy Architectures*, Proceedings of the 1st ACM Computer Security Architectures Workshop, November, 2007. Alexandria, VA.

William Enck and Sandra Rueda and Yogesh Sreenivasan and JoshuaSchiffman and Luke St. Clair and Trent Jaeger and Patrick McDaniel, *Protecting Users from "Themselves"*, Proceedings of the 1st ACM Computer Security Architectures Workshop, November, 2007. Alexandria, VA.

Boniface Hicks and David King and Patrick McDaniel, *Jifclipse: Development Tools for Security-Typed Applications*, Proceedings of the 2nd ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS '07), ACM Press, June, 2007. San Diego, CA.

Boniface Hicks and Sandra Rueda and Trent Jaeger andPatrick McDaniel, *Integration of SELinux and Security-typed Languages*, Proceedings of the 2007 Security-Enhanced Linux Workshop, March, 2007. Baltimore, MD.

Sophie Qiu and Fabian Monroe and Andreas Terzis and Patrick McDaniel, *Efficient Techniques for Detecting False Origin Advertisements in Inter-domain Routing*, Proceedings of The Second Workshop on Secure Network Protocols (NPSec), November, 2006. Santa Barbara.

Shiva Chaitanya and Kevin Butler and Patrick McDaniel andAnand Sivasubramaniam, *Design, Implementation and Evaluation of Security iniSCSI-based Network Storage Systems*, Proceedings of 2nd International Workshop on StorageSecurity and Survivability (StorageSS 2006), October, 2006. Alexandria, Virginia.

Trent Jaeger and Patrick McDaniel and Luke St. Clair and RamonCaceres and Reiner Sailer, *Shame on Trust in Distributed Systems*, Proceedings of the First Workshop on Hot Topics inSecurity (HotSec '06), July, 2006. Vancouver, B.C., Canada.

Kevin Butler and Patrick McDaniel and Sophie Qiu, *BGPRV: A Library for Fast and Efficient Routing Data Manipulation*, Proceedings of DETER Community Workshop, June, 2006. Arlington, VA.

Kevin Butler and Patrick McDaniel, *Testing Large Scale BGP Security in Replayable NetworkEnvironments*, Proceedings of DETER Community Workshop, June, 2006. Arlington, VA.

Boniface Hicks and David King and Patrick McDaniel andMichael Hicks, *Trusted Declassification: High-level Policy for aSecurity-Typed Language*, Proceedings of ACM SIGPLAN Workshop on ProgrammingLanguages and Analysis for Security, 65-74, June, 2006. Ottawa, Canada.

Ali Al-Lawati and Dongwon Lee and Patrick McDaniel, *Blocking in Private Information Matching*, Proceedings of Second International ACM SIGMOD Workshop on Information Quality in Information Systems, June, 2005. Baltimore, MD.

William Aiello and Charles Kalmanek and Patrick McDaniel and Shubho 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 and Patrick McDaniel, *Searching for Privacy: Design and Implementation of a P3P-Enabled Search Engine*, Proceedings of 2004 Workshop on Privacy Enhancing Technologies (PETS), May, 2004. Toronto, Canada.

Hao Wang and Somesh Jha and Patrick McDaniel and Miron Livn, *Security Policy Reconciliation in Distributed Computing Environments*, Proceedings of 5th International Workshop on Policies for 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 Dave Kormann and Patrick McDaniel, *Analysis of Security Vulnerabilities in the Movie Production and Distribution Process*, Proceedings of 2003 ACM Workshop on Digital Rights Management, ACM, October, 2003. Washington, DC, also appeared in Telecommunications Policy Research 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-server port-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 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 AngelaSchuett and Patrick McDaniel and Gavin Kenny and HaithamCruickshank 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 SurvivabilityConference 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 SurvivabilityConference 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 andAtul Prakash and Peter Dinsmore, *Multicast Security Policy Requirements and Building Blocks(Draft)*, Internet Research Task Force, Secure MulticastResearch Group (SMuG), November, 2000.

Tom Hardjono and Hugh Harney and Patrick McDaniel and Andrea Colegroveand Peter Dinsmore, *Group Security Policy Token (Draft)*, Internet Research Task Force, Secure MulticastResearch Group (SMuG), November, 2001.

Patrick McDaniel and Hugh Harney and Peter Dinsmore and Atul Prakash, *Multicast Security Policy (Draft)*, Internet Research Task Force, Secure MulticastResearch 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 LargeScale Software*, Masters Thesis, Ball State University, Muncie, IN, June, 1991.

Technical Reports

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.

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 Earlenice 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 Ocateau 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 Ocateau 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 Ocateau 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 Monroe, *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.

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 Kiyan Ahmadi-zadeh 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 PatrickMcDaniel, *On the Performance, Feasibility, and Use of Forward SecureSignatures*, Technical Report TD-5QHGBK, AT&T Labs - Research, Florham Park, NJ, August, 2003.

Simon Byers and Lorrie Cranor and Eric Cronin and DaveKormann and Patrick McDaniel, *Analysis of Security Vulnerabilities in the Movie Productionand 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 SecureGroup Communication*, Technical Report CSE-TR-438-00, Electrical Engineering and Computer Science, Universityof Michigan, December, 2000.

Patrick McDaniel and Atul Prakash, *Lightweight Failure Detection in Secure GroupCommunication*, Technical Report CSE-TR-428-00, Electrical Engineering and Computer Science, Universityof Michigan, June, 2000.

Patrick McDaniel and Atul Prakash, *Antigone: Implementing Policy in Secure GroupCommunication*, Technical Report CSE-TR-426-00, Electrical Engineering and Computer Science, Universityof Michigan, May, 2000.

Patrick McDaniel and Sugih Jamin, *Windowed Certificate Revocation*, Technical Report CSE-TR-413-99, Electrical Engineering and Computer Science, Universityof 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 RevocationLists?"*, Technical Report 99.8.1, AT&T Labs - Research, Florham Park, NJ, August, 1999.

Andrew Adamson and Charles J. Antonelli and Kevin Coffman andPatrick McDaniel and Jim Rees, *Secure Distributed Virtual Conferencing: Multicast orBust*, 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, Universityof Michigan, , 1998.

Patrick McDaniel and Sugih Jamin, *A Scalable Key Distribution Hierarchy*, Technical Report CSE-TR-366-98, Electrical Engineering and Computer Science, Universityof 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

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, CISA 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 ISSNNet Workshop, Ottawa, Canada, June, 2009.

Utility Grid Automation and Risk Management, Clean Technology Conference and Expo, Houston, Texas, May, 2009.

Scalable Integrity-Justified Content Provenance, Center for Applied Cybersecurity Research, Indiana University, Bloomington, IN, April, 2009.

Scalable Integrity-Justified Content Provenance, Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI, April, 2009.

What is Security, Dickenson Law School, Penn State University, State College, PA, April, 2009.

Scalable Integrity-Justified Content Provenance, Department of Computer Science and Engineering, Notre Dame University, South Bend, IN, April, 2009.

Electronic Voting: The Good, the Bad, and the Reality, Software Engineering Research Center Showcase, Muncie, IN, November, 2008.

Ohio Voting Systems Integrity: The EVEREST Report, Networking and Security Research Center, Computer Science and Engineering, Pennsylvania State University, State College, PA, October, 2008.

Data Provenance: Challenges and Technology, Cyber Physical System Security Forum, Cyber Security Research and Development Review, Washington DC, October, 2008.

System-Wide Information Flow Enforcement, NICIAR PI Meeting, Washington DC, September, 2008.

Presto: Configuration Management at Massive Scale, NSF Workshop on Assurable and Usable Security Configuration, George Mason University, Fairfax, VA, August, 2008.

Asymmetry in Performance and Security Requirements for I/O in High-end Computing, NSF HECURA FSIO PI Meeting, Arlington, VA, August, 2008.

Authentication and Web Security, Security and Privacy in IT-EMTM 604 Guest Lecture, University of Pennsylvania, Philadelphia, PA, May, 2008.

SPAM and SPAM Mitigation, Computer Science Department, St. Vincent's University, Latrobe, PA, April, 2008.

Phones, The Press, Research and Grad School ... or how to make trouble and have fun doing it, Computer Science Department, St. Vincent's University, Latrobe, PA, April, 2008.

Applications and Services in Telecommunications Networks, NSF Wireless Security Workshop, Georgia Institute of Technology, Atlanta, GA, March, 2008.

Vulnerabilities and Opportunities in SMS-Capable Cellular Networks, Computer Science Department, Carleton University, Ottawa, Canada, March, 2008.

Ohio Voting Systems Integrity: The EVEREST Report, Case-Western Reserve University, Cleveland, OH, February, 2007.

Ohio Voting Systems Integrity: The EVEREST Report, Ohio State University, Columbus, OH, February, 2007.

Ohio Voting Systems Integrity: The EVEREST Report, Ohio University, Athens, OH, February, 2007.

Ohio Voting Systems Integrity: The EVEREST Report, Miami University, Ohio, Oxford, OH, February, 2007.

Ohio Voting Systems Integrity: The EVEREST Report, Bowling Green State University, Bowling Green, OH, February, 2007.

Vulnerabilities and Opportunities in SMS-Capable Cellular Networks, Computer Science Department, Indiana University of Pennsylvania, Indiana, PA, September, 2007.

Asymmetry in Performance and Security Requirements for I/O in High-End Computing, HECIWG FSIO 2007 Workshop, NSF, Arlington, VA, August, 2007.

Toward Valley-Free Interdomain Routing, IEEE International Conference on Communications (ICC) 2007, Glasgow, Scotland, June, 2007.

Extending Developer Tools for Security-Typed Languages, Software Engineering Research Center Fall Showcase, West Lafayette, IN, June, 2007.

Open Functionality in SMS/Cellular Networks, Computer and Information Science, University of Oregon, Eugene, OR, May, 2007.

Open Functionality in SMS/Cellular Networks, Computer Security Symposium, St. Cloud State University, St. Cloud, MN, May, 2007.

Authentication and Web Security, Security and Privacy in IT-EMTM 604 Guest Lecture, University of Pennsylvania, Philadelphia, PA, April, 2007.

Grains of SANs: Building Storage Area Networks from Memory Spots, CISCO Remote Faculty Seminar, University Park, PA, April, 2007.

Grains of SANs: Building Storage Area Networks from Memory Spots, 2007 IEEE Security and Privacy Crystal Ball Workshop, Hawthorne, NY, January, 2007.

Password Exhaustion: Predicting the End of Password Usefulness, 2nd International Conference on Information Systems Security, Kolkata, India, December, 2006.

Privacy Preserving Web-based Email, 2nd International Conference on Information Systems Security, Kolkata, India, December, 2006.

Physical and Digital Convergence: Where the Internet is the Enemy, Eighth International Conference on Information and Communications Security (ICICS '06), Raleigh, NC, December, 2006.

Extending Developer Tools for Security-Typed Languages, Software Engineering Research Center Fall Showcase, Muncie, IN, November, 2006.

Open Functionality in SMS/Cellular Networks, Johns Hopkins University, Computer Science Department, Baltimore, MD, September, 2006.

Open Functionality in SMS/Cellular Networks, George Mason University, Computer Science Department, Fairfax, VA, September, 2006.

Exploiting Open Functionality in SMS-Capable Cellular Networks, Motorola Security Symposium, Itasca, IL, September, 2006.

IsleB: Testing Large Scale BGP Security in Replayable Network Environments, NSF/DETER Community Workshop, Arlington, VA, June, 2006.

BGPRV: A Library for Fast and Efficient Routing Data Manipulation, NSF/DETER Community Workshop, Arlington, VA, June, 2006.

Jifclipse: Extending Developer Tools for Security-Typed Languages, Software Engineering Research Center Spring Showcase, Schaumburg, IL, June, 2006.

Trends in Security: Critical Engineering in the Large, Schlumberger InnovateIT! 2006, Cambridge, MA, May, 2006.

Information Flow Revisited: Software Engineering to Provable Security, Network Center of Excellence, Motorola Labs, Schaumburg, IL, May, 2006.

Authentication and Web Security, Security and Privacy in IT-EMTM 604 Guest Lecture, University of Pennsylvania, Philadelphia, PA, April, 2006.

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

Exploiting Open Functionality in SMS-Capable Cellular Networks, Computer Science Department, University of Virginia, Charlottesville, VA, January, 2006.

Software Engineering Tools for Security-Typed Languages: Using Eclipse to Make Secure Programming Practical, Software Engineering Research Center Showcase, Muncie, IN, November, 2005.

Exploiting Open Functionality in SMS-Capable Cellular Networks, AT&T IP Services Security Council, Middletown, NJ, October, 2005.

Exploiting Open Functionality in SMS-Capable Cellular Networks, Computer Science Department, Carnegie Mellon University, Pittsburgh, PA, October, 2005.

Exploiting Open Functionality in SMS-Capable Cellular Networks, Computer Science Department, Yale University, New Haven, CT, October, 2005.

Exploiting Open Functionality in SMS-Capable Cellular Networks, Computer Science Department, SUNY-Stony Brook, Stony Brook, NY, October, 2005.

Exploiting Open Functionality in SMS-Capable Cellular Networks, Networking and Security Research Center, Computer Science and Engineering, Pennsylvania State University, State College, PA, October, 2005.

Isleb: Trace Driven Modeling of Internet-Scale BGP Attacks and Countermeasures, 2nd Annual DETER/EMIST Workshop, Newport Beach, CA, September, 2005.

Critical Infrastructure Security through Provably Secure Network Mediation, 2nd Japan/US Workshop on Critical Information Infrastructure Protection (CIIP), Tokyo, Japan, June, 2005.

Extending Developer Tools for Security-typed Languages, Software Engineering Research Center Showcase, West Lafayette, IN, June, 2005.

Origin Authentication in Interdomain Routing, 2005 IEEE Communications Quality and Reliability (CQR) International Workshop, St. Petersburg, FL, April, 2005.

Analysis of Security Vulnerabilities in the Movie Production and Distribution Process, Messiah College, Senior Seminar Series, Grantham, PA, April, 2005.

Origin Authentication in Interdomain Routing, Intel Research, Folsom CA, April, 2005.

Key Distribution Strategies For Low-Power Wireless Networks, Network Center of Excellence, Motorola Labs, Schaumburg, IL, April, 2005.

Policy Evolution: Autonomic Environmental Security, Software Engineering Research Center Showcase, Muncie, IN, December, 2004.

Information Assurance for Enterprise Networks, BAE Systems, Networking Seminar, Reston, VA, November, 2004.

Origin Authentication in Interdomain Routing, Computer Science Department, Purdue University, West Lafayette, IN, October, 2004.

Origin Authentication in Interdomain Routing, Electrical Engineering and Computer Science Department, University of Michigan, Ann Arbor, MI, October, 2004.

Origin Authentication in Interdomain Routing, Computer Science Department, University of Wisconsin, Madison, MD, September, 2004.

Analysis of Security Vulnerabilities in the Movie Production and Distribution Process, Computer Science and Engineering Student Organization, University Park, PA, September, 2004.

Useless Metaphors? Why Specifying Policy is So Hard, Workshop on Usable Privacy and Security Software, Center for Discrete Mathematics and Theoretical Computer Science (DIMACS), New Brunswick, New Jersey, July, 2004.

Analysis of Security Vulnerabilities in the Movie Production and Distribution Process, Information Systems Research Seminar, Stern School of Business, New York University, New York, NY, April, 2004.

Analysis of Security Vulnerabilities in the Movie Production 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 Movie Production 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 Movie Production 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 Study*Defense, Department of Electrical Engineering and ComputerScience, University of Michigan, Ann Arbor, MI, September, 1997.