

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Gregory G. Raleigh, et al.
U.S. Patent No.: 9,277,445 Attorney Docket No.: 39843-0162IP1
Issue Date: March 1, 2016
Appl. Serial No.: 14/684,033
Filing Date: April 10, 2015
Title: WIRELESS END-USER DEVICE WITH DIFFERENTIAL
TRAFFIC CONTROL POLICY LIST AND APPLYING FORE-
GROUND CLASSIFICATION TO WIRELESS DATA SER-VICE

DECLARATION OF DR. KEVIN R. B. BUTLER

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: 09-28-2023

By: 

Kevin R. B. Butler, Ph.D.

TABLE OF CONTENTS

TABLE OF CONTENTS	2
I. ASSIGNMENT	5
II. QUALIFICATIONS	5
III. SUMMARY OF CONCLUSIONS FORMED	10
IV. LEVEL OF ORDINARY SKILL IN THE ART	11
V. LEGAL PRINCIPLES	12
A. Claim Interpretation.....	13
B. Priority	13
C. Anticipation	14
D. Obviousness.....	14
VI. MATERIALS CONSIDERED	16
VII. OVERVIEW OF THE '445 PATENT.....	18
A. Specification	18
B. Claims	21
C. Prosecution History	26
VIII. INTERPRETATION OF THE '445 PATENT CLAIMS.....	26
IX. [GROUND 1] – RAO-OESTVALL-MONTEMURRO MAKES CLAIMS 1, 2, 4-9, 14, 16, 19, 20, 23, and 26 OBVIOUS.....	27
A. Overview of Rao.....	27
B. Overview of Oestvall.....	35
C. Overview of Montemurro	39
D. Combination of Rao, Oestvall, and Montemurro	41
1. <i>Both Rao's system and Oestvall's system selectively allow and block network traffic from applications based on certain criteria.....</i>	42
2. <i>A POSITA would have been led to modify Rao's system to allow/block an application's network traffic based on the application's</i>	

	<i>“trusted/untrusted” status as taught by Oestvall to thereby reduce battery drain</i>	<i>45</i>
3.	Like Rao, Montemurro’s system selectively regulates network traffic from applications based on certain criteria.....	50
4.	A POSITA would have been led to additionally modify the Rao-Oestvall system to apply different policies depending on which network is selected to handle an application’s network traffic as taught by Montemurro.....	52
E.	Analysis of Claims 1, 2, 4-9, 14, 16, 19, 20, 23, and 26.....	59
1.	Claim 1	59
2.	Claim 2	78
3.	Claim 4	82
4.	Claim 5	83
5.	Claim 6	85
6.	Claim 7	86
7.	Claim 8	87
8.	Claim 9	89
9.	Claim 14	91
10.	Claim 16	93
11.	Claim 19	95
12.	Claim 20	97
13.	Claim 23	98
14.	Claim 26	99
X.	[GROUND 2] – RAO-OESTVALL-MONTEMURRO- ARAUJO MAKES CLAIMS 10-12, 15, 17, 18, 22, and 25 OBVIOUS.....	100
A.	Overview of Araujo	100
B.	Combination of Rao-Oestvall-Montemurro and Araujo.....	103
C.	Analysis of Claims 10-12, 15, 17, 18, 22, and 25.....	107

1.	Claims 10 and 12	107
2.	Claim 11	112
3.	Claim 15	113
4.	Claim 17	114
5.	Claim 18	119
6.	Claim 22	120
7.	Claim 25	122
XI.	[GROUND 3] – RAO-OESTVALL-MONTEMURRO-FREUND MAKES CLAIMS 3, 13, 21, and 24 OBVIOUS	124
A.	Overview of Freund	124
B.	Combination of Rao-Oestvall-Montemurro and Freund	128
C.	Analysis of Claims 3, 13, 21, and 24	130
8.	Claim 3	130
9.	Claims 13 and 24	132
10.	Claim 21	134
XII.	CONCLUSION	136

I, Kevin R. B. Butler of Gainesville, Florida, declare that:

I. ASSIGNMENT

1. I have been retained on behalf of Samsung Electronics Co., Ltd. (“Samsung”) to offer technical opinions related to U.S. Patent No 9,277,445 (“the ’445 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 ’445 patent.

2. I have been asked to provide my independent analysis of the ’445 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 ’445 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 ’445 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. I have summarized in this section my educational background, career history, publications, and other relevant qualifications.

6. I received a B.Sc. degree in Electrical Engineering from Queen's University in 1999, an M.S. degree in Electrical Engineering from Columbia University in 2003, and a Ph.D. in Computer Science and Engineering from the Pennsylvania State University in 2010.

7. I am a Professor with tenure in Computer and Information Science and Engineering and Director of the Florida Institute for Cybersecurity Research at the University of Florida. I founded and directed the Oregon Systems Infrastructure and Information Security (OSIRIS) Lab at the University of Oregon, where I was an assistant professor of computer and information science for four years before moving to Florida under the Rising to National Preeminence initiative. I have authored over 115 peer-reviewed publications including book chapters, journal articles, conference proceedings papers, and workshop papers. My research is in the area of computer systems security, including embedded systems, mobile devices, and firmware, as well as network security, including the security of Internet routing and security of telecommunications networks. I received a National Science Foundation CAREER award in 2013, an International Educator of the Year award within the Herbert Wertheim College of Engineering at the University of Florida in 2017, a University of Florida Term Professorship for 2018-2021 and 2021-2024, and an Arnold and Lisa Goldberg Rising Star Endowed Professorship in Computer Science for 2018-2024, which I relinquished in 2021

upon promotion to Full Professor. I also received an Outstanding Community Service Award from the IEEE Technical Committee on Security and Privacy in 2017. I am a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE), and a Senior Member of the Association for Computing Machinery (ACM). I have been involved with international standards-setting bodies; in particular, I was co-chair and leader of the Security Workstream for the International Telecommunications Union (ITU)'s Technology, Innovation, and Competition Working group within the Focus Group on Digital Financial Service from 2015-2016, and from 2017-2022, I served as Co-Chair of the Security, Infrastructure, and Trust Working Group within the ITU's Financial Inclusion Global Initiative. I currently serve on four journal editorial boards, have served on numerous funding panels for the National Science Foundation and reviewed grant proposals on behalf of science and engineering boards in Austria, Canada, and Israel. I have served on over 115 technical program committees for selecting papers to appear at academic conferences on computer security, and I have served as program committee chair and general conference chair for multiple conferences. I have also given over 100 presentations and invited talks, including invited lectures at the University of Oxford, ETH Zurich, the Chinese Academy of Sciences, Dartmouth College, Columbia University, and UCLA. My research has

been featured in news outlets such as the Wall Street Journal, BBC News, and WIRED.

8. I have experience with networking and power consumption of networked computing systems. At Flarion Technologies in 2003, I implemented packet diversion and IP header modification programs in the FreeBSD operating system for mobile IP packet testing, to be deployed on WiFi devices where power consumption was a factor considered in benchmarking results. In 2004 at AT&T Labs-Research, I led the design and implementation of mechanisms to support the secure delivery of routing information within the Border Gateway Protocol and evaluated their efficacy using routing data. I have also led the development of a survey of security mechanisms for the Border Gateway Protocol that has been cited over 500 times.

9. I have experience with wireless digital communication systems. As a research assistant at Columbia University in 2001-2002, I incorporated authentication protocols into a Java-based software stack for the Session Initiation Protocol used for Internet telephony and in modern cellular telephony networks. More recently, I led a project that demonstrated the extraction of data from smartphone firmware images and demonstrated that legacy command sets (i.e., “AT commands” developed for modems in the 1980s) were being used to provide undocumented features on these devices that could be accessed over a USB

connection, as well as methods for enabling the transmissions of these commands.

I also led the investigation of the processors on smartphones that are used for communicating with the cellular network and developed an analysis framework that found vulnerabilities in the implementation of cellular communication network protocols implemented in these devices.

10. I have experience with the development and analysis of software and firmware. In 1998 at the Royal Bank of Canada, I developed client-server applications, including design of graphical user interfaces on the client side, to port business processes from mainframe environments. Further, in 2006 I compiled and modified OpenEmbedded firmware to support the SlugOS environment to allow experimentation with storage devices, in order to develop a disk prototype for preventing a type of malware called a rootkit from persisting on a system after reboot. Since then, I have led efforts to analyze firmware on embedded devices, particularly firmware from USB flash drives that uses the Intel 8051 microcontroller, and demonstrated how such binary firmware could be lifted to an intermediate representation to enable control flow graph recovery and symbolic analysis.

11. I have experience with peripherals and portable devices. In 2009, I developed a USB device capable of attesting the integrity of the host computer it was attached to while at Symantec Research. This work was later patented (U.S.

Patent 8,856,918, Host validation mechanism for preserving integrity of portable storage data. Petros Efstathopoulos, Bruce Montague, Dharmesh Shah, Kevin Butler. October 7, 2014.). Since then, I have overseen the development of USB devices that allow for tracking the provenance of data at the block level and the development of mobile device software that automates the collection of USB enumeration data.

12. I have also been involved with numerous projects incorporating encryption, such as a mechanisms using additive homomorphic encryption to support accounting audits for preserving the confidentiality of wiretap records and cryptographic schemes for assuring the secure time release of data.

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

III. SUMMARY OF CONCLUSIONS FORMED

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

- ☐ **Ground 1:** Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe

that claims 1, 2, 4-9, 14, 16, 19, 20, 23, and 26 of the '445 patent are made obvious over Rao in view of Oestvall and Montemurro.

- ☐ **Ground 2:** Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claims 10-12, 15, 17, 18, 22, and 25 of the '445 patent are made obvious over Rao in view of Oestvall, Montemurro, and Araujo.
- ☐ **Ground 3:** Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claims 3, 13, 21, 24 of the '445 patent are made obvious over Rao in view of Oestvall, Montemurro, and Freund.

IV. LEVEL OF ORDINARY SKILL IN THE ART

15. 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 '445 patent was filed April 10, 2015, and claims priority to several provisional applications, the earliest of which was filed January 28, 2009 (“Critical Date”). Because I do not know at what date the invention as claimed was made, if ever, I have used the Critical Date of the '445 patent as the point in time for claim interpretation purposes. My opinion does not change if the invention date is earlier.

16. Based on my knowledge and experience in the field and my review of the '445 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.

17. 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. Based on my knowledge, skill, and experience, I have an understanding of the capabilities of one of ordinary skill. For example, from my industry experience, I am familiar with what an engineer would have known and found predictable in the art. From teaching and supervising my post-graduate students, I also have an understanding of the knowledge that a person with this academic experience possesses. Furthermore, I possess those capabilities myself.

V. LEGAL PRINCIPLES

18. I am not a lawyer and I will not provide any legal opinions in this IPR. Although not a lawyer, I have been advised that certain legal standards are to be

applied by technical experts in forming opinions regarding the meaning and validity of patent claims.

A. Claim Interpretation

19. I understand that claim terms are generally given their plain and ordinary meaning based on the patent's specification and file history as understood by a person of ordinary skill in the art at the time of the purported invention. 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 of the invention was made (not today).

B. Priority

20. I understand that a continuation application is a later-filed application that has the same disclosure (specification and figures) as an earlier filed application to which the later-filed application claims priority. A continuation is generally entitled to the same priority date as the later-filed application to which it claims priority.

C. Anticipation

21. I understand that a patent claim is invalid as anticipated if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. I also understand that, to anticipate, the reference must teach all of the limitations arranged or combined in the same way as described in the claim. I do not rely on anticipation in this declaration.

22. With respect to inherency, I understand that the fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. Instead, the inherent characteristic must necessarily flow from the teaching of the prior art.

D. Obviousness

23. I understand that a patent claim is invalid if the claimed invention would have been obvious to a person of ordinary skill in the field at the time of the purported invention, which is often considered the time the application was filed. Even if all of the claim limitations are not found in a single prior art reference that anticipates the claim, the claim can still be invalid.

24. To obtain a patent, a claimed invention must have, as of the priority date, been nonobvious in view of the prior art in the field. I understand that an invention is obvious when the differences between the subject matter sought to be patented 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 person having ordinary skill in the art.

25. I understand that, to prove that prior art or a combination of prior art makes a patent obvious it is necessary to: (1) identify the particular references that, singly or in combination, make the patent obvious; (2) specifically identify which elements of the patent claim appear in each of the asserted references; and (3) explain a motivation, teaching, need, market pressure or other legitimate reason that would have inspired a person of ordinary skill in the art to combine prior art references to solve a problem.

26. I also understand that certain objective indicia can be important evidence regarding whether a patent is obvious or nonobvious. Such indicia include:

- ☐ Commercial success of products covered by the patent claims;
- ☐ A long-felt need for the invention;
- ☐ Failed attempts by others to make the invention;
- ☐ Copying of the invention by others in the field;
- ☐ Unexpected results achieved by the invention as compared to the closest prior art;
- ☐ Praise of the invention by the infringer or others in the field;
- ☐ The taking of licenses under the patent by others;

- ☐ Expressions of surprise by experts and those skilled in the art at the making of the invention; and
- ☐ The patentee proceeded contrary to the accepted wisdom of the prior art.

27. To the extent these factors have been brought to my attention, if at all, I have taken them into consideration in providing my opinions and conclusions.

VI. MATERIALS CONSIDERED

28. 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 during the early 2000s–2010s, and I taught, participated in organizations, and worked closely with many such persons in the field during that time frame.

29. 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 '445 patent; my own knowledge and experiences gained from my work experience in the field of the '445 patent and

related disciplines; and my experience in working with others involved in this field and related disciplines.

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

- ☐ U.S. Patent No. 9,277,445 to Raleigh, et al. (“the ’445 Patent”) (SAMSUNG-1001) and its accompanying prosecution history (SAMSUNG-1002),
- ☐ Complaint for Patent Infringement in *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al.*, 2:22-cv-00422, E.D. Tex., October 26, 2022 (SAMSUNG-1004)
- ☐ U.S. Patent Publication No. 2006/0039354 A1 (“Rao”) (SAMSUNG-1005),
- ☐ U.S. Patent Publication No. 2007/0038763 A1 (“Oestvall”) (SAMSUNG-1006),
- ☐ U.S. Patent Publication No. 2009/0207817 A1 (“Montemurro”) (SAMSUNG-1007),
- ☐ U.S. Patent Publication No. 2009/0217065 A1 (“Araujo”) (SAMSUNG-1008),
- ☐ U.S. Patent No. 5,987,611 (“Freund”) (SAMSUNG-1009),
- ☐ M. V. Pedersen, F. H. P. Fitzek, and T. Larsen, “Implementation and Performance Evaluation of Network Coding for Cooperative

Mobile Devices,” ICC Workshops - 2008 IEEE International
Conference on Communications Workshops, Beijing, China:
IEEE, May 2008, pp. 91–96. doi: 10.1109/ICCW.2008.22
 (“Pedersen”) (SAMSUNG-1010),

- U.S. Patent Publication No. No. 2008/0080458 (“Cole”) (SAMSUNG-1011),
- U.S. Patent No. 8,381,127 (“Singh”) (SAMSUNG-1012),
- W. R. Stevens, “TCP/IP Illustrated, Volume 1,” 2003, ISBN: 0-13-141155-1 (“Stevens”) (SAMSUNG-1013),
- D. P. Bovet, “Understanding the Linux Kernel,” 2000, ISBN: 0-596-00002-2 (“Bovet”) (SAMSUNG-1014).

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

VII. OVERVIEW OF THE ’445 PATENT

A. Specification

32. The ’445 Patent describes “apply[ing] a differential traffic control policy to an application requesting Internet service access” through a “system 2700 for application-specific differential network access control.” SAMSUNG-1001, Abstract, 100:28-102:56, FIG. 27.

33. In particular, 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.

34. In general, 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 (*id.*, 101:53-102:11), or (ii) “restrict network access of a particular service usage activity” (*id.*, 102:12-37).

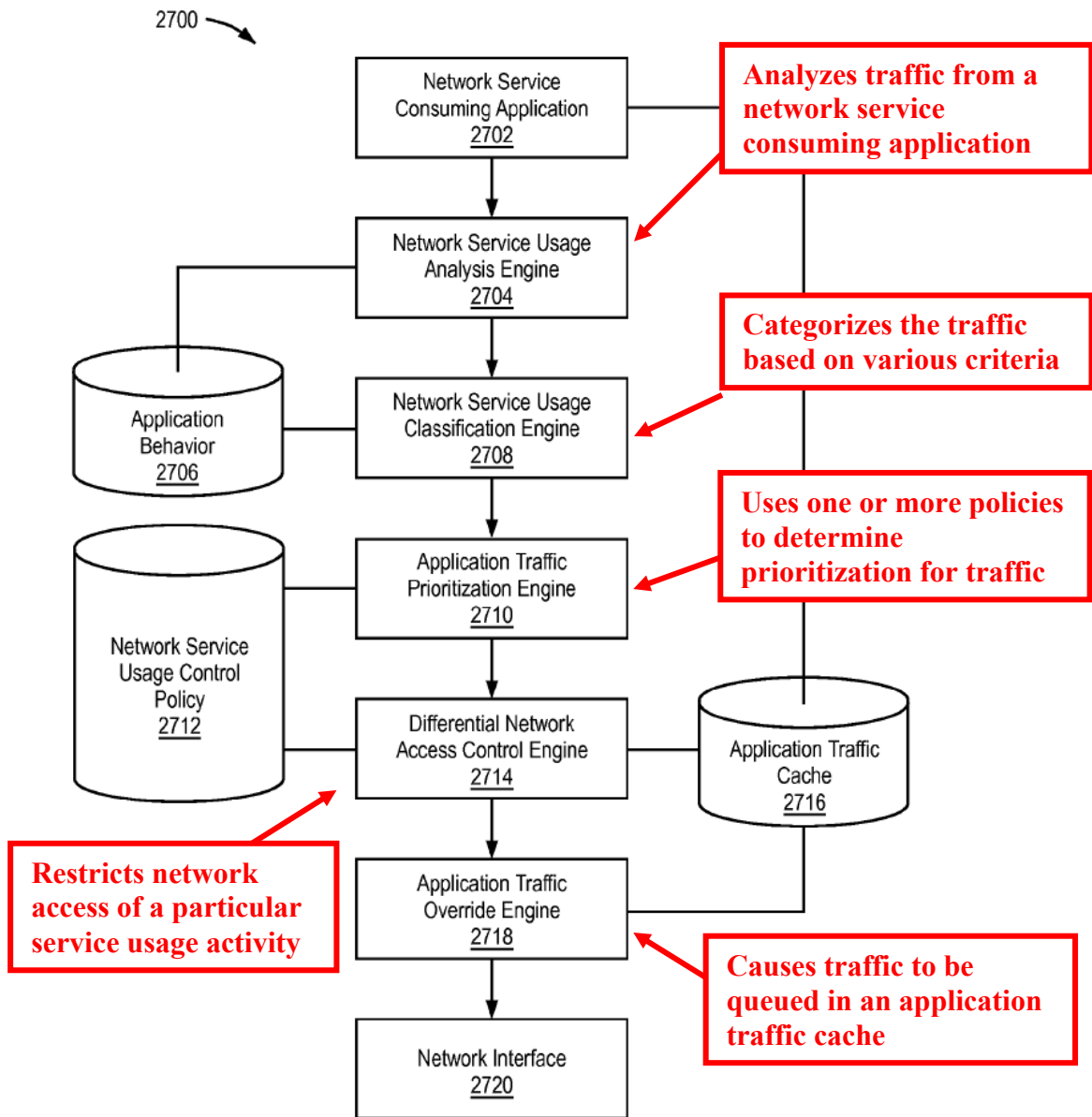


FIG. 27

SAMSUNG-1001, FIG. 27 (annotated)¹

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

B. Claims

35. The table below includes identifiers for the '445 patent claims and limitations, which are referenced throughout.

Claim	Identifier	Claim Language
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; and
	[1c]	one or more processors configured to
	[1d]	classify, as a first classification, whether data for Internet service activities is to be communicated through the WWAN modem or the WLAN modem, and
	[1e]	classify, as a second classification, whether a particular application associated with an Internet service access request, and capable of both interacting with a user in a user interface foreground of the device, and at least some Internet service activities when not interacting with a user in the device user interface foreground, is interacting with the user in the device user interface foreground, and
	[1f]	apply a differential traffic control policy to the Internet service access request, based on (i) the first and second classifications performed by the one or more processors, and (ii) a differential traffic control policy list distinguishing between a first one or more applications resident on the device and a second one or more applications resident

Claim	Identifier	Claim Language
		on the device,
	[1g]	such that, when the particular application is one of the first one or more applications, the one or more processors are operable to block the Internet service access request in a first state of the first and second classifications, wherein data for Internet service activities is classified as to be provided through the WWAN modem, and the particular application is not classified as interacting with a user in the device user interface foreground, and
	[1h]	allow the Internet service access request under at least one different state of the first and second classifications.
2	[2]	The wireless end-user device of claim 1, wherein the one or more processors are configured to classify that the particular application is interacting with the user in the device user interface foreground when the user of the device is directly interacting with that application or perceiving any benefit from that application.
3	[3]	The wireless end-user device of claim 1, further comprising the user interface, wherein the user interface is to provide the user of the device with information regarding why the differential traffic control policy is applied to the particular end-user application.
4	[4]	The wireless end-user device of claim 1, further comprising the user interface, wherein the user interface is to inform a user of the wireless end-user device when there are options to set, control, override, or modify service usage controls that affect the differential traffic control policy and/or the differential traffic control policy list.
5	[5]	The wireless end-user device of claim 1, wherein the differential traffic control policy is part of a multimode profile having different policies for different networks.
6	[6]	The wireless end-user device of claim 5, wherein the one or more processors are further configured to select a

Claim	Identifier	Claim Language
		traffic control policy from the multimode profile based at least in part on a network type of a network connection currently in use by the wireless end-user device.
7	[7]	The wireless end-user device of claim 6, wherein the one or more processors are further configured to, when the network type of a 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.
8	[8]	The wireless end-user device of claim 1, wherein the one or more processors are further to apply the differential traffic control policy such that, when the particular application is one of the second one or more applications, the one or more processors are operable to allow the Internet service access request when data for Internet service activities is classified as to be provided through the WWAN modem, and the particular application is not classified as interacting with a user in the device user interface foreground.
9	[9]	The wireless end-user device of claim 1, wherein the one or more processors are to apply the differential traffic control policy to one of but not both of a WWAN modem connection to a roaming WWAN network and a WWAN modem connection to a home WWAN network.
10	[10]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the differential traffic control policy based on a power state of the device.
11	[11]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the differential

Claim	Identifier	Claim Language
		traffic control policy based on a device usage state.
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 differential traffic control policy based on power control state changes for one or more of the modems.
13	[13]	The wireless end-user device of claim 1, wherein the differential traffic control policy defines that the first one or more applications can only have WWAN network access events during particular time windows.
14	[14]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to update the differential traffic control policy and/or the differential traffic control policy list based on information received from a network element.
15	[15]	The wireless end-user device of claim 1, further comprising an agent to block, modify, remove, or replace user interface messages generated by the particular application based on the applied differential traffic control policy.
16	[16]	The wireless end-user device of claim 1, wherein the one or more processors operable to block the Internet service access request are configured to selectively block the Internet service access request by intercepting open, connect, and/or write requests by the particular application to a network stack.
17	[17]	The wireless end-user device of claim 16, wherein the one or more processors are configured to respond to an intercepted request by the particular application by emulating network messaging.
18	[18]	The wireless end-user device of claim 17, 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

Claim	Identifier	Claim Language
		indicating the network request was not successful.
19	[19]	The wireless end-user device of claim 1, wherein the one or more processors are configured to classify that the particular application is interacting with a user in the device user interface foreground based on a state of user interface priority for the application.
20	[20]	The wireless end-user device of claim 1, wherein the second one or more applications are not subject to a differential network access control that is applicable to the first one or more applications.
21	[21]	The wireless end-user device of claim 1, further comprising a policy agent to: monitor Internet service activity usage for a third application that is neither one of the first one or more applications nor one of the second one or more applications; and to report the activity usage to a network element when Internet service activity usage by the third application exceeds a data usage threshold.
22	[22]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to classify between: user applications; system applications, utilities, functions, or processes; and operating system application, utilities, functions, or processes.
23	[23]	The wireless end-user device of claim 1, wherein the second one or more applications comprises foreground services.
24	[24]	The wireless end-user device of claim 1, wherein block comprises intermittently block when the Internet service access request occurs during selected time windows.
25	[25]	The wireless end-user device of claim 1, wherein the one or more processors are configured to prevent the first one or more applications from changing the power state of the modem, and to not prevent the second one or more applications from changing the power state of the

Claim	Identifier	Claim Language
		modem.
26	[26]	The wireless end-user device of claim 1, wherein the at least one different classification state comprises a state wherein data for Internet service activities is classified as to be provided through the WWAN modem, and the particular application is classified as interacting with a user in the device user interface foreground.

C. Prosecution History

36. The '445 Patent was allowed after the Patent Owner narrowed the independent claim to distinguish from the cited references cited during prosecution. SAMSUNG-1002, 23-31. In allowing the claims, the Examiner noted that the references cited during prosecution do not render obvious the [1a]-[1h] limitations. *Id.*

37. During prosecution, the Examiner did not consider any of Rao, Oestvall, Montemurro, Araujo, and Freund. *See generally* SAMSUNG-1002. As I explain below, these references render obvious the Challenged Claims, including the [1a]-[1h] limitations.

VIII. INTERPRETATION OF THE '445 PATENT CLAIMS

38. 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.” 37 C.F.R. § 42.100(b). 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 of 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 ’445 patent as the point in time for claim interpretation purposes. My opinion does not change if the invention date is earlier.

IX. [GROUND 1] – RAO-OESTVALL-MONTEMURRO MAKES CLAIMS 1, 2, 4-9, 14, 16, 19, 20, 23, and 26 OBVIOUS

A. Overview of Rao

39. Rao describes “a remote access architecture” for “improv[ing] or increas[ing] the performance, operational characteristics, and user experience on [a] client based on the applications running on the client.” SAMSUNG-1005, Abstract, [0080]. Rao’s architecture may be implemented with respect to “any network topology,” such as “peer-to-peer” and “client/server” topologies. *Id.*, [0084]. Further, Rao’s architecture can be implemented with respect to “any workstation, desktop computer, laptop or notebook computer, server, handheld computer, mobile telephone, any other computer, or other form of computing or

telecommunications device that is capable of communication and that has sufficient processor power and memory capacity to perform the operations described herein.” *Id.*, [0130].

40. In particular, Rao describes a system for performing “intelligent and client centric prioritization of application network communications on a client based on the type and/or priority of an application.” *Id.*, [0179], FIG. 5A. As Rao describes, this technique can be used to prioritize “data communications” of some applications over others (e.g., “real-time data communications” over data communications from “non-real-time data communication applications”), and can be used to “compliment Quality of Service (QOS) networks where network traffic prioritization occurs in intermediary network devices, such as switches and routers.” *Id.*, [0184].

41. An example of this system is shown in FIG. 5A (reproduced below).

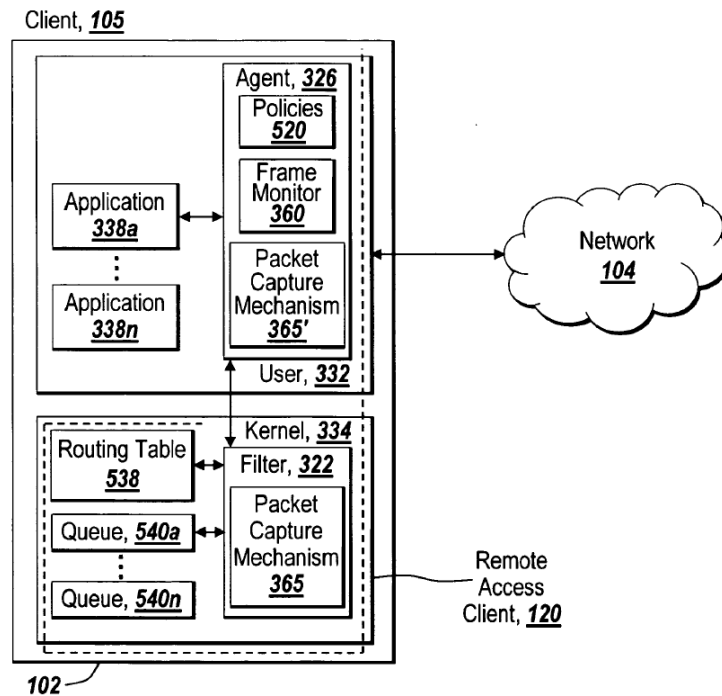


Fig. 5A

SAMSUNG-1005, FIG. 5A

42. In Rao's system, a "remote access client 105 of computing device 102 is connected to network 104" through one or more "LAN or WAN links" and/or "wireless connections." *Id.*, [0179]. Further, "[t]he client 105 may execute one or more applications 338 a-338 n, which access the network 104 via the agent 326 and filter 322 of the remote access client 120." *Id.* As examples, Rao's applications can communicate with one or more servers on the network 104, such as "an application server providing email services such as Microsoft Exchange," "a web or Internet server," "a desktop sharing server," or "a collaboration server." *Id.*, [0090].

43. Further, Rao's system implements "one or more policies 520 for specifying client-side prioritization of network communications related to applications 338 a-338 n." *Id.*, [0182]. These policies "may be specified by any suitable means and/or mechanisms." *Id.* For instance, these policies can "define prioritization" based on criteria such as:

- (i) "the name of the application,"
- (ii) "the type of application,"
- (iii) "the type of one or more protocols used by the application[s],"
- (iv) "the size of the payload of the network packet"
- (v) "whether an application is running in the foreground or the background of the client," and/or
- (vi) "the destination network address, such as host name or IP address, and/or destination port number." *Id.*

44. Rao deploys these policies by intercepting packets of network traffic by the applications, determining the priority of the packets based on the application that is associated with each packet, and selectively communicating the packets to the network based on the determined priority. *Id.*, [0184]-[0190], FIG. 5B.

550

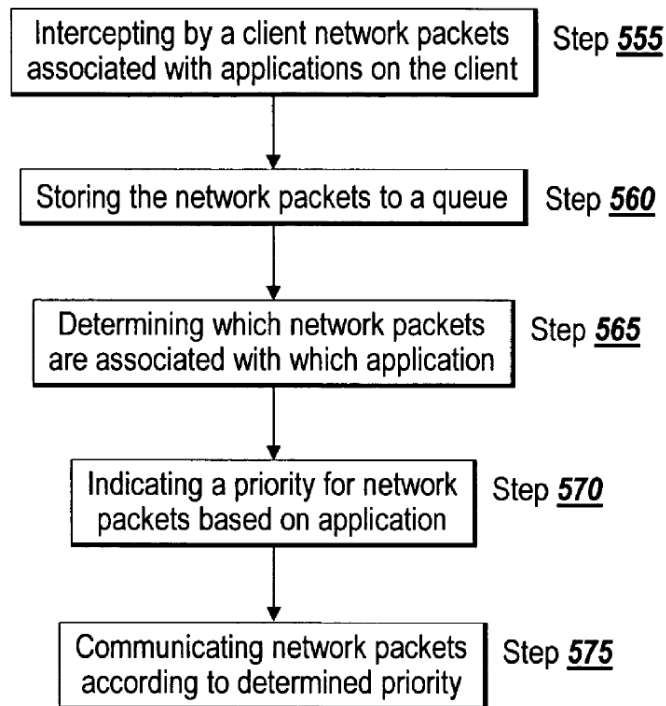


Fig. 5B

SAMSUNG-1005, FIG. 5A

45. In particular, Rao's system includes "a packet capture mechanism 365, 365' ... for intercepting network traffic of any of the applications 338 a-338 n of the client 105." *Id.*, [0080], [0184]-[0186], FIG. 5A.

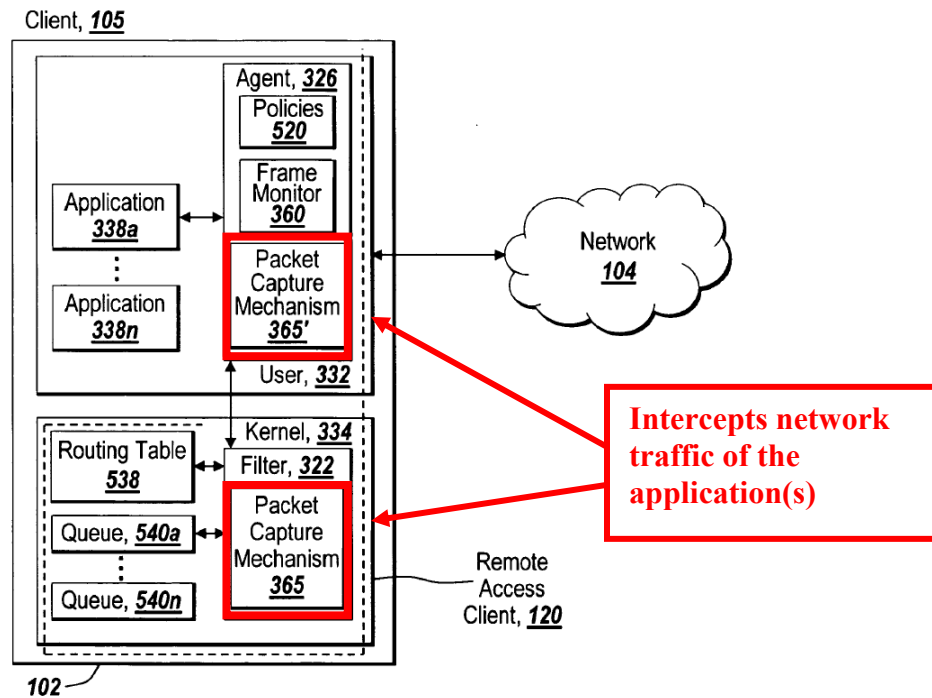


Fig. 5A

SAMSUNG-1005, FIG. 5A (annotated)

46. Further, Rao's system "determines the association of network packets with applications 338 a-338 n in order to determine priorities and apply any priority based policies 520." *Id.*, [0187].

47. Rao's system also determines information regarding each of the applications associated with the intercepted packets. For example, "the remote access client 120 may determine whether the application 338 a-338 n associated with the network packet is running in the foreground or the background of the client 105." *Id.*, [0188]. As further examples, "the remote access client 120 may determine any priorities, such as process task priority, assigned to the application

338 a-338 n by the operating system of the client 105” and/or “any other characteristics or statistics of the application 338 a-338 n such as size, memory usage, total execution time, and/or frequency of use.” *Id.*

48. Rao’s system prioritizes the intercepted packets based on one or more policies specified with respect to the applications. *Id.*, [0182].

49. In some cases, Rao’s system prioritizes the captured packets by allowing certain packets to be transmitted to the network. For example, Rao’s system can use “[a] filter 322 [to] place, arrange, or coordinate network packets into queues 540 a-540 n in support of the priorities.” *Id.*, [0191]. “[T]he network packets of the highest priority queue 540 a-540 n are communicated first, and then the next highest priority queue 540 a-540 n second, and so on.” *Id.*, [0194]. These “queues 540 a-540 n may be included in a network driver, such as an NDIS driver for the filter 322.” *Id.*, [0143], [0180].

50. In some cases, Rao’s system prioritizes the captured packets by blocking network packets from being transmitted to the network, either permanently or temporarily. *Id.*, [0102], [0207], [0040], [0194].

51. As an example, in some cases, Rao’s system blocks network packets from being transmitted to the network on a permanent basis, such as by “drop[ping] or accept[ing] the network packets depending on their content” (e.g., effectively deprioritizing those captured packets entirely) SAMSUNG-1005,

[0102]. For instance, the “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. *Id.* Further, Rao describes that its system can “use the policies 520 to determine which network packets to queue and/or discard.” *Id.*, [0207].

52. As another example, in some cases, Rao’s system blocks network packets from being transmitted to the network on a temporary basis, by “preventing ... at least one network packet of the second application from being communicated via the network stack ahead of the one or more network packets of the first application.” *Id.*, [0040]. In particular, a client can “hold[] ... in the queue a network packet associated with the second application, and releas[e] the held network packet upon communication of the one or more network packets associated with the first application prioritized ahead of the held network packet.” *Id.* See also *id.*, [0194].

53. Further, as Rao explains, “holding” network packets in this manner can be beneficial, for example, in “provid[ing] a packet by packet prioritization across all applications ... and intercepted network packets” and to implement prioritization according to different levels of “granularity.” *Id.*, [0191].

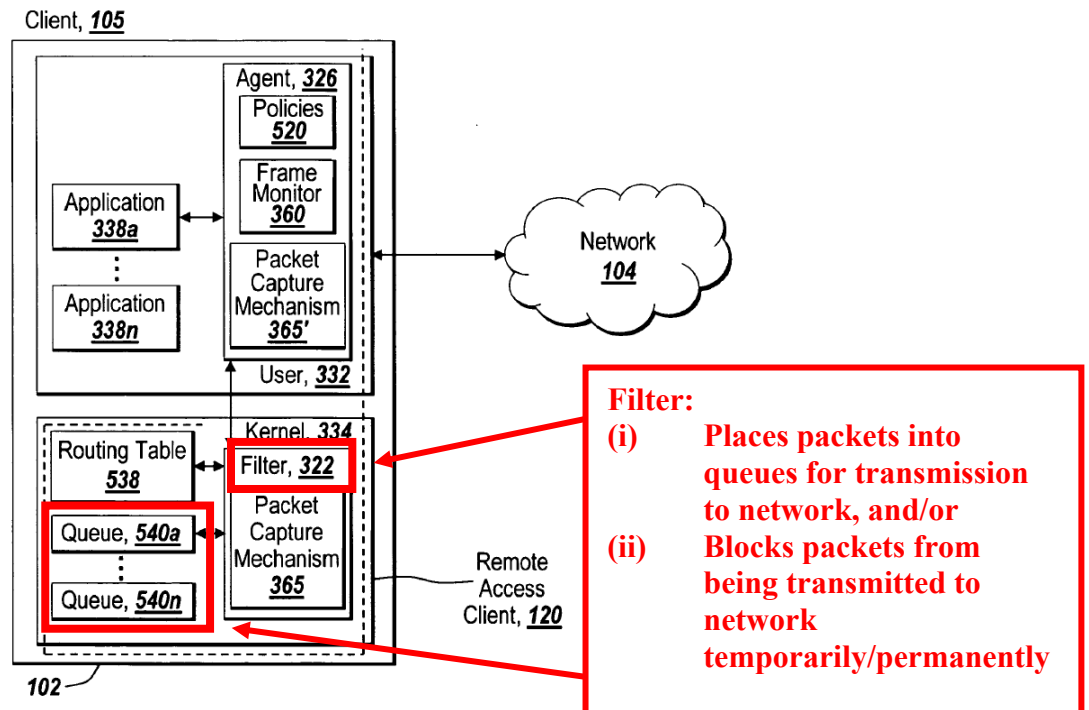


Fig. 5A

SAMSUNG-1005, FIG. 5A (annotated)

B. Overview of Oestvall

54. Oestvall describes “a method of enabling a multitasking computing device to preserve or conserve resources, such as battery power.” SAMSUNG-1006, [0002]. Oestvall’s method can be performed by “any kind of computing device,” including “radio telephones, smart phones, communicators, personal computers, lap top computers, game consoles, computers and application specific devices.” *Id.*, [0002].

55. In particular, Oestvall teaches that a device can classify applications with respect to various criteria, and selectively provide resources to the applications based on their classifications. *Id.*, [0008]-[0017], [0019]-[0025].

56. As an example, Oestvall describes that applications can be classified with respect to “‘trust’ or certification criteria—i.e. criteria which define the level of trustworthiness of the application.” *Id.*, [0010]. For instance, applications can be classified as (i) “untrusted” applications and (ii) “trusted” applications. *Id.*, [0015], FIG. 1.

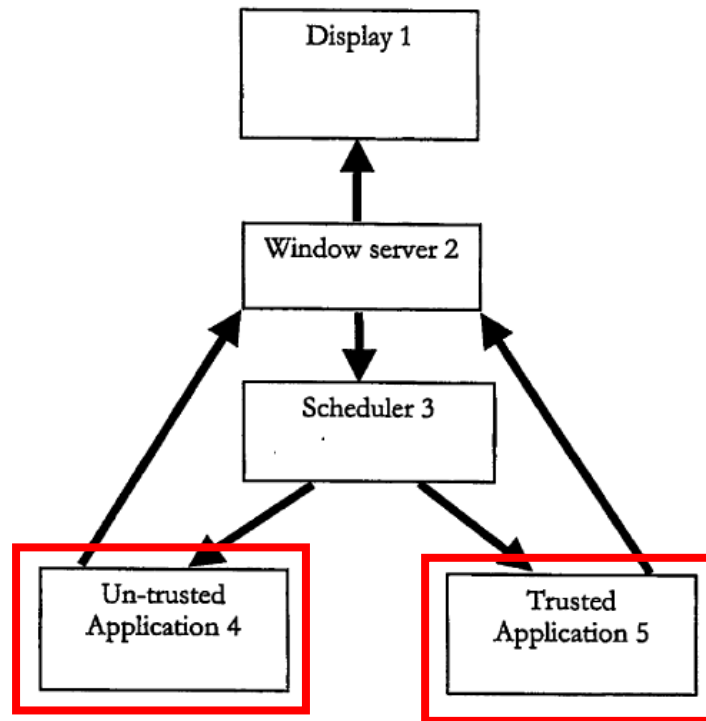


Figure 1

SAMSUNG-1006, FIG. 1 (annotated)

57. As another example, Oestvall describes that applications can be classified as “in the background or foreground on [a] display.” *Id.*, [0023]. Further, applications may switch between being in the background or the foreground of the display. *Id.*, [0014], [0021], [0025].

58. Further, Oestvall teaches that the device can provide resources to the applications differently, based on these classifications. *Id.*, [0010]-[0017], [0021]-[0025].

59. For example, Oestvall describes that the device can selectively:

- (i) Prevent an “untrusted” application in the background from running (e.g., by preventing the application from “being given any services or consuming any resources”) (*id.*, [0023]),
- (ii) Allow an “untrusted” application in the foreground to run (*id.*, [0021], [0025]), and
- (iii) Allow a “trusted” application to run, regardless of whether it is in the foreground or background (*id.*, [0015]).

60. That is, Oestvall’s device selectively provides resources to applications that it deems sufficiently important to consume resources (e.g., “trusted” applications and “untrusted” applications in the foreground), while selectively denying resources to applications that it deems not sufficiently important to consume resources (e.g., “untrusted” applications in the background).

61. As Oestvall describes, this method “is a valuable addition to power conservation strategies, especially (although without limitation) to battery operated devices.” *Id.*, [0024]. For example, the method can be performed to “prevent background untrusted applications from ‘polling’ for data over a wireless network,

an activity that can potentially drain a battery quickly.” *Id.* Accordingly, the “battery life” of the device is “increased.” *Id.*, [0009].

C. Overview of Montemurro

62. Montemurro describes “a policy-based mechanism to configure connections and routes” for “[c]ommunication devices capable of at least two communication modes (e.g. WLAN, WMAN and WWAN and/or wired modes).” SAMSUNG-1007, Abstract.

63. Montemurro’s system includes a “TCP/IP network stack 206A” having a “routing table 210” that specifies “which network interface 208 will be used for transmission of [a] packet” (e.g., WLAN 208A, WMAN 208B, and/or WWAN 208C managed by the connection table 206C). *Id.*, [0030], FIG. 2.

64. Further, Montemurro’s system includes “a 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 (also referenced as network interfaces) 208.” *Id.*, [0027]. Specifically, the “rules engine 206A configures (i.e. modifies, periodically in response to changes of state and the evaluation of its rules) connection table 206C and routing table 210 to optimize the flow of communications over multiple communications modes (e.g. interfaces 208 and respective networks 104 and

106)... to ensure that data goes out [sic] the most appropriate network (via respective interface 208).” *Id.*, [0034]-[0035].

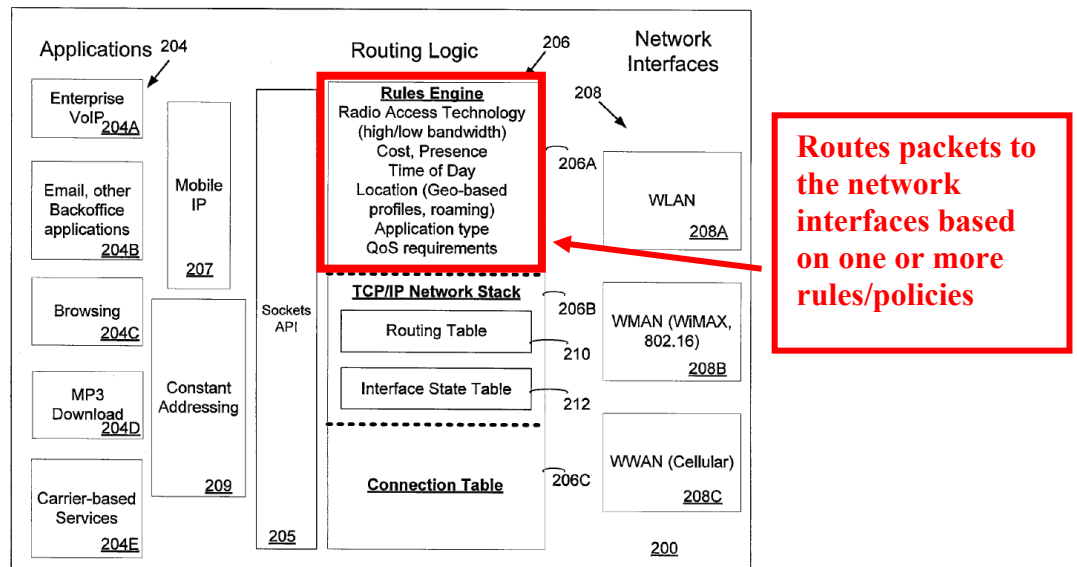


Figure 2

SAMSUNG-1007, FIG. 2 (annotated)

65. In general, the “[r]ules engine 206A configures the communication operations with a set of rules/policies,” which can “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.* Further, these “rules/policies” can specify that certain applications use certain types of networks under certain conditions. *Id.*, [0019].

66. As Montemurro describes, these “rules/policies” can be used “to optimize communications for multi-mode capable devices” by accounting for

“different radio access technologies,” each of which may have “different properties ... such as bandwidth, range, cost, and power consumption, among other considerations.” *Id.*, [0030].

D. Combination of Rao, Oestvall, and Montemurro

67. A POSITA would have found it obvious to modify Rao’s system of prioritizing network packets based on the specific application classification criteria taught by Oestvall and Montemurro. *See* Sections IX.A-C. Combining Rao, Oestvall, and Montemurro 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.

68. In particular, a POSITA would have recognized (i) that Rao, Oestvall, and Montemurro are directed to similar operations having similar purposes (e.g., controlling an application’s access to a network in order to preserve limited system resources), and (ii) that Oestvall and Montemurro provide specific classification criteria for achieving specific technical benefits (e.g., reducing battery consumption in a network-enabled device and optimizing communications using multiple different networks, respectively).

1. *Both Rao's system and Oestvall's system selectively allow and block network traffic from applications based on certain criteria*

69. Rao's system includes several applications configured to transmit network packets to a network (e.g., the Internet via one or more wireless connections). *See* Section IX.A; SAMSUNG-1005, [0095],[0125], [0179]. Rao's system controls each of the applications' access to the network by intercepting packets of network traffic by the applications, determining the priority of the packets based on the application that is associated with each packet, and selectively communicating the packets to the network based on the determined priority. SAMSUNG-1005, [0184]-[0190], FIG. 5B.

70. In particular, Rao's system prioritizes network packets by implementing one or more policies 520 for controlling network traffic. SAMSUNG-1005, [0182]. These policies can "define prioritization" based on various criteria, such as:

- (i) "the name of the application,"
- (ii) "the type of application,"
- (iii) "the type of one or more protocols used by the application[s],"
- (iv) "the size of the payload of the network packet"
- (v) "whether an application is running in the foreground or the background of the client," and/or

- (vi) “the destination network address, such as host name or IP address, and/or destination port number.” *Id.*, [0182].

71. Further, based on these policies, Rao’s system can selectively use a filter to (i) allow network packets to be transmitted to the network or (ii) block the network packets from being transmitted to the network, either permanently or temporarily. *Id.*, [0191], [0194], [0207].

72. For instance, Rao’s system can allow network packets to be transmitted to the network by using “[a] filter 322 [to] place, arrange, or coordinate network packets into queues 540 a-540 n in support of the priorities” and transmitting the network packets from those queues. *Id.*, [0191]. Specifically, these network packets can be placed into a “highest priority queue,” such that the network packets are allowed, i.e., immediately transmitted to the network (e.g., prior to the transmission of network packets placed into lower priority queues). *Id.*, [0194].

73. Further, Rao describes that its system can prioritize the captured packets by blocking network packets from being transmitted to the network, either permanently or temporarily. For example, Rao describes that its system can “use the policies 520 to determine which network packets to queue and/or discard,” such that the network packets are either allowed or blocked on a permanent basis. *Id.*, [0207]. 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., *id.*, [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 or system resources (e.g., memory) are selectively freed up for higher priority packets/communications.

74. For instance, a POSITA would have understood or found it obvious to configure Rao’s system 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 by dropping them) *Id.*, As an example, the “filter 322” can be used to “discard[] packets” having the lowest priority (e.g., “unwanted packets”), such that the packets are permanently blocked from being transmitted to the network. *Id.*

75. Like Rao, Oestvall describes an application-based priority system for controlling access to resources. SAMSUNG-1006, [0008]-[0017], [0019]-[0025]. Further, Oestvall contemplates similar criteria as Rao, and teaches that specific combinations of these criteria can be selected to achieve a specific technical benefit. *Id.*, [0008]-[0017], [0019]-[0025].

76. In particular, Oestvall teaches that certain types of applications (e.g., “untrusted” applications) that are running in the background of the client should be assigned a low priority, such that they cannot access a network. *Id.*, [0008], [0014]-[0017], [0021], [0023], [0024].

77. Further, Oestvall teaches that certain other types of applications (e.g., “trusted” applications) should be assigned a high priority, such that they can continue to access a network. *Id.*, [0008], [0014]-[0017], [0021], [0023], [0024].

78. As Oestvall describes, these combinations of criteria can be used to “prevent background untrusted applications from ‘polling’ for data over a wireless network, an activity that can potentially drain a battery quickly.” *Id.*, [0024].

2. *A POSITA would have been led to modify Rao’s system to allow/block an application’s network traffic based on the application’s “trusted/untrusted” status as taught by Oestvall to thereby reduce battery drain*

79. A POSITA would have readily recognized that Rao’s remote access client 120 could use a filter to discard packets from background untrusted applications, thereby effectively deprioritizing those packets entirely. In doing so, the Rao’s remote access client 120 would prevent the packets from being communicated over network 104 and, as a consequence, increase the battery life of a mobile device client 105 as taught by Oestvall. Indeed, while Oestvall teaches increasing battery life by preventing such applications from running and thereby

engaging in any network communications, a POSITA would have recognized that the power usage associated with using a wireless modem to transmit network packets to a network far exceeds the power usage associated with an application generating those network packets. For example, Pedersen describes that the performance of mathematical computations on network packets using network coding algorithms consumes substantially less energy compared to the wireless transmission of bits. *See, generally*, SAMSUNG-1010. As Pedersen explains, “we see that the network coding itself has nearly no impact on the overall energy consumption compared to the wireless part.” *Id.*, 6. Accordingly, a POSITA would have readily recognized that Rao’s system could be used to enable a similar increase in battery life by specifically preventing the battery draining activity identified by Oestvall – i.e., by specifically preventing the network/packet communications that result in excessive drain of the battery of a wireless device.

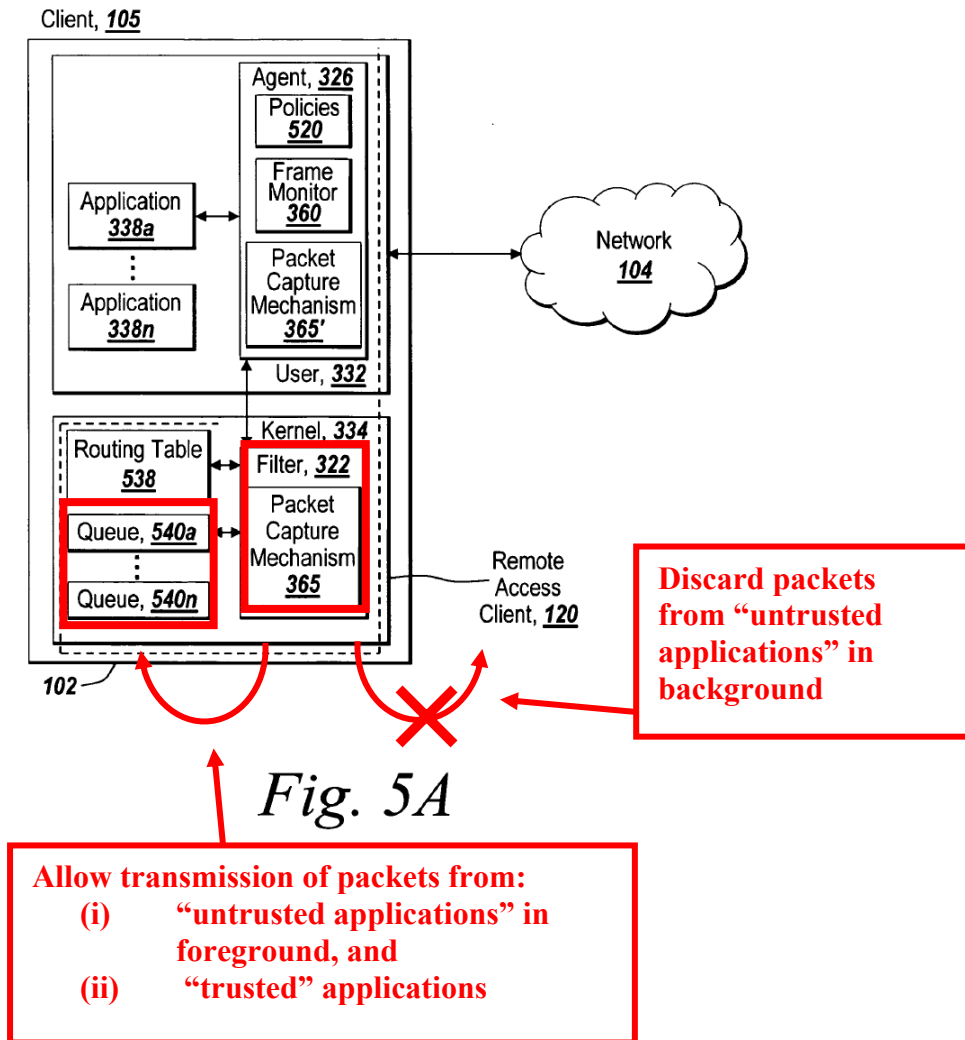
80. That is, a POSITA would have recognized that Rao’s system is ready for improvement in this way based on Oestvall’s teachings and that such an improvement would enable the system to not only provide the benefits identified by Rao but also provide the additional benefit taught by Oestvall of increased battery life when client 105 is a wireless mobile device. Moreover, this increase in battery life would be obtained without necessitating a complete shutdown of the application as disclosed by Oestvall. In particular, a POSITA would have

recognized, based on Rao, that a system system can reduce battery drain while controlling the network activities of applications to a much greater degree of granularity than offered by Oestvall's relatively blunt approach of completely shutting down applications to achieve this benefit.

81. As an example of this modification, a POSITA would have configured Rao's "filter 322" to selectively block network packets and/or transmit network packets to the network, specifically based on the criteria specified by Oestvall. In particular, the "filter 322" would selectively "discard[]" network packets from applications that are "untrusted" and running in the background (e.g., a classification of applications that should be assigned a low priority, as taught by Oestvall). Accordingly, these applications can no longer poll for data over a wireless network (i.e., an activity that Oestvall teaches as being particularly burdensome on a battery).

82. Further, the "filter 322" would selectively allow the transmission of network packets from applications that are either (i) "untrusted" and running in the foreground or (ii) "trusted," regardless of whether they are running in the foreground or the background (e.g., classifications of applications that should be assigned a high priority, as taught by Oestvall). Accordingly, applications that are sufficiently important can continue to exchange data in accordance with one or more Internet services.

83. An example modification to Rao's system in view of Oestvall's teachings ("Rao-Oestvall system") is shown below.



SAMSUNG-1005, FIG. 5A (annotated)

84. While the Rao-Oestvall system reduces battery drain by blocking an application's transmission of network packets on a permanent basis as taught by Rao (as distinguished from shutting down the application entirely to reduce battery drain as taught by Oestvall), a POSITA also would have found it obvious to configure the Rao-Oestvall system to additionally or alternatively selectively block

network packets on a temporary basis as also taught by Rao, in at least some situations where more granular control of battery draining activities is desired.

85. For example, Rao describes that its system can block network packets from being transmitted to the network on a temporary basis, by “preventing ... at least one network packet of the second application from being communicated via the network stack ahead of the one or more network packets of the first application.” SAMSUNG-1005, [0040]. In particular, a client can “hold[] ... in the queue a network packet associated with the second application, and releas[e] the held network packet upon communication of the one or more network packets associated with the first application prioritized ahead of the held network packet,” such that the transmission of the network packet is temporarily delayed. *Id.* See also *id.*, [0194]. As Rao explains, “holding” network packets in this manner can be beneficial, for example, in “provid[ing] a packet by packet prioritization across all applications ... and intercepted network packets” and to implement prioritization according to different levels of “granularity.” *Id.*, [0191].

86. A POSITA would have recognized that such a “holding” of network packets of lower priority applications until the packets of higher priority applications have been transmitted, increases the likelihood that the battery will have sufficient remaining energy to ensure that the transmission of the packets of the higher priority applications is successful, thereby preferentially allocating the

limited battery energy resource to those higher priority applications over the lower priority applications. This enables lower priority applications, such as “untrusted” applications in the background, to still be able to communicate over the network but to do so in accordance with their lower level of priority and without interfering with the activities of other applications having higher priorities, such as “untrusted” applications in the foreground or “trusted” applications.

87. Accordingly, consistent with Rao’s teachings, the system can control the battery draining activities of applications according to a greater degree of granularity than offered by Oestvall alone and, in doing so, achieve a similar reduction in battery drain while also minimizing disruption to the operation of the applications.

3. *Like Rao, Montemurro’s system selectively regulates network traffic from applications based on certain criteria*

88. Like Rao, Montemurro describes an application-based priority system for controlling access to resources. SAMSUNG-1007, Abstract, [0011], [0027]-[0036]. Further, Montemurro contemplates similar criteria as Rao, and teaches that specific combinations of these criteria can be selected to achieve a specific technical benefit. *Id.*, Abstract, [0011], [0027]-[0036].

89. In particular, like Rao, Montemurro describes that controlling an application’s access to a network based at least in part on (i) the “application type,”

(ii) the “destination IP address” of the traffic, and (iii) the protocol for transmitting data (e.g., wireless protocols for transmitting data over the WLAN, WWAN, etc.). *Id.*, [0029], [0054]. Regarding network protocols specifically, Rao describes that its system can “be used in any other types of networking environments with other networking protocols” (SAMSUNG-1005, [0182], [0082]), of which Montemurro’s wireless protocols are an example.

90. Based on these factors (among others), Montemurro’s system selects a particular network interface for transmitting packets by that application. For instance, a “rules engine 206A executes and modifies, as applicable, the routing table 210 to ensure that data goes out [sic] the most appropriate network (via respective interface 208).” SAMSUNG-1007, [0035]. Further, various “rules/policies” can be deployed to selectively allow certain types of applications to access certain networks, while preventing those applications from accessing other networks. *Id.*, [0029].

91. As Montemurro explains, these “rules/policies” can be used “to optimize communications for multi-mode capable devices” by accounting for “different radio access technologies,” each of which may have “different properties ... such as bandwidth, range, cost, and power consumption, among other considerations.” *Id.*, [0030].

4. *A POSITA would have been led to additionally modify the Rao-Oestvall system to apply different policies depending on which network is selected to handle an application's network traffic as taught by Montemurro*

92. A POSITA would have further modified the Rao-Oestvall system to allow/block an application's network traffic based on the type of network to which a device is connected as taught by Montemurro. Specifically, a POSITA would have recognized that Montemurro teaches considering at least some of the same factors as Rao when determining whether to allow or block an application's network traffic (e.g., the "application type," the "destination IP address" of the traffic, and the protocol for transmitting data). *See* Sections IX.A and IX.C. Further, a POSITA would have recognized based on Montemurro's teachings that using these factors (among others) to select an appropriate type of network for transmitting the data would optimize "multi-mode capable devices" (e.g., by accounting for "different radio access technologies," each of which may have "different properties ... such as bandwidth, range, cost, and power consumption, among other considerations"). SAMSUNG-1007, [0030].

93. In particular, in Rao's system, a remote access client 120 includes a "routing table 538 compris[ing] information about a source computing device and a destination computing device to identify a communication path or connection between a source and destination communication points" on the network.

SAMSUNG-1005, [0181]. Further, Rao describes that a system can be connected to a network using “one or more “LAN or WAN links” and/or “wireless connections. *Id.*, [0179]. To the extent that Rao does not expressly describe using the “routing table 538” to select between different “communication paths” that include a wireless LAN link or a wireless WAN link, a POSITA nevertheless would have found it obvious to modify the “routing table 538” to make such a selection in view of Montemurro.

94. As an example of this modification, in at least some implementations, a POSITA would have configured Rao’s system to include multiple sets of queues, where each set corresponds to a different network interface (e.g., network interfaces for accessing a WWAN, WLAN, etc.). This is because a POSITA would have understood or recognized that Rao’s single set of queues is used to prioritize network traffic for a *single* network at a time (e.g., the “network 104” which is described as being one of “a local-area network (LAN), such as a company Intranet, a metropolitan area network (MAN), or a wide area network (WAN), such as the Internet or the World Wide Web,” *id.*, [0095]), and that in situations in which the device is connected to *multiple* networks concurrently (e.g., WWAN, WLAN, etc., as described by Montemurro), a different respective set of queues could be used to prioritize network traffic for each network specifically. For instance, a POSITA would have recognized that this would allow the system to

prioritize data in a manner that is specifically tailored to the properties of each network and/or the usage conditions of each network (e.g., the degree of which each network is congested). Indeed, a POSITA would have recognized that the purpose of prioritizing network packets relative to one another is to optimize the transmission of the network packets over a specific network (e.g., taking into account the properties and/or usage conditions of that network), and that it would not have made sense to commingle network packets intended for transmission using different networks in a common set of queues, as this would have resulted in least some network packets being prioritized according to the properties and/or usage conditions of networks to which they are not intended to be transmitted. As an alternative, a POSITA would have recognized that network packets can be prioritized using sets of queues that are specific to each network, such that network packets can be prioritized relative to only other network packets that are intended for transmission over the same network, in order to better account for the properties and/or usage conditions of each network individually.

95. Further, in view of Montemurro, a POSITA would have configured Rao's routing table 538 in at least some implementations such that a given communication generated by an application (e.g., one or more packets) would be selectively routed by the remote access client 120 to a certain network (e.g., WWAN, WLAN, etc.) or blocked from a network based on criteria such as (i) the

“application type,” (ii) the “destination IP address” of the traffic, and (iii) the protocol for transmitting data. According to this configuration, the “packet capture mechanism 365, 365” would intercept network packets generated by the applications (step 1 below). Upon the system selecting a particular network that is appropriate for one or more packets (step 2 below), those packets would be provided to the set of queues corresponding to the selected network for prioritization and transmission (e.g., in accordance with the Rao-Oestvall combination, as described above) (see steps 3a, and 3b below). Conversely, upon determining that a particular network is not appropriate for the one or more packets, the packets would not be provided to the set of queues corresponding to that network and that network’s policies would not be applied.

96. An example modification to the Rao-Oestvall system in view of Montemurro’s teachings (“Rao-Oestvall- Montemurro combination” or “ROMC”) is shown below.

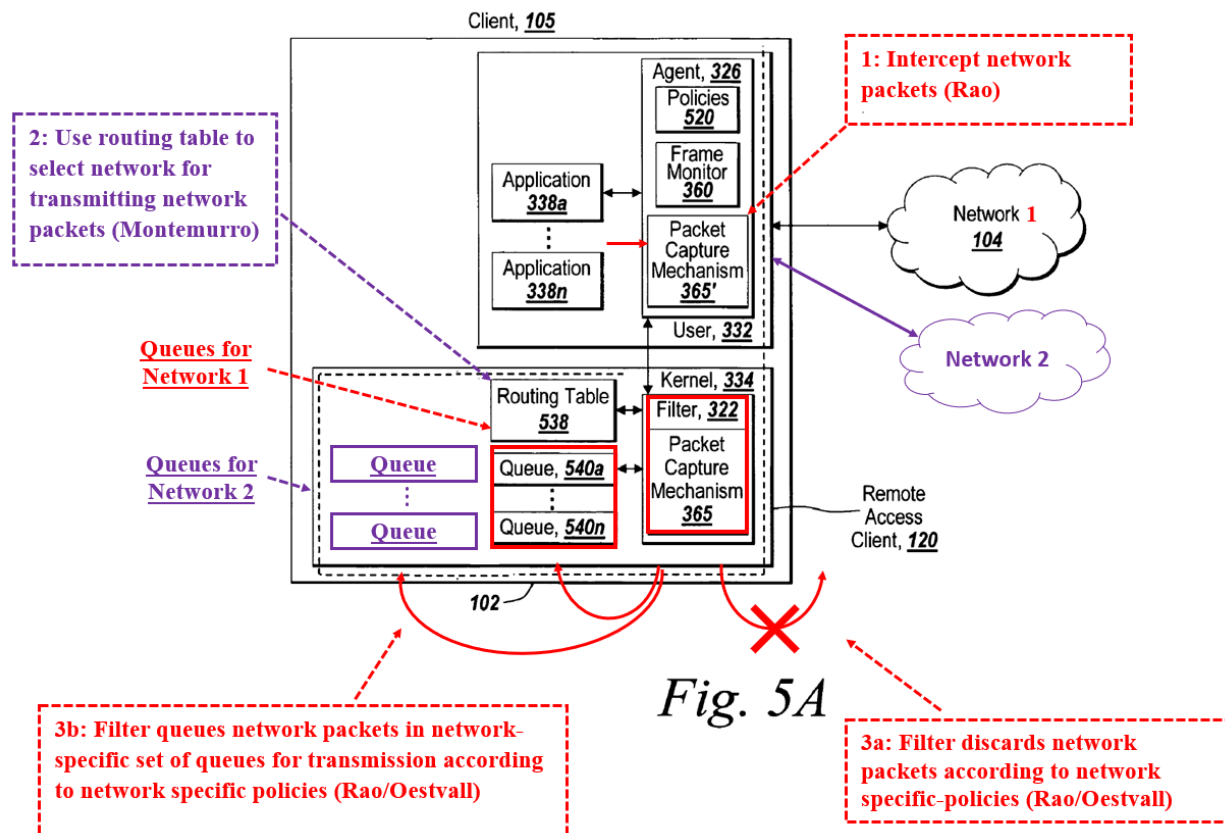


Fig. 5A

SAMSUNG-1005, FIG. 5A (revised and annotated)

97. In doing so, a POSITA would have been led to apply Montemurro's techniques to thereby enable Rao's system to intelligently select among the various networks to optimize "multi-mode capable devices," such as by accounting for "different radio access technologies," each of which may have "different properties ... such as bandwidth, range, cost, and power consumption, among other considerations." SAMSUNG-1007, [0030]. Further, by modifying Rao's system to first perform Montemurro's network selection prior to prioritizing network traffic according to the Rao-Oestvall combination, the combined system would

enjoy both the “multi-mode” optimization benefits taught by Montemurro and the application-specific network prioritization benefits as taught by Rao and Oestvall.

98. For instance, in view of Montemurro, if a first network (e.g., WWAN) is selected from among multiple networks to transmit an application’s network traffic, a POSITA would have found it obvious to apply a first policy specific to the first network to the network traffic. As an example first policy, the device would selectively place network packets in a set of queues that are *specific to the first network* in order to selectively allow or block an application’s network traffic with respect to the first network. For instance, a POSITA would have found it obvious to allow or block network traffic from applications based on the application’s “trusted/untrusted” status (e.g., as taught by Oestvall) and whether the application is running in the foreground or the background) (e.g., as taught by both Oestvall and Rao). *See* Section IX.D. 2.

99. Further, if a second network (e.g., a WLAN) is selected from among multiple networks to transmit an application’s network traffic instead, a POSITA would have found it obvious to apply a second *different* policy *specific to the second network* in order to selectively allow or block an application’s network traffic with respect to the second network. As an example second policy, the device would selectively place network packets in a set of queues that are *specific to the second network* in order to selectively allow or block an application’s

network traffic with respect to the second network. That is, the first and second policies would differ at least because the first and second policies selectively place network packets in different respective sets of queues.

100. A POSITA would have found it obvious, in some cases, to configure the second policy in a similar manner as the first policy (i.e., with the exception that the policies selectively place network packets in different respective sets of queues). For example, a POSITA would have recognized or understood that if the characteristics of the first and second networks are similar to another, the second policy could likewise be configured to allow or block network traffic from applications based on the application's "trusted/untrusted" status (e.g., as taught by Oestvall) and whether the application is in running in the foreground or the background) (e.g., as taught by both Oestvall and Rao) as with the first policy. *See* Section IX.D.2.

101. A POSITA also would have found it obvious, in some cases, to configure the second policy in a different manner as the first policy. For example, a POSITA would have found it obvious to modify the second policy (e.g., relative to the first policy) to account for any differences in the bandwidth and/or cost between using the first and second networks to transmit data (e.g., as taught by Montemurro). As an example, a POSITA would have found it obvious to make the second policy more restrictive (e.g., if the second network were more expensive

and/or has a smaller bandwidth than the first network), or make the second policy less restrictive (e.g., if the second network were less expensive and/or has a larger bandwidth than the first network). This is because a POSITA would have understood or recognized that policies for prioritizing network traffic are used to make better use of limited resources, and that if those resource limitations were less for a particular network, the policies could be modified to adapt the device's usage of that network to account for that difference.

102. Accordingly, a POSITA would have found using such a combination of classifications as a basis for prioritizing network communications of applications as one obvious way to balance the well-known, market-based desire to improve a user's experience with an application, with the similarly well-known desire to adapt to the different performance characteristics of different types of networks.

E. Analysis of Claims 1, 2, 4-9, 14, 16, 19, 20, 23, and 26

1. *Claim 1*

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

103. The Rao-Oestvall-Montemurro combination ("ROMC") renders obvious [1pre].

104. For example, Rao describes a device that is configured to communicate data wirelessly with a WAN and the Internet, such as to obtain email

services, access a web or Internet service, access a desktop sharing server, and/or access a collaboration server (*wireless end-user device*). SAMSUNG-1005, [0090], [0125]; Section IX.A.

[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

105. ROMC renders obvious [1a].

106. Rao describes a device that is configured to communicate data wirelessly with a WWAN and the Internet (e.g., using a “wireless network adapter” and/or a “modem”) (*WWAN modem*). SAMSUNG-1005, [0125].

107. Further, Rao describes that the device is configured to communicate data for Internet service activities via the WWAN, such as to obtain email services, access a web or Internet service, access a desktop sharing server, and/or access a collaboration server (*communicate data for Internet service activities between the device and at least one WWAN, when configured for and connected to the WWAN*). *Id.*, [0090].

108. To the extent that Rao does not expressly describe a “WWAN modem,” a POSITA would have understood or found it obvious to implement a WWAN modem in Rao’s system in view of Rao’s teaching that (i) a device can access a WAN or the Internet wirelessly, and (ii) a “modem” can be used to interface the device with “any type of network.” *Id.*, [0125]. Further, network

configurations for mobile devices that enabled WWAN connectivity via modems were conventional by the Critical Date. For example, Cole 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-1010, [0035], FIG. 2.

[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

109. ROMC renders obvious [1b].

110. Rao describes a device that is configured to communicate data wirelessly with a WLAN and the Internet (e.g., using a “wireless network adapter” and/or a “modem”) (*WLAN modem*). SAMSUNG-1005, [0125].

111. Further, as I explained in [1a], Rao describes that the device is configured to communicate data for Internet service activities via the WLAN, such as to obtain email services, access a web or Internet service, access a desktop sharing server, and/or access a collaboration server (*communicate data for Internet service activities between the device and at least one WLAN, when configured for and connected to the at least one WLAN*). *Id.*, [0090].

112. To the extent that Rao does not expressly describe a “WLAN modem,” a POSITA would have understood or found it obvious to implement a

WLAN modem in Rao's system in view of Rao's teaching that (i) a device can access a LAN or the Internet wirelessly, and (ii) a "modem" can be used to interface the device with "any type of network." *Id.*, [0125]. Further, a POSITA would have understood that connections provided by the WLAN modem can be used to access the Internet. *Id.*, [0125] ("the computing device 102 may include a network interface 118 to interface to ... the Internet through a variety of connections including, but not limited to, ... LAN or WAN links (e.g., 802.11, T1, T3, 56 kb, X.25), ... wireless connections, or some combination of any or all of the above").

113. Further, Montemurro also describes that "[c]ommunication devices [are] capable of at least two communication modes (e.g. WLAN, WMAN and WWAN and/or wired modes)." SAMSUNG-1007, Abstract. To the extent that Rao does not expressly describe a "WLAN modem," a POSITA would have found it obvious to modify Rao's system to include a "WLAN modem" in order to provide the device with multiple communications modes (e.g., to allow the device to connect to multiple types of networks), as taught by Montemurro.

114. Further, network configurations for mobile devices that enabled WLAN connectivity via modems were conventional by the Critical Date. For example, Cole 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-1010, [0035], FIG. 2.

[1c] one or more processors configured to

115. ROMC renders obvious [1c].

116. Rao describes “a computing device useful for practicing an embodiment of the [subject matter described by Rao].” SAMSUNG-1005, [0118], FIG. 1D.

117. As Rao describes, “[e]ach computing device 102 includes a central processing unit [121]”² (**one or more processors**) that includes “any logic circuitry that responds to and processes instructions fetched from the main memory unit 104.” *Id.*, [0118]. *See also id.*, [0121] (“main processor 100”); FIG. 1E.

² Rao [0118] erroneously refers to the “central processing unit” as “102,” rather than “121” as depicted in FIG. 1D.

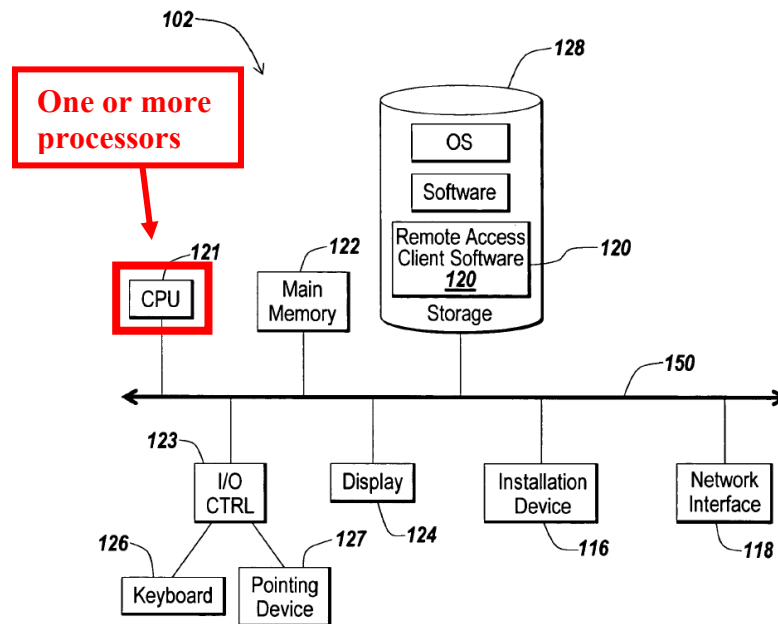


Fig. 1D

SAMSUNG-1005, FIG. 1D (annotated)

118. Further, as I explain below, a POSITA would have found it obvious to perform various operations using the processors. See [1d]-[1h], [2], [6]-[12], [14], [16]-[17], [19], [22], [26].

[1d] classify, as a first classification, whether data for Internet service activities is to be communicated through the WWAN modem or the WLAN modem

119. ROMC renders obvious [1d].

120. As I explained in Section IX.D.4, in view of Montemurro, a POSITA would have configured Rao's routing table 538 in at least some implementations

such that a given communication generated by an application (e.g., one or more packets, constituting *data for Internet service activities*) would be selectively routed by the remote access client 120 to a certain network (e.g., WWAN, WLAN, etc.). In doing so, the ROMC system would *classify, as a first classification, whether data for Internet service activities is to be communicated through the WWAN modem or the WLAN modem* in order to allow an application to access the selected network. *See also* [1a], [1b].

[1e] classify, as a second classification, whether [i] a particular application associated with an Internet service access request, and [ii] capable of both interacting with a user in a user interface foreground of the device, and at least some Internet service activities when not interacting with a user in the device user interface foreground, [iii] is interacting with the user in the device user interface foreground

121. ROMC renders obvious [1e], which includes features [1e(i)], [1e(ii)] and [1e(iii)].

122. Regarding [1e(i)], Rao describes that an application can communicate with one or more servers on the network 104, an example of which is the Internet. SAMSUNG-1005, [0090], [0095], [0125]. Further, Rao describes that an application can access services provided by a server 102e connected to the network 104 (i.e., the Internet), such as those provided by “an application server providing email services such as Microsoft Exchange,” “a web or Internet server,” “a desktop

sharing server,” or “a collaboration server” (*a particular application associated with an Internet service access request*). SAMSUNG-1005, [0090]; FIG. 1A.

123. In particular, in Rao, an application may attempt to access an Internet service by transmitting packets to that Internet service (*Internet service access request*). *See, e.g., id.*, [0179], [0184].

124. A POSITA would have understood or found it obvious that Rao contemplates its applications being “associated with an Internet service access request” based on Rao’s teachings of its applications communicating over the Internet and receiving service from servers. *Id.*, [0090]. That is, based on these teachings, a POSITA would have understood or found it obvious that Rao’s applications would be configured to send packetized communications over the Internet to such servers requesting access to their corresponding services (*an Internet service access request*) to enable such applications to receive mail, Web, and/or other data content. *Id.*, [0090].

125. Regarding [1e(ii)], as I explained above, Rao describes that applications can request access to Internet services. *Id.*, [0090]. Further, Rao describes that an application may be “running in the foreground or the background of the client.” *Id.*, [0182]. *See also id.*, [0188]-[0189]. A POSITA would have understood or found it obvious that Rao’s applications envision interactions with users in the foreground (e.g., such that the user can engage in email, web, desktop

sharing, and/or collaboration activities) (*capable of ... interacting with a user in a user interface foreground of the device*).

126. Further, Rao contemplates that applications that are running in the background may perform at least some Internet service activities, such as by generating network packets (*capable of ... at least some Internet service activities when not interacting with a user in the device user interface foreground*). *Id.*, [0003]. For example, a POSITA would have understood or found it obvious that Rao's email application can perform Internet service activities in the background (e.g., polling an email server for updates and/or retrieving emails in the background). *Id.*, [0003], [0090].

127. To the extent that Rao does not expressly describe that an application would be capable of both (i) interacting with a user in a user interface foreground of the device, and (ii) at least some Internet service activities when not interacting with a user in the device user interface foreground, this feature would have been obvious in view of Oestvall. For example, Oestvall describes that a device includes applications that are capable of both:

- (i) Running the "foreground" and "present[ing] a user interface with which a user can interact" (*interacting with a user in a user interface foreground of the device*), and

- (ii) Running in the “background” and “not being interacted with by an end-user and ... present[ing] no user interface with which a user could interact (but it could for example present an icon indicating its presence and the fact that it was still active)” (***not interacting with a user in the device user interface foreground***). SAMSUNG-1006, [0006], [0015].

128. Further, Oestvall describes that an application can perform network activities, and that applications may be capable of consuming “resources” (e.g., by performing network service activities such as “‘polling’ for data over a wireless network”) when in the background (***capable of ... at least some ... activities when not interacting with a user in the device user interface foreground***). *Id.*, [0023]-[0024].

129. In view of Oestvall, a POSITA would have understood or found it obvious that Rao’s applications can interact with users in the foreground by “present[ing] a user interface with which a user can interact” in order to allow users to engage in activities such as email, web, desktop sharing, and/or collaboration) (***“interacting with a user in a user interface foreground of the device”***). *Id.*, [0006].

130. Further, in view of Oestvall, a POSITA would have understood or found it obvious that Rao’s applications can perform Internet service activities

(e.g., an email application polling an email server for updates and/or retrieving emails), even if the user is not interacting with the application and/or the application is not presenting a user interface with which a user could interact ***(capable of ... at least some Internet service activities when not interacting with a user in the device user interface foreground)***. *Id.*, [0024].

131. Regarding [1e(iii)], Rao describes that the device classifies “whether an application is running in the foreground or the background of the client 105” ***(classify, as a second classification, whether a particular application ... is interacting with the user in the device user interface foreground)***. SAMSUNG-1005, [0182], [0188]-[0189].

132. Oestvall also describes that the device uses a “window server component 2 ... to determine if an application is in the background or foreground on display” ***(classify, as a second classification, whether a particular application ... is interacting with the user in the device user interface foreground)***.

SAMSUNG-1006, [0008], [0016]-[0017], [0022]-[0023].

[1f] apply a differential traffic control policy to the Internet service access request, based on (i) the first and second classifications performed by the one or more processors, and (ii) a differential traffic control policy list distinguishing between a first one or more applications resident on the device and a second one or more applications resident on the device,

133. ROMC renders obvious [1f].

134. Rao describes that an application is associated with an *Internet service access request*. [1e].

135. Further, a POSITA would have found it obvious to select a particular network to transmit an application's network traffic in accordance with the Internet service access request, and apply a particular differential traffic control policy to the Internet service access request based on the selected network (*apply a differential traffic control policy to the Internet service access request based on the first classification performed by the one or more processors*). See Section IX.D.4; [1d].

136. As an example, in view of Montemurro, if a first network (e.g., WWAN) is selected to transmit an application's network traffic, a POSITA would have found it obvious to apply a first policy specific to the first network to the network traffic. Further, if a second network (e.g., a WLAN) is selected to transmit an application's network traffic instead, a POSITA would have found it obvious to apply a second different policy specific to the second network instead.

137. Further, upon selecting a network and a corresponding policy, a POSITA would have found it obvious, in at least some implementations, to apply the selected policy by allowing or blocking an applications' network traffic (*applying a differential traffic control policy to the Internet service access request*) based on whether the application is running in the foreground or the

background (... *based on the second classification performed by the one or more processors*) (e.g., as taught by both Oestvall and Rao) and the application's "trusted/untrusted" status (...*and distinguishing between a first one or more applications resident on the device and a second one or more applications resident on the device*) (e.g., as taught by Oestvall). See Section IX.D.4.

138. For example, a POSITA would have found it obvious to configure the ROMC system to prioritize network packets according to one or more policies for controlling network traffic, as taught by Rao. SAMSUNG-1005, [0182]. These policies can "define prioritization" based on various criteria, including:

- (i) "the name of the application,"
- (ii) "the type of application,"
- (iii) "the type of one or more protocols used by the application[s],"
- (iv) "the size of the payload of the network packet"
- (v) "whether an application is running in the foreground or the background of the client," and/or
- (vi) "the destination network address, such as host name or IP address, and/or destination port number." SAMSUNG-1005, [0182].

139. Specifically, in applying Rao's policies to differentially distinguish how the network traffic of distinct applications will be handled, Rao's system

considers any one or more of the above criteria, including “whether an application is running in the foreground or the background of the client” (... *based on the second classification performed by the one or more processors*). SAMSUNG-1005, [0182].

140. Further, by also considering the “type[s]” of applications and/or differently named applications, among other criteria, the application of Rao’s policies for handling application traffic is further based on *distinguishing between a first one or more applications resident on the device and a second one or more applications resident on the device*. SAMSUNG-1005, [0182].

141. Rao describes that “[t]he policies ... may comprise any type and format of syntax and/or language for specifying a policy, and may be provided via any type and/or form of medium,” which a POSITA would have understood would encompass one or more lists (*a differential traffic control policy list*). SAMSUNG-1005, [0183]. However, to the extent that Rao does not expressly describe representing these applications in the form of a list, a POSITA nevertheless would have found it obvious to implement such a list, as they would have recognized that a list is a commonplace “format of syntax and/or language” for enumerating data.

142. Further, in accordance with its policies, Rao’s system selectively uses a filter to (i) allow network packets to be transmitted to the network or (ii) block

the network packets from being transmitted to the network, thereby applying the policies to the Internet service access request embodied by those network packets.

SAMSUNG-1005, [0191], [0194], [0207]. *See also* [1e]; Section IX.D.4.

143. To the extent that Rao alone does not expressly describe applying a differential traffic control policy based on the second classification and the differential traffic control policy list, these features nevertheless would have been obvious further in view of Oestvall.

144. Like Rao, Oestvall describes an application-based priority system for controlling access to resources. SAMSUNG-1006, [0008]-[0017], [0019]-[0025]. Further, Oestvall contemplates at least some of the same criteria as Rao, and teaches that specific combinations of these criteria can be selected to achieve a specific technical benefit. SAMSUNG-1006, [0008]-[0017], [0019]-[0025].

145. Specifically, Oestvall describes that applications can be classified based on “‘trust’ or certification criteria” (*a differential traffic control policy list*) as (i) “untrusted” applications (...*distinguishing between a first one or more applications resident on the device*) and (ii) “trusted” applications (... *and a second one or more applications resident on the device*). SAMSUNG-1006, [0010], [0015], FIG. 1.

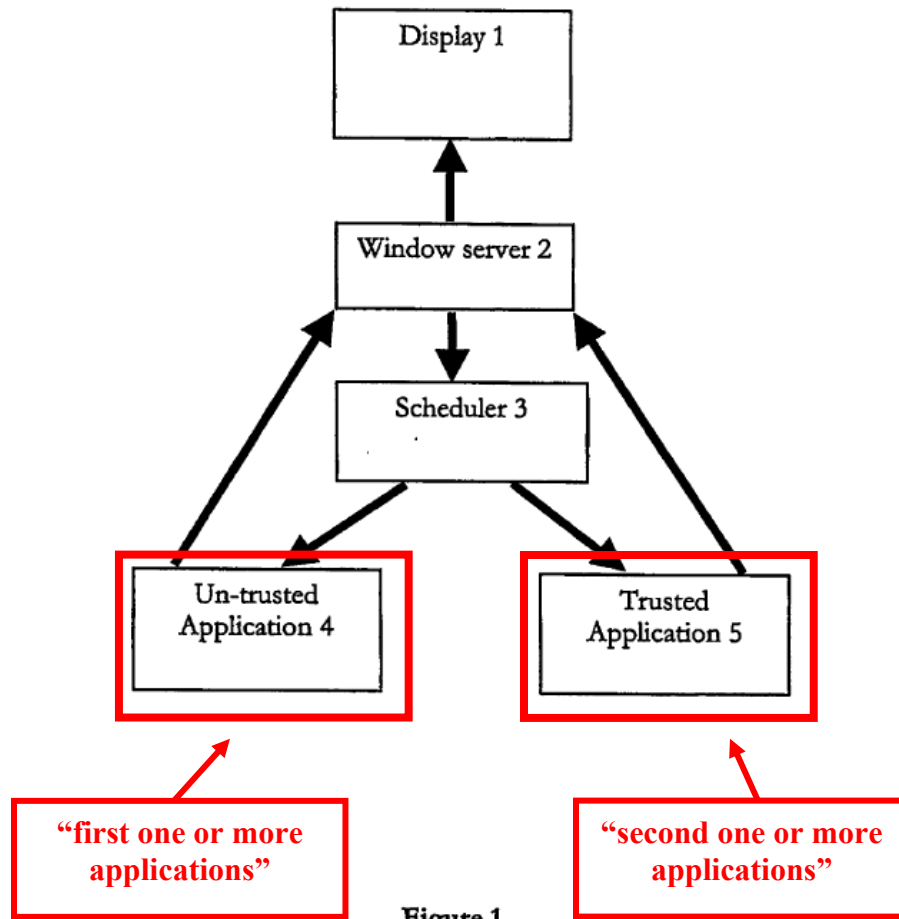


Figure 1

SAMSUNG-1006, FIG. 1 (annotated)

146. To the extent that Oestvall does not expressly describe representing these applications in the form of a list, a POSITA nevertheless would have found it obvious to implement such a list, as they would have recognized that a list is a commonplace format of syntax and/or language for enumerating data.

147. Further, like Rao, Oestvall describes that applications can be classified as “in the background or foreground on [a] display” (*performing the second classification*). SAMSUNG-1006, [0023]. *See also* [1e].

148. In addition, Oestvall describes applying a traffic control policy to an application differently, depending on these classifications (*apply a differential traffic control policy to the Internet service access request*). For example, Oestvall’s system denies resources to applications that are not sufficiently important to consume resources, and provides resources to applications that are sufficiently important to consume resources (e.g., to selectively allow certain applications to “‘poll[]’ for data over a wireless network”). SAMSUNG-1006, [0008], [0010], [0015]-[0017], [0022]-[0025].

[1g] such that, when the particular application is one of the first one or more applications, the one or more processors are operable to block the Internet service access request in a first state of the first and second classifications, wherein data for Internet service activities is classified as to be provided through the WWAN modem, and the particular application is not classified as interacting with a user in the device user interface foreground

149. ROMC renders obvious [1g].

150. As I explained in Section IX.D.4 and [1f], a POSITA would have found it obvious to (i) select a particular network to transmit an application’s network traffic in accordance with the Internet service access request and (ii) apply

a particular differential traffic control policy to the Internet service access request based on the selected network and the characteristics of the application.

151. For example, in view of Montemurro, if a WWAN is selected from among multiple networks to transmit an application's network traffic (*a first state of the first ... classifications, wherein data for Internet service activities is classified as to be provided through the WWAN modem*), a POSITA would have found it obvious to apply a policy specific to the WWAN to the network traffic.

152. Further, upon selecting the WWAN, the ROMC system would, in at least some implementations, prioritize the application's network packets based on the specific application classification criteria taught by Rao and Oestvall.

153. In particular, the "filter 322" would selectively "discard" network packets (*block the Internet service access request*) from applications that are "untrusted" (...*when the particular application is one of the first one or more applications*) and running in the background (*in a first state of the ... second classifications, wherein ... the particular application is not classified as interacting with a user in the device user interface foreground*) (e.g., a classification of applications that should be assigned a low priority, as taught by Oestvall). See Section IX.D.4.

154. Thus, when the application is "untrusted" (*one of the first one or more applications*) and selected for WWAN communications and in the

background (*first state of the first and second classifications*), the network packets—and its corresponding Internet service access request—would be blocked permanently. See Section IX.D.4. Accordingly, these applications can no longer poll for data over a wireless network (i.e., an activity that Oestvall teaches as being particularly burdensome on a battery). See Section IX.D.4; SAMSUNG-1006, [0024].

[1h] allow the Internet service access request under at least one different state of the first and second classifications

155. ROMC renders obvious [1h].

156. As I explained in [1g], upon selecting the WWAN, the ROMC system would, in at least some implementations, prioritize the application’s network packets based on the specific application classification criteria taught by Rao and Oestvall.

157. In particular, the “filter 322” would selectively “allow” network packets (*allow the Internet service access request*) when the application is “untrusted” (*one of the first one or more applications*) and selected for WWAN communications and in the foreground (...*under at least one different state of the first and second classifications*). The allowance of the network packets over the WWAN would occur, for example, as a result of the “untrusted” application

changing from being in the background to being in the foreground and thereby enjoying a higher priority per Rao's and Oestvall's teachings. *See* Section IX.D.4.

158. In particular, by virtue of the application now being in the foreground, these network packets would be placed into a "highest priority queue," thereby having their communication be unfettered as taught by Oestvall such that the network packets are immediately transmitted to the network (e.g., prior to the transmission of network packets placed into lower priority queues). SAMSUNG-1005, [0194]; Section IX.D.4. Indeed, in view of Oestvall, a POSITA would have found it obvious in at least some implementations to treat untrusted applications that are running in the foreground identically to trusted applications (regardless of whether they are running in the foreground or the background), and would have treated network packets from each of these applications similarly. Accordingly, applications that are sufficiently important can continue to exchange data in accordance with one or more Internet services. *See* Section IX.D.4; [1f].

2. *Claim 2*

[2] *The wireless end-user device of claim 1, wherein the one or more processors are configured to classify that the particular application is interacting with the user in the device user interface foreground when the user of the device is directly interacting with that application or perceiving any benefit from that application.*

159. ROMC renders obvious [2].

160. As I explained in [1e], in ROMC, a device classifies “whether an application is running in the foreground or the background of the client 105,” as taught by Rao. SAMSUNG-1005, [0182], [0188]-[0189]. Further, Rao describes that, in at least some cases, “an application [that] is running in the foreground [is] currently in active use by the user.” SAMSUNG-1005, [0003].

161. As I also explained in also discussed in [1f]-[1g], in ROMC, the device performs this classification upon generating and intercepting a network packet by the application, in order to determine the priority of that network packet.

162. Accordingly, a POSITA would have understood or found it obvious that, when the ROMC device classifies that “an application is running in the foreground ... of the client 105,” this classification would be performed based on the *current state* of the application (e.g., at the time that the packet was generated and intercepted by the ROMC system, such that the network packet can be accurately prioritized). Specifically, this classification would be performed ***when a user of the device is directly interacting with that application*** (e.g., by engaging in “active use” of the application, as taught by Rao) and/or is ***perceiving any benefit from that application*** (e.g., by viewing the application as it is running in the foreground and/or perceiving that the application is ready for input by the user, as also taught by Rao). SAMSUNG-1005, [0003].

163. As I also explained in [1e], Oestvall describes that the device uses a “window server component 2 ... to determine if an application is in the background or foreground on display.” SAMSUNG-1005, [0008], [0016]-[0017], [0022]-[0023]. Further, the device performs this classification upon an application requesting access to an Internet service. [1e]. Oestvall additionally describes that “[a] foreground application ... present[s] a user interface with which a user can interact.” SAMSUNG-1006, [0006].

164. A POSITA would have understood or found it obvious that, when the ROMC device classifies that “an application is in the ... foreground on display,” this classification would be performed based on the *current state* of the application. Specifically, this classification would be performed ***when a user of the device is directly interacting with that application*** (e.g., by interacting with a user interface of the application, as taught by Oestvall) and/or is ***perceiving any benefit from that application*** (e.g., by viewing the user interface as it is running in the foreground and/or perceiving that the application is ready for input by the user via a presented user interface, as also taught by Oestvall). SAMSUNG-1006, [0006].

165. Further, the use of user interface priority in coordinating application operation was well-known before the Critical Date. For example, Singh (SAMSUNG-1012) describes a “window management function [that] determine[s] a relationship of windows with one another.” SAMSUNG-1012, 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. *Id.*

166. As another example, Freund (SAMSUNG-1009) 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-1009, 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 key strokes).” SAMSUNG-1009, 10:40-44. A POSITA would have known that mouse clicks and

key strokes 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 4*

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

167. ROMC renders obvious [4].

168. As I explained in [1f], in ROMC, a device would apply a differential traffic control policy to the Internet service access request. For example, Rao contemplates prioritizing network packets by implementing one or more policies for controlling network traffic (*a differential traffic control policy*). SAMSUNG-1005, [0182]; [1f].

169. Further, Rao describes that a system can “provide a configuration mechanism such as a user interface, graphical or otherwise, design and constructed for configuring or specifying the policies” (*a user interface ... to inform a user of the wireless end-user device when there are options to set, control, override, or modify service usage controls that affect the differential traffic control policy and/or the differential traffic control policy list*). SAMSUNG-1005, [0183].

170. A POSITA would have understood or found it obvious that the ROMC device provides a user interface that enables a user to set, control, override, and/or modify one or more aspects of Rao’s policies, in order to provide a user with a greater degree of control over the manner in which network packets are prioritized.

4. *Claim 5*

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

171. ROMC renders obvious [5].

172. As I explained in Section IX.D.4 and [1f], a POSITA would have found it obvious to (i) select a particular network to transmit an application’s network traffic in accordance with the Internet service access request and (ii) apply a particular differential traffic control policy to the Internet service access request based on the selected network and the characteristics of the application (*wherein*

the differential traffic control policy is part of a multimode profile having different policies for different networks).

173. For instance, in view of Montemurro, if a first network (e.g., WWAN) is selected from among multiple networks to transmit an application's network traffic, a POSITA would have found it obvious to apply a first policy specific to the first network to the network traffic. As an example first policy, the device would selectively place network packets in a set of queues that are specific to the first network to selectively allow or block an application's network traffic with respect to the first network.

174. Further, if a second network (e.g., a WLAN) is selected from among multiple networks to transmit an application's network traffic instead, a POSITA would have found it obvious to apply a second different policy specific to the second network to selectively allow or block an application's network traffic with respect to the second network. That is, the first and second policies would differ at least because the first and second policies selectively place network packets in different respective sets of queues.

175. This configuration would allow the system "to optimize communications for multi-mode capable devices" by accounting for "different radio access technologies," each of which may have "different properties ... such as

bandwidth, range, cost, and power consumption, among other considerations,” as taught by Montemurro. SAMSUNG-1007, [0030].

5. *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 a network type of a network connection currently in use by the wireless end-user device.*

176. ROMC renders obvious [6].

177. As I explained in Section IX.D.4 and [1f], a POSITA would have found it obvious to (i) select a particular network to transmit an application’s network traffic in accordance with the Internet service access request and (ii) apply a particular differential traffic control policy to the Internet service access request based on the selected network and the characteristics of the application.

178. As an example, in view of Montemurro, if a particular network (e.g., WWAN or WLAN) is selected from among multiple networks to transmit an application’s network traffic, a POSITA would have found it obvious to apply a policy specific to the first network to the network traffic during use of the first network by the application (*select a traffic control policy from the multimode profile based at least in part on a network type of a network connection currently in use by the wireless end-user device*) such that the network traffic is continuously or periodically provided to the appropriate set of queues and transmitted to the first network without delay. *See* Section IX.D.4; [5].

179. This configuration would allow the system “to optimize communications for multi-mode capable devices” by accounting for “different radio access technologies,” as taught by Montemurro. SAMSUNG-1007, [0030].

6. *Claim 7*

[7] The wireless end-user device of claim 6, wherein the one or more processors are further configured to, when the network type of a 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

180. ROMC renders obvious [7].

181. As I explained in [5] and [6], in view of Montemurro a POSITA would have found it obvious to configure the ROMC system such that it applies different “rules/policies” for controlling network traffic for different networks (*multimode profile*).

182. Further, Montemurro teaches that when a device is connected to a WLAN (*when the network type of a network connection is at least one type of WLAN connection*), the device can select from among different policies or rules to control network traffic (*select a traffic control policy from the multimode profile based on a type of network connection from the WLAN to the Internet*).

183. For instance, as shown in FIG. 3, Montemurro describes that when a device is connected to a “WWAN” (SAMSUNG-1007, FIG. 3, 302), the device can route network traffic differently across the WLAN and to the Internet

depending on the time of day. Specifically, during work hours, “a virtual private network (VPN) connection is established via Internet 112 between the device 102 and an enterprise server” (a first *type of network connection from the WLAN to the Internet*). *Id.*, [0040]. In contrast, during non-work hours, “a SIP connection to the user's appropriate “home” server (e.g. a backend server 120 providing SIP services) is established for SIP services when the user is not working” (a second *type of network connection from the WLAN to the Internet*). *Id.*, [0041]. In doing so, the device would route network traffic differently (*select a traffic control policy from the multimode profile*) based at least in part on whether network traffic from the WLAN to the Internet is to be provided via a “VPN connection” or a “SIP connection” (...*based at least in part on a type of network connection from the WLAN to the Internet*).

184. This configuration would allow the system to intelligently route network traffic to an appropriate network (e.g., a work network or a home network) depending on the type of work that the user is likely to be performing at a given time.

7. Claim 8

[8] The wireless end-user device of claim 1, wherein the one or more processors are further to apply the differential traffic control policy such that, when the particular application is one of the second one or more applications, the one or more processors are operable to allow the Internet service access request when data for Internet service activities is classified

as to be provided through the WWAN modem, and the particular application is not classified as interacting with a user in the device user interface foreground.

185. ROMC renders obvious [8].

186. As I explained in [1g], upon selecting the WWAN (*when data for Internet service activities is classified as to be provided through the WWAN modem*), the ROMC system would, in at least some implementations, prioritize the application's network packets based on the specific application classification criteria taught by Rao and Oestvall.

187. In particular, the “filter 322” would selectively “allow” network packets (apply the differential traffic control policy by allowing the Internet service access request) from applications that are “trusted” (*...when the particular application is one of the second one or more applications*), even if those applications are running in the background (*...and the particular application is not classified as interacting with a user in the device user interface foreground*) (e.g., a classification of applications that should be assigned a higher priority, as taught by Oestvall). *See* Section IX.D.4.

188. In particular, by virtue of an application being a “trusted” application, its network packets would be placed into a “highest priority queue,” thereby having their communication be unfettered as taught by Oestvall such that the network packets are immediately transmitted to the network (e.g., prior to the transmission

of network packets placed into lower priority queues). SAMSUNG-1005, [0194];
Section IX.D.4. Accordingly, applications that are sufficiently important can
continue to exchange data in accordance with one or more Internet services. *See*
Section IX.D.4; [1f].

8. *Claim 9*

[9] *The wireless end-user device of claim 1, wherein the one or more processors are to apply the differential traffic control policy to one of but not both of a WWAN modem connection to a roaming WWAN network and a WWAN modem connection to a home WWAN network*

189. ROMC renders obvious [9].

190. As discussed in [1a], Rao discloses a WWAN.

191. Similarly, Montemurro also discloses a WWAN. SAMSUNG-1007, [0011], [0013], [0028]. Further, Montemurro discloses that, depending on the location, a network can be a “roaming” network. SAMSUNG-1007, [0029].

192. In view of Montemurro, a POSITA would have understood that a WWAN network can include a portion that is a ***home WWAN*** (e.g., not “roaming”) and a portion that is a ***roaming WWAN***, depending on the location.

193. As I explained in [1c], [1d], and [1f], and Section IX.D.4, the ROMC system includes ***one or more processors configured to apply the differential traffic control policy*** to an Internet service access request based on a classification whether data for Internet service activities is to be communicated through the WWAN modem or the WLAN modem.

194. Further, as modified by Montemurro, the ROMC system would selectively apply the differential traffic control policy depending on whether data communication for Internet service activities is provided by a roaming WWAN or a home WWAN.

195. In particular, as I explained in Section IX.D.4, a POSITA would have found it obvious to modify Rao-Oestvall system to further consider the type of network(s) to which a device is connected and available for use by the device, as taught by Montemurro, in order to improve the prioritization of network traffic by the device, while also accounting for the characteristics of a network. For example, as Montemurro teaches, several factors can be considered in determining whether a network is appropriate for an application's network traffic, including "bandwidth" of that network and/or the "cost" that is associated with using that network. SAMSUNG-1008, [0030].

196. In view of Montemurro, a POSITA would have applied different differential traffic control policies, depending on which network is selected to transmit an application's network traffic. For instance, if a roaming WWAN were selected from among multiple networks to transmit an application's network traffic, a POSITA would have found it obvious to apply a first policy specific to the roaming WWAN (e.g., the differential traffic control policy, as introduced in [1f]). As an example first policy, in at least some implementations, the device

would selectively place network packets in a set of queues that are specific to the roaming WWAN in order to selectively allow or block an application's network traffic with respect to the roaming WWAN.

197. Further, if a home WWAN is selected from among multiple networks to transmit an application's network traffic instead, a POSITA would have found it obvious to apply a second, ***different*** policy specific to the home WAN network (*i.e.,, **not apply the differential traffic control policy**, and instead apply a ***different*** differential traffic control policy*). As an example second policy, in at least some implementations, the device would selectively place network packets in a set of queues that are specific to the home WWAN in order to selectively allow or block an application's network traffic with respect to the home WWAN. That is, a second and ***different*** policy would be applied at least because the second policy selectively places network packets in a different set of queues compared to the first policy. Accordingly, a particular differential traffic control policy would be ***applied to one of but not both of a WWAN modem connection to a roaming WWAN network and a WWAN modem connection to a home WWAN network.***

9. Claim 14

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

198. ROMC renders obvious [14].

199. As I explain in [1f], in ROMC, a device would apply a differential traffic control policy to the Internet service access request. For example, Rao contemplates prioritizing network packets by implementing one or more policies for controlling network traffic (*the differential traffic control policy*). SAMSUNG-1005, [0182]; [1f].

200. Further, Rao describes that these policies “may be provided by or downloaded via a gateway.” SAMSUNG-1005, [0183]. For example, “[t]he policies 520 may comprise any type and format of syntax and/or language for specifying a policy, and may be provided via any type and/or form of medium, such as electronically by one or more network packets or via a file, such as an XML file.” SAMSUNG-1005, [0183].

201. In view of Rao, POSITA would have understood or found it obvious that a device can specify at least some of its policies, such as adding new policies (*update the differential traffic control policy and/or the differential traffic control policy list*), by downloading and implementing policies from a gateway, such as in the form of a network packet or file (*...based on information received from a network element*). For example, a POSITA would have recognized that such a configuration would allow for centralized control and/or remote administration of multiple devices in prioritizing network packets, and/or would

allow devices to maintain up-to-date policies with which to prioritize network packets.

10. *Claim 16*

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

202. ROMC renders obvious [16].

203. As I explain in [1f] and [1g], the ROMC device will ***selectively block the Internet service access request*** in a first state of the first and second classifications.

204. Further, Rao describes that the device includes a “network stack 310” that “include[s] one or more network drivers.” SAMSUNG-1005, [0100], FIG. 1C. Further, Rao describes that network packets can be communicated “via a secure socket layer.” SAMSUNG-1005, [0035].

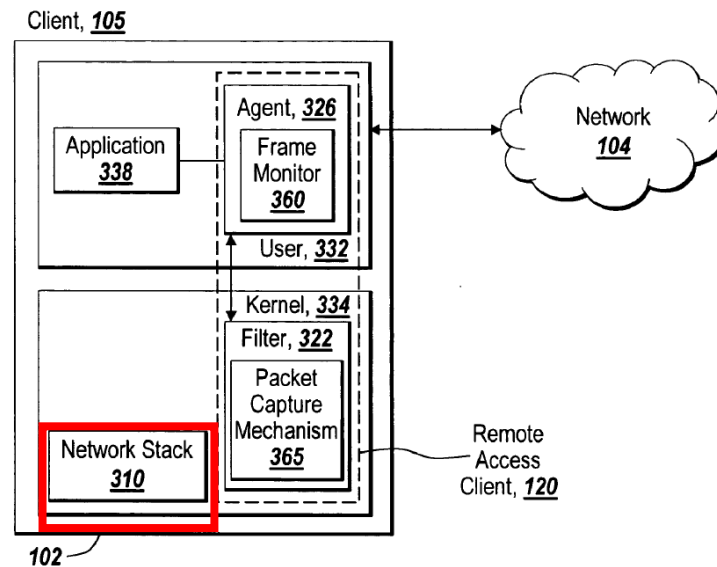


Fig. 1C

SAMSUNG-1005, FIG. 5A (annotated)

205. Rao teaches that the device “may intercept network packets of one or more applications 338 a-338 n transparently to the application 338 a-338 n ... and any of the network layers of a network stack.” SAMSUNG-1005, [0185]. Rao teaches that such a blocking technique is beneficial in that it allows the prioritization technique to “support any type of application 338 a-338 n on the client 105.” SAMSUNG-1005, [0185].

206. In view of Rao, a POSITA would have understood or found it obvious that the ROMC 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 or found it obvious that such requests could

include requests to the network stack to open, connect to, and/or write data to a socket (e.g., using the “secure socket layer”) (*open, connect, and/or write requests by the particular application to a network stack*). 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 the Internet service access request by intercepting open, connect, and/or write requests by the particular application to a network stack*), as performing such an operation would allow Rao’s prioritization technique to “support any type of application” on a device, as taught by Rao.

11. *Claim 19*

[19] The wireless end-user device of claim 1, wherein the one or more processors are configured to classify that the particular application is interacting with a user in the device user interface foreground based on a state of user interface priority for the application

207. ROMC renders obvious [19].

208. As I explained in [1e], in ROMC, the device classifies “whether an application is running in the foreground or the background of the client 105,” as taught by Rao. SAMSUNG-1005, [0182], [0188]-[0189].

209. Further, Oestvall describes that an application’s user interface can have a different *state of user interface priority*, depending on whether it is in the foreground or the background. SAMSUNG-1006, [0006]. For instance, when the application is in the background, the user interface has a low state of priority, such

that the user interface is relegated to an icon (e.g., “[a]n application is in the background if it is not being interacted with by an end-user and it presents no user interface with which a user could interact (but it could for example present an icon indicating its presence and the fact that it was still active.”) SAMSUNG-1006, [0006].

210. Further, when the application is in the foreground, the user interface has a high state of priority, such that the user interface is presented to the user for interaction (e.g., “A foreground application conversely does present a user interface with which a user can interact.”). SAMSUNG-1006, [0006].

211. A POSITA would have understood or found it obvious that, when the ROMC device classifies “whether an application is running in the foreground or the background of the client 105,” this classification could be efficiently implemented *based on a state of a user interface priority of that application* (e.g., by assessing the state of the user interface priority for the application, such as whether the application’s user interface is visible, is available for interaction with a user, and/or is merely represented by an icon, as taught by Oestvall). SAMSUNG-1006, [0006]. Moreover, the use of states of user interface priority in coordinating application operation was well known before the Critical Date and a POSITA would have found obvious the use of states of user interface priority for classification in Rao-Oestvall. SAMSUNG-1012, 9:19-35.

212. The use of user interface priority in coordinating application operation was well known before the Critical Date. For example, Singh (SAMSUNG-1012) describes a “window management function [that] determine[s] a relationship of windows with one another.” SAMSUNG-1012, 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. *Id.*

12. *Claim 20*

[20] The wireless end-user device of claim 1, wherein the second one or more applications are not subject to a differential network access control that is applicable to the first one or more applications.

213. ROMC renders obvious [20].

214. As I explained in Section IX.D.4 and [1f], a POSITA would have found it obvious to modify Rao’s system of prioritizing network packets based on the specific application classification criteria taught by Oestvall and the network

criteria taught by Montemurro. In particular, a POSITA would have found it obvious to modify Rao's system to prioritize network packets (provide a *differential network access control*) for "untrusted" applications (*first one or more applications*) in a particular manner (e.g., blocking the applications' attempt to access a WWAN when the applications are running the background). *See* [1g]. Further, a POSITA would have found it obvious to modify Rao's system to prioritize network packets (provide a *differential network access control*) for "trusted" applications (*second one or more applications*) in a different manner (e.g., allowing the applications to access a WWAN instead). *See* [8]. Accordingly, the "trusted" applications (*second one or more applications*) would *not be subject to a differential network access control* that is applicable to the "untrusted" applications (*first one or more applications*).

13. *Claim 23*

[23] The wireless end-user device of claim 1, wherein the second one or more applications comprises foreground services.

215. ROMC renders obvious [23].

216. As I explained in [1e], the ROMC system can include "trusted" applications (*second one or more applications*). Further, as described by both Rao and Oestvall, an application can provide services in the foreground.

217. For example, Rao describes that applications can request access to Internet services. SAMSUNG-1005, [0090]. Further, Rao describes that an

application may be “running in the foreground” (...*comprising foreground services*). SAMSUNG-1005, [0182]. *See also* SAMSUNG-1005, [0188]-[0189].

218. Similarly, Oestvall describes that application can interact with users in the foreground by “present[ing] a user interface with which a user can interact” in order to allow users to engage in activities such as email, web, desktop sharing, and/or collaboration (...*comprising foreground services*). SAMSUNG-1006, [0006].

14. *Claim 26*

[26] The wireless end-user device of claim 1, wherein the at least one different classification state comprises a state wherein data for Internet service activities is classified as to be provided through the WWAN modem, and the particular application is classified as interacting with a user in the device user interface foreground.

219. ROMC renders obvious [26].

220. As I explained in Section IX.D. 4 and [1h], the ROMC system would allow the Internet service access request under at least one different state of the first and second classifications.

221. Specifically the ROMC system would allow network packets when the application is “untrusted” and selected for WWAN communications (*the at least one different classification state comprises a state wherein data for Internet service activities is classified as to be provided through the WWAN modem*) and

in the foreground (*...and the particular application is classified as interacting with a user in the device user interface foreground*). [1h].

**X. [GROUND 2] - RAO-OESTVALL-MONTEMURRO-ARAUJO
MAKES CLAIMS 10-12, 15, 17, 18, 22, and 25 OBVIOUS**

A. Overview of Araujo

222. Araujo describes “a power-management policy” for managing a “machine's power usage.” SAMSUNG-1008, Abstract. Araujo’s device classifies programs with respect to various criteria, and selectively provides resources to the programs based on their classifications. *Id.*, [0027]. In particular, the device determines “[w]hether a program is permitted to consume power ... based on a finding as to whether the program's status justifies the consumption of power under the circumstances that are present.” *Id.* For example, programs “may have a status that reflects its worthiness to consume power,” such as a “‘VIP’ status that allows them to consume power in situations where other programs would not.” *Id.*

223. Further, the device provides resources to the applications differently, based on whether the applications are “worthy” to consume power. *Id.*, [0024]. For example, 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]. In response, the device selectively performs various operations with respect to the request, including “[a]llowing” or

“[b]locking” the request based on a power management policy. *Id.*, [0035], [0050], FIG. 3 (302), FIG. 4 (406).

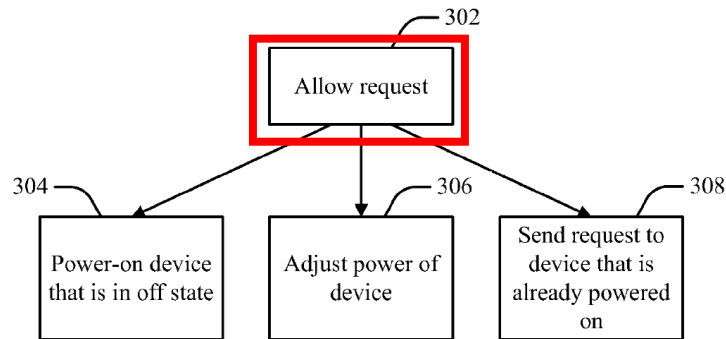


FIG. 3

SAMSUNG-1008, FIG. 3 (annotated)

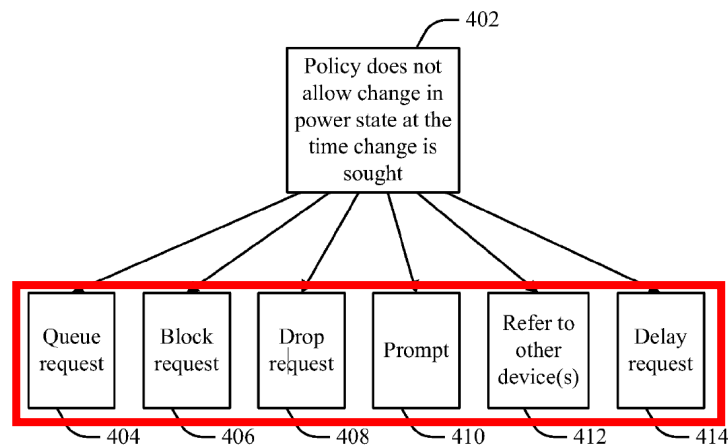
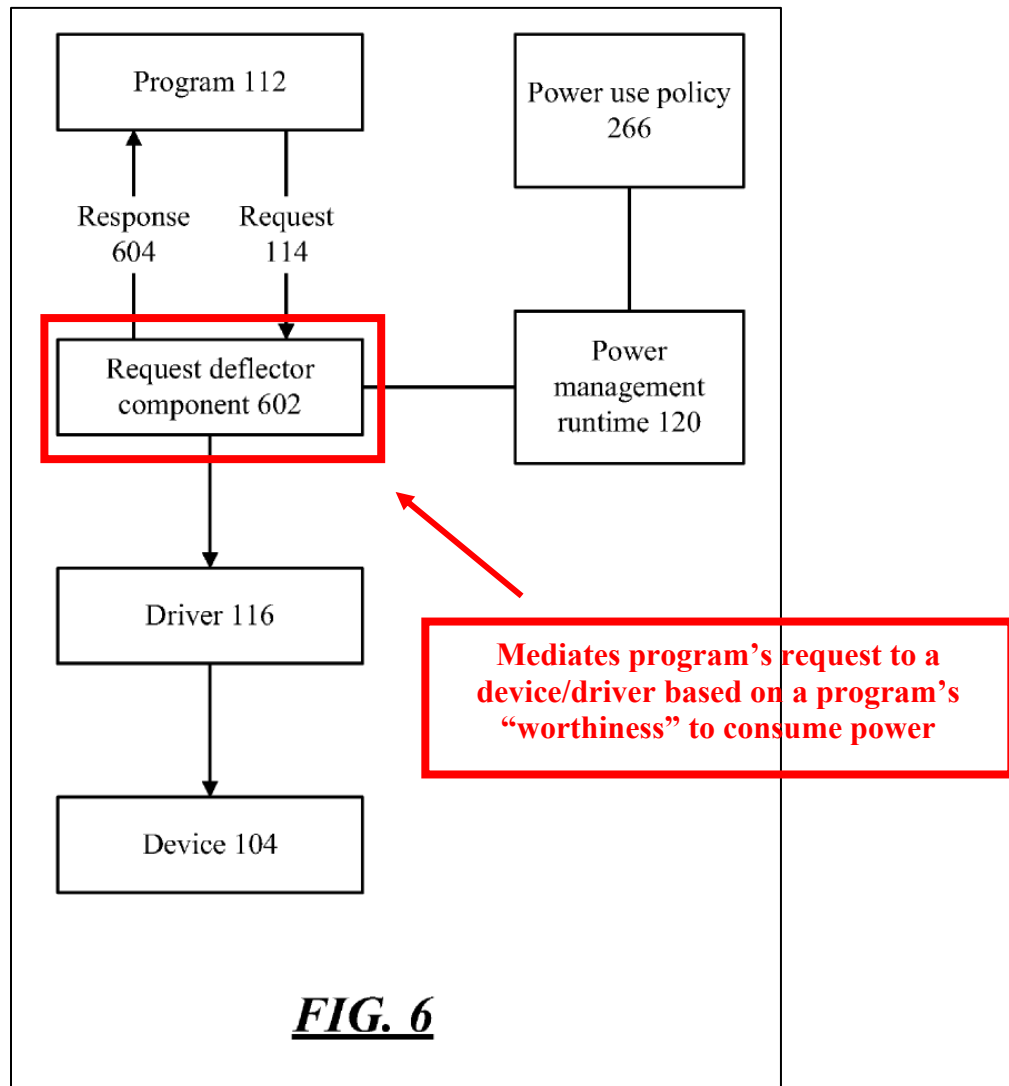


FIG. 4

SAMSUNG-1008, FIG. 4 (annotated)

224. 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.” *Id.*, [0024], [0050]. In particular, if “[a] request 114 may be carried out under [a] 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.*



SAMSUNG-1008, FIG. 6 (annotated)

225. 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).

226. Araujo's "a power-management policy" can be used to "justify [a program] consuming power, depending on what the program is doing." *Id.*, [0004]. Accordingly, a device implementing Araujo's policy can better "use the energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge." *Id.*, [0001].

B. Combination of Rao-Oestvall-Montemurro and Araujo

227. A POSITA would have found it obvious to modify the ROMC system to include Araujo's "request deflector component" in order to allow the ROMC system to better "use the energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge." SAMSUNG-1008, [0001]; Section X.A. This modification 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.

228. As I explained in Sections IX.D.3-4, the ROMC system controls each of the applications' access to the network by intercepting packets of network traffic by the applications, determining the priority of the packets based on the application that is associated with each packet, and selectively communicating the packets to the network based on the determined priority. As taught by Rao, these operations can be performed, at least in part, by one or more "network drivers of a network stack 310" (e.g., by "customiz[ing], modifi[ng] 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" described in Rao). SAMSUNG-1005, [0100]. As an example, the ROMC system can include "[a] filter 322 [to] place, arrange, or coordinate network packets into queues 540 a-540 n in support of the priorities," and these "queues 540 a-540 n may be included in a network driver, such as an NDIS driver for the filter 322." *Id.*, [0143], [0180], [0191].

229. In view of Araujo, a POSITA would have understood that an application's request to the network driver (e.g., including network packets for transmission to a network) can be intercepted and mediated by a "request deflector component" that is "interposed" between each application and the network driver, in order to selectively allow or block an application from transmitting data to the

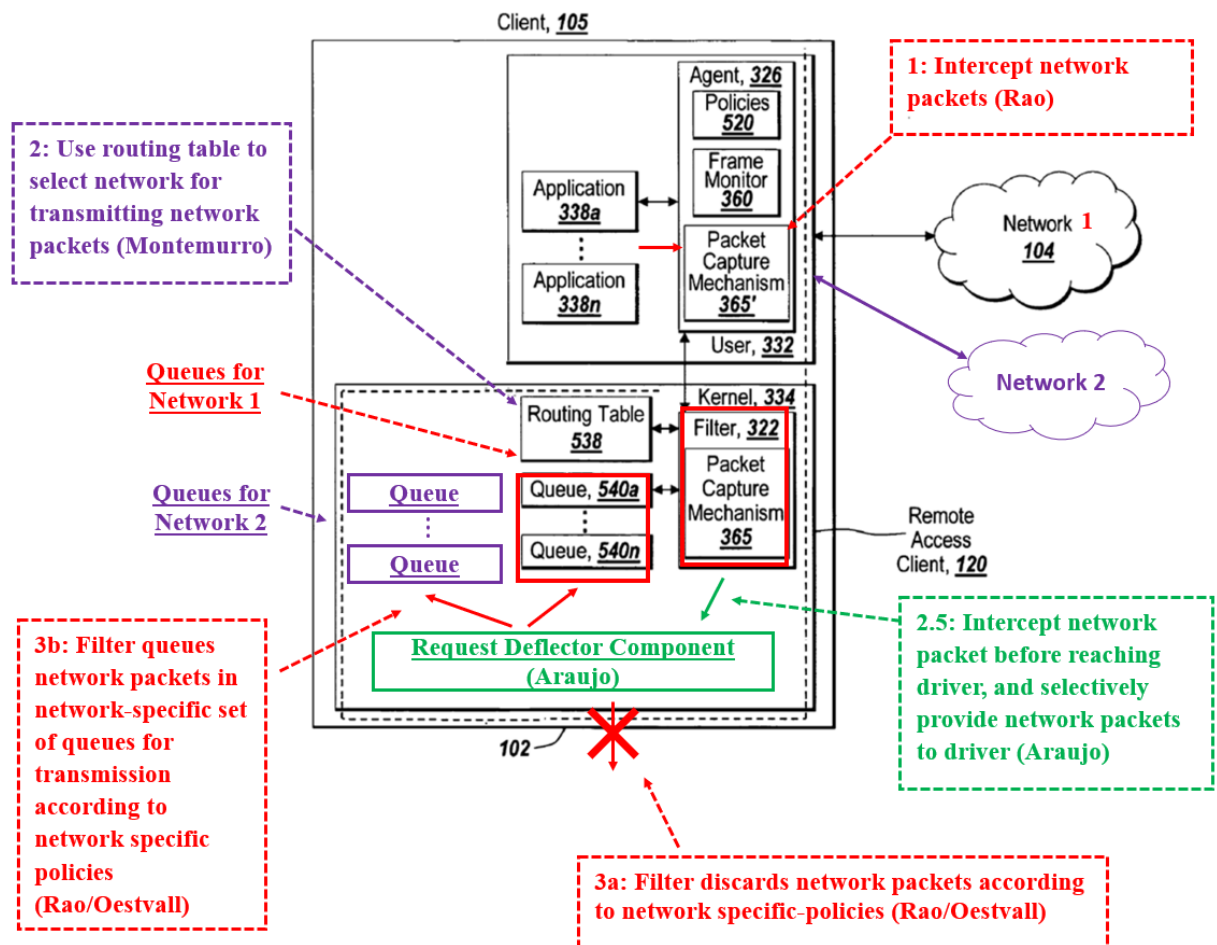
network. SAMSUNG-1008, [0050]. In particular, a POSITA would have understood or recognized that incorporating Araujo's "request deflector component" into the ROMC system would allow the ROMC system to determine whether each of the applications has a "status [that] justifies the consumption of power under the circumstances that are present," and selectively block or allow requests by those applications based on the determination. SAMSUNG-1008, [0027]. Accordingly, the ROMC system can better "use the energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge." SAMSUNG-1008, [0001].

230. As an example of this modification, a POSITA would have "interposed" Araujo's "request deflector component" between the ROMC's applications and the network driver(s) (i.e., including the queues 540a-540n) to process network packets subsequent to the selection of a network by the routing table 538 (e.g., based on Montemurro's criteria). 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 request and, hence, the network packets from proceeding to the network driver for communicating with the selected network based on the determination (see step 2.5 below). Upon determining that the application's status justifies the consumption of

power, the “request deflector component” can allow the request, and hence, the network packets to proceed to the appropriate network driver and be prioritized according to the Rao-Oestvall combination (see steps 3a and 3b below).

Alternatively, upon determining that the application’s status does not justify the consumption of power, the “request deflector component” can block the request and, hence, the network packets from reaching the network driver, either permanently or temporarily. Accordingly, the “request deflector component” would provide an additional layer of control for regulating each of the applications’ access to the network (e.g., to supplement the functionality taught by Rao, Oestvall, and Montemurro).

231. An example modification to the Rao-Oestvall-Montemurro system in view of Araujo’s teachings (“Rao-Oestvall-Montemurro-Araujo combination,” ROMAC) is shown below.



Rao's FIG. 5A (revised and annotated)

C. Analysis of Claims 10-12, 15, 17, 18, 22, and 25

1. Claims 10 and 12

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

232. ROMAC renders obvious [10] and [12].

233. As I explained in [1f] and Section X.B, the ROMAC system would use a network driver to apply *a differential traffic control policy* to the Internet service access request.

234. Further, as modified by Araujo, the ROMAC system would selectively allow network packets to proceed to the network driver for prioritization (*dynamically change the application of the differential traffic control policy*). Section X.B. As Araujo teaches, this configuration allows the ROMAC system to determine whether each of the applications has a “status [that] justifies the consumption of power under the circumstances that are present.” SAMSUNG-1008, [0027].

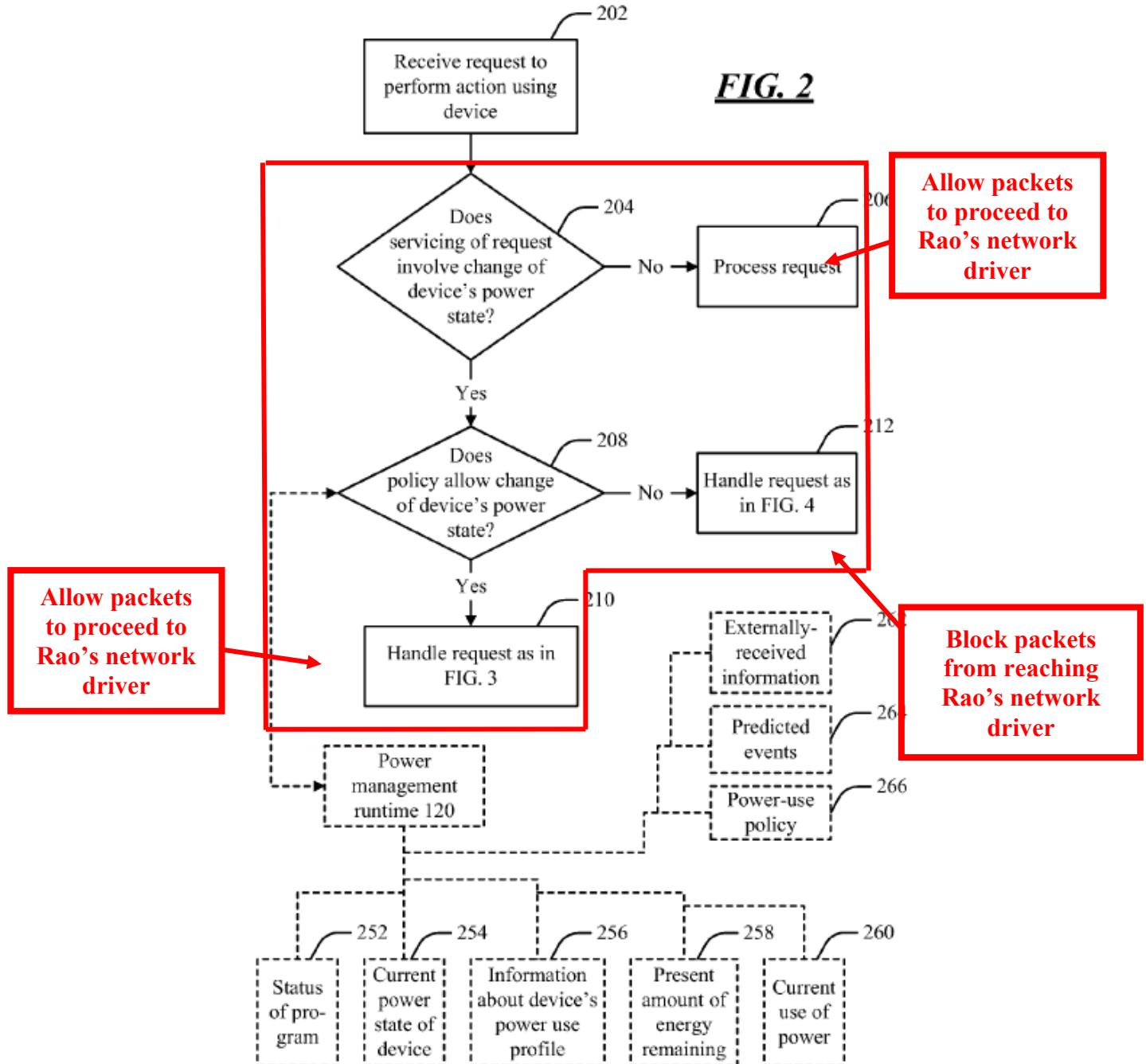
235. An example configuration of the ROMAC system is shown in Section X.B above. Specifically, in the ROMAC system, Araujo’s “request deflector component” would be “interposed” between the applications and the network driver(s) (i.e., including the queues 540a-540n) to process network packets subsequent to the selection of a network by the routing table 538 (e.g., based on Montemurro’s criteria). *See* Section X.B. Further, the “request deflector component” would selectively allow or block an application’s network packets—

representing an Internet service access request by that application—from reaching the network driver for communicating with the selected network based on whether that application is considered sufficiently important to consume power. *See* Section X.B.

236. As modified by Araujo, the ROMAC system would determine whether to allow an application’s request to proceed to the network driver based on a device’s power state, such as the power state of the device’s network card or modem (*...based on a power state of the device [10]*). SAMSUNG-1008, FIG. 2 (204), [0025]. Specifically, this configuration would enable the ROMAC system to account for whether a device’s components “may already be powered on and/or in an appropriate power state” in order to better regulate power consumption by the device. SAMSUNG-1008, [0037]. For example, if a device’s network card or modem are already powered on and/or is “in an appropriate power state,” the ROMAC system determines that an application’s use of those components “does not affect power management,” and selectively allows the application’s network packets to proceed to the network driver in order to service the application’s request. *Id.*

237. In particular, the ROMAC system would determine whether to allow an application’s request to proceed to the network driver based on power control state changes for a device, such as a network card or modem (*...based on power*

control state changes for one or more of the modems [12]). For example, as shown in FIG. 2, if servicing the application's request would not involve a change in the power state of the device's components, the ROMAC system would process the request and "proceed[s] as normal." SAMSUNG-1008, FIG. 2 (206), [0025]. Accordingly, the network packets representing the request would be forwarded to the network driver for prioritization. In contrast, if servicing the request would involve a change in the power state of the device's components, the ROMAC system determines whether a policy would allow a change of the device's power state, and selectively (i) allows the request and transmits the network packets to the network driver (e.g., as shown in FIG. 3) (SAMSUNG-1008, FIG. 2 (210), FIG. 3, [0035]), or (ii) queues the request, blocks the request, drops the request, delays the request, and/or refers the request to another device, thereby blocking the network packets from reaching the network driver, either permanently or temporarily (e.g., as shown in FIG. 4) (*id.*, FIG. 2 (212), FIG. 3, [0035]).



SAMSUNG-1008, FIG. 2 (annotated)

2. *Claim 11*

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

238. ROMAC renders obvious [11].

239. As I explained in [1f] and Section X.B, the ROMAC system would use a network driver to ***apply a differential traffic control policy*** to the Internet service access request. Further, as modified by Araujo, the ROMAC system would selectively allow network packets to proceed to the network driver for prioritization (***dynamically change the application of the differential traffic control policy***). See Section X.B. See also [12].

240. As modified by Araujo, the ROMAC system would determine whether to allow an application's request to proceed to the network driver based on ***a device usage state***, such as:

- (i) the “[s]tatus of program” that is being used by a user (SAMSUNG-1008, [0027], FIG. 2),
- (ii) the “[c]urrent power state of the device” (*id.*, [0028], FIG. 2), and/or
- (iii) “[p]resent use of power” by the device (*id.*, [0031], FIG 2).

241. As Araujo explains, each of these factors reflects an application's “worthiness to consume power” in a given situation. *Id.*, [0027]. Accordingly, by mediating an application's request based on factors that reflect the use of the

device and/or the “programs” stored thereon, the ROMAC system can better “use the energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge.” *Id.*, [0001].

3. *Claim 15*

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

242. ROMAC renders obvious [15].

243. Araujo describes that “if a power state change is not allowable under a policy,” the system can generate “a dialog box ... on a display that informs the person in front of the display that the card is off.” SAMSUNG-1008, [0041].

244. In view of Araujo, a POSITA would have understood or found it obvious that a system can present information to a user regarding a blocked Internet service access request, thereby blocking, modifying, removing, and/or replacing what was previously displayed on the user interface (***block, modify, remove, or replace user interface messages generated by the particular application based on the applied differential traffic control policy***). This would allow the system to alert the user to changes in the operation of the device and/or to provide the user with a greater degree of control over the device, as taught by Araujo.

245. As an example, POSITA would have understood or found it obvious that, in presenting information to a user regarding a blocked Internet service access request, the system would block, modify, remove, and/or replace what would be displayed on the user interface had the Internet service access request not been blocked, thereby allowing the user to understand the operational state of the device and to take corrective actions as desired.

246. Further, in view of Araujo, a POSITA would have understood that this functionality can be provided, at least in part, using “[s]oftware ... stored in [a] data remembrance component(s) 704)” and “execute[d] on ... one or more processor(s) 702) (*agent*). SAMSUNG-1008, [0055].

4. *Claim 17*

[17] The wireless end-user device of claim 16, wherein the one or more processors are configured to respond to an intercepted request by the particular application by emulating network messaging

247. ROMAC renders obvious [17].

248. As I explained in Section X.B, the ROMAC system would include Araujo “request deflector component” to “intercept[] requests and respond[] to the requests based on power management considerations before the request reach[es] a device driver.” SAMSUNG-1008, [0024], [0050].

249. Specifically, Araujo explains that “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-1008, [0038], [0041]. Further, “[t]he program may also be notified that the reason for the request is that the device is off. For example, 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.”).

250. In view of Araujo, a POSITA would have understood or found it obvious that a system can respond to an intercepted request by a particular 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 particular application***). In doing so, the system would provide an application with a greater degree of information regarding its attempt to access a network, as taught by Araujo.

251. Further, a POSITA would have found it obvious to notify the application by emulating conventional network messages, such as those generated by an Application Programming Interface (API) for facilitating network access for applications (***...by emulating network messaging***), as doing so would provide functionality in a manner that is transparent to the application, thereby providing

support for any type of application (e.g., as taught by Rao). *See also* SAMSUNG-1013, 1-20.

252. In particular, communications between an application and a network driver/card are well known to occur in many computing devices through use of APIs to enable an application to converse with the network card/device without having to be burdened with the specific details of how the network card operates. In doing so, an application would both send and receive messages from the network card with the API simplifying the operation of the application by simplifying and standardizing its communications with the network card.

253. For instance, as described in Stevens, the TCP/IP protocol suite provides an example of an API that is used by applications to send and receive messages. *See, generally*, SAMSUNG-1013. *See also id.*, 1-20. The process of sending or receiving a message occurs from the application's perspective without its having any requirement for knowing how the card operates. As an example, Stevens' FIG. 1.3 (reproduced below) demonstrates that an application (e.g., a file transfer (FTP) client) can communicate with another entity (e.g., an FTP server) without requiring any specific knowledge of the hardware details. Instead, the application can use command (e.g., the send() command) to move information to another party and another command (e.g., the recv() command) to receive information (e.g., as taught by Freund). Further, the application does not need to

know that there are two different data communication interfaces (e.g., Ethernet and Token Ring) in use. Instead, “[t]he application layer is concerned with the details of the application and not with the movement of data across the network. The lower three layers know nothing about the application but handle all the communication details.” *Id.*, 4. The send() and recv() commands are examples of functions available through an API and the same abstraction allows communication of network data from an application to the network card on a host without the host requiring implementation specifics of a given network card/device. As Stevens explains, “[t]wo popular application programming interfaces (APIs) for applications using the TCP/IP protocols are called sockets and TLI (Transport Layer Interface).” *Id.*, 17.

Section 1.2

Layering 5

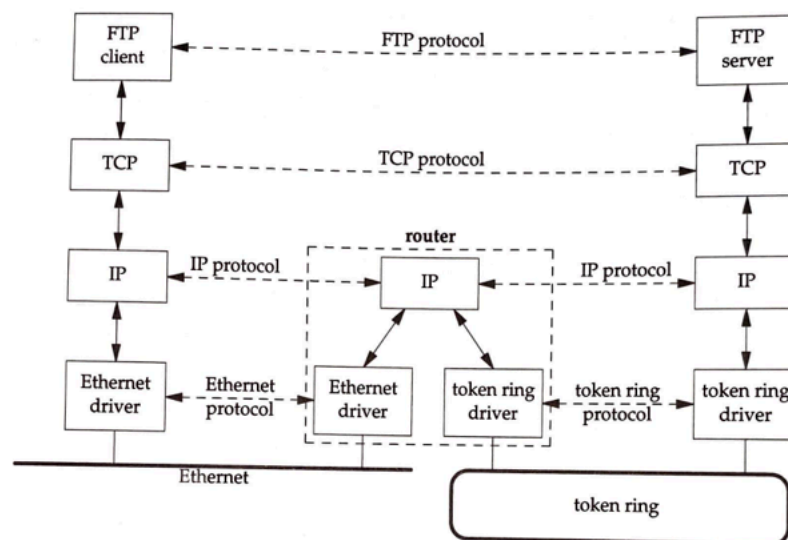


Figure 1.3 Two networks connected with a router.

SAMSUNG-1013, FIG. 1.3

254. Given (1) the common use of APIs as of the Critical Date and the desire to use them to free an application from having to know the implementation specifics of a given network card/device; and (2) the desire, as taught by Rao, to make prioritization/filtering operations used to efficiently allocate/control resources transparent to the application—thereby similarly freeing an application from having to know the details of these operations—a POSITA would have found it obvious for Araujo’s error or result code indicating a lack of network access to look like (i.e., emulate) a corresponding API message denying network access. In doing so, the application would not be burdened by having to have knowledge of implementation details specific to the particular network card and would also not be burdened by having to understand messages specific to the particular prioritization control schemes of the ROFAC system used to efficiently allocate and conserve system resources. Instead, the messaging enabling or denying network access would simply appear like (i.e., “emulate”) a conventional API message received from the network card/device.

255. Araujo’s use of an “error code or result code” is also consistent with the specification of the ’445 Patent, which describes that “an emulated network API” can block an application’s connection attempt and send “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.

5. *Claim 18*

[18] The wireless end-user device of claim 17, 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.

256. ROMAC renders obvious [18].

257. As I explained in Section X.B, the ROFAC system would include Araujo’s “request deflector component” to “intercept[] requests and respond[] to the requests based on power management considerations before the requests reach a device driver.” SAMSUNG-1008, [0024], [0050]. Further, as I explained in [17], the ROMAC system would notify an application that a request will not be processed and/or transmit an error code or result code to the application by emulating conventional network messages (*emulating network messaging*).

258. A POSITA would have understood or recognized that, in blocking the request from reaching the network driver, the ROMAC system would block the request from passing 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). SAMSUNG-1005, [0100].

259. Further, a POSITA would have understood or recognized that, in notifying an application that a request will not be processed and/or transmitting an error code or result code to the application, the ROFAC would *return to the particular application a message indicating the network request was not successful.* SAMSUNG-1008, [0038], [0041]. *See also id.*, [0017].

6. *Claim 22*

[22] The wireless end-user device of claim 1, wherein the one or more processors are further configured to classify between: user applications; system applications, utilities, functions, or processes; and operating system application, utilities, functions, or processes.

260. ROMAC renders obvious [22].

261. As taught by Montemurro, a system includes various applications, functions, or processors, such as (i) “[o]perating system software” (*operating system application, utilities, functions, or processes*), (ii) “predetermined set of applications that control basic device operations, including at least data and voice communication applications, will normally be installed on handheld device 600 during its manufacture” (*system applications, utilities, functions, or processes*), and (ii) “[a]dditional applications ... installed by a user” (*user applications*), each of which provides different respective functionality. SAMSUNG-1007, [0055]-[0057].

262. In view of Montemurro, a POSITA would have understood or recognized that the ROMAC system would differentiate between these types of applications, functions, or processes (*classify between* these types of applications, functions, or processes) such that they are executed by the processor(s) in the correct mode, which was well known by the Critical Date. SAMSUNG-1014, 22-35. As an example, as described by Bovet (SAMSUNG-1014), it was well known that a “CPU can run either in User Mode or in Kernel Mode” and/or in other “execution states.” SAMSUNG-1004, 22. As Bovet explains, the CPU must select the proper mode for executing each particular program, such that the program has access to the correct resources. For instance:

“When a program is executed in User Mode, it cannot directly access the kernel data structures or the kernel programs. When an application executes in Kernel Mode, however, these restrictions no longer apply. Each CPU model provides special instructions to switch from User Mode to Kernel Mode and vice versa. A program executes most of the time in User Mode and switches to Kernel Mode only when requesting a service provided by the kernel. When the kernel has satisfied the program's request, it puts the program back in User Mode.

Id.

263. That is, as corroborated by Bovet, a ROMAC system would differentiate between these types of applications, functions, or processes such that the CPU executes them according to the correct CPU mode (e.g., “User Mode or in Kernel Mode”). For instance, as corroborated by Bovet, it was well known (i) to

selectively run user applications, functions, or processes in a “User Mode,” and (ii) to selectively run system and/or operating system applications, functions, or processes in a “Kernel Mode.” *Id.*, 22-35.

7. *Claim 25*

[25] The wireless end-user device of claim 1, wherein the one or more processors are configured to prevent the first one or more applications from changing the power state of the modem, and to not prevent the second one or more applications from changing the power state of the modem.

264. ROMAC renders obvious [25].

265. As I explained in [10], if servicing a request would involve a change in a device’s power state (e.g., the power state of a network card or modem), the ROMAC system determines whether a policy would allow a change of the device’s power state. SAMSUNG-1008, FIG. 2 (210), FIG. 3, [0035]. If the policy would not allow such a change, the ROMAC system would block the network packets from reaching the network driver, either permanently or temporarily (e.g., as shown in FIG. 4). *Id.*, FIG. 2 (212, FIG. 3, [0035]. Accordingly, the power state of the network card or modem would remain unchanged (***prevent ... applications from changing the power state of the modem***).

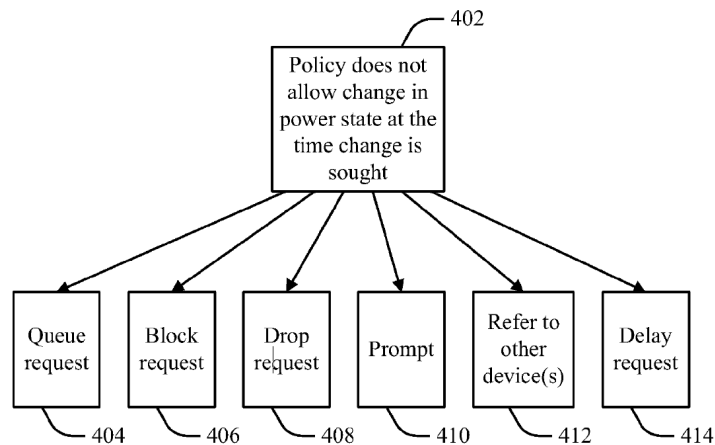


FIG. 4

SAMSUNG-1008, FIG. 4

266. Further, as I explained in Sections X.B, Araujo teaches that a device can selectively allow 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). SAMSUNG-1008, [0024], [0050]. Further, as I explained in Sections IX.B and IX.4, Oestvall teaches that certain applications (e.g., “trusted” applications) (*second one or more applications*) are more important than other applications (e.g., “untrusted” applications) (*first one or more applications*) and should be given preferential treatment by a device. SAMSUNG-1006, [0010]-[0017], [0021]-[0025].

267. In view of Araujo and Oestvall, a POSITA would have found it obvious to allow “trusted” applications to change the power state of the modem *(not prevent the second one or more applications from changing the power state of the modem)*, while not allowing “untrusted” applications to change the power state of the modem (e.g., when they are running in the background) *(prevent the first one or more applications from changing the power state of the modem)*.

Accordingly, the ROMAC system can better “use the energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge.”

SAMSUNG-1008, [0001].

**XI. [GROUND 3] - RAO-OESTVALL-MONTEMURRO-FREUND
MAKES CLAIMS 3, 13, 21, and 24 OBVIOUS**

A. Overview of Freund

268. Freund describes “[a] computing environment with methods for monitoring access to an open network, such as WAN or the Internet.”

SAMSUNG-1009, Abstract. Freund’s system includes “a client-side monitoring component for monitoring Internet access” (“Client Monitor”) and a “supervisor 323 [that] directs runtime monitoring operations.” *Id.*, 3:50-4:4, 14:62-67, 14:51-62, FIG. 3A (310a-310c). Freund’s system “monitor[s] and regulate[s] Internet access on a per application basis,” and “specif[ies] which applications can (and cannot) access the Internet.” *Id.*, 10:44-50.

269. For instance, Freund's system "allows user (e.g., administrator) configuration of rules which govern use of the protocols monitored by the system." *Id.*, 23:65-27:50. Rules can be specified based on various criteria, such as the "particular application" that is being used and the "particular Internet sites" that the user is attempting to access." *Id.*, 23:65-24:15. Further, "[r]ules can also be set which are time-based in nature. For instance, an administrator can establish a rule setting a time limit (e.g., 30 minutes) for how long a user can access the Internet each day." *Id.*

270. Further, Freund's system can "monitor[] access to the Internet by individual applications ... to not only track Internet traffic but also [to] determine in many cases data exchanged on a per application basis." *Id.*, 11:10-15. As Freund teaches, "this system can "avert ... [i]nadvertent disruptions of the network by individual users, such as bandwidth hording [sic] by a user using RealAudio for listening to a Web audio 'broadcast.'" *Id.*, 11:21-28.

271. In an exemplary monitoring process, Freund's system performs "bandwidth and interactive use monitoring" in which a "Client Monitor maintains a list of active Applications (processes) with various fields to track activities and a global activity record." *Id.*, 30:10-29, FIGS. 13A-13B. For each of the applications on a device, Freund's "Client Monitor" intercepts the application's requests to access the Internet (e.g., "Winsock ... calls" to a "communications

driver”). *Id.*, 29:17-30:9, FIG. 13A (1301). Further Freund’s “Client Monitor” determines the amount of Internet data that is transmitted and/or received by the application (e.g., “data lengths”), and tracks the amount of data (e.g., by “[a]dd[ing] the data lengths to a DataIn or DataOut accumulator or counter”). *Id.*, 30:24-29, FIG. 13A (1302(D)).

272. Further, Freund’s system selectively allows or prevents the application from accessing the Internet based on the amount of data used by that application. *Id.* For example, “[i]f [an] application is not allowed to access the Internet ... then [the] client monitor can stop [that] application from accessing the Internet and/or warn user.” *Id.*, 5:61-64. In particular, with respect to bandwidth monitoring, “[i]f the DataIn or DataOut fields exceed rule-based quantity either for the specific Application or the user/workstation, the Client Monitor disables future Internet access and/or warns the user.” *Id.*, 30:24-29, FIG. 13A (1302(E)).

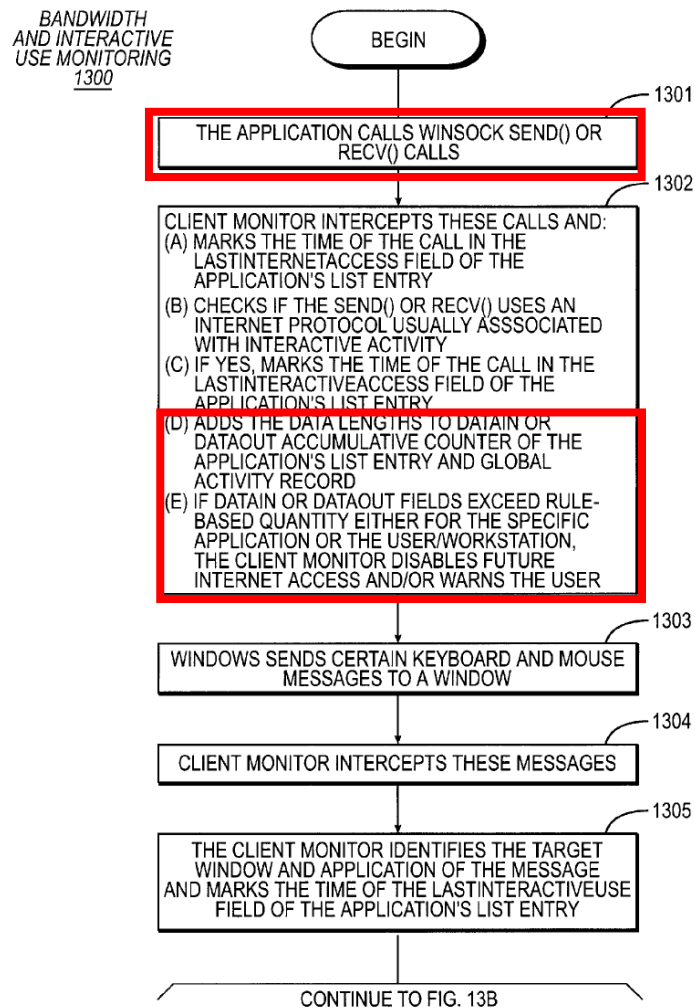


FIG. 13A

SAMSUNG-1007, FIG. 3A (annotated)

273. Further, Freund’s “Client Monitor” “maintain[s] a detailed log of access related activities, for facilitating administration needs,” and provides the log to a “Supervisor” implemented on a remote server. *Id.*, 3:50-4:4, 4:29-32; 4:51-63; 14:62-67, 28:24-28; 28:51-53.

B. Combination of Rao-Oestvall-Montemurro and Freund

274. In view of Freund, a POSITA would have found it obvious to modify the ROMC system to regulate an application to access a network (e.g., the Internet) based on time-based criteria and/or the amount of network data that has been used by that application. *See* Section XI.A. Combining ROMC with Freund 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.

275. In particular, a POSITA would have recognized that, like the ROMC system, Freund's system is configured to control an application's access to a network in order to preserve limited system resources. SAMSUNG-1009, 11:19-28. Further, a POSITA would have recognized that Freund describes specifying techniques for regulating an application's access to a network based on both (i) time-based criteria and (ii) a "bandwidth and interactive use monitoring" technique for selectively blocking an application's request to access a network in order to achieve a specific technical benefit (e.g., to "avert ... [i]nadvertent disruptions of the network by individual users, such as bandwidth hording [sic] by a user"). SAMSUNG-1009, 11:19-28.

276. In view of Freund, a POSITA would have found it obvious to modify the ROMC system to allow users to control an application's access to a network

based on time-based criteria (e.g., in order to “monitor and regulate the amount of time employees spend on the Internet”). As an example of this modification, a POSITA would have modified Rao’s policies such that they can additionally include time-based criteria, as specified by Freund. For instance, as taught by Freund, these criteria can include “specify[ing] the start date and expiration date (if any)” for a rule and/or “particular time intervals (e.g., during weekdays and/or during weekends) when the rule is enforced.” SAMSUNG-1009, 27:4-16.

277. Further, in view of Freund, a POSITA would have found it obvious to modify the ROMC system to additionally include Freund’s “bandwidth and interactive use monitoring” in order to prevent an application from hoarding the bandwidth of a network. SAMSUNG-1008, 11: 19-28. In particular, a POSITA would have recognized that Freund’s “bandwidth and interactive use monitoring” enhances the ROMC system’s ability to control an application’s access to a network and to preserve limited system resources by accounting for the aggregate amount of data transmitted by an application over the network.

278. As an example of this modification, a POSITA would have modified the Rao-Oestvall system to additionally include Freund’s “Client Monitor” in Rao’s client device. Specifically, a POSITA would have configured the “Client Monitor” to (i) intercept an application’s requests to access the Internet, (ii) determine and track the amount of Internet data that is transmitted and/or received

by that application, and (iii) disable future Internet access by that application if the amount of data exceeds a particular application-specific data limitation (see step 1b below).

279. If an application is permitted to access the Internet (e.g., the amount of data used by the application does not yet exceed the application-specific data limitation), the network packets generated by that application would be prioritized in accordance with the ROMC combination, as I explained in Section IX.D.

C. Analysis of Claims 3, 13, 21, and 24

8. Claim 3

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

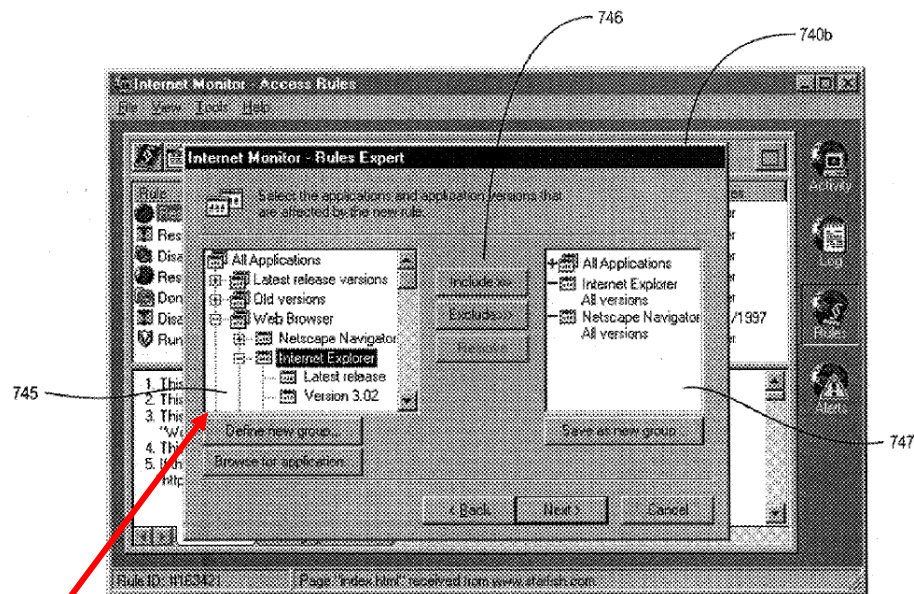
280. The Rao-Oestvall-Montemurro-Freund combination (“ROMFC”) renders obvious [3].

281. As I explained in [4], Rao describes that a system can “provide a configuration mechanism such as a user interface, graphical or otherwise, design and constructed for configuring or specifying the policies.” SAMSUNG-1005, [0183]. In view of Rao, a POSITA would have understood or found it obvious that such a user interface would *provide the user of the device with information regarding why the differential traffic control policy is applied to the particular*

end-user application (e.g., by providing the user with detailed information regarding each of the policies).

282. A POSITA would have further found it obvious to implement such a feature in view of Freund in order to provide a user with a greater degree of control over the manner in which network packets are prioritized.

283. For example, Freund describes a “rule wizard interface” that “allows user (e.g., administrator) configuration of rules which govern use of the protocols monitored by the system” through a graphical user interface. SAMSUNG-1009, 24:16-27:50. Specifically, the “rule wizard interface” allows a user “to selectively include or exclude applications (and versions thereof) which are to be affected by the new rule.” SAMSUNG-1009, 25:20-33; FIG. 7D. That is, the user interface would *provide the user of the device with information regarding why the differential traffic control policy is applied to the particular end-user application* (e.g., due to a user’s selection of that application).



User interface allows user to select specific applications that are affected by a rule

FIG. 7D

SAMSUNG-1009, FIG. 7D

9. Claims 13 and 24

[13] *The wireless end-user device of claim 1, wherein the differential traffic control policy defines that the first one or more applications can only have WWAN network access events during particular time windows.*

[24] *The wireless end-user device of claim 1, wherein block comprises intermittently block when the Internet service access request occurs during selected time windows.*

284. ROMFC renders obvious [13] and [24].

285. As I explained in Sections XI.A-B, in view of Freund, a POSITA would have found it obvious to modify the ROMC system to regulate an application's access to a network (e.g., the Internet) based on time-based criteria.

In particular, Freund teaches that a user can specify policies or rules that block certain applications from accessing a network during certain times of day.

SAMSUNG-1009, 27:-4-16 (“This allows an administrator, for instance, to specify that a rule blocking a RealAudio application remains in force during working hours on weekdays-that is, at times when network traffic is already congested.”).

286. Specifically, a POSITA would have found it obvious to configure a rule or policy (*the differential traffic control policy*) such that at least some of applications (*...defines that the first one or more applications*) can access a particular network only during certain times of the day (*...can only have WWAN network access events during particular time windows [10]*). Accordingly, Internet service access requests occurring outside of the specified times would be blocked (*wherein block comprises intermittently block when the Internet service access request occurs during selected time windows [24]*).

287. Specifically, a POSITA would have recognized that time-based limitations allow the device to reduce network usage during specific times in which “network traffic is already congested” (e.g., on an application-by-application basis or for each of the applications) thereby improving the performance of the network.

10. *Claim 21*

[21] The wireless end-user device of claim 1, further comprising a policy agent to: monitor Internet service activity usage for a third application that is neither one of the first one or more applications nor one of the second one or more applications; and to report the activity usage to a network element when Internet service activity usage by the third application exceeds a data usage threshold.

288. ROMFC renders obvious [21].

289. As I explained in XI.B, in view of Freund, a POSITA would have found it obvious to modify the ROMC system to monitor the amount of network data that has been used by each application individually.

290. As I also explained in Section XI.B, according to this combination, a POSITA would have configured a “Client Monitor” to:

- (i) Intercept an application’s requests to access the Internet (e.g., “Winsock ... calls” to a “communications driver”) (SAMSUNG-1009, 29:17-30:9, FIG. 13A (1301)),
- (ii) Determine the amount of Internet data that is transmitted and/or received by that application (e.g., “data lengths”), and track that amount of data (e.g., by “[a]dd[ing] the data lengths to a DataIn or DataOut accumulator or counter of the Application's list entry and global activity record”) (determine that *Internet service activity usage by an third application*), (SAMSUNG-1007, 30:24-29, FIG. 13A (1302(D))), and

- (iii) “[D]isable[] future Internet access” by that application if the amount of data exceeds a particular application-specific limitation (e.g., “[i]f the DataIn or DataOut fields exceed rule-based quantity either for the specific Application”) (*...exceeds a data usage threshold.*) (SAMSUNG-1007, 30:24-29, FIG. 13A).

291. Further, as I explained in Section X.B, Freund’s “Client Monitor” “maintain[s] a detailed log of access related activities, for facilitating administration needs,” and provides the log to a “Supervisor” implemented on a remote server. *Id.*, 3:50-4:4, 4:29-32; 4:51-63; 14:62-67, 28:24-28; 28:51-53. In view of Freund, a POSITA would have found it obvious to report an application exceeding the data usage threshold (*report the activity usage*) to a remote “Supervisor” (*...to network element when Internet service activity usage by the third application exceeds a data usage threshold*) in order to “facilitat[e] administration needs.” *Id.*

292. Further, a POSITA would have understood or recognized that Freund’s “bandwidth and interactive use monitoring” technique could be applied to any of the applications that are running on the device, and thus would have applied this technique to any of the applications that are running on the ROMFC system.

293. As an example, a POSITA would have recognized that (i) “trusted” applications and “untrusted” applications (e.g., as described by Oestvall) could be

further differentiated based on additional criteria, such as “the type of one or more protocols used by the application[s]” and “the size of the payload of the network packet,” and (ii) the applications could be prioritized differently based on these criteria (e.g., as taught by Rao). For instance, a POSITA would have recognized that “trusted” applications may be instead categorized into at least two different categories of applications, including a higher priority category (*second one or more applications*) and a lower priority category (and *a third application that is neither one of the first one or more applications nor one of the second one or more applications*) in accordance with Rao’s criteria. However, regardless each application’s categorization, a POSITA would have been motivated to apply Freund’s technique to track the network usage each of applications individually to obtain more granular data regarding each application’s data usage.

XII. CONCLUSION

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

295. 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.

296. 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.

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

Dated: 09-28-2023

By: 
Kevin R. B. Butler

APPENDIX A

KEVIN RAYMOND BOYCE BUTLER

Professor	Address :	E301 CSE Building
Department of Computer & Information Science and Engineering		PO Box 116120
University of Florida		Gainesville FL 32611
email: butler@ufl.edu	Phone:	+1 (352) 294-2090
URL: http://www.kevinbutler.org	Fax:	+1 (352) 392-1220

Current Academic Appointment

Professor, Department of Computer and Information Science and Engineering, University of Florida, Aug. 2021 - *present*

Director, Florida Institute for Cybersecurity Research, University of Florida, Aug. 2022 - *present*

Educational Background

PH.D. in Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, August 2010 (Dissertation Title: *Leveraging Emerging Storage Functionality for New Security Services*; Advisor: Dr. Patrick McDaniel)

M.S. in Electrical Engineering, Columbia University, New York, NY, USA, May 2003 (Advisor: Dr. Henning Schulzrinne)

B.Sc. in Electrical Engineering, Queen's University, Kingston, ON, Canada, May 1999

Honors & Awards

Best Paper Award, ACM HotStorage, 2023.

Meta Research Award, Meta Research Labs, 2022-2023.

Best Paper Finalist, IEEE European Symposium on Security and Privacy, 2022.

University Term Professor, University of Florida, 2021-2024.

Best Paper Nominee, IEEE Conference on Virtual Reality, 2021.

Doctoral Dissertation Advisor/Mentoring Award, Herbert Wertheim College of Engineering, University of Florida, 2019.

Distinguished Poster Award, ACM CODASPY, 2019.

Arnold and Lisa Goldberg Rising Star Endowed Professorship, University of Florida, 2018-2024 (*relinquished in 2021 upon promotion to Professor*).

University Term Professor, University of Florida, 2018-2021.

Recognition of Service Award, Association for Computing Machinery, 2018.

Research Promotion Initiative Award, University of Florida, 2018.

Senior Member, Association for Computing Machinery, 2018.

International Educator of the Year, Herbert Wertheim College of Engineering, University of Florida, 2017.

Senior Member, IEEE, 2017.

Outstanding Community Service Award, IEEE Technical Committee on Security and Privacy, 2017.

Rising to National Preeminence Hire, University of Florida, 2014.

Best Teacher Award, Dept. of Computer and Information Science, University of Oregon, 2013.
CAREER Award, National Science Foundation, 2013.
Alumni Association Dissertation Award, Pennsylvania State University, 2010.
Symantec Intern Project Showcase Winner, Symantec Corp, 2009.
Graduate Research Assistant Award, Computer Science and Engineering Department, Pennsylvania State University, 2009.
Symantec Graduate Fellowship, Symantec Research Labs, 2009-2010.
Special Award of Meritous Service, Third International Conference on Information Systems Security, December 2007.
University Graduate Fellowship, Pennsylvania State University, 2006.
C. Norwood Wherry Memorial Graduate Fellowship, Pennsylvania State University, 2004.

Expert Witness Experience

During the course of my expert witness consulting engagements, I have written numerous expert reports, given six depositions, and have testified four times across two jury trials, with regards to both patent infringement and invalidity.

Testifying Expert, *Headwater Research LLC v. Samsung America Inc.*, No. 2-22-cv-00422, 2-22-cv-00467, 2-23-cv-00103 (E.D. Texas), retained by Fish and Richardson, representing defendant, April 2023 - present.

Testifying Expert, *Webroot, Inc. et al. v. Trend Micro Inc.*, No. 6:22-cv-00239-ADA-DTG (W.D. Texas), retained by Paul Hastings LLP and White & Case LLP, regarding intrusion detection devices, representing defendant. July 2022-present.

Consulting Expert, *Department of Justice, Antitrust Division, defendant confidential*, retained by USDOJ, regarding mobile devices. June 2022-June 2023.

Testifying Expert, *Research in Motion Limited ats Glen Snowball (File No. 13-57203CP), Blackberry Limited ats Michael Blackette (File No. 500-06-000583-118)*, retained by Torys LLP, regarding the Blackberry network, representing defendant. March 2021-present.

Testifying Expert, *IOENGINE LLC vs Roku Inc.* regarding portable devices, engaged by plaintiff in patent infringement case, October 2021-present.

Testifying Expert, *Finjian, Inc. v. Juniper Networks, Inc.* (3:17-cv-0569-WHA, District Court, N.D. California), retained by Irell and Manella LLP, regarding intrusion detection systems, representing defendant. June 2019-August 2019.

Testifying Expert, *Ingenico Inc v. IOENGINE LLC (1:18-cv-00826, District Court, D. Delaware)*, retained by Dechert LLP, regarding secure portable devices, representing defendant. October 2018-December 2022.

Testifying Expert, *IOENGINE LLC v. Imation Corp.* (1:14-cv-01572, District Court, D. Delaware), retained by Simpson Thacher & Bartlett LLP, regarding secure portable storage devices, representing plaintiff. March 2015-February 2017.

Testifying Expert, *IOENGINE LLC v. Interactive Media Corp.* (1:14-cv-01571, District Court, D. Delaware), retained by Simpson Thacher & Bartlett LLP, regarding secure portable storage devices, representing plaintiff. March 2015-January 2017.

Consulting Expert, *Vir2us, Inc.*, retained by Bunsow, De Mory, Smith, and Allison LLP, regarding virtualization and antivirus software. December 2014 - April 2015

Consulting Expert, *Envosys v. AT&T*, retained by Baker Botts, regarding location services in mo-

bile devices, representing defendant. October 2013-December 2013.

Research Support (\$36.7M total, \$9.34M investigator share)

Major Peer-Reviewed Grants (\$36.0M total, \$10.8M as PI, \$9.00M investigator share)

- **PI**, NSF CNS-2206950, “Collaborative Research: SaTC: Frontiers: Securing the Future of Computing for Marginalized and Vulnerable Populations”, National Science Foundation, \$7,500,000 (\$2,630,872 investigator share), 10/1/2022-9/30/2027.
- **Site PI**, NSF CNS-2054911, “Collaborative Research: SaTC: CORE: Medium: Enabling Practically Secure Cellular Infrastructure”, National Science Foundation, \$1,199,985 (\$598,019 investigator share), 1/1/2022-12/31/2024.
- **co-PI**, NSF CNS-2055123, “SaTC: CORE: Medium: Countering Surveillanceware Using Deception-Based Generative Models and Systems Mechanisms”, National Science Foundation, \$1,199,997 (\$618,531 investigator share), 1/1/2021-12/31/2024.
- **co-PI**, ONR N00014-20-1-2205, “Reconstructing Human Physiological Features from Audio Samples”, Office of Naval Research, \$700,000 (\$333,232 investigator share), 6/11/2021-6/10/2024.
- **co-PI**, DHS 70RSAT20CB0000017, “Deploying Defenses for Cellular Networks Using the AWARE Testbed”, DHS, \$3,122,033 (\$657,536 investigator share), 9/30/2020-9/29/2024.
- **PI**, ONR BAA-N00014-19-S-B001 Grant 12941701, “Mobile Interface Security Analysis”, Office of Naval Research, \$700,000 (\$376,242 investigator share), 1/1/2020-12/31/2022.
- **PI**, AFOSR AACOE, “Interpretable Security Reference Monitor for Deep Networks”, Air Force Office of Scientific Research, \$185,000 (\$185,000 investigator share), 12/1/2019-8/31/2021.
- **co-PI**, ONR DOD-19-STTR, “ArtusProtocol”, Office of Naval Research, \$800,000 (\$400,000 investigator share), 8/1/2019-7/31/2021.
- **co-PI**, AFOSR FA8650-19-1-1741, “University Center of Excellence: CYAN: Enabling Cyber Defense in Analog and Mixed Signal Domain”, Air Force Office of Scientific Research, \$5,000,000 (\$300,000 investigator share), 10/1/2019-9/30/2024. Selected for funding by AFOSR on 5/24/2019.
- **co-PI**, AFRL-FA9550-19-1-0169, “AFOSR University Center of Excellence in Assured Autonomy in Contested Environments (AACOE)”, Air Force Office of Scientific Research and Air Force Research Labs, \$5,999,515 (\$389,999 investigator share), 3/1/2019-2/28/2024.
- **co-PI**, DARPA HR00118S0052, “RACE: Resilient Communications for Everyone”, Defense Advanced Research Projects Agency, \$1,133,856 (\$382,698 investigator share), 3/1/2019-2/28/2023. Selected for funding by DARPA on 11/20/2018.
- **PI**, NSF/SRC CNS-1815883, “SaTC: STARSS: Small: Domain Informed Techniques for Detecting and Defending Against Malicious Firmware”, National Science Foundation, \$499,990 (\$250,000 investigator share), 11/01/2018-10/31/2021.

- **co-PI**, NSF CNS-1662976, “Collaborative Research: SURPASS: NSF SFS Unique Scholarship Program in Hardware and Systems Security”, National Science Foundation, \$2,508,541 (\$35,408 investigator share), 01/01/2017-12/31/2021.
- **co-PI**, NSF CNS-1562485, “TWC: Medium: Digital Healthcare-Associated Infection: Measurement, Defense and Prevention in a Modern Digital Healthcare Ecosystem”, National Science Foundation, \$1,200,000 (\$387,931 investigator share), 06/01/2016-05/31/2020.
- **PI**, “Developing Research Capability in Cyber-Physical Systems at the University of Florida”, Defense University Research Instrumentation Program (DURIP), Army Research Office, \$199,919 (\$100,000 investigator share), 09/01/2015-08/31/2016.
- **PI**, NSF CNS-1445983/1540216, “EAGER: Collaborative: Secure and Efficient Data Provenance”, National Science Foundation, \$205,000 (\$110,000 investigator share), 10/01/2014-03/31/2016.
- **PI**, NSF CNS 1254198/1540217, “CAREER: Securing Critical Infrastructure with Autonomously Secure Storage”, National Science Foundation, \$400,000, 04/01/2013-03/31/2018.
- **PI**, NSF CNS 1118046/154028, “TC:Small:Protection Mechanisms for Portable Storage”, National Science Foundation, \$515,530, 09/01/2011-08/31/2016.
- **co-PI**, “GAANN Program on Computer Systems Security”, US Department of Education, \$1,476,931 (\$184,616 investigator share), 08/16/2015-08/15/2018.
- **co-PI**, DARPA BAA 10-81, “Characterizing and Implementing Efficient Primitives for Privacy-Preserving Computation”, Defense Advanced Research Projects Agency and Air Force Research Labs, \$550,000 (\$262,375 investigator share), 05/01/2011-01/31/2015.

Industry and Other Support

- **co-PI**, “Mitigating Threat of Re-Identification from Eye-Tracking Data”, Meta Privacy-Enhancing Technology Award, \$100,000 ((\$49,000 investigator share)), 9/1/2022-8/31/2023.
- **co-PI**, “Center for Aerospace Resilience”, Florida Department of Education, \$875,000 (\$126,214 investigator share), 7/1/2020-7/31/2021.
- **PI**, “Secure Enclave Computing”, Royal Bank of Canada, \$87,347, 11/01/2019-01/01/2021.
- **PI**, NSF 1823067, “Travel Grant Support for ACM WiSec”, National Science Foundation, \$9,000, 05/27/2018-05/26/2019.
- **Co-PI**, “Formal Analysis of SGX Platform Software”, Intel Corporation, \$50,000 (\$25,000 investigator share), 01/01/2018-12/31/2018.
- **PI**, “Smartphones and Mobile money: Analysis and Recommendations for Security”, GSMA Mobile For Development Foundation, \$28,500 (\$13,500 investigator share), 12/01/2017-03/31/2018.
- **PI**, “Provenance-Based Enforcement Mechanisms”, MIT Lincoln Laboratory, \$137,000, 11/01/2013-10/31/2016.

- **PI**, “Securing Storage for Insider Threat Mitigation”, *Florida Cyber Consortium Seed Grant*, \$40,000 (\$20,000 investigator share), 2015.
- **co-PI**, “Resilience in BGPsec”, *Battelle*, \$180,000 \$80,000 investigator share, 02/01/2012-08/31/2013.
- **co-PI**, “A Cyber-Security Center of Excellence for Oregon”, *Oregon Engineering, Technology, and Industry Council*, \$180,000 (\$60,000 investigator share), 06/01/2014-05/31/2015.
- **co-PI**, “I3: An Interdisciplinary Approach to Internet Privacy”, *University of Oregon Research, Innovation and Graduate Education*, \$50,000, 04/10/2014-03/31/2015.
- **PI**, NSF CNS 1329307, “Oregon Security Day”, *National Science Foundation*, \$8,000, 03/01/2013-04/30/2014.
- **Recipient**, “USB Fingerprinting”, *Ellisys, equipment donation*, \$8,000, 2011.
- **Recipient**, “Project HAWAII”, *Microsoft Research, equipment donation*, \$1,000, 2011.

Publications (4986 citations [Google Scholar, July 2023], h-index=39, i10-index=73)

Book Chapters

1. Adam Bates, Devin Pohly, and Kevin R. B. Butler. “Secure and Trustworthy Provenance Collection for Digital Forensics.” In C. Wang, R. M. Gerges, Y. Guan, and S. K. Kasera, eds., *Digital Fingerprinting* (pp. 141–176). New York: Springer-Verlag, 2016.
2. Kevin Butler, William Enck, Patrick Traynor, Jennifer Plasterr, and Patrick McDaniel. “Privacy Preserving Web-Based Email”. *Algorithms, Architectures and Information Systems Security*, Statistical Science and Interdisciplinary Research. World Scientific Computing, November 2008.

Journal Publications

3. Brendan David-John, Kevin Butler, and Eakta Jain. “Privacy-preserving Datasets of Eye-tracking Samples with Applications in XR.” *IEEE Transactions on Visualization and Computer Graphics*, January 2023. 11 pages. *Selected for presentation at IEEE VR 2023 conference.*
4. Weidong Zhu and Kevin Butler. “NASA: NVM-Assisted Secure Deletion for Flash Memory.” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, July 2022 (early access). Accepted for presentation at the International Conference on Embedded Software (EMSOFT) 2022.
5. Tuba Yavuz, Farhaan Fowze, Grant Hernandez, Ken (Yihang) Bai, Kevin Butler, and Dave (Jing) Tian. “ENCIDER: Detecting Timing and Cache Side Channels in SGX Enclaves and Cryptographic APIs.” *IEEE Transactions on Dependable and Secure Computing*, March 2022 (early access). 18 pages.
6. Brendan David-John, Diane Hosfelt, Kevin Butler, and Eakta Jain. “A Privacy-Preserving Approach to Streaming Eye-Tracking Data.” *IEEE Transactions on Visualization and Computer Graphics*, March 2021 (early access). 11 pages. *Best paper nominee at IEEE VR 2021 conference.*
7. Farhaan Fowze, Grant Hernandez, Dave (Jing) Tian, Kevin Butler, and Tuba Yavuz. “ProXray: Pro-

- tol Model Learning and Guided Firmware Analysis.” *IEEE Transactions on Software Engineering*, September 2019.
8. Grant Hernandez, Dave (Jing) Tian, Farhaan Fowze, Tuba Yavuz, Patrick Traynor, and Kevin Butler. “Towards Automated Firmware Analysis in the IoT Era.” *IEEE Security and Privacy*, 17(5), pg. 38-46, Sept.-Oct. 2019.
 9. Joseph Choi and Kevin Butler. “Secure Multiparty Computation and Trusted Hardware: Examining Adoption Challenges and Opportunities”. *Security and Communication Networks*, vol 2019, Article ID 1368905, 28 pages, April 2019.
 10. Benjamin Mood and Kevin Butler. “PAL: A System for Optimizing Secure Function Evaluation in Mobile Devices”. *Journal of Information Security and Applications*, 40(2018), pg. 78-91, March 2018.
 11. Bradley Reaves, Luis Vargas, Nolen Scaife, Dave (Jing) Tian, Logan Blue, Patrick Traynor, and Kevin Butler. “Characterizing the Security of the SMS Ecosystem with Public Gateways”. *ACM Transactions on Privacy and Security*, 22(1), Article 2, January 2018.
 12. Nolen Scaife, Patrick Traynor, and Kevin Butler. “Making Sense of the Ransomware Mess (and planning a sensible path forward)”. *IEEE Potentials*, 36(6), pg. 28-31, Nov/Dec. 2017.
 13. Dave (Jing) Tian, Kevin R. B. Butler, Joseph Choi, Patrick D. McDaniel, and Padma Krishnaswamy. “Securing ARP/NDP From the Ground Up.” *IEEE Transactions on Information Forensics and Security*, 12(9), pg. 2131-2143, September 2017.
 14. Adam Bates, Dave (Jing) Tian, Grant Hernandez, Thomas Moyer, Kevin R. B. Butler, and Trent Jaeger. “Taming the Costs of Trustworthy Provenance through Policy Reduction.” *ACM Transactions on Internet Technology*, 17(4), Article 34, September 2017.
 15. Bradley Reaves, Jasmine Bowers, Nolen Scaife, Adam Bates, Arnav Bhartiya, Patrick Traynor, and Kevin Butler. “Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications”. *ACM Transactions on Privacy and Security*, 20(3), Article 11, August 2017.
 16. Bradley Reaves, Jasmine Bowers, Sigmund Albert Gorski III, Rahul Bobate, Raymond Cho, Hiranava Sas, Sharique Hussain, Hamza Karachiwala, Nolen Scaife, Byron Wright, Kevin Butler, William Enck, and Patrick Traynor. “*droid: Assessment and Evaluation of Android Application Analysis Tools”. *ACM Computing Surveys*, 49(3), Article 55, November 2016.
 17. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. “Outsourcing Secure Two-Party Computation as a Black Box”. *Security and Communication Networks*, 9(14), pg. 2261-2275, September 2016.
 18. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. “Secure Outsourced Garbled Circuit Evaluation for Mobile Devices.” *Journal of Computer Security*, 24(2), pg. 137-180, 2016.
 19. Adam Bates, Kevin Butler, Micah Sherr, Clay Shields, Patrick Traynor, and Dan Wallach. “Accountable Wiretapping -or- I Know That You Can Hear Me Now”. *Journal of Computer Security*, 23 (2015), pg. 167-195, 2015.
 20. Adam Bates, Benjamin Mood, Joe Pletcher, Hannah Pruse, Masoud Valafar, and Kevin Butler. “On Detecting Co-Resident Cloud Instances Using Network Flow Watermarking Techniques”. *International Journal of Information Security*, 13(2), pg. 171-189, April 2014.
 21. Thomas Moyer, Kevin Butler, Joshua Schiffman, Patrick McDaniel, and Trent Jaeger. “Scalable Web

- Content Attestation”. *IEEE Transactions on Computers*, 61(5), pg. 686-699, May 2012.
22. Kevin Butler, Stephen McLaughlin, Thomas Moyer, and Patrick McDaniel. “New Security Architectures Based on Emerging Disk Functionality”. *IEEE Security and Privacy*, 8(5), pg. 34-31, Sept./Oct. 2010.
 23. Kevin Butler, Toni Farley, Patrick McDaniel, and Jennifer Rexford. “A Survey of BGP Security Issues and Solutions”. *Proceedings of the IEEE*, 98(1), pg. 100-122, January 2010.
 24. Patrick Traynor, Kevin Butler, William Enck, Kevin Borders, and Patrick McDaniel. “*malnets*: Large-Scale Malicious Networks via Compromised Wireless Access Points”. *Journal of Security and Communication Networks (SCN)*. 2009.
 25. Kevin Butler, Sunam Ryu, Patrick Traynor, and Patrick McDaniel. “Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems”. *IEEE Transactions on Parallel and Distributed Systems*, 20(12), pg. 1803-1815, December 2009.
 26. Patrick McDaniel, William Aiello, Kevin Butler, and John Ioannidis, Origin Authentication in Interdomain Routing. *Computer Networks*, 50(16), pg. 2953-2980, 14 November 2006.

Conference Publications

Top-4 Security Conferences

27. Daniel Olszewski, Allison Lu, Carson Stillman, Kevin Warren, Cole Kitroser, Alejandro Pascual, Divyajyoti, Kevin Butler, and Patrick Traynor. ““Get in Researchers; We’re Measuring Reproducibility”: A Reproducibility Study of machine Learning Papers in Tier 1 Security Conferences”. 30th ACM Conference on Computer and Communications Security (CCS’23), Copenhagen, Denmark, November 2023. *Acceptance rate TBD*.
28. Kyungtae Kim, Sungwoo Kim, Kevin Butler, Antonio Bianchi, and Dave (Jing) Tian. “Fuzz The Power: Dual-role State Guided Black-box Fuzzing for USB Power Delivery”. *32nd USENIX Security Symposium (Security’23)*, Anaheim, CA, USA, August 2023. *Acceptance rate TBD*.
29. Yazhou Tu, Liqun Shen, Md Imran Hossen, Sara Rampazzi, Kevin Butler, and Xiali Hei. “Auditory Eyesight: Demystifying μ s-Precision Keystroke Tracking Attacks on Unconstrained Keyboard Inputs”. *32nd USENIX Security Symposium (Security’23)*, Anaheim, CA, USA, August 2023. *Acceptance rate TBD*.
30. Yan Long, Pirouz Naghavi, Blas Kojusner, Kevin Butler, Sara Rampazzi, and Kevin Fu. “Side eye: Characterizing the Limits of POV Acoustic Eavesdropping from Smartphone Cameras with Rolling Shutters and Movable Lenses”. *44th IEEE Symposium on Security and Privacy (Oakland’23)*, San Francisco, CA, USA, May 2023. *Acceptance rate TBD*.
31. Tyler Tucker, Hunter Searle, Kevin Butler, and Patrick Traynor. “Blue’s Clues: Practical Discovery of Non-Discoverable Bluetooth Devices”. *44th IEEE Symposium on Security and Privacy (Oakland’23)*, San Francisco, CA, USA, May 2023. *Acceptance rate TBD*.
32. Logan Blue, Kevin Warren, Hadi Abdullah, Cassidy Gibson, Luis Vargas, Jessica O’Dell, Kevin Butler, and Patrick Traynor. “Who Are You (I Really Wanna Know)?” *31st USENIX Security Symposium (Security’22)*, Boston, MA, USA, Aug 2022. *Acceptance rate: 18.1%*.
33. Kyungtae Kim, Taegyu Kim, Ertza Warriach, Byoungyoung Lee, Kevin Butler, Antonio Bianchi,

- and Dave (Jing) Tian. “FuzzUSB: Hybrid Stateful Fuzzing of USB Gadget Stacks.” *43rd IEEE Symposium on Security and Privacy (Oakland’22)*, San Francisco, CA, USA, May 2022. *Acceptance rate: 14.5%.*
34. Grant Hernandez, Marius Muench, Dominik Maier, Alyssa Milburn, Shinjo Park, Tobias Scharnowski, Tyler Tucker, Patrick Traynor, and Kevin Butler. “FirmWire: Transparent Dynamic Analysis for Cellular Baseband Firmware.” *2022 ISOC Network and Distributed System Security Symposium (NDSS’22)*, San Diego, CA, USA, April 2022. *Acceptance rate: 16.2%.*
 35. Grant Hernandez, Dave (Jing) Tian, Anurag Yadav, Byron J. Williams, and Kevin Butler. “Big-MAC: Fine-Grained Policy Analysis of Android Firmware.” *29th USENIX Security Symposium (Security’20)*, Boston, MA, USA, August 2020. (*Acceptance rate: 16.1%.*)
 36. Dave (Jing) Tian, Grant Hernandez, Joseph Choi, Vanessa Frost, Peter Johnson, and Kevin Butler. “LBM: A Security Framework for Peripherals within the Linux Kernel.” *40th IEEE Symposium on Security and Privacy (Oakland’19)*, San Francisco, CA, USA, May 2019. (*Acceptance rate=12.0%.*)
 37. Luis Vargas, Logan Blue, Vanessa Frost, Christopher Patton, Nolen Scaife, Kevin Butler, and Patrick Traynor. “Digital Healthcare-Associated Infection Analysis of a Major Multi-Campus Hospital System.” *26th ISOC Network and Distributed System Security Symposium (NDSS’19)*, San Diego, CA, USA, February 2019. (*Acceptance rate=17.1%*)
 38. Hadi Abdullah, Washington Garcia, Christian Peeters, Patrick Traynor, Kevin Butler, and Joseph Wilson. “Practical Hidden Voice Attacks against Speech and Speaker Recognition Systems.” *26th ISOC Network and Distributed System Security Symposium (NDSS’19)*, San Diego, CA, USA, February 2019. (*Acceptance rate=17.1%*)
 39. Luis Vargas, Gyan Hazarika, Rachel Culpepper, Kevin Butler, Thomas Shrimpton, Doug Szjada, and Patrick Traynor. “Mitigating Risk while Complying with Data Retention Laws.” *25th ACM Conference on Computer and Communications Security (CCS’18)*, Toronto, ON, Canada, October 2018. (*Acceptance rate=17.0%*)
 40. Dave (Jing) Tian, Grant Hernandez, Joseph Choi, Vanessa Frost, Christie Ruales, Patrick Traynor, Hayawardh Vijaykumar, Lee Harrison, Amir Rahmati, Mike Grace, and Kevin Butler. “ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem.” *27th USENIX Security Symposium (Security’18)*, Baltimore, MD, USA, August 2018. (*Acceptance rate=19.1%*)
 41. Dave (Jing) Tian, Nolen Scaife, Deepak Kumar, Michael Bailey, Adam Bates, and Kevin Butler. “SoK: “Plug & Pray” Today – Understanding USB Insecurity in Versions 1 through C.” *2018 IEEE Symposium on Security and Privacy (Oakland’18)*, San Francisco, CA, USA, May 2018. *Nominated for Distinguished Paper Award. (Acceptance rate=11.5%)*
 42. Christian Peeters, Hadi Abdullah, Nolen Scaife, Jasmine Bowers, Patrick Traynor, Bradley Reaves, and Kevin Butler. “Sonar: Detecting SS7 Redirection Attacks Via Call Audio-Based Distance Bounding.” *2018 IEEE Symposium on Security and Privacy (Oakland’18)*, San Francisco, CA, USA, May 2018. (*Acceptance rate=11.5%*)
 43. Grant Hernandez, Farhaan Fowze, Dave (Jing) Tian, Tuba Yavuz, and Kevin Butler. “FirmUSB: Vetting USB Device Firmware using Domain Informed Symbolic Execution.” *24th ACM Conference on Computer and Communications Security (CCS’17)*, Dallas, TX, USA October 2017. (*Acceptance rate=18.1%.*)

44. Dave (Jing) Tian, Adam Bates, Kevin Butler, and Raju Rangaswami. "ProvUSB: Block-level Provenance-Based Data Protection for USB Storage Devices." *23rd ACM Conference on Computer and Communications Security (CCS'16)*, Vienna, Austria, October 2016. (Acceptance rate=16.5%.)
45. Dave (Jing) Tian, Nolen Scaife, Adam Bates, Kevin Butler, and Patrick Traynor. "Making USB Great Again with USBFILTER". *25th USENIX Security Symposium (Security'16)*, Austin, TX, USA, August 2016. (Acceptance rate=15.5%.)
46. Bradley Reaves, Dave Tian, Nolen Scaife, Logan Blue, Patrick Traynor, and Kevin Butler. "Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways". *2016 IEEE Symposium on Security and Privacy (Oakland'16)*, San Jose, CA, USA, May 2016. (Acceptance rate=13.3%.)
47. Adam Bates, Dave Tian, Kevin Butler, and Thomas Moyer. "Trustworthy Whole-System Provenance for the Linux Kernel". *24th USENIX Security Symposium (Security'15)*, Washington, DC, USA, August 2015. (Acceptance rate=15.7%)
48. Bradley Reaves, Nolen Scaife, Adam Bates, Patrick Traynor, and Kevin Butler. "Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World". *24th USENIX Security Symposium (Security'15)*, Washington, DC, USA, August 2015. (Acceptance rate=15.7%)
49. Benjamin Mood, Debayan Gupta, Kevin Butler, and Joan Feigenbaum. "Reuse It Or Lose It: More Efficient Secure Computation Through Reuse of Encrypted Values". *21st ACM Conference on Computer and Communications Security (CCS'14)*, Scottsdale, AZ, USA, November 2014. (Acceptance rate=19%)
50. Adam Bates, Joe Pletcher, Tyler Nichols, Braden Hollembaek, Dave Tian, Abdulrahman Alkhelaifi, and Kevin Butler. "Securing SSL Certificate Verification through Dynamic Linking". *21st ACM Conference on Computer and Communications Security (CCS'14)*, Scottsdale, AZ, USA, November 2014. (Acceptance rate=19%)
51. Adam Bates, Ryan Leonard, Hannah Pruse, Daniel Lowd, and Kevin Butler. "Leveraging USB to Establish Host Identity Using Commodity Devices." *21st ISOC Network and Distributed System Security Symposium (NDSS'14)*, San Diego, CA, USA, February 2014. (Acceptance rate=18.6%)
52. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. "Secure Outsourced Garbled Circuit Evaluation for Mobile Devices". *22nd USENIX Security Symposium (Security'13)*, Washington, DC, USA, August 2013. (Acceptance rate=16.2%.)
53. Benjamin Kreuter, ahbi shelat, Benjamin Mood, and Kevin Butler. "PCF: A Portable Circuit Format For Scalable Two-Party Secure Computation". *22nd USENIX Security Symposium (Security'13)*, Washington, DC, USA, August 2013. (Acceptance rate=16.2%.)
54. Adam Bates, Kevin Butler, Micah Sherr, Clay Shields, Patrick Traynor, and Dan Wallach. "Accountable Wiretapping -or- I Know That You Can Hear Me Now". *19th ISOC Network and Distributed System Security Symposium (NDSS'12)*, San Diego, CA, USA, February 2012. (Acceptance rate=17.6%)
55. Kevin Butler, Stephen McLaughlin, and Patrick McDaniel. Rootkit Resistant Disks. *15th ACM Conference on Computer and Communications Security (CCS'08)*, Alexandria, VA, USA, October 2008. (Acceptance rate=18.1%)
56. Patrick Traynor, Kevin Butler, William Enck, and Patrick McDaniel. Realizing Massive-Scale Con-

ditional Access Systems Through Attribute-Based Cryptosystems. *15th Annual Network and Distributed System Security Symposium (NDSS'08)*, San Diego, CA, USA. February 2008. (Acceptance rate=17.8%)

57. Kevin Butler, William Aiello, and Patrick McDaniel. Optimizing BGP Security by Exploiting Path Stability. *13th ACM Conference on Computer and Communications Security (CCS'06)*, Alexandria, VA, USA, November 2006. (Acceptance rate=14.8%)

Other Conference Publications

58. Christian Peeters, Tyler Tucker, Anushri Jain, Kevin Butler, and Patrick Traynor. "LeopardSeal: Detecting Call Interception via Audio Rogue Base Stations". *21st ACM International Conference on Mobile Systems, Applications, and Services (MobiSys'23)*, Helsinki, Finland, June 2023. Acceptance rate: 20.7%
59. Washington Garcia, Pin-Yu Chen, Hamilton Scott Clouse, Somesh Jha, and Kevin Butler. "Less is More: Dimension Reduction Finds On-Manifold Adversarial Examples in Hard-Label Attacks". *IEEE Conference on Secure and Trustworthy Machine Learning (SatML 2023)*, Raleigh, NC, USA, February 2023. Acceptance rate: 25.3%
60. Daniel Olszewski, Weidong Zhu, Sandeep Sathyanarayana, Kevin Butler, and Patrick Traynor. "HallMonitor: A Framework for Identifying Network Policy Violations in Software". *2022 IEEE Conference on Communications and Network Security (CNS 2022)*, Austin, TX, USA, October 2022. (Acceptance rate TBD.)
61. Cassidy Gibson, Vanessa Frost, Katie Platt, Washington Garcia, Luis Vargas, Sara Rampazzi, Vincent Bindschaedler, Patrick Traynor, and Kevin Butler. "Analyzing the Monetization Ecosystem of Stalkerware." *22nd Privacy Enhancing Technologies Symposium (PETS 2022)*, Sydney, Australia, July 2022. (Acceptance rate: 24%)
62. Washington Garcia, Scott Clouse, and Kevin Butler. "Disentangling Categorization in Multi-agent Emergent Communication." *2022 Conference of the North American Chapter of the Association for Computational Linguistics (NAACL 2022)*, Seattle, WA, USA, July 2022. Acceptance rate: 21%
63. Shantanu Ghosh, Zheng Feng, Kevin Butler, and Mattia Prosperi. "DR-VIDAL: Doubly Robust Variational Information-theoretic Deep Adversarial Learning for Counterfactual Prediction and Treatment Effect Estimation." *2022 American Medical Informatics Association Annual Symposium (AMIA 2022)*, Washington, DC, USA, November 2022.
64. Brendan David-John, Kevin Butler, and Eakta Jain. "For Your Eyes Only: Privacy-Preserving Eye-Tracking Datasets." *14th ACM Symposium on Eye Tracking Research and Applications (ETRA 2022)* Seattle, WA, USA, June 2022. (Acceptance rate: 42%)
65. Mounir Elbharabawy, Blas Kojusner, Mohammad Mannan, Kevin Butler, Byron Williams, and Amr Youssef. "SAUSAGE: Security Analysis of Unix domain Socket Usage in Android." *7th IEEE European Symposium on Security and Privacy (Euro S&P'22)*, Genoa, Italy, June 2022. (Acceptance rate TBD. Best paper finalist.)
66. Arslan Khan, Joseph Choi, Dave (Jing) Tian, Tyler Ward, Kevin Butler, Patrick Traynor, John M. Shea and Tan Wong. "Privacy-Preserving Localization Using Enclaves." *12th IEEE Ubiquitous Computing, Electronics and Mobile Communication Conference (IEEE UEMCON 2021)*, Virtual Confer-

ence, December 2021.

67. Washington Garcia, Animesh Chhotaray, Joseph Choi, Suman Adari, Kevin Butler, and Somesh Jha. "Brittle Features of Device Authentication." *11th ACM Conference on Data and Application Security and Privacy (CODASPY'21)*, virtual event, April 2021. (Acceptance rate: 24.5%.)
68. Joseph Choi, Dave (Jing) Tian, Grant Hernandez, Christopher Patton, Benjamin Mood, Thomas Shrimpton, Patrick Traynor, and Kevin Butler. "A Hybrid Approach to Secure Function Evaluation using SGX." *14th ACM ASIA Conference on Computer and Communications Security (ASIACCS'19)*, Auckland, New Zealand, July 2019. (Acceptance rate [full papers]: 17%.)
69. Vanessa Frost, Dave (Jing) Tian, Christie Ruales, Patrick Traynor, and Kevin Butler. "Examining DES-based Cipher Suite Support within the TLS Ecosystem." *14th ACM ASIA Conference on Computer and Communications Security (ASIACCS'19)*, Auckland, New Zealand, July 2019. (Acceptance rate: 22%.)
70. Jasmine Bowers, Imani Sherman, Kevin Butler, and Patrick Traynor. "Characterizing Security and Privacy Practices in Emerging Digital Credit Applications." *12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'19)*, Miami, FL, USA, May 2019. (Acceptance rate=25.5%)
71. Dave (Jing) Tian, Joseph Choi, Grant Hernandez, Patrick Traynor, and Kevin Butler. "A Practical Intel SGX Setting for Linux Containers in the Cloud." *9th ACM Conference on Data and Application Security and Privacy (CODASPY'19)*, Dallas, TX, USA, March 2019. (Acceptance rate=23.5%)
72. Lianying Zhao, Joseph Choi, Didem Demirag, Kevin Butler, Mohammad Mannan, Erman Ayday, and Jeremy Clark. One-Time Programs Made Practical. *23rd International Conference on Financial Cryptography and Data Security (FC'19)*, St. Kitts, February 2019. (Acceptance rate=18.5%)
73. Robert Karam, Tamzidul Hoque, Kevin Butler, and Swarup Bhunia. Mixed-Granular Architectural Diversity for Device Security in the Internet of Things. *Asian Hardware Oriented Security and Trust Symposium (AsianHOST 2017)*, Beijing, China, October 2017.
74. Tyler Ward, Joseph Choi, Kevin Butler, John M. Shea, Patrick Traynor, and Tan Wong. Privacy Preserving Localization Using a Distributed Particle Filtering Protocol. *IEEE MILCOM*, Baltimore, MD, October 2017.
75. Jasmine Bowers, Bradley Reaves, Imani N. Sherman, Patrick Traynor, and Kevin Butler. Regulators, Mount Up! Analysis of Privacy Policies for Mobile Money Services. *13th Symposium on Usable Privacy and Security (SOUPS 2017)*, Santa Clara, CA, July 2017. (Acceptance rate=26.5%)
76. Adam Bates, Wajih Ul Hassan, Kevin Butler, Alin Dobra, Brad Reaves, Patrick Cable, Thomas Moyer, and Nabil Schear. Transparent Web Service Auditing via Network Provenance Functions. *26th World Wide Web Conference (WWW 2017)*, Perth, Australia, April 2017. (Acceptance rate=17.0%)
77. Benjamin Mood, Debayan Gupta, Henry Carter, Kevin Butler, and Patrick Traynor. "Frigate: A Validated, Extensible, and Efficient Compiler and Interpreter for Secure Computation". *1st IEEE European Symposium on Security and Privacy (Euro S&P 2016)*, Saarbrücken, Germany, March 2016. (Acceptance rate=17.3%.)
78. Sriharsha Etigowni, Dave (Jing) Tian, Grant Hernandez, Saman Zonouz, and Kevin Butler. CPAC: Securing Critical Infrastructure with Cyber-Physical Access Control. *32nd Annual Computer Security Applications Conference*, Los Angeles, CA, USA, December 2016. (Acceptance rate=22.8%)

79. Thomas Moyer, Patrick Cable, Karishma Chadha, Robert Cunningham, Nabil Schear, Warren Smith, Adam Bates, Kevin Butler, Frank Capobianco, and Trent Jaeger. "Leveraging Data Provenance to Enhance Cyber Resilience". *1st IEEE Cybersecurity Development Conference (SecDev 2016)*, Boston, MA, November 2016. (Acceptance rate=52.2%.)
80. Bradley Reaves, Dave Tian, Nolen Scaife, Logan Blue, Patrick Traynor, and Kevin Butler. "Detecting SMS Spam in the Age of Legitimate Bulk Messaging". *9th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'16)*, Darmstadt, Germany, July 2016. (Acceptance rate=35%.)
81. Nolen Scaife, Henry Carter, Patrick Traynor, and Kevin Butler. "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data". *36th IEEE International Conference on Distributed Computing Systems (ICDCS 2016)*, Nara, Japan, June 2016. (Acceptance rate=17.6%)
82. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. "Outsourcing Secure Two-Party Computation as a Black Box". *14th International Conference on Cryptology and Network Security (CANS 2015)*, Marrakesh, Morocco, December 2015. (Acceptance rate=52.9%.)
83. Dave Tian, Adam Bates, and Kevin Butler. "Defending Against Malicious USB Firmware with GoodUSB". *31st Annual Computer Security Applications Conference (ACSAC 2015)*, Los Angeles, CA, USA, December 2015. (Acceptance rate=24.4%.)
84. Ethan Shernan, Henry Carter, Jing (Dave) Tian, Patrick Traynor, and Kevin Butler. "More Guidelines Than Rules: CSRF Vulnerabilities from Noncompliant OAuth 2.0 Implementations". *12th Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA 2015)*, Milano, Italy, July 2015. (Acceptance rate=22.7%)
85. Jing (Dave) Tian, Kevin Butler, Patrick McDaniel, and Padma Krishnaswamy. "Securing ARP From the Ground Up". *5th ACM Conference on Data and Application Security and Privacy (CODASPY 2015)*, San Antonio, TX, USA, March 2015. (Acceptance rate=33.3%)
86. Adam Bates, Joe Pletcher, Tyler Nichols, Braden Hollembaek, and Kevin Butler. "Forced Perspectives: Evaluating an SSL Trust Enhancement at Scale". *2014 ACM Internet Measurement Conference (IMC'14)*, Vancouver, BC, Canada, November 2014. (Acceptance rate=22.9%)
87. Adam Bates, Benjamin Mood, Masoud Valafar, and Kevin Butler. "Towards Secure Provenance-Based Access Control in Cloud Environments". *3rd ACM Conference on Data and Application Security and Privacy (CODASPY 2013)*, San Antonio, TX, USA, February 2013. (Acceptance rate=31.8%)
88. Vasant Tendulkar, Joe Pletcher, Ashwin Shashidharan, Ryan Snyder, Kevin Butler, and William Enck. "Abusing Cloud-based Browsers for Fun and Profit". *28th Annual Computer Security Applications Conference (ACSAC 2012)*, Orlando, FL, USA, December 2012. (Acceptance rate=19.0%)
89. Devin J. Pohly, Stephen McLaughlin, Patrick McDaniel, and Kevin Butler. "Hi-Fi: Collecting High-Fidelity Whole-System Provenance". *28th Annual Computer Security Applications Conference (ACSAC 2012)*, Orlando, FL, USA, December 2012. (Acceptance rate=19.0%)
90. Benjamin Mood, Lara Letaw, and Kevin Butler. "Memory-Efficient Garbled Circuit Generation for Mobile Devices". *16th IFCA International Conference on Financial Cryptography and Data Security (FC'12)*, Bonaire, February 2012. (Acceptance rate=26.1%)
91. Kevin Butler, Stephen McLaughlin, and Patrick McDaniel, "Kells: A Protection Framework for Portable Data". *26th Annual Computer Security Applications Conference (ACSAC 2010)*, Austin, TX,

USA, December 2010. (*Acceptance rate=16.3%*)

92. Machigar Ongtang, Kevin Butler, and Patrick McDaniel. "Porscha: Policy Oriented Secure Content Handling in Android." *26th Annual Computer Security Applications Conference (ACSAC 2010)*, Austin, TX, USA, December 2010. (*Acceptance rate=16.3%*)
93. Kevin Butler, Stephen McLaughlin, and Patrick McDaniel. "Disk-Enabled Authenticated Encryption" (short paper). *26th IEEE Symposium on Massive Storage Systems and Technologies (MSST 2010)*, Incline Village, NV, USA, May 2010. (*Acceptance rate=45.5%*.)
94. Thomas Moyer, Kevin Butler, Joshua Schiffman, Patrick McDaniel, and Trent Jaeger. Scalable Web Content Attestation. *25th Annual Computer Security Applications Conference (ACSAC 2009)*, Honolulu, HI, USA, December 2009. (*Acceptance rate=19.0%*.)
95. William Enck, Kevin Butler, Thomas Richardson, Patrick McDaniel, and Adam Smith. Defending Against Attacks on Main Memory Persistence. *24th Annual Computer Security Applications Conference (ACSAC 2008)*, Anaheim, CA, USA, December 2008. (*Acceptance rate=24.3%*)
96. Dhananjay Bapat, Kevin Butler, and Patrick McDaniel. Towards Automatic Privilege Separation. *3rd International Conference on Information Systems Security (ICISS 2007)*, Delhi, India, December 2007. (*Acceptance rate=25.0%*)
97. Lisa Johansen, Kevin Butler, Michael Rowell, and Patrick McDaniel. Email Communities of Interest. *Fourth Conference on Email and Anti-Spam (CEAS 2007)*, Mountain View, CA, USA, August 2007. (*Acceptance rate=19.0%*.)
98. Anusha Sriraman, Kevin Butler, Patrick McDaniel, and Padma Raghavan. Analysis of the IPv4 Address Space Delegation Structure. *IEEE Symposium on Computers and Communications (ISCC'07)*, Aveiro, Portugal, July 2007. (*Acceptance rate=40%*.)
99. Sunam Ryu, Kevin Butler, Patrick Traynor, and Patrick McDaniel. Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems. *3rd IEEE International Symposium on Security in Networks and Distributed Systems (SSNDS'07)*, Niagara Falls, ON, Canada, May 2007. (*Acceptance rate=40%*)
100. Kevin Butler, Patrick Traynor, William Enck, Jennifer Plasterr, and Patrick McDaniel. Privacy Preserving Web-Based Email. *2nd International Conference on Information Systems Security (ICISS 2006)*, Kolkata, India, December 2006. (*Acceptance rate=30.4%*)
101. Trent Jaeger, Kevin Butler, David King, Serge Hallyn, Joy Latten, and Xiolan Zhang. Leveraging IPsec for Mandatory Per-Packet Access Control. *2nd IEEE Communications Society/CreateNet International Conference on Security and Privacy in Communication Networks (SecureComm'06)*, August 2006, Baltimore, MD, USA. (*Acceptance rate=25.4%*.)
102. Kevin Butler and Patrick McDaniel, Understanding Mutable Internet Pathogens, or How I Learned to Stop Worrying and Love Parasitic Behavior. *1st International Conference on Information Systems Security (ICISS 2005)*, December 2005, Kolkata, India. (*Invited paper.*)

Workshop Publications

103. Jennifer Sheldon, Weidong Zhu, Adnan Abdulla, Kevin Butler, Md Jahidul Islam, and Sara Rappazzi. "Position: Deep Note: Can Acoustic Interference Damage the Availability of Hard Disk Storage

in Underwater Data Centers?” *15th ACM Workshop on Hot Topics in Storage and Files Systems (Hot-Storage 2023)*, Boston, MA, USA, July 2023. *Best Paper Award*.

104. Brendan David-John, Diane Hosfelt, Kevin Butler, and Eakta Jain. “Let’s SOUP Up XR: Collected thoughts from an IEEE VR workshop on privacy in mixed reality.” *1st International Workshop on Security for XR and XR for Security (VR4Sec)*, in conjunction with SOUPS 2021, virtual event, August 2021.
105. Sushrut Shringarputale, Patrick McDaniel, Kevin Butler, and Thomas La Porta. “Co-residency Attacks on Containers are Real.” *2020 ACM Cloud Computing Security Workshop (CCSW’20)*, Orlando, FL, USA, November 2020.
106. Suman Adari, Washington Garcia, and Kevin Butler. “Adversarial Video Captioning”. *2019 Dependable and Secure Machine Learning Workshop (DSML’19)*, Portland, OR, USA, June 2019.
107. Siddhant Deshmukh, Henry Carter, Grant Hernandez, Patrick Traynor, and Kevin Butler. “Efficient and Secure Template Blinding for Biometric Authentication”. *2nd IEEE Workshop on Security and Privacy in the Cloud (SPC 2016)*, Philadelphia, PA, USA, October 2016.
108. Debayan Gupta, Benjamin Mood, Joan Feigenbaum, Kevin Butler and Patrick Traynor. “Using Intel Software Guard Extensions for Efficient Two-Party Secure Function Evaluation.” *2016 Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC’16)*, Barbados, February 2016.
109. Adam Bates, Kevin Butler, and Thomas Moyer. “Take Only What You Need: Leveraging Mandatory Access Control Policy to Reduce Provenance Storage Costs.” *7th Annual Workshop on Theory and Practice of Provenance (TaPP’15)*, Edinburgh, Scotland, July 2015.
110. Adam Bates, Kevin Butler, Andreas Haeberlen, Micah Sherr, and Wenchao Zhou. “Let SDN Be Your Eyes: Secure Forensics in Data Center Networks.” *NDSS Workshop on Security of Emerging Network Technologies (SENT)*, San Diego, CA, USA, February 2014.
111. Matt Bishop, Emily Rine Butler, Kevin Butler, Carrie Gates, and Steven Greenspan. “Forgive and Forget: Return to Obscurity”. *New Security Paradigms Workshop (NSPW 2013)*, Banff, AB, Canada, September 2013.
112. Peter McKay, Bryan Clement, Sean Haverty, Elijah Newton, and Kevin Butler. “Read My Lips: Towards Use of the Microsoft Kinect as a Visual-Only Automatic Speech Recognizer.” *2013 Workshop on Home Usable Privacy and Security (HUPS)*, Newcastle, UK, July 2013.
113. Adam Bates, Benjamin Mood, Joe Pletcher, Hannah Pruse, Masoud Valafar, and Kevin Butler. “Detecting Co-Residency with Active Traffic Analysis Techniques”. *4th ACM Cloud Computing Security Workshop (CCSW 2012)*, Raleigh, NC, USA, October 2012. (*Acceptance rate=12.0% for full papers.*)
114. Lara Letaw, Joe Pletcher, and Kevin Butler. “Host Identification via USB Fingerprinting”. *6th IEEE International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE 2011)*, Oakland, CA, USA, May 2011. (*Acceptance rate=34.8%.*)
115. Kevin Butler, William Enck, Harri Hursti, Stephen McLaughlin, Patrick Traynor, and Patrick McDaniel. Systemic Issues in the Hart InterCivic and Premier Voting Systems: Reflections Following Project EVEREST. *2008 USENIX/ACCURATE Electronic Voting Workshop (EVT’08)*, July 2008. San Jose, CA, USA. (*Acceptance rate=44.1%*)
116. Shiva Chaitanya, Kevin Butler, Anand Sivasubramaniam, Patrick McDaniel and Murali Vilayan-

nur. Design, implementation and evaluation of security in iSCSI-based network storage systems. *2nd International Workshop on Storage Security and Survivability (StorageSS 2006)*, October 2006. Alexandria, VA, USA. (Acceptance rate=68%)

117. Patrick McDaniel, Kevin Butler, Stephen McLaughlin, Radu Sion, Erez Zadok, and Marianne Winslett. "Towards a Secure and Efficient System for End-to-End Provenance". *USENIX Workshop on Theory and Practice of Provenance (TaPP)*, February 2010. (Acceptance rate=68.8%)
118. Kevin Butler and Petros Efstathopoulos. U Can't Touch This: Block-Level Protection for Portable Storage. *International Workshop on Software Support for Portable Storage (IWSSPS 2009)*, October 2009. Grenoble, France.
119. Kevin Butler, Stephen McLaughlin, and Patrick McDaniel. Non-Volatile Memory and Disks: Avenues for Policy Architectures. *1st Computer Security Architectures Workshop (CSAW 2007)*, November 2007. Fairfax, VA, USA. (Acceptance rate=30%)
120. Kevin Butler and Patrick McDaniel, Testing Large Scale BGP Security in Replayable Network Environments. *DETER Community Workshop on Cyber Security Experimentation and Test*, June 2006. Arlington, VA, USA.
121. Sophie Qiu, Kevin Butler, and Patrick McDaniel, BGPRV: Retrieving and Processing BGP Data with Efficiency and Convenience. *DETER Community Workshop on Cyber Security Experimentation and Test*, June 2006. Arlington, VA, USA.

Technical Reports

122. Efe Bozkir, Süleyman Özdel, Mengdi Wang, Brendan David-John, Hong Gao, Kevin Butler, Eakta Jain, and Enkelejda Kasneci. "Eye-tracked Virtual Reality: A Comprehensive Survey on Methods and Privacy Challenges." *arXiv:2305.14080*, May 2023.
123. Washington Garcia, Pin-Yu Chen, Somesh Jha, Scott Clouse, and Kevin Butler. "Hard-label Manifolds: Unexpected Advantages of Query Efficiency for Finding On-manifold Adversarial Examples." *arXiv:2013.03325*, March 2021.
124. Kevin Butler. "Digital Financial Services security audit guideline." Security, Infrastructure and Trust Working Group, Financial Inclusion Global Initiative, published by International Telecommunications Union (ITU), March 2021.
125. Kevin Butler and Vijay Mauree. "Digital Financial Services security assurance framework." Security, Infrastructure and Trust Working Group, Financial Inclusion Global Initiative, published by International Telecommunications Union (ITU), January 2021.
126. Washington Garcia, Joseph Choi, Suman Adari, Somesh Jha, and Kevin Butler. "Explainable Black-Box Attacks Against Model-based Authentication." *arXiv:1810.00024*, September 2018.
127. Kevin Butler, Patrick Traynor, and Tiago Novais. "MM App Security Best Practices." Official Document MM.01, GSM Association, London, United Kingdom, June 2018.
128. Kevin Butler, Leon Perlman, Paul Makin, Henry Gerwitz, Patrick Traynor, Yury Grin, Evgeniy Bondarenko, and Richard Miller. "ITU-T Focus Group Digital Financial Services: Security Aspects of Digital Financial Services (DFS)." Focus Group Technical Report, International Telecommunications Union, Geneva, Switzerland, January 2017.

129. Adam Bates, Joe Pletcher, Tyler Nichols, Braden Hollembaek, and Kevin Butler. "Towards Usable System-Wide Trust Agility." Technical Report CIS-TR-2013-13, Department of Computer and Information Science, University of Oregon, Eugene, OR, October 2013.
130. Benjamin Mood and Kevin Butler. "Optimizing Secure Function Evaluation for Mobile Devices". Technical Report CIS-TR-2013-10, Department of Computer and Information Science, University of Oregon, Eugene, OR, September 2013.
131. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. "Secure Outsourced Garbled Circuit Evaluation for Mobile Devices". Technical Report GT-CS-12-09, College of Computing, Georgia Institute of Technology, Atlanta, GA, December 2012.
132. Kevin Butler and Petros Efstathopoulos. U Can't Touch This: Block-Level Protection for Portable Storage. Technical Report Symantec-SRL/MV2009-11, Symantec Research Labs, Mountain View, CA, June 2009.
133. Kevin Butler, Stephen McLaughlin, Thomas Moyer, Joshua Schiffman, Patrick McDaniel, and Trent Jaeger. Firma: Disk-Based Foundations for Trusted Operating Systems. Technical Report NAS-TR-0114-2009, Networking and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, May 2009.
134. Kevin Butler, Stephen McLaughlin, Thomas Moyer, Patrick McDaniel, and Trent Jaeger. Switch-Blade: Policy-Driven Disk Segmentation. Technical Report NAS-TR-0098-2008, Networking and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, November 2008.
135. P. McDaniel, K. Butler, W. Enck, H. Hursti, S. McLaughlin, P. Traynor, M. Blaze, A. Aviv, P. Cerny, S. Clark, E. Cronin, G. Shah, M. Sherr, G. Vigna, R. Kemmerer, D. Balzarotti, G. Banks, M. Cova, V. Felmetsger, W. Robertson, F. Valeur, J. Hall, and L. Quilter, EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing. Public Report, Ohio Secretary of State, December 2007.
136. Kevin Butler, Stephen McLaughlin, Patrick McDaniel, and Youngjae Kim. Autonomously Secure Disks. Technical Report NAS-TR-0072-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, May 2007. (*Updated September 2007.*)
137. Lisa Johansen, Kevin Butler, William Enck, Patrick Traynor, and Patrick McDaniel. Grains of SANs: Building Storage Area Networks from Memory Spots. Technical Report NAS-TR-0060-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, January 2007.
138. Luke St. Clair, Lisa Johansen, Kevin Butler, William Enck, Matthew Pirretti, Patrick Traynor, Patrick McDainel, 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, May 2006. (*Updated January 2007.*)

Articles for Media

139. Patrick Traynor and Kevin Butler. "Mobile money in developing countries: study reveals secu-

urity flaws in apps”. *The Guardian*. 24 September 2015. http://www.theguardian.com/global-development-professionals-network/2015/sep/24/mobile-money-apps-security-flaws-study-reveals?CMP=tw_t_gu

Patents

U.S. Patent 8,856,918, Host validation mechanism for preserving integrity of portable storage data. Petros Efstathopoulos, Bruce Montague, Dharmesh Shah, Kevin Butler. October 7, 2014.

U.S. Patent 10,685,114, Malware Detection Via Data Transformation Monitoring. Walter N. Scaife, Kevin Butler, Henry Carter, Patrick G. Traynor. June 16, 2020.

U.S. Patent 11,265,717, Detecting SS7 Redirection Attacks with Audio-Based Distance Bounding. Patrick G. Traynor, Christian Peeters, Bradley G. Reeves, Hadi Abdullah, Kevin Butler, Jasmine Bowers, Walter N. Scaife. March 1, 2022.

U.S. Patent 11,568,044, Method and Apparatus For Vetting Universal Serial Bus Device Firmware. Kevin Butler, Tuba Yavuz, Jing Tian, Grant Hernandez, Farhaan Fowze. January 31, 2023.

U.S. Patent 11,640,464, Protocol Model Learning and Guided Firmware Analysis. Tuba Yavuz, Farhaan Fowze, Kevin Raymond Boyce Butler, Jing Tian, Grant Haydock Hernandez. May 2, 2023.

U.S. Patent 11,663,388, Automated Security Analysis of Baseband Firmware. Grant Haycock Hernandez, Kevin R. Butler, Patrick G. Traynor. May 31, 2023.

Teaching

University of Florida

- *CIS 4360: Computer and Information Security*, undergraduate, Fall 2020, Fall 2019, Fall 2018, Fall 2017.
- *CIS 5370: Computer and Information Security*, graduate, Spring 2023, Spring 2019, Spring 2018, Spring 2017.
- *CIS 6930: Special Topics: Mobile and Embedded System Security*, graduate, Spring 2020.
- *CNT 5410: Computer and Network Security*, graduate, Fall 2015.

University of Oregon

- *CIS 415: Operating Systems (substantially revised)*, Spring 2014, Spring 2013, Spring 2012, Spring 2011.
- *CIS 607: Seminar on Generating Trustworthy Data (new)*, Winter 2014.
- *CIS 607: Seminar on Embedded Systems and Security (new)*, Spring 2013.
- *CIS 433/533: Computer and Network Security*, Winter 2013, Winter 2011.
- *CIS 607: Seminar on Computer Security in the Physical World (new)*, Spring 2012.
- *CIS 330: C/C++ and UNIX (substantially revised)*, Winter 2012.
- *CIS 610: Advanced Topics in Systems Security (new)*, Fall 2011.
- *CIS 607: Seminar on Security in Systems, Storage, and Clouds (new)*, Fall 2010.

The Pennsylvania State University

- *EE/CSE 458: Computer Networks*, Summer 2006.

Professional Service

Editorial Positions, Panels, and Boards

Editorial Boards:

Associate Editor, ACM Transactions on Security and Privacy (TOPS), 2021-present.

Associate Editor, Journal of Computer Security, 2020-present.

Associate Editor, IEEE Transactions on Dependable and Secure Computing (*Impact Factor: 4.41*), 2019-2023.

Associate Editor, ACM Digital Threats: Research and Practice, 2017-2022.

Editorial Board, International Journal of Cybersecurity Science and Technology, 2017-2022.

Review Board, IEEE Systems Journal, Special Issues on Security and Privacy in Complex Systems, 2012.

Scientific Grant Panels:

Review Panelist, National Science Foundation, 2022, 2021, 2020, 2018, 2017, 2016, 2014 (2), 2013, 2012.

Review Panelist, American Association for the Advancement of Science (AAAS), 2019.

Grant Reviewer, Austrian Science Fund, 2018.

Grant Reviewer, Natural Science and Engineering Research Council of Canada, 2022, 2019, 2018, 2017.

Grant Reviewer, Israel Science Foundation, 2016.

Conference Steering Committees:

Steering Committee Member, ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2019 -*present*.

Steering Committee Member, Annual Computer Security Applications Conference, 2014 -*present*.

Service to National and International Organizations:

Council Member, Computing Research Association Computing Community Consortum, 2023-present.

Co-Chair, Security, Infrastructure, and Trust Working Group, Financial Inclusion Global Initiative, International Telecommunications Union, 2017-2022.

Co-Chair and Leader of Security Workstream, Technology, Innovation, and Competition Working Group, Focus Group on Digital Financial Services, International Telecommunications Union, 2015-2016.

Conference & Workshop Chairships

1. **Technical Program Co-Chair**, 32nd USENIX Security Symposium (USENIX Security'22), Boston, MA, USA, August 2022.
2. **Conference General Chair**, 36th and 37th Annual Computer Security Applications Conference (ACSAC'20, ACSAC'21), Austin, TX, USA, 2020,2021.
3. **Technical Program Co-Chair**, 16th EAI International Conference on Security and Privacy in Communication Networks (Securecomm 2020), Washington, DC, USA, October 2020.
4. **Technical Program Co-Chair**, 2020 USENIX Summit on Hot Topics in Security (HotSec'20), Boston, MA, USA, August 2020 (*suspended due to COVID-19 pandemic*)
5. **Technical Program Co-Chair**, 11th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'18), Stockholm, Sweden, July 2018.
6. **Conference General Chair**, 38th IEEE Symposium on Security and Privacy, San Jose, CA, May 2017.
7. **Vice Chair and Registration Chair**, 37th IEEE Symposium on Security and Privacy, San Jose, CA, May 2016.
8. **Technical Program Chair**, 30th Annual Computer Security Applications Conference (ACSAC 2014), New Orleans, LA, December 2014.
9. **Technical Program Co-Chair**, 29th Annual Computer Security Applications Conference (ACSAC 2013), New Orleans, LA, December 2013.

Other Conference & Workshop Organization Activities (118 Tech. Program Committees)

Top-4 Security Conferences

10. **USENIX Security Symposium**: *TPC Member*, 2021, 2020, 2019, 2018, 2017, 2015, 2014; *Short Talks Co-Chair*, 2017.
11. **IEEE Symposium on Security and Privacy (Oakland)**: *TPC Member*, 2024, 2023, 2021, 2020, 2018, 2017, 2016, 2012; *Publications Chair*, 2014, 2013, 2012, 2011, *Submissions Chair*, 2008.
12. **ISOC Network and Distributed Security Symposium (NDSS)**: *TPC Member*, 2021, 2020, 2019, 2018, 2017, 2016.
13. **ACM Conference on Computer and Communications Security (CCS)**: *TPC Member*, 2020, 2016, 2015, 2014, 2013; *TPC Member (Industry Track)*, 2007, 2004.

Other Conferences and Workshops

14. **Privacy Enhancing Technologies Symposium (PETS)/Journal of Privacy Enhancing Technologies**, *Senior PC Member*, 2023, *TPC Member/Editorial Board*, 2014-2016.
15. **IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)**: *TPC Member*, 2023.
16. **ACM Conference on Security in Wireless and Mobile Networks (WiSec)**: *TPC Member*, 2023, 2022, 2021, 2020, 2019, 2017, 2016, 2015, 2014.
17. **IEEE Secure Development Conference (SecDev)**: *TPC Member*, 2023, 2022.
18. **USENIX Annual Technical Conference (ATC)**: *TPC Member*, 2021, 2020.
19. **IEEE European Symposium on Security and Privacy (Euro S&P)**: *TPC Member*, 2020.
20. **USENIX Workshop on Cyber Security Experimentation and Test (CSET)**: *TPC Member*, 2019, 2015, 2014, 2013.
21. **International Workshop on the Theory and Practice of Provenance (TaPP)**: *TPC Member*, 2019.
22. **USENIX Enigma Conference**: *TPC Member*, 2019, 2018.
23. **ACM Cloud Computing Security Workshop (CCSW)**: *TPC Member*, 2019, 2014.
24. **International Provenance and Annotation Workshop (IPAW)**: *TPC Member*, 2018.
25. **ACM Symposium on Information, Computer and Communications Security (ASIACCS)**: *TPC Member*, 2018, 2017, 2015, 2014.
26. **Annual Computer Security Applications Conference (ACSAC)**: *TPC Member*, 2018, 2017, 2012, 2011; *Test of Time Awards Chair*, 2019; *Panels Chair*, 2012, 2011; *Publicity Chair*, 2010.
27. **World Conference on Information Security Applications (WISA)**: *TPC Member*, 2017.
28. **International Conference on Cryptology and Network Security (CANS)**: *TPC Member*, 2017.
29. **New Security Paradigms Workshop (NSPW)**: *TPC Member*, 2016, 2015, 2014, 2013.
30. **IEEE Mobile Security Technologies Workshop (MOST)**: *TPC Member*, 2015, 2014.
31. **Symposium and Bootcamp on the Science of Security (HotSoS)**: *TPC Member*, 2015.
32. **Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC)**: *TPC Member*, 2015.
33. **European Symposium on Research in Computer Security (ESORICS)**: *TPC Member*, 2014, 2013, 2012.
34. **Smart Energy Grid Security Workshop (SEGS)**: *TPC Member*, 2014, 2013.
35. **Conference on Privacy, Security and Trust (PST)**: *TPC Member*, 2014, 2013.
36. **Global Internet Symposium (GI)**: *TPC Member*, 2014.
37. **IEEE International Conference on Big Data (BigData)**: *TPC Member*, 2013.
38. **IEEE LCN Network Security Workshop (WNS)**: *TPC Member*, 2013.
39. **International Workshop on Security in Information Systems (WOSIS)**: *TPC Member*, 2013,

2012.

40. **International Conference on Applied Cryptography and Network Security (ACNS):** *TPC Member*, 2013.
41. **International Workshop on Security (IWSEC):**, *TPC Member*, 2012, 2008, 2007.
42. **Workshop on Secure Network Protocols (NPSec):** *Publicity Chair*, 2012.
43. **LCN Workshop on Security in Communication Networks (SICK):** *TPC Member*, 2012.
44. **USENIX Workshop on Hot Topics in Security (HotSec):** *TPC Member*, 2012.
45. **International Workshop on Security (IWSEC):** *TPC Member*, 2011, 2010.
46. **International Conference on Security and Privacy in Communication Networks (SecureComm):** *TPC Member*, 2011.
47. **International Conference on Availability, Reliability and Security (ARES):** *TPC Member*, 2011, 2010, 2009, 2008, 2007.
48. **International Conference on Internet Monitoring and Protection (ICIMP):** *TPC Member*, 2011, 2010.
49. **International Conference on Financial Cryptography and Data Security (FC):** *TPC Member*, 2011.
50. **International Conference on Information Systems Security (ICISS):** *TPC Member*, 2009, 2008, 2007; *Submissions and Web Chair*, 2007.
51. **IEEE International Workshop on Software Security Process:** *TPC Member*, 2009.
52. **International Conference on International Conference on Information Security and Assurance (ISA):** *TPC Member*, 2009, 2008; *Publicity Co-Chair*, 2008.
53. **International Workshop on Security in Systems and Networks (SSN):** *TPC Member*, 2009, 2007.
54. **Conference on Future Generation Communication and Networking (FGCN):** *TPC Member*, 2008, 2007.
55. **IEEE International Workshop on Security in Software Engineering (IWSSE):** *TPC Member*, 2008, 2007.
56. **IEEE/IFIP Conference on Dependable Systems and Networks (DSN):** *TPC Member (Fast Abstracts)*, 2008.
57. **International Workshop on Secure Software Engineering (SecSE):** *TPC Member*, 2008.

Conference Session Chair: USENIX Security'18, ACSAC'17, WWW'17, IEEE SP'16, CCS'16, CCS'14, HotSec'12, IEEE SP'12, CCS'09

Journal & Book Reviewing

IEEE Transactions on Dependable and Secure Computing (TDSC), 2019, 2014, 2010; Communications of the ACM (CACM), 2019; IEEE Transactions on Computers (TC), 2019, 2012, 2009; IEEE Security and Privacy, 2018, 2013, 2010; Journal of Computer Security (JCS), 2018; IEEE Transactions on Information Forensics and Security (TIFS), 2017, 2013, 2011; Journal of Internet Services and

Applications (JISA), 2017; ACM Transactions on Information and System Security (TISSEC), 2016, 2015, 2014, 2010, 2009, 2008, 2006; IEEE Transactions on Reliability (TR), 2014; ACM Transactions on Internet Technologies (TOIT), 2013, 2010, 2009; ACM Computing Surveys, 2013; ACM Transactions on Storage (TOS), 2013, 2011; Elsevier Computers and Security, 2013, 2011; International Journal of Computer Mathematics, 2011; IEEE Transactions on Parallel and Distributed Systems (TPDS), 2011, 2008; Wiley and Sons (Book proposal reviewer), 2010; EURASIP Journal on Information Security (JIS), 2011, 2010; Elsevier Journal of Computer Networks, 2010, 2005; International Journal of Software and Informatics (IJSI), 2010; International Journal of Security and Networks (IJSN), 2009, 2007; The Computer Journal (Oxford), 2009; ACM/IEEE Transactions on Networking (TON), 2008; Wireless Personal Communications, 2008; IEEE Communications Surveys and Tutorials, 2007; IEEE Transactions on Software Engineering (TSE), 2007; Software: Practice and Experience, 2007; Handbook of Information Security, 2004.

Conference & Workshop Reviewing

USENIX OSDI, 2016; IEEE INFOCOM, 2014, 2007; IEEE Symposium on Security and Privacy (S&P), 2013, 2009, 2008, 2007; ISOC Symposium on Network and Distributed Systems Security (NDSS), 2013, 2012, 2009, 2007; ACM Conference on Data and Application Security and Privacy (CODASPY), 2013; IEEE Computer Security Foundations Symposium (CSF), 2011; ACM Symposium on Computer and Communications Security (CCS), 2010, 2009, 2008, 2006; Annual Computer Security Applications Conference (ACSAC), 2010, 2007, 2006, 2005; USENIX Workshop on Hot Topics in Security (HotSec), 2010, 2007; ACM Symposium on Access Control Models and Technologies (SACMAT), 2010, 2009, 2008, 2006; IFCA International Conference on Financial Cryptography and Data Security (FC), 2010, 2008, 2007; Information Security Conference (ISC), 2009; USENIX Security Symposium, 2009, 2008, 2007, 2006, 2004; IEEE GLOBECOM, 2008; IFIP Conference on Data and Applications Security (DBSEC), 2008, 2006; USENIX Conference on File and Storage Technologies (FAST), 2008; IEEE International Conference on Computer Engineering and Systems (ICCES), 2007; IEEE International Conference on Distributed Computing Systems (ICDCS), 2007; IEEE Sarnoff Symposium, 2007; IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2007; ACM International Workshop on Storage Security and Survivability (StorageSS), 2006; International Workshop on Security (IWSEC), 2006; International Conference on Emerging Trends in Computer Science (ETRICS), 2006; International Conference on Applied Cryptography and Network Security (ACNS), 2006; European Symposium on Research in Computer Security (ESORICS), 2005.

University Service

Sabbatical Committee, Member, College of Engineering, University of Florida, 2021-present.

Steering Committee, Member, University of Florida, 2018-present.

Graduate Admissions Committee, Member, CISE, University of Florida, 2019-present.

Consortium for Media and Trust Director Search Committee, Member, University of Florida, 2019.

Faculty Search Committee, Chair, CISE, University of Florida, 2018-2021.

Faculty Search Committee, Member, CISE, University of Florida, 2017-2018.

Awards Committee, Member, CISE, University of Florida, 2015-present.

Graduate Affairs Committee, Member, CISE, University of Florida, 2014-2018.

Graduate Education Committee, Member, CIS, University of Oregon, 2010-2014.

Undergraduate Curriculum Committee, Member, CIS, University of Oregon, 2012-2014.

General Education Committee, Member, University of Oregon, 2013-2014.

Students

Graduate Advisees

Past Ph.D Advisees:

- Washington Garcia, Fall 2022, now **Research Scientist**, University of Dayton Research Institute.
- Grant Hernandez, Summer 2020, now **Senior Security Engineer**, Qualcomm.
- Dave (Jing) Tian, Summer 2019, now **Assistant Professor of Computer Science**, Purdue University (NSF CAREER award, 2022).
- Adam Bates, Summer 2016, now **Associate Professor of Computer Science**, University of Illinois at Urbana-Champaign (NSF CAREER award, 2018).
- Benjamin Mood Spring 2016, now **Assistant Professor of Computer Science**, Point Loma Nazarene University.

Current Ph.D. Advisees: Yunhao Wu (PhD, Spring 2024), Weidong Zhu (PhD, Spring 2024, co-advised with Sara Rampazzi), Cassidy Gibson (PhD, Spring 2025, co-advised with Patrick Traynor), Anna Crowder (PhD, Spring 2026), Caroline Fedele (PhD, Spring 2026), Magdalena Pasternak (PhD, Spring 2026), Carson Stillman (PhD, Spring 2028), Kevin Childs (PhD, Spring 2030).

Past Master's Degree Students: Benjamin Simon (MS, Spring 2023), Reza Shahriari (MS, Fall 2023), Blas Kojusner (MS, Fall 2022), Hunter Searle (MS, Summer 2022), Vanessa Frost (MS, Spring 2022), Joseph Choi (MS, Spring 2021), Joseph Pletcher (MS, Spring 2013), Adam Bates (MS, Spring 2012), Benjamin Mood (MS, Spring 2012), Masoud Valafar (MS, Fall 2011).

Other Graduate Student Advising

PhD Committee Member: Ghulam Memon (PhD, University of Oregon, Fall 2013), Saeed Sadeghian (PhD, University of Calgary, Fall 2015), Henry Carter (PhD, Georgia Institute of Technology, Spring 2016), Mehdi Sadi (PhD, University of Florida, Spring 2017), Bradley Reaves (PhD, University of

Florida, Summer 2017), Robert Karam (PhD, University of Florida, Summer 2017), Luka Malisa (PhD, ETH Zurich, Summer 2017), Fengchao Zhang (PhD, University of Florida, Spring 2018), Kai Yang (PhD, University of Florida, Summer 2018), Nolen Scaife (PhD, University of Florida, Spring 2019), Ruimin Sun (PhD, University of Florida, Spring 2019), Francesco Pittaluga (PhD, University of Florida, Spring 2019), Jonathan Smith (PhD, University of Florida, Spring 2020), Beong Heyn Kim (PhD, University of Toronto, Spring 2020), Christopher Patton (PhD, University of Florida, Summer 2020), Xiaoyong Yuan (PhD, University of Florida, Summer 2020), Farhaan Fowze (PhD, University of Florida, Summer 2020), Tamzidul Hoque (PhD, University of Florida, Summer 2020), Jasmine Bowers (PhD, University of Florida, Summer 2020), Olufemi Odegbile (PhD, University of Florida, Spring 2021), Luis Vargas (PhD, University of Florida, Spring 2021), Atul Prasad Deb Nath (PhD, University of Florida, Spring 2021), Abdulrahman Alaqi (PhD, University of Florida, Spring 2021), Aritra Dhar (PhD, ETH Zurich, Summer 2021), Olufemi Odegbile (PhD, University of Florida, Summer 2021), Yazhou Tu (PhD, University of Louisiana at Lafayette, Fall 2021), Shubhra Deb Paul (PhD, University of Florida, Spring 2022), Hadi Abdullah (PhD, University of Florida, Spring 2022), Christian Peeters (PhD, University of Florida, Summer 2022), Brendan David-John (University of Florida, Summer 2022), Sarah Amir (PhD, University of Florida, Summer 2022), Jonathan Cruz (PhD, University of Florida, Fall 2022), Logan Blue (PhD, University of Florida, Spring 2023), Animesh Chhotaray (PhD, University of Florida, Spring 2023), Martin Georgiev (PhD, University of Oxford, Spring 2023), Sujan Kumar Saha (PhD, University of Florida, Spring 2023), Minh Vu (PhD, University of Florida, Spring 2024), Chaoyi Ma (PhD, University of Florida, Spring 2023), Yihang (Ken) Bai (PhD, University of Florida, Spring 2024), Anurag Swarnim Yadav (PhD, University of Florida, Spring 2024), Manish Merugu (PhD, University of Florida, Spring 2025), Yichen Jian (PhD, University of Florida, Spring 2025), Christopher Brant (PhD, University of Florida, Spring 2025), Mohammad Sami Ul Islam Sami (PhD, University of Florida, Spring 2025), Seth Layton (PhD, University of Florida, Spring 2026), Ethan Wilson (PhD, University of Florida, Spring 2026), Wenxuan Bao (PhD, University of Florida, Spring 2026).

Other Committee Membership: Ming Liu (University of Florida, thesis proposal committee, Spring 2016), Reza Motamedi (University of Oregon, thesis proposal committee, Spring 2014), Jason Gustafson (University of Oregon, MS Committee, Winter 2012), Amir Amir Farzad (University of Oregon, MS committee, Spring 2013).

Undergraduate Students

Hannah Pruse (Honors BS, Oregon, Spring 2013 - **NSF Graduate Fellow**), Ryan Leonard (Honors BS, Oregon, Spring 2013), Peter McKay (Honors BS, Oregon, Spring 2013), Braden Hollembaek (Honors BS, Oregon, Spring 2014), Abdul Alkhelaifi (Honors BS, Oregon Spring 2014), Devan Patel (BS, Florida, Spring 2015), Cynthia Omauzo (CS, Prairie View A&M, CRA DREU, hosted Summer 2015), Jared Trinkler (BS, University Scholar, Florida, Spring 2017), Joshua Uduehi (CRA DREU, BS, Indiana University, hosted Summer 2017), Suman Adari (BS, Florida, Spring 2021), Christie Ruales (BS, CRA/ACSA SWSIS Scholar, University Scholar, Florida, Spring 2021), César Arguello (BS, Florida, Spring 2022), Katie Platt (BS, Florida, Fall 2022), Gabriella Neris (BS, Florida, Spring 2023).

Presentations & Invited Talks

1. **Keynote Address:** From Blue Boxes to Black Boxes: Adventures in Uncovering Device Function-

- ality. *IEEE Workshop on Offensive Technology (WOOT)*, San Francisco, CA, May 2013.
2. From Blue Boxes to Black Boxes: Telecommunications Security Research at the Florida Institute for Cybersecurity Research. *Florida Cybersecurity Advisory Council*, Gainesville, FL, May 2013.
 3. Privacy-Preserving Computation for Resource-Constrained Devices. *NATO Science and Technology Office ET Meeting*, Washington, DC, November 2022.
 4. Investigating External Surfaces in Android Devices. *Microsoft Research*, Cambridge, United Kingdom, February 2020.
 5. Firmware-Informed Approaches to Securing Systems and Devices. *ARM Research*, Cambridge, United Kingdom, February 2020.
 6. Cybersecurity and Election Security: Innovations in Research and Technology (with Juan Gilbert). *Orange and Blue Plate Luncheon*, Tallahassee, FL, February 2020.
 7. Making MPC More Accessible Through Informed Compiler Design. *Workshop on Teaching Secure Computation*, Washington, DC, January 2020.
 8. Analyzing Applications to Assess Security. *FIGI Security Clinic*, Geneva, Switzerland, December 2019.
 9. Application Security Framework for DFS. *FIGI Security Clinic*, Geneva, Switzerland, December 2019.
 10. Security Research at the Florida Institute for Cybersecurity Research (with Patrick Traynor). *UF Eye Opener Breakfast*, Gainesville, FL, USA, October 2019.
 11. “Plug and Pray” Today: Reflecting on a Decade of Peripheral Security Research. *UCLA*, Los Angeles, CA, USA, April 2019.
 12. Cybersecurity Challenges in a Diverging Internet. *Jean Monnet Centre of Excellence Annual Workshop on the European Union*, Gainesville, FL, USA, April 2019.
 13. Designing a Security Management Framework for Digital Financial Services. *ITU Security, Infrastructure, Trust Working Group Meeting*, Washington, DC, USA, April 2019.
 14. Developing a Consortium on Trust in Media and Technology. *Invited Panelist. University of Florida Foundation National Board Meeting*, Atlanta, GA, USA, March 2019.
 15. Designing a Security Management Framework for Digital Financial Services. *Financial Inclusion Global Symposium*, Cairo, Egypt, January 2019.
 16. Staying Safe in Cyberspace: Understanding the Threats and Defenses. *The Village at Gainesville*, Gainesville, FL, USA, October 2018.
 17. Domain Informed Techniques for IoT Security (with Tuba Yavuz). *ARM Research*, San Jose, CA, USA, October 2018.
 18. A Discussion on Security Education in Academia. *Invited Panelist. ACM Conference on Communications and Communication Security (CCS)*, Toronto, ON, Canada, October 2018.
 19. New Attack Surfaces Against Mobile Platforms. *Columbia University Cybersecurity and Payments Roundtable*, New York, NY, August 2018.
 20. **Keynote Address:** Secure and Efficient Whole-System Data Provenance: A Retrospective. *2nd Workshop on Provenance-based Security*, London, UK, July 2018.
 21. “Plug and Pray” Today: Reflecting on a Decade of USB Security Research. *University of Oxford*,

Oxford, UK, July 2018.

22. “Plug and Pray” Today: Reflecting on a Decade of USB Security Research. *Chinese Academy of Sciences*, Beijing, China, June 2018.
23. Characterizing Tooling and Interfaces for Mobile Applications and Devices. *Samsung Research America*, Mountain View, CA, USA, May 2018.
24. “Plug and Pray” Today: Reflecting on 10 Years of USB Security Research. *Symantec Research Labs*, Culver City, CA, USA, May 2018.
25. A Security Framework for for DFS Featurephone Applications. *ITU FIGI Security, Information, and Trust Working Group Meeting*, Washington, DC, USA, April 2018.
26. Application Security for DFS Featurephone Applications. *Financial Inclusion Global Initiative Symposium*, Bangalore, India, November 2017.
27. Towards More Robust Interactions with Telephones and Peripherals (with Patrick Traynor). *Florida International University*, Miami, FL, October 2017.
28. **Keynote Address:** Making USB Safer for Hosts and Peripherals. *Third International Conference on Future Network Systems and Security (FNSS 2017)*, Gainesville, FL, August 2017.
29. Making USB Safer for Hosts and Peripherals. *ETH Zurich*, Zurich, Switzerland, July 2017.
30. Security Challenges in Mobile Devices. *FinTech, DFS and Payments Summit, Columbia Business School*, New York, NY, June 2017.
31. Webinar: Trends and Challenges in Mobile Money and Mobile Banking Application Security. *Digital Financial Services Observatory, Columbia University*, June 2017.
32. Towards Firmware Vetting on Legacy Embedded Platforms. *10th Workshop on Fault-Tolerant Spaceborne Computing Employing New Technologies*, Albuquerque, NM, May 2017.
33. Technical Deep Dive: Foundations of Hardware-Assisted Secure Multiparty Computation with SGX. *10th Workshop on Fault-Tolerant Spaceborne Computing Employing New Technologies*, Albuquerque, NM, May 2017.
34. Security and Privacy Challenges for Mobile Money Applications. *ITU Digital Financial Services Workshop: Exploring Innovation in Transactions and Financing in the Caribbean*, Port of Spain, Trinidad and Tobago, April 2017.
35. Everybody Jammin’ Up on Those Tings: Challenges for the Internet of Insecure Things. *Forum on Internet of Things: Smarter Living in the Caribbean*, Port of Spain, Trinidad and Tobago, April 2017.
36. Application Security for DFS Applications. *ITU Workshop on DFS and Financial Inclusion*, Washington, DC, April 2017.
37. **Keynote Address:** Making USB Safer for Hosts and Peripherals. *Computer Science Research Day, University of Georgia*, Athens, GA, April 2017.
38. Security in the DFS Ecosystem - Final Recommendations. *ITU Focus Group Meeting on Digital Financial Services*, Geneva, Switzerland, December 2016.
39. Making USB Great Again: New Defenses for Hosts and Devices. *MIT Lincoln Laboratory*, Lexington, MA, USA, October 2016.
40. Making USB Great Again: New Defenses for Hosts and Devices. *Dartmouth College*, Hanover, NH, USA, October 2016.

41. Recommendations for Securing Digital Finance. *ITU Focus Group Meeting on Digital Financial Services*, Dar es Salaam, Tanzania, September 2016.
42. Secure and Efficient Data Provenance. *DARPA Transparent Computing PI Meeting*, Cambridge, MA, USA, July 2016.
43. Security for Digital Alternative Data and SME Supply Chain Finance. *G20 Global Partnership for Financial Inclusion (GPFI) Forum*, Chengdu, China, July 2016.
44. Privacy-Preserving Computing Made Practical. *9th Workshop on Fault-Tolerant Spaceborne Computing Employing New Technologies*, Albuquerque, NM, USA, June 2016.
45. Host Fingerprinting for Identity and Integrity Assurance Using Machine Learning. *9th Workshop on Fault-Tolerant Spaceborne Computing Employing New Technologies*, Albuquerque, NM, USA, June 2016.
46. Security and Privacy Challenges for Mobile Money in Mobile Devices. *5th Columbia Business School Digital Financial Services and Emerging Payments Summit*, New York, NY, USA, May 2016.
47. Trustworthy Collection Architectures for Data Provenance. *Concordia University*, Montreal, QC, Canada, May 2016.
48. Analyzing the Security of Sticky SIMs. *ITU Focus Group Meeting on Digital Financial Services*, Washington, DC, USA, April 2016.
49. Secure and Trustworthy Computers, Devices, and Systems. *South Carolina Governor's School for Science and Mathematics*, Harstville, SC, USA, December 2015.
50. Security Recommendations for the DFS Ecosystem. *ITU Focus Group Meeting on Digital Financial Services*, Geneva, Switzerland, December 2015.
51. Securing Storage for Insider Threat Mitigation. *Florida Cyber Consortium Research Symposium*, Tampa, FL, USA, October 2015.
52. Tales From the Crypt(o): Spooky Stories of Ideal-World Cryptography Meeting Real-World Implementation. *University of Calgary*, Calgary, AB, Canada, November 2015.
53. Vulnerability Analysis of Branchless Banking Apps in the Developing World. *ITU Focus Group Meeting on Digital Financial Services*, Kuala Lumpur, Malaysia, October 2015.
54. New Trends in Cybersecurity: Securing Critical Cyber-Infrastructure. *US Department of State/Department of Justice Cybercrime and Cybersecurity Workshop for Lusophone Africa*, Maputo, Mozambique, September 2015.
55. Trustworthy Collection Architectures for Data Provenance. *MIT Lincoln Laboratory*, Lexington, MA, USA, August 2015.
56. Be Who You Are: Establishing Host Identity in Local and Remote Systems. *EURECOM Institute*, Sophia Antipolis, France, July 2015.
57. Be Who You Are: Establishing Host Identity in Local and Remote Systems. *Symantec Research Labs*, Mountain View, CA, USA, April 2015.
58. Be Who You Are: Challenges of Establishing Host Identity in Local and Remote Systems. *Rutgers University*, New Brunswick, NJ, USA, March 2015.
59. Certificate Validation and the Future of SSL Security. *Chi Sigma IO, University of Florida*, Gainesville, FL, USA, November 2014.

60. Forced Perspectives: Evaluating an SSL Trust Enhancement at Scale. *2014 ACM Internet Measurement Conference (IMC'14)*, Vancouver, BC, Canada, November 2014.
61. USB Host Fingerprinting. *Lockheed Martin*, Orlando, FL, October 2014.
62. Improving Security Through Collaborative Frameworks. *IEEE CollaborateCom (Invited Panelist)*, Miami, FL, October 2014.
63. Establishing Host Identity in Systems and Storage. *University of Florida*, Gainesville, FL, April 2014.
64. Establishing Host Identity Through Indirect Measurement. *Pennsylvania State University*, University Park, PA, April 2014.
65. **Keynote Address:** Trust No One? Addressing the Challenges of Bottom Up Trust in Systems and Storage. *Symantec Cutting Edge*, Springfield, OR, March 2014.
66. Leveraging Emerging Storage Functionality for New Security Services. *Oregon State University*, Corvallis, OR, June 2012.
67. Protecting Portable Storage with Host Validation. *Queen's University*, Kingston, ON, Canada, April 2012.
68. Protecting Portable Storage with Host Validation. *NSERC ISSNet Security Workshop*, Kingston, ON, Canada, April 2012.
69. Attacks and Defenses Against the Cloud Infrastructure. *Oregon Security Day*, Eugene, OR, April 2012.
70. Leveraging Emerging Storage Functionality for New Security Services. *Portland State University*, Portland, OR, November 2011.
71. Leveraging Emerging Storage Functionality for New Security Services. *Galois*, Portland, OR, August 2011.
72. Securing Homecare Rehabilitation Environments. *UW/MSR Research Retreat*, Cle Elum, WA, August 2011.
73. Challenges and Alternatives to the Host Identification Problem. *Oregon Security Day*, Eugene, OR, April 2011.
74. Porscha: Policy Oriented Secure Content Handling in Android. *ACSAC 2010*, Austin, TX, December 2010.
75. Kells: A Protection Framework for Portable Data. *ACSAC 2010*, Austin, TX, December 2010.
76. Protection Mechanisms for Portable Devices. *Symantec Research Labs*, Mountain View, CA, November 2010.
77. Challenges and Alternatives to the Host Identification Problem. *2nd ACM Northeast Forensics Exchange (NeFX2010)*, Washington, DC, September 2010.
78. Disk-Enabled Authenticated Encryption. *MSST 2010*, Incline Village, NV, May 2010.
79. Leveraging Emerging Storage Functionality for New Security Services. *Polytechnic Institute of New York University*, Brooklyn, NY, March 2010.
80. Leveraging Emerging Storage Functionality for New Security Services. *Simon Fraser University*, Surrey, BC, Canada, March 2010.

81. Leveraging Emerging Storage Functionality for New Security Services. *Stevens Institute of Technology*, Hoboken, NJ, March 2010.
82. Leveraging Emerging Storage Functionality for New Security Services. *University of Tennessee*, Knoxville, TN, March 2010.
83. Leveraging Emerging Storage Functionality for New Security Services. *University of Oregon*, Eugene, OR, March 2010.
84. Leveraging Emerging Storage Functionality for New Security Services. *Naval Postgraduate School*, Monterey, CA, February 2010.
85. Towards a Secure and Efficient System for End-to-End Provenance. *TaPP'10*, San Jose, CA, February 2010.
86. Rootkit-Resistant Disks. *Security Reading Group*, *University of Toronto*, Toronto, ON, Canada, November 2009.
87. Rootkit-Resistant Disks. *Digital Security Seminar*, *Carleton University*, Ottawa, ON, Canada, November 2009.
88. U Can't Touch This: Protections for Portable Storage. *IWSSPS 2009*, Grenoble, France, Oct. 2009.
89. FlowStor: Preserving Information Flow on Portable Storage Devices. *Symantec Corporation*, Mountain View, CA, USA, August 2009.
90. Leveraging Emerging Disk Functionality for New Security Services. *Symantec Research Labs*, Mountain View, CA, USA, June 2009.
91. Rootkit-Resistant Disks. *CCS'08*, Alexandria, VA, USA, October 2008.
92. Experimenting with BGP Security Mechanisms Using the DETER Framework. *Boeing Integrated Defense*, Philadelphia, PA, USA, October 2008.
93. Terabyte Home Security and Access Control. *Seagate Research*, Pittsburgh, PA, USA, August 2008.
94. Towards Automated Privilege Separation. *ICISS 2007*, Delhi, India, December 2007.
95. Non-Volatile Memory and Disks: Avenues for Policy Architectures. *CSAW 2007*, Fairfax, VA, USA, November 2007.
96. Autonomously Secure Disks. *Software Reading Group*, *University of Michigan*, Ann Arbor, MI, USA, September 2007.
97. Leveraging Non-Volatile Memory for Storage Security. *2007 USENIX Security Symposium, Works in Progress*, Boston, MA, USA, August 2007.
98. Analysis of the IPv4 Address Delegation Structure. *ISCC 2007*, Aveiro, Portugal, July 2007.
99. Performance Optimizations of IPsec for Storage. *2007 SNIA Summer Security Summit*, Pittsburgh, PA, June 2007.
100. Optimizing BGP Security by Exploiting Path Stability. *CCS'06*, Alexandria, VA, November 2006.
101. Threats and Attacks in Interdomain Routing. *P2INGS Quarterly Meeting*, Tempe, AZ, February 2004.
102. Network Operations in Tier-1 Internet Service Providers. *Columbia University*, New York, NY, March 2001.
103. Network Operations in Tier-1 Internet Service Providers. *Telcordia Technologies*, Morristown, NJ,

August 2000.

Press Coverage

Research-Related Coverage

1. “Exploiting Decades-Old Telephone Tech to Break Into Android Devices.” Lily Hay Newman, *Wired*, August 29, 2018. <https://www.wired.com/story/at-commands-android-vulnerability/>
2. “Modern smartphones vulnerable to old-school attack.” Francis Navarro, *Komando.com*, August 28, 2018. <https://www.komando.com/happening-now/483269/modern-smartphones-vulnerable-to-old-school-attack>
3. “ATak na Androida: modemowe komendy standardu z lat 80 pozwalają przejąć kontrolę nad smartfonem” (Translation from Polish: “ATack on Android: modem commands from the 80’s standard allow you to take control of your smartphone”.) Adam Golanski, *Dobreprogramy*, August 28, 2018. <https://www.dobreprogramy.pl/ATak-na-Androida-modemowe-komendy-standardu-z-lat-80-pozwalaja-przejac-kontrolę-nad-smartfonem,News,90526.html>
4. “Смартфоны ASUS, HTC, Huawei, Lenovo, LG, Samsung, Sony легко взломать технологией, созданной для древнего модема Подробнее” (Translation from Russian: “Smartphones ASUS, HTC, Huawei, Lenovo, LG, Samsung, Sony can easily crack technology created for the ancient modem.”) Roman Georgiev, *CNews Russia*, August 28, 2018. http://safe.cnews.ru/news/top/2018-08-28_smartfony_asushtchuaweilenovolsamsungsony
5. “AT Command Hitch Leaves Android Phones Open to Attack.” Lindsey O’Donnell, *Threatpost*, August 27, 2018. <https://threatpost.com/at-command-hitch-leaves-android-phones-open-to-attack/136938/>
6. “New security risk for smartphones bring you a ‘ghost user’.” Ida Torres, *Android Community*, August 27, 2018. <https://androidcommunity.com/new-security-risk-for-smartphones-brings-you-a-ghost-user-20180827/>
7. “Android at the mercy of AT commands.” Nick Farrell, *Fudzilla*, August 27, 2018. <https://fudzilla.com/news/mobile/47037-android-at-the-mercy-of-at-commands>
8. “Android-Smartphones durch Modem-Befehle verwundbar” (Translation from German: “Android Smartphones vulnerable through modem commands”.) Sebastian Gruner, *Golem.de: IT-News Für Profis*, August 27, 2018. <https://www.golem.de/news/at-commands-android-smartphones-durch-modem-befehle-verwundbar-1808-136205.html>
9. “Telefony s Androidem lze ovládnout přes USB pomocí AT příkazů”(Translation from Czech: “Android phones can be controlled via USB using AT commands”). Petr Krcmar, *Root.cz Linux News*, August 27, 2018. <https://www.root.cz/clanky/telefony-s-androidem-lze-ovladnout-pres-usb-pomoci-at-prikazu/>
10. “У 11 производителей Android-смартфонов обнаружили уязвимость к AT-командам” (Translation from Russian: “11 manufacturers of Android-smartphones found a vulnerability to AT-commands”.) *Tproger*, August 27, 2018. <https://tproger.ru/news/at-commands-deface-smartphones/>
11. “Smartphones From 11 OEMs Vulnerable to Attacks via Hidden AT Commands.” Catalin Cimpanu,

Bleeping Computer, August 25, 2018. <https://www.bleepingcomputer.com/news/security/smartphones-from-11-oems-vulnerable-to-attacks-via-hidden-at-commands/>

12. "Smartphone security risk compared to 'having a ghost user on your phone'." Jonathan Griffin, *University of Florida News*, August 22, 2018. <http://news.ufl.edu/articles/2018/08/smartphone-security-risk-compared-to-having-a-ghost-user-on-your-phone.php>
13. "Ransomware 'stopped' by new software." *BBC News*, July 2016. <http://www.bbc.com/news/technology-36772461>
14. "United States and Mozambique Host Cybersecurity and Cybercrime Workshop in Maputo for Lusophone Africa." *US Department of State*, September 2015. <http://www.state.gov/r/pa/prs/ps/2015/09/247088.htm>
15. "Researchers Find Security Flaws in Developing-World Money Apps." Jennifer Valentino-Devries. *Wall Street Journal*, August 2015. <http://blogs.wsj.com/digits/2015/08/11/researchers-find-security-flaws-in-developing-world-money-apps/>
16. "Hack could let browsers use cloud to carry out big attacks on the cheap." Dan Goodin, *Ars Technica*, November 2012. <http://arstechnica.com/security/2012/11/hack-could-let-browsers-use-cloud-to-carry-out-big-attacks-on-the-cheap/>

Other Coverage

17. "Voters in Two States Report Threatening 'Vote for Trump' Emails", Nick Corasanitti, Ben Decker, and Stephanie Saul, *The New York Times*, 20 October 2020. <https://www.nytimes.com/2020/10/20/us/politics/florida-alaska-trump-emails.html>
18. "What Would It Take to Shut Down the Entire Internet?" Daniel Kolitz, *Gizmodo*, 30 September 2019. <https://gizmodo.com/what-would-it-take-to-shut-down-the-entire-internet-1837984019>
19. "Devious Ransomware Frees You If You Infect Two Other People." Lily Hay Newman, *Wired*, 13 December 2016. <https://www.wired.com/2016/12/popcorn-time-ransomware/>
20. "UF experts: iPhone issue could set precedent." Christopher Curry and Dahlia Ghabour, *Gainesville Sun*, 26 February 2016. <http://www.gainesville.com/article/20160226/ARTICLES/160229743/-1/archive?Title=UF-experts-iPhone-issue-could-set-precedent>
21. "Biometric Security Comes To Your Smartphone." Mitch Kroner, *Think Out Loud, Oregon Public Broadcasting*, 24 September 2013. <http://www.opb.org/radio/programs/thinkoutloud/segment/biometric-security-comes-to-your-smartphone/>

Previous Academic Appointments

Associate Professor, Department of Computer and Information Science and Engineering, University of Florida, Aug. 2014 - Aug. 2021

Associate Director of the Florida Institute for Cybersecurity Research. Previous co-director of the Southeastern Security for Enterprise and Infrastructure Center.

Assistant Professor, Department of Computer and Information Science, University of Oregon, Sep. 2010 - Aug. 2014

Research and teaching classes in systems security. Founder and leader of the Oregon Systems

Infrastructure Research and Information Security Laboratory. Co-director of the Center for Cyber Security.

- **Leadership:** Organizer of Computer Security Day at the University of Oregon (2014, 2013, 2012, 2011, recipient of CAS program grant for three years), liaison to Oregon Engineering and Technology Council (2010-2012), faculty advisor to UO Security Club (2012-2014), faculty liaison to Women in Computer Science (2012-2013).
- **Committee Service:** University Committee on General Science Major (2014), Graduate Education Committee (2010-2012, 2014-present), Computing Resources Committee (2011-2012), Industrial Affairs Committee (2012-2014), Strategic Planning Committee (2013).

Research Assistant, Department of Computer Science, Pennsylvania State University, Jan. 2005 - Aug. 2010

- **Senior Personnel**, NSF HECURA: Collaborative Research: Secure Provenance in High-End Computing Systems, NSF (CCF), \$307,073, Aug. 2009 - present.
- Funded by NSF HECURA grant 0621429 from Aug. 2006 - Jul. 2010, investigating security of storage systems.
- Funded by NSF grant CNS-0335241 from Aug. 2005 - Aug. 2006, investigating BGP security solutions and large-scale simulation.

Lead Graduate Student, Systems and Internet Infrastructure Security (SIIS) Laboratory, Pennsylvania State University, Sep. 2007 - Dec. 2008

- Administrative and logistical lead student in the SIIS lab. Ran weekly lab meetings of 13 members, met with students individually for mentoring and development of leadership and research skills. Responsible for most daily operational activities in the lab.

Instructor, Department of Electrical Engineering, Pennsylvania State University, Jun.-Aug. 2006

- Instructor for *EE/CSE 458*, the senior undergraduate course on computer networking.

Guest Lecturer, Department of Computer Science, Pennsylvania State University, 2005-present

- *CSE 543 (Computer Security)*: presented lectures on cryptography and public key infrastructures.
- *CSE 597A (Advanced Topics in System Security)*: lectured on virtual machine security.
- *CSE 411 (Operating Systems)*: presented lectures on storage systems.
- *CSE 545 (Advanced Network Security)*: lectured on BGP security.

Teaching Assistant, Stern School of Business, New York University, Fall 2005

- Lectured, graded, and provided logistics for Computer and Network Security course offered for MBA students.

Teaching Assistant, Department of Computer Science and Engineering, Pennsylvania State University, Fall 2004

- Held lab hours and graded for Computer System Architecture course.

Graduate Research Assistant, Department of Computer Science, Columbia University, Oct. 2001 - May 2002

- Worked on SIP security, implementing authentication into the Panasonic PINTL JAIN SIP stack.

Teaching Assistant, Department of Computer Science, Queen's University, Fall 1998

- Held office hours and graded for Introduction to Computer Science course.

Industrial Experience

Co-Founder and Chief Operating Officer, CryptoDrop LLC, 2017-2019.

- Anti-ransomware startup based in Gainesville, Florida.

Research Intern, Symantec Research Labs, Mountain View, CA, Jun - Aug. 2009

- Examined host-based validation for portable storage devices, and implemented a prototype using embedded Linux.

Research Intern, Seagate Research, Pittsburgh, PA, May - Aug. 2008

- Developed security infrastructures for distributed storage in a home user environment, focussing on distributed access control mechanisms.

Research Intern, AT&T Labs - Research, Florham Park, NJ, Dec. 2003 - Aug. 2004

- Investigated security threats in BGP and created an overview of threats and currently deployed solutions. Developed cryptographic constructions allowing efficient security solutions and performed simulations based on trace data.

Technical Intern, Flarion Technologies, Bedminster, NJ, Summer 2002

- Implemented packet diversion and IP header modification program in BSD for mobile IP packet testing.

Research Scientist, Telcordia Technologies, Morristown, NJ, Sep. 2000 - Nov. 2001

- Built and maintained an HFC lab to emulate a cable plant; researched routing and service assurance methodologies for multiple service providers accessing common transport.

Technical Specialist, UUNET, Toronto, ON, May 1999 - Aug. 2000

- Monitored and troubleshot intermediate and backbone connections across the UUNET Canadian network, as well as dealing with network security and web server issues.

Summer Intern, Royal Bank of Canada, Toronto, ON, Summer 1997, 1998

- Investigated financing opportunities for life science and high tech companies through financial and technical analysis; ported applications from mainframe to client-server environments.