IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Gregory G. Raleigh	Attorney Docket No.39843-0185IP1
U.S. Patent No.:	11,405,429	
Issue Date:	August 2, 2022	
Appl. Serial No.:	16/907,887	
Filing Date:	June 22, 2020	
Title:	SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES	

DECLARATION OF DR. PATRICK MCDANIEL

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

Date: January 28, 2025 By: _____
Patrick McDaniel, Ph.D.

SAMSUNG 1003

Table of Contents

I. ASSIGNMENT 4

II. QUALIFICATIONS AND BACKGROUND INFORMATION 4

III. OVERVIEW OF CONCLUSIONS FORMED 17

IV. LEVEL OF ORDINARY SKILL IN THE ART 18

V. LEGAL STANDARDS 19
- A. Terminology 19
- B. Legal Standards 19
- C. Anticipation 20
- D. Obviousness 20

VI. MATERIALS CONSIDERED 25

VII. TECHNOLOGY OVERVIEW 26
- A. Mobile Devices 26
- B. Policy-based Management 29
- C. Channels 33

VIII. THE '429 PATENT 38
- A. Overview of the '429 Patent 38
- B. Prosecution History of the '429 Patent 39

IX. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES 39
- A. U.S. Pat. App. Pub. No. 2009/0077643 ("Schmidt") 39
- B. U.S. Pat. App. Pub. No. 2005/0101323 ("De Beer") 51
- C. Schmidt-De Beer Combination 59
  - Overview 59
  - Facilitating wireless network communications using a wireless modem 60
  - Securing transmissions from the modem 64
  - Providing a secure partition in device memory that stores data conventionally stored in a physical SIM's memory 68
  - Implementing roaming capability in Schmidt's vSIM-based environment 82
  - Schmidt-DB Combination 87
- D. U.S. Pat. App. Pub. No. 2004/0148237 ("Bittmann") 90
- E. Schmidt-De Beer-Bittmann Combination 95
- F. Smith, *Virtual Machines: Versatile Platforms for Systems and Processes* ("Smith") 100
- G. Schmidt-De Beer-Smith Combination 102

X. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '429 CLAIMS UNPATENTABLE 106
A. Ground 1A: Combination of Schmidt and De Beer Renders Obvious Claims 1-3 and 8-12 106
B. Ground 1B: Combination of Schmidt, De Beer, and Bittmann Renders Obvious Claims 4-7 161
C. Ground 1C: Schmidt in view of DB and Smith renders claims 10-12 obvious 170
XI. CONCLUSION 172

I. ASSIGNMENT

1. I have been retained on behalf of Samsung Electronics Co., Ltd. ("Samsung") to offer technical opinions related to 11,405,429 ("the '429 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 '429 patent.

2. I have been asked to provide my independent analysis of the '429 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 '429 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 '429 patent.

II. QUALIFICATIONS AND BACKGROUND INFORMATION

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

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

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

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

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

8. Prior to 2017, I was an Assistant Professor (2004-2007), Associate Professor (2007-2011), Full Professor (2011-2015), and Distinguished Professor

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

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

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

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

members from Stanford, the University of California, Berkeley, The University of California-San Diego, and the University of Virginia.

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

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

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

corporate policies and practices relating to the security of mobile devices, networks, and software systems.

15. As shown in Appendix A, I have published extensively in the field of mobile security, network and security management, computer systems, routing and queueing, authentication, systems security, applied cryptography and network security. In addition to writing several articles for industry journals and conferences, I have authored portions of numerous books related to computer systems, applied cryptography and network security. I have served on the editorial boards of several peer-reviewed journals including ACM Transactions on Internet Technology, for which I was the Editor-in-Chief. I was also an Associate Editor for ACM Transactions on Information and System Security and IEEE Transactions of Software Engineering, two highly regarded journals in the field. My curriculum vitae, attached as Appendix A, includes a list of publications on which I am an author. It contains details regarding my experience, education, publications, and other qualifications to provide an expert opinion in connection with this proceeding.

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

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

18. I have reviewed the ’429 patent (SAMSUNG-1001), and relevant excerpts of the prosecution history (SAMSUNG-1002) of the ’429 patent. Among various textbooks, documents, and publications, I have also reviewed the following prior art references:

SAMSUNG-1005 U.S. Pat. App. Pub. No. 2009/0077643 (“Schmidt”)

SAMSUNG-1006 U.S. Pat. App. Pub. No. 2005/0101323 (“De Beer”)

SAMSUNG-1007 U.S. Pat. App. Pub. No. 2004/0148237 (“Bittmann”)

SAMSUNG-1008 (Excerpts) Smith, et al., 2005. “Virtual Machines: Versatile Platforms for Systems and Processes,” Elsevier, Inc, 2005, ISBN 1-55860-910-5 (“Smith”)

SAMSUNG-1012 Declaration of June Munford

SAMSUNG-1020 U.S. Pat. App. Pub. No. 2009/0149165 (“Minborg”)

SAMSUNG-1021	U.S. Pat. App. Pub. No. 2007/0117538 (“Weiser”)
SAMSUNG-1022	(Excerpts) Telecom Dictionary, Athos Publishing, 2007.
SAMSUNG-1023	(Excerpts) Eberspächer, Jörg (2001). GSM Switching, Services and Protocols, Second Edition. John Wiley & Sons Ltd. ISBN: 978-0-470-85394-8.
SAMSUNG-1025	3rd Generation Partnership Project; Technical Specification Group Terminals; “Characteristics of the USIM application” (Release 7), 3GPP TS 31.102 V7.0.0 (“3GPP USIM”).
SAMSUNG-1026	U.S. Pat. No. 5,764,693 (“Taylor”)
SAMSUNG-1027	U.S. Pat. No. 6,470,182 (“Nelson”)
SAMSUNG-1028	U.S. Pat. App. Pub. No. 2006/0015749 (“Mittal”)
SAMSUNG-1029	Kasper, et al., 2008, February. “Subscriber authentication in cellular networks with trusted virtual sims.” In 2008 10th International Conference on Advanced Communication Technology (Vol. 2, pp. 903-908). IEEE. (“Kasper”)

SAMSUNG-1030 TCG Mobile Reference Architecture, version 1.0, Revision 1, June 12, 2007. ("TCG Mobile Reference Architecture")

SAMSUNG-1031 TCG Mobile Trusted Module Specification, version 1.0, Revision 6, June 26, 2008. ("TCG Mobile Trusted Module Specification")

SAMSUNG-1032 U.S. Pat. App. Pub. No. 2006/0020781A1 ("Scarlata")

SAMSUNG-1033 U.S. Pat. No. 6,421,722 ("Bauer")

SAMSUNG-1034 U.S. Pat. App. Pub. No. 2007/0178888 ("Alfano")

SAMSUNG-1035 U.S. Pat. App. Pub. No. 2008/0117958 ("Pattenden")

SAMSUNG-1036 Stone, G.N., Lundy, B. and Xie, G.G., 2001. Network policy languages: a survey and a new approach. IEEE network, 15(1), pp.10-21. ("Stone")

SAMSUNG-1037 U.S. Pat. No. 6,556,823 ("Clapton")

SAMSUNG-1038 U.S. Pat. App. Pub. No. 2007/0149252 ("Jobs")

SAMSUNG-1040 David K. Gifford. 1982. Cryptographic sealing for information secrecy and authentication. Commun. ACM

25, 4 (April 1982), 274–286. https://doi.org/10.1145/358468.358493

SAMSUNG-1042 Jansen, Wayne A. and Richard P. Ayers. “Forensic Tools for Mobile Phone Subscriber Identity Modules.” J. Digit. Forensics Secur. Law 1 (2006): 75-94.

SAMSUNG-1049 National Institute of Standards and Technology. 2001. Security Requirements for Cryptographic Modules, downloaded from the Internet at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf on December 5, 2024

SAMSUNG-1050 Verma, et. al., (2002). Policy-based management of content distribution networks. IEEE network, 16(2), 34-39. (“Verma”)

SAMSUNG-1051 Lobo, et. al., (1999). A policy description language. AAAI/IAAI, 1999, 291-298. (“Lobo”)

SAMSUNG-1052 Westerinen, et al., IETF RFC 3198, Terminology for Policy-Based Management, November 2001, downloaded from the Internet on May 27, 2024.

SAMSUNG-1054 (Excerpts) Keith Mayes and Konstantinos Markantonakis. 2008. Smart Cards, Tokens, Security and Applications (1st. ed.). (“Mayes”)

SAMSUNG-1055 (Excerpts) Gasser, Morrie. Building a Secure Computer System. New York, NY: Van Nostrand Reinhold, 1988. (“Gasser”)

SAMSUNG-1056 (Excerpts) Malhotra, Ravi. 2002. IP Routing: Help for Network Administrators. O’Reilly Media. ISBN: 978-0-596-00275-0 (“Malhotra”)

SAMSUNG-1057 Jude, Michael. "Policy-Based Management: Beyond the Hype." Business Communications Review 31.3 (2001): 52-56. (“Jude”)

SAMSUNG-1058 Merkle, Ralph C. 1978. Secure communications over insecure channels. Commun. ACM 21, 4 (April 1978), 294–299. https://doi.org/10.1145/359460.359473 (“Merkle”)

SAMSUNG-1059 ARM. 2004. PrimeCell Infrastructure AMBA 3 TrustZone Protection Controller (BP147) Revision: r0p0 Technical Overview, downloaded from the Internet at https://documentation-service.arm.com/static/5e9565afc8052b1608762aae%3Ftoken%3D&ved=2ahUKEwiZq56_3pGKAxVUCnkGHcR9OGIQFnoECAwQAQ&usg=AOvVaw2PG8jUG9TU8fpiRxmGKNyM on December 5, 2024

SAMSUNG-1060 Network Associates, Inc. 1999. PGP, Version 6.5.1. An Introduction to Cryptography.

SAMSUNG-1061 Stuart E. Madnick and John J. Donovan. 1973. Application and analysis of the virtual machine approach to information system security and isolation. In Proceedings of the workshop on virtual computer systems. Association for Computing Machinery, New York, NY, USA, 210–224. https://doi.org/10.1145/800122.803961

SAMSUNG-1062 U.S. Pat. App. Pub. No. 2008/0122796 (“Jobs-796”)

SAMSUNG-1063	European Telecommunications Standards Institute. 1998. Terrestrial Trunked Radio (TETRA); Security Aspects; Subscriber Identity Module to Mobile Equipment (SIM – ME) interface. ETSI ETS 300 812 ed.1 (1998-11), downloaded from the Internet at https://www.etsi.org/deliver/etsi_i_ets/300800_300899/300812/01_20_9826/ets_300812e01c.pdf on December 12, 2024
SAMSUNG-1064	IETF RFC 1122, Requirements for Internet Hosts – Communication Layers, October 1989, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc1122 on December 12, 2024.
SAMSUNG-1065	IETF RFC 793, Transmission Control Protocol, September 1981, downloaded from the internet at https://www.ietf.org/rfc/rfc793.txt on December 11, 2024.
SAMSUNG-1066	U.S. Pat. App. Pub. No. 2005/0108534 (“Bajikar”)

SAMSUNG-1067 Smith, et al., 2005. “The architecture of virtual machines. Computer,” 38(5) (“Smith-2005”)

SAMSUNG-1068 ISO/IEC 7498-1, “Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model,” downloaded from the internet at https://www.ecma-international.org/wp-content/uploads/s020269e.pdf on January 10, 2025 (“OSI”)

SAMSUNG-1069 Gonçalves, et al., 2009, October. A graphical user interface for policy composition in CIM-SPL. In 2009 International Conference on Ultra Modern Telecommunications & Workshops (pp. 1-7). IEEE. (“Gonçalves”)

SAMSUNG-1070 Agrawal, et. al., 2007, May. Issues in designing a policy language for distributed management of IT infrastructures. In 2007 10th IFIP/IEEE International Symposium on Integrated Network Management (pp. 30-39). IEEE. (“Agrawal-2”)

19. Counsel (Fish & Richardson) has informed me that I should consider these materials through the lens of one of ordinary skill in the art related to the '429 patent at the time of the earliest possible priority date of the '429 patent, and I have done so during my review of these materials. I have been informed by Counsel to use the filing date January 28, 2009.

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

21. My opinions, as explained below, are based on my education, experience, and expertise in the fields relating to the '429 Patent. Unless otherwise stated, my testimony below refers to the knowledge of one of ordinary skill in the art as of the earliest possible priority date. Any figures that appear within this document have been prepared with the assistance of Counsel and reflect my understanding of the '429 Patent and the prior art discussed below.

III. OVERVIEW OF CONCLUSIONS FORMED

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

- Ground 1A renders claims 1-3, 8-12 obvious.
- Ground 1B renders claims 4-7 obvious.
- Ground 1C renders claims 10-12 obvious.

23. In support of these conclusions, I provide an overview of the references in Section IX and more detailed comments regarding the obviousness of claims 1-12 ("**the Challenged Claims**") of the '429 patent in Section X.

IV. LEVEL OF ORDINARY SKILL IN THE ART

24. In my opinion, one of ordinary skill in the art relating to, and at the time of, the Priority Date would have been someone with (1) at least a bachelor's degree in computer science, computer engineering, electrical engineering, or a related field, and (2) at least two years of industry experience in wireless communications security. Additional education could substitute for industry experience, and *vice versa*. *Id.* Further, all positions in this declaration are from the vantage point of a POSITA as of January 28. 2009.

25. Based on my experiences, I have a good understanding of the capabilities of a POSITA. Indeed, I have taught, participated in organizations, and worked closely with many such persons over the course of my career. Based on my knowledge, skill, and experience, I have an understanding of the capabilities of a POSITA. For example, from my industry experience, I am familiar with what a POSITA would have known and found predictable in the art. From teaching and

supervising my post-graduate students, I also have an understanding of the knowledge that a person with this academic experience possesses. Furthermore, I possess those capabilities myself.

V. LEGAL STANDARDS

A. Terminology

26. I have been informed by Counsel and understand that the best indicator of claim meaning is its usage in the context of the patent specification as understood by one of ordinary skill. I further understand that the words of the claims should be given their plain meaning unless that meaning is inconsistent with the patent specification or the patent's history of examination before the Patent Office. Counsel has also informed me, and I understand that, the words of the claims should be interpreted as they would have been interpreted by one of ordinary skill at the time of the invention was made (not today). The '429 patent was filed June 22, 2020, and claims priority to many provisional applications, the earliest of which was filed January 28, 2009, which I refer to as the "Critical Date" in this proceeding. Because I do not know at what date the invention as claimed was made, if ever, I have used the Critical Date of the '429 patent as the point in time for claim interpretation purposes. My opinion does not change if the invention date is earlier.

B. Legal Standards

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

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

C. Anticipation

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

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

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

D. Obviousness

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

33. I have been informed by Counsel and understand that a claim is unpatentable for obviousness and that obviousness may be based upon a combination of references. I am informed by Counsel and understand that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. However, I am informed by Counsel and understand that a patent claim composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art.

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

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

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

37. I have been informed by Counsel and understand that an obviousness evaluation can be based on a single reference or a combination of multiple prior art references. I understand that the prior art references themselves may provide a suggestion, motivation, or reason to combine, but that the nexus linking two or

more prior art references is sometimes simple common sense. I have been informed by Counsel and understand that obviousness analysis recognizes that market demand, rather than scientific literature, often drives innovation, and that a motivation to combine references may be supplied by the direction of the marketplace.

38. I have been informed by Counsel and understand that if a technique has been used to improve one device, and a person of ordinary skill at the time of invention would have recognized that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.

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

40. I have been informed by Counsel and understand that a proper obviousness analysis focuses on what was known or obvious to a person of

ordinary skill at the time of invention, not just the patentee. Accordingly, I understand that any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.

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

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

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

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

VI. MATERIALS CONSIDERED

45. My analysis and conclusions set forth in this declaration are based on my educational background and experiences in the field (*see* Section II). Based on my knowledge and experience, I believe that I am considered to be an expert in the field. Also, based on my knowledge and experience, I understand and know of the capabilities of persons of ordinary skill in the field around 2009, and I taught, participated in organizations, and worked closely with many such persons in the field during that time frame.

46. As part of my independent analysis for this declaration, I have considered the following: the background knowledge/technologies that were commonly known to persons of ordinary skill in this art during the time before the earliest claimed priority date for the '429 patent; my own knowledge and experiences gained from my work experience in the field of the '429 patent and related disciplines; and my experience in working with others involved in this field and related disciplines.

47. In addition, I have analyzed the publications and materials listed above.

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

VII. TECHNOLOGY OVERVIEW

49. In this section I provide a broad overview of the relevant technology and state of the technical community before the priority date of the '429 patent. This description is not intended to be exhaustive, but to provide sufficient background to support and contextualize my analysis below.

A. Mobile Devices

50. In 2009, use of smartphones experienced a significant surge, marking a pivotal moment in the evolution of mobile technology. The year saw a growing number of consumers transitioning from traditional feature phones (e.g., flip phones) to more capable and versatile smartphones. Key factors driving this uptake included advancements in mobile operating systems such as Apple's iOS and Google's Android, offering a user-friendly interface and access to a burgeoning app[1] ecosystem. Additionally, the earlier introduction of 3G networks enabled

[1] The "app" refers to software applications that generally run on smartphones, e.g., email, browsers, streaming, and social media applications. An

faster mobile data speeds, prompting users to embrace smartphones for tasks beyond voice and messaging. As a result, smartphone sales soared, laying the groundwork for the transformative impact they would have on communication, productivity, and entertainment in the years to come.

51. However, smartphones in 2009 were resource-limited compared to the current devices. For example, smartphones of 2009 were equipped with single-core processors, usually running at speeds below 1 GHz. These processors lacked the computing power of today's multi-core CPUs found in modern smartphones. As a result, tasks that required significant processing, such as running complex applications or playing graphically intensive games, were often slow and less efficient. Similarly, memory capacities in smartphones of 2009 were generally limited, typically ranging from 128 MB to 512 MB. Long term storage was also limited, consisting of between 4 to 16GB of space. Devices were connected to wireless networks using WWAN (cellular) and WLAN (Wi-Fi) modems.[2]

---

app market is the application and developer infrastructure for creating and providing apps to smartphone users.

[2] The term modem refers to a *modulator*/*demodulator*, which is a device to process electrical signals received and sent over a physical media (e.g., copper

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

---

wire) or over the air. In mobile devices, modems are software supported radios that process specific network access protocols.

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

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

B. Policy-based Management

54. A key challenge in 2009 was finding ways to address the rapidly increasing needs of mobile users using the resource-limited devices and networks. One approach was to use policies, often expressed as rules, to manage competing demand for resources. Solutions to these problems were developed by adapting known techniques in computer systems and networks (e.g., priority queuing), as well as developing new, faster devices and networks.

55. Policy for computational systems has been a part of the technical landscape since the 1970s, with a primary focus on differentiating resource usage in various environments. For example, a policy might specify that data from interactive applications, such as multi-player games, are assigned the highest

priority to ensure the best user experience. These policies were implemented to manage and allocate computing resources efficiently in diverse computing environments. For instance, differentiated services emerged as a crucial policy in this context, especially as mobile devices such as phones began to traverse heterogeneous environments, transitioning between Wi-Fi and cellular networks seamlessly. By employing policies like differentiated services, computing systems could optimize resource allocation, ensuring a smooth and reliable user experience while adapting to changing network conditions and device capabilities in these dynamic environments. Such techniques were particularly important to address the challenges faced by early mobile devices.

56. A policy can be defined as a set of rules to administer, manage, and control access to network resources.[4] There are many alternatives for specifying policies, but one common approach is to specify a policy as a condition and corresponding action. For example, Verma defines a policy as an expression of the form "if *condition* then *action*" (emphasis added) where "the conditional part describes a specific situation that can be encountered by a network device, and the action component specifies the action that is to be performed by the device in that situation." SAMSUNG-1050, 2. Lobo extends condition-action to "event-

[4] See, e.g., SAMSUNG-1052.

condition-action" such that "[a]n event-condition-action rule is triggered when the event occurs, and if the condition is true the action is executed." SAMSUNG-1051, 1. For simplicity, I describe the condition-action example, but a POSITA would have understood that event-condition-action and other forms were known and could have been used.

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

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

{traffic_class = {video, voice}, used_bw <= allotted_bw}

{allotted_bw = 50M, loss_rate (data) > 40% : allotted_bw := 40M}

SAMSUNG-1036, 10.

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

60. Gonçalves similarly describe policy conditions that are "ORed or ANDed." SAMSUNG-1069, 4. Further, CIM-SPL defined conditions as Boolean expressions of arbitrary complexity. SAMSUNG-1070, 5. In summary, Boolean conditions including multiple clauses were well-known as of the Critical Date.

61. The action aspect determines how the system reacts when the condition evaluates to TRUE. Verma teaches that an "action may be construed as a procedure that is defined and stored in the repository (e.g. a piece of Java code, or a program in a language like CacheL or PONDER)" or a "set of simple operations that need to be performed." SAMSUNG-1050, 2. Such reactions depend both on the type of a system and its goals. For example, when a provisioning system determines that CPU utilization of a system exceeds a

threshold, it might provision a new server, providing additional computing capacity; a CDN might replicate a piece of content to more distribution nodes.

62. The policies can be specified using many different syntaxes. For example, Stone provides an overview of policy languages. *See* SAMSUNG-1036, *generally*. Some hardware and software vendors often defined their own proprietary policy-specification languages.

63. In some systems, rules were simply coded by administrators using the appropriate syntax, such as PDL, Ponder, or a vendor-specific syntax. Some systems also provided user interfaces that permitted users to specify policies. For example, Agrawal writes that "[a] policy definition tool (PDT) is a user interface by which policy authors create and modify policies." SAMSUNG-1039, 3.

C. Channels

64. A channel is "a stream of information transmitted as part of a distinct communication, or conversation, or for a particular purpose or end use." SAMSUNG-1022, 3. In telephony systems, including cellular telephony systems, a channel is a pathway or medium through which voice or data communications are transmitted.

65. Channels facilitate the transfer of information between communicating devices, such as telephones, through various signaling and data transmission protocols. They play a fundamental role in telecommunication by

structuring and managing data flow, ensuring that signals travel effectively, and managing interactions between different parts of the telephony network. SAMSUNG-1023, 8.

66. Channels in telephony systems are used to transport various types of data, primarily voice calls, signaling information, and, in modern systems, digital data like SMS and internet traffic. SAMSUNG-1023, 1, 2, 10, 14. Each channel is designed to support specific functions within the telecommunication system. For example, voice channels are optimized to carry human speech, while data channels are designed to transfer text or multimedia data. SAMSUNG-1023, 2, 16, 17, 18. Efficient use of channels ensures that calls and data transmissions are clear, timely, and uninterrupted, and channels are structured to handle both the high volume and diverse types of traffic in a telecommunication system.

67. There are two types of channels in telecommunication systems: physical and logical channels. SAMSUNG-1023, 11.

68. *Physical channels* refer to the actual hardware and electromagnetic mediums that carry signals in telephony systems. SAMSUNG-1023,s 11. These are the tangible, physical means (and modulation protocols) by which signals are transmitted and include traditional wiring (like copper lines) and radio frequencies in cellular communications. SAMSUNG-1023, 11, 22. A physical channel represents a specific pathway through the physical network. For example, in a 2G

GSM cellular system, a frequency band or a specific time slot on a frequency can serve as a physical channel, and only one call or data session can occupy that channel at any given time.[5] SAMSUNG-1023, 2, 3, 5. The bandwidth of physical channels determines the amount of data that can be transmitted over them. SAMSUNG-1023, 6.

69. In contrast, *logical channels* represent virtual pathways within a physical channel. Logical channels organize and manage the data flow on physical channels by designating separate functions and types of data (such as payload transport, signaling, broadcast, synchronization, among others) within the same physical pathway. SAMSUNG-1023, 11. This abstraction allows for efficient use of physical infrastructure, as multiple logical channels can operate within a single physical channel. SAMSUNG-1023, 15. Logical channels are essential in modern telecommunication because they help multiplex multiple services or sessions over the same physical infrastructure, allowing users to access a range of services (such as voice, SMS, and internet) simultaneously.

[5] One notable exception are systems with *Code Division Multiple Access* (CDMA) where user signals are instead separated by orthogonal codes (therein allowing users to use the same frequency band simultaneously). SAMSUNG-1023, 4.

70. Logical channels can be further partitioned into signaling (also called "control") and data (also called "traffic") channels. SAMSUNG-1023, 11.

71. *Control/signal channels* carry signaling information that manages, coordinates, and maintains telecommunication sessions. SAMSUNG-1023, 12. Control channels do not (typically) carry voice or data content; instead, they transmit the instructions necessary to establish, maintain, and terminate connections between users and other components within the GSM system architecture (e.g., base stations, gateways, switching centers, among others).

72. In cellular systems, for example, control channels are responsible for tasks like call setup, handovers (when a call moves from one cell tower to another), and paging (locating a mobile device when there is an incoming call or message). SAMSUNG-1023, 14. An example of a control channel in the GSM system is the Broadcast Control Channel (BCCH), which sends network information to all devices within a cell, allowing devices to identify and connect to the network. SAMSUNG-1023, 7, 13.

73. *Data/traffic channels* carry the actual user information, such as voice, text messages, or internet data. SAMSUNG-1023, 11, 12. In telephony systems, data channels are optimized to transmit real-time data, such as voice calls, and non-real-time data, such as SMS. An example of a data channel is the Traffic Channel (TCH), which carries the user's voice data during a call. SAMSUNG-1023, 11, 12.

Unlike control channels, data channels are dedicated to delivering the content of the communication itself rather than the signals required to establish or manage the communication.

74. The distinction between control and data channels ensures efficient use of network resources. Control channels handle essential system management functions without interfering with data transferred by users, while data channels are optimized for handling the actual content of user communications. This structure is critical for managing high volumes of traffic and providing reliable service, especially in large-scale cellular networks where millions of users may be making simultaneous calls, sending texts, or using data services. SAMSUNG-1023, 12, 13.

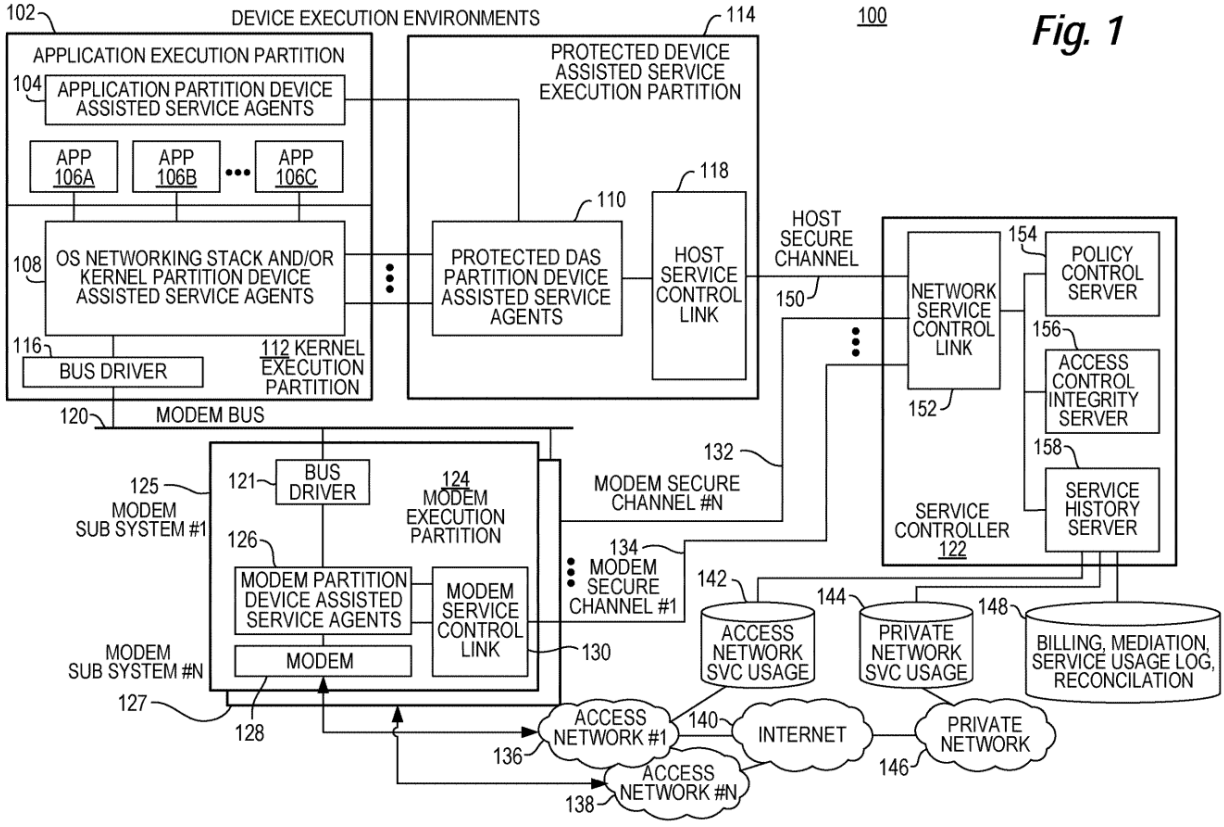
75. In the interest of further efficiency, in limited circumstances, carriers use a control channel to carry data such as *Short Message Service* (SMS) messages, e.g,, as explained in Eberspächer. SAMSUNG-1023, 19. Specifically, SMS messages can be sent over a *Stand-alone Dedicated Control Channels* (SDCCH), a type of control channel, without allocating a dedicated data channel. SAMSUNG-1023, 19. The SMS data, which is limited in size, is placed in otherwise-empty space within SDCCH messages, making use of space that would otherwise be wasted, and thereby improving efficiency.

76. Channels are generally transitory, created as they are needed, then destroyed to conserve resource such that "[o]ne channel may be distinguished from other channels by the time of occurrence of the transmission," among other factors. SAMSUNG-1022, 3

VIII. THE '429 PATENT

A. Overview of the '429 Patent

77. The '429 Patent is directed to a "security techniques for device assisted services." SAMSUNG-1001, Abstract. The '429 patent describes "secure service measurement and/or control execution partition," "a service profile [is] executed at least in part in a secure execution environment of a processor" (where "the service profile is associated with a service plan"), "monitoring use of the service based on the service profile; and verifying the use of the service based on the monitored use of the service." *Id.*



SAMSUNG-1001, FIG. 1.

B. Prosecution History of the ’429 Patent

78. During prosecution, Applicant overcame a nonstatutory double patenting rejection by filing a terminal disclaimer over a related application to which the application for the ’429 patent claims priority. SAMSUNG-1002, 126, 24, 29. No art-based rejections were issued during prosecution. SAMSUNG-1002, *generally*.

IX. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES

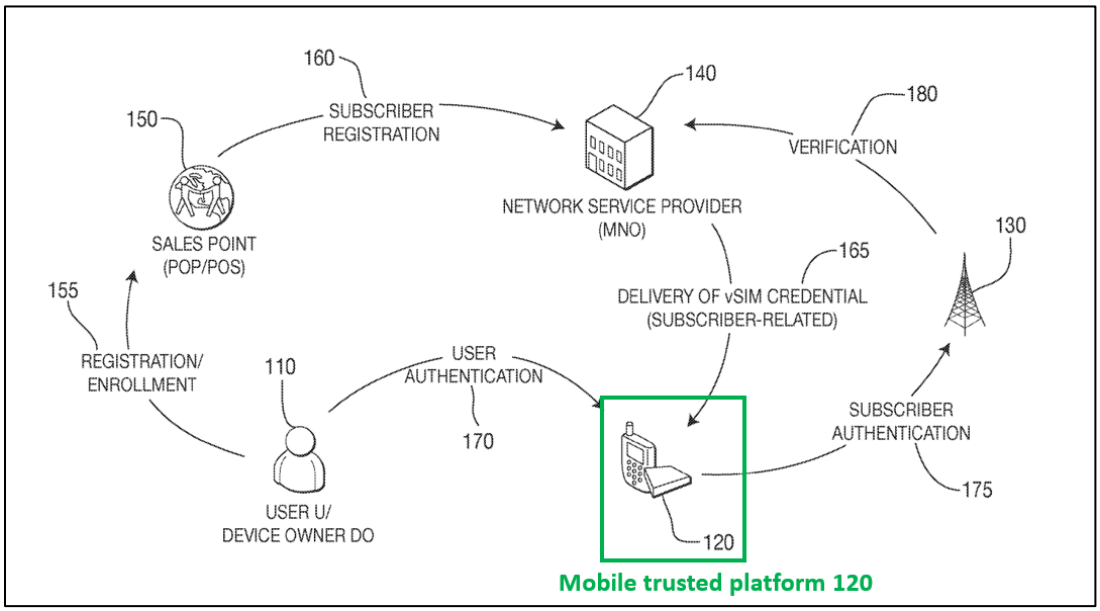
A. U.S. Pat. App. Pub. No. 2009/0077643 (“Schmidt”)

79. Schmidt discloses a device architecture that facilitates provisioning and use of a "software-based access authorization credential," referred to as a virtual subscriber identity module (vSIM) credential, for wireless cellular network communications. SAMSUNG-1005, [0023], [0026]-[0027].

80. Schmidt's vSIM-based solution overcomes shortcomings in "the current subscriber identity module (SIM) function carried out within a SIM card or UICC." SAMSUNG-1005, [0002]. For example, Schmidt notes that "the cost of the UICCs, their impractical form factor, and limited functionality prevent them from being used in applications where the mobile network operator may only be known some time after the purchase of the wireless device." SAMSUNG-1005, [0002]. Additionally, "though the SIM card or UICC is generally considered to be highly secure, this security is not linked strongly to security properties of the whole device on which it resides," which "limits the application of scaling security concepts for advanced services and applications such as mobile financial transactions." SAMSUNG-1005, [0003].

81. Schmidt's system is implemented using a "'wireless transmit/receive unit (WTRU) includes but is not limited to a user equipment (UE) ... a cellular telephone, a personal digital assistant (PDA), a computer, a mobile trusted platform, or any other type of user device capable of operating in a wireless environment." SAMSUNG-1005, [0023]. FIG. 1 (reproduced below) shows a

mobile device, which Schmidt refers to as a mobile trusted platform 120, deployed as part of an example communication system architecture that is "configured to use services and determine subscriber identity using a software based virtual subscriber identity module (vSIM)." SAMSUNG-1005, [0024].



SAMSUNG-1005, FIG. 1 (annotated).

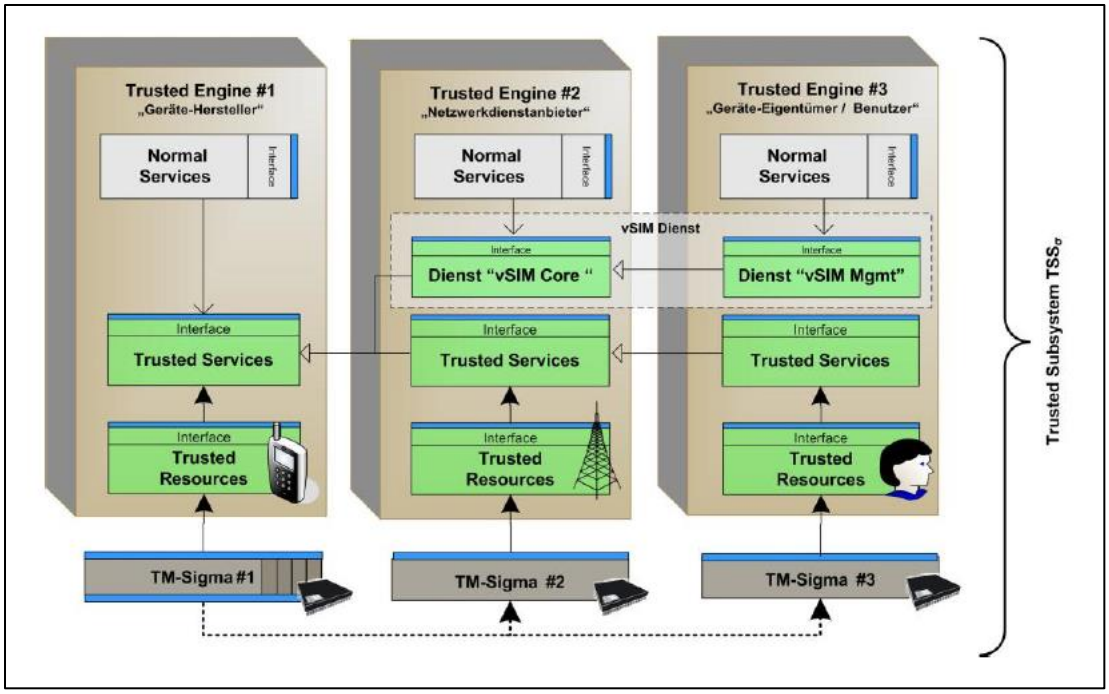
82. A POSITA would have understood that Schmidt's system includes a mobile device (e.g., a cellular phone, PDA, or other user device capable of operating in a wireless system) that implements therein a mobile trusted platform. First, a POSITA would have understood from Schmidt's illustration of a mobile trusted platform 120 as a cellular telephone in FIG. 1 (reproduced above) that a cellular telephone implements a mobile trusted platform.

83. In addition, the paper Kasper, et al., authored by the same inventors as identified on Schmidt patent, states that:

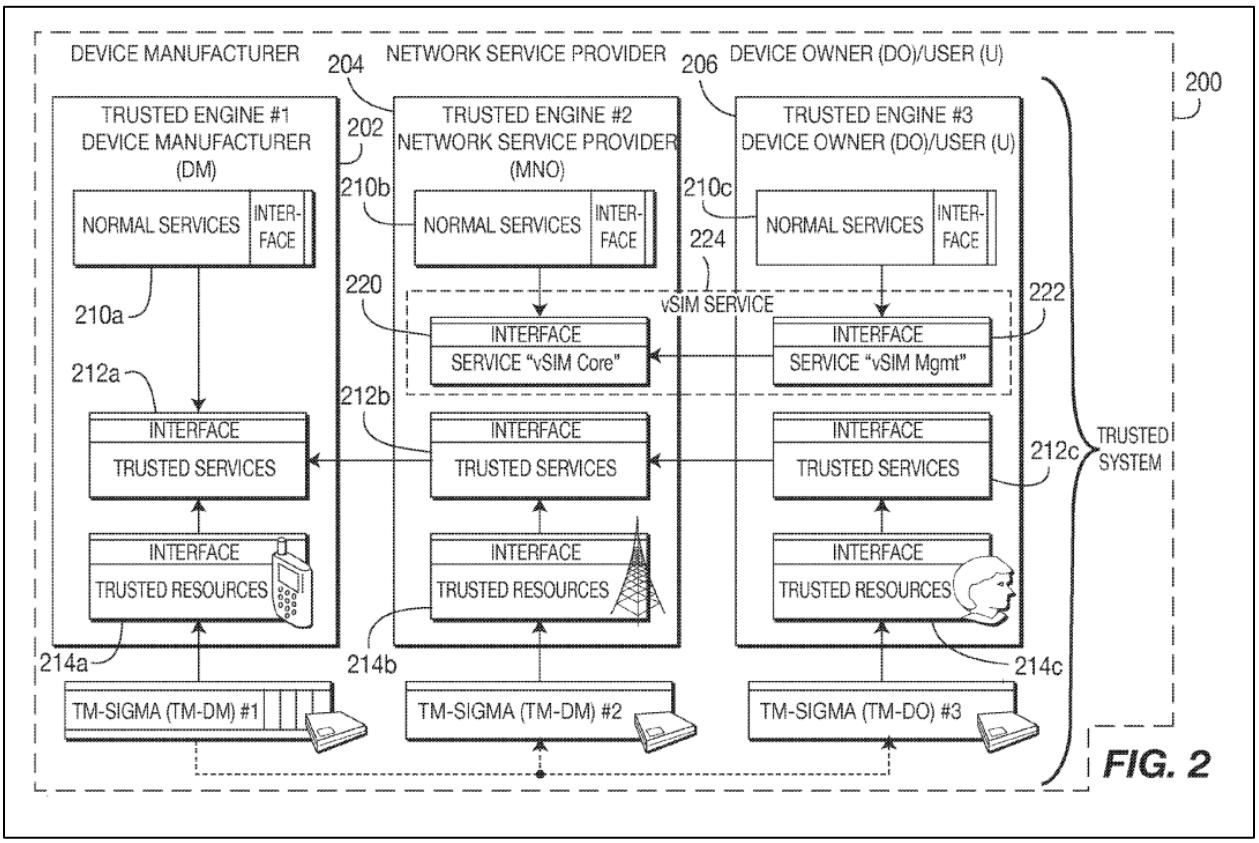
> In its TCG Mobile Reference Architecture, the Mobile Phone Work Group of the Trusted Computing Group (TCG MPWG) specifies a new concept to enable trust into future ***mobile devices***. It offers new potentials for implementing trust in mobile computing platforms by introducing ***multiple trusted engines*** on behalf of different stakeholders supported by a hardware-based trust anchor [1], [2]. Due to the capabilities of a mobile trusted platform (MTP) to support multiple trusted engines with protected storage, strong isolation and secure communication within a defined security perimeter, the MTP is able to take over the SIM functionality. SAMSUNG-1029, 1.[6]

84. Further, since Kasper's FIG. 1 closely resembles Schmidt's FIG. 2, a POSITA would have understood that they are both describing trusted engines in a mobile device.

[6] Emphasis added throughout unless otherwise noted.



SAMSUNG-1029, FIG 1 (Kasper, Kuntze, Schmidt paper).



SAMSUNG-1005, FIG. 2 (Schmidt, Kuntze, Kasper patent).

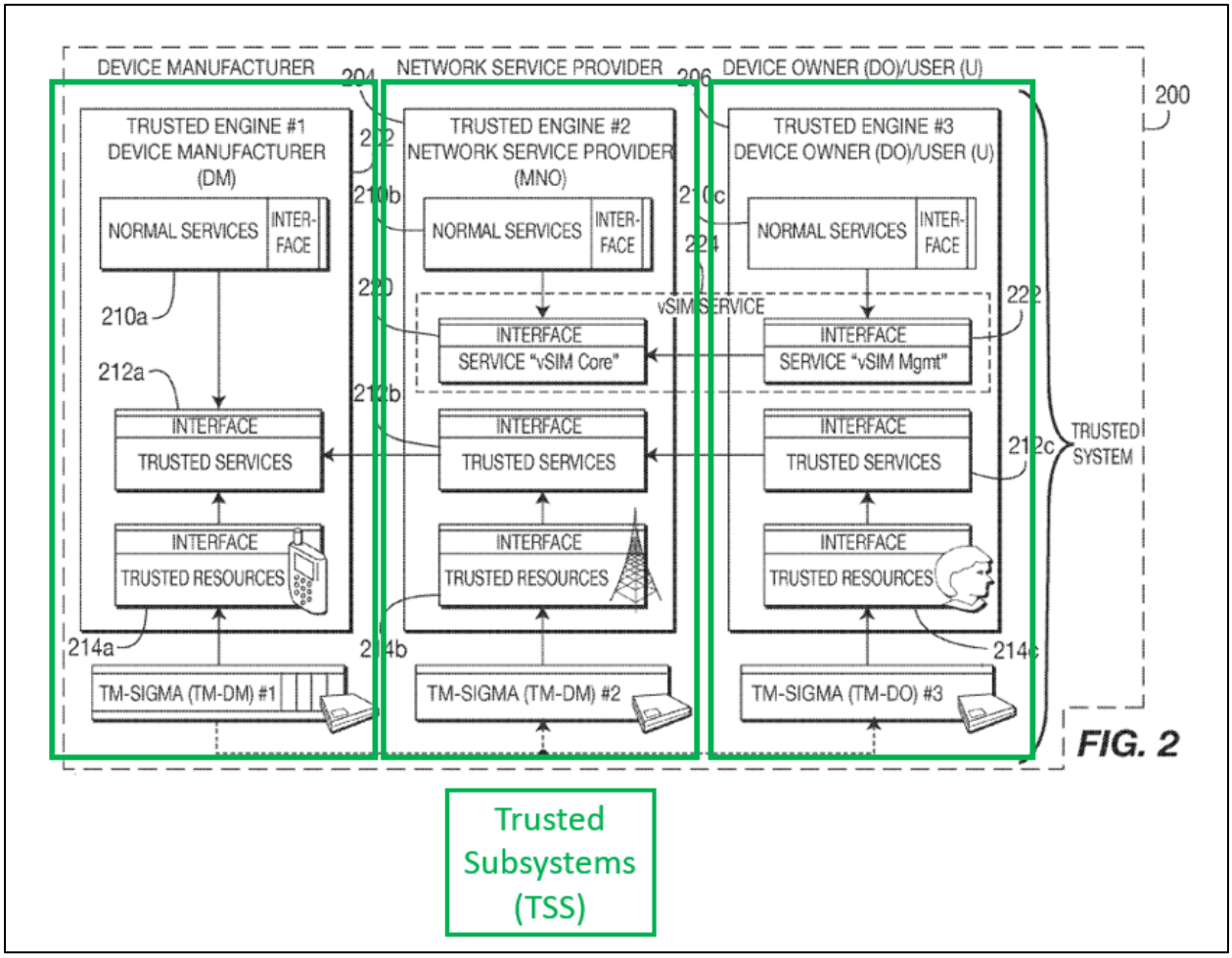
85. The MTP coordinates with a Mobile Network Operator (MNO) to obtain the vSIM credential and subsequently use it (instead of a physical SIM card) for "subscriber authentication for a general network infrastructure." SAMSUNG-1005, [0027], [0134]-[0142], FIG. 11.

86. As shown in FIG. 1 above, the device owner (DO) "intends to establish a long-term relationship with the MNO in order to use a mobile communications network and the services offered therein (for example, GSM, UMTS telephone, data services, or specialized location-based services)." SAMSUNG-1005, [0024], [0026]. To enable the device's access to the MNO's network, "the MNO provides the MTP" the "vSIM credential," which includes "a subscriber-related portion and a user-related portion." SAMSUNG-1005, [0027]. To use the network, "a registered device user" is "initially authorized by the communications network" using the "user-related portion of the vSIM credential," and subsequently, "the subscriber-related portion of the vSIM credential" is used to perform "network authentication." SAMSUNG-1005, [0027].

87. Schmidt's vSIM architecture for a mobile trusted platform MTP, illustrated in FIG. 2 below, "is protected by a trusted operating system which is based on a permanently assigned trusted anchor and which supports multiple

separate and trusted execution environments or sub systems."[7] SAMSUNG-1005, [0025]. As shown below, the MTP includes three trusted subsystems (TSSs) that operate on behalf of the device manufacturer (TSS-DM), the network service provider (TSS-MNO), and the device-owner/user (TSS-DO). SAMSUNG-1005, [0028].

[7] A "trust anchor" (or "root of trust") is an authority that is trusted. Trust anchors can be used to authenticate (or verify the integrity of) other entities, therein broadening the set of trusted entities. SAMSUNG-1060, 29-31. For example, if a trust anchor authenticates another component, that other component becomes trusted.



SAMSUNG-1005, FIG. 2 (annotated); see also id., FIG. 3-6 (providing similar environment and associated TSSs).

88. Each trusted engine includes trusted resources. SAMSUNG-1005, [0028], FIG. 2.

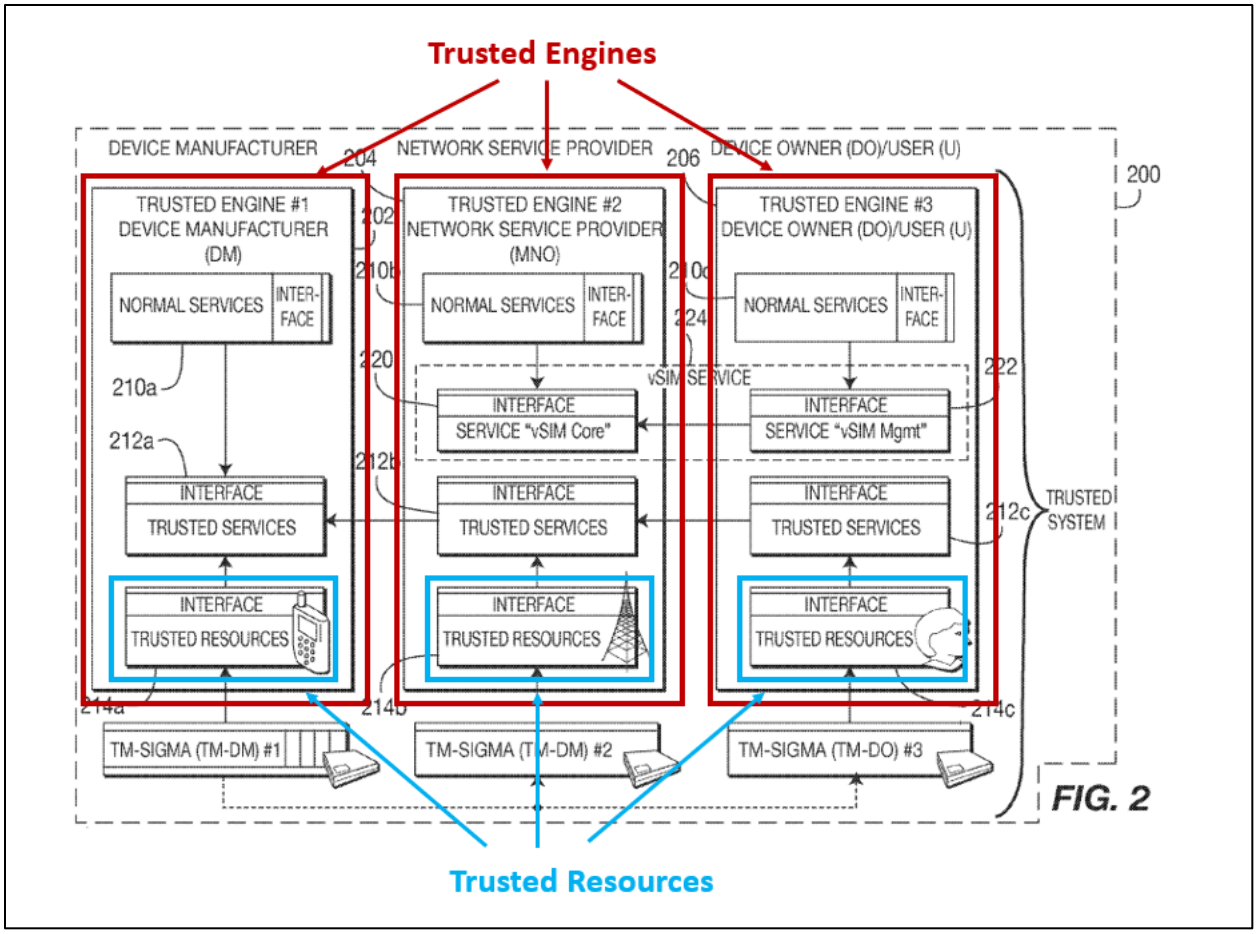
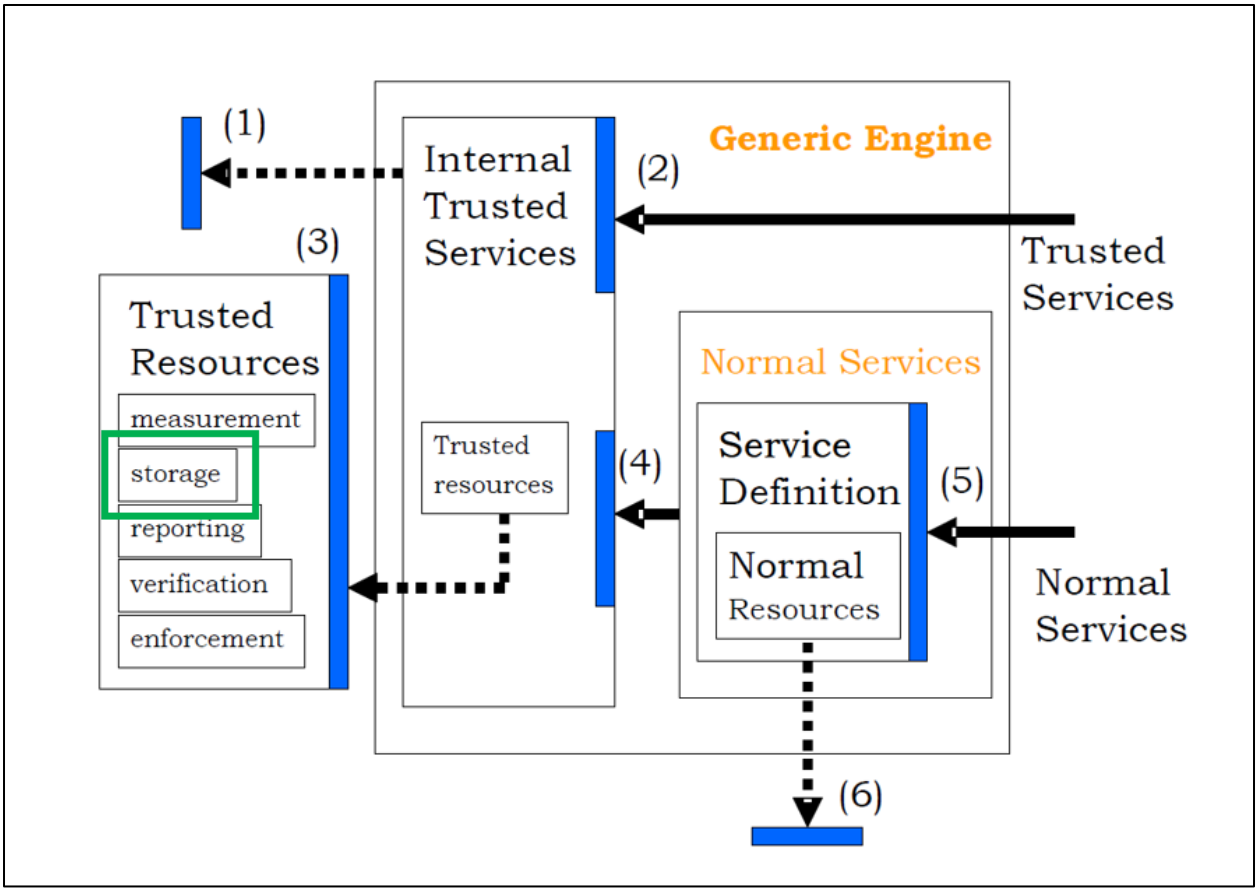


FIG. 2

SAMSUNG-1005, FIG. 2 (annotated); see also Id. FIG. 3.

89. A POSITA would have understood that trusted resources include, among other things, trusted or protected storage that is dedicated to the trusted engine/trusted subsystem. For example, the Trusted Computing Group's Mobile Reference Architecture illustrated a "generic engine" that is coupled to "trusted resources," including storage.



SAMSUNG-1030, FIG. 3. (annotated)

90. Similarly, Scarlata explains that a "TPM is a hardware component that resides within a processing system and provides various facilities and services for enhancing the security of the processing system." SAMSUNG-1032, [0003]. Scarlata further explains that the "sub-components of a TPM may include an execution engine and ***secure non-volatile (NV) memory or storage***," and the "secure NV memory is used to store sensitive information, such as encryption keys, and the execution engine protects the sensitive information according to the security policies to be implemented by the TPM." *Id.*

91. Each TSS has a particular role in device operation. TSS-DM "controls all internal and external communications and secures the communications channel." SAMSUNG-1005, [0032]. For example, all protocol messages of the trusted subsystems "are transmitted by the communications services of the TSS-DM." SAMSUNG-1005, [0032]. In addition, TSS-DM "is responsible for the integrity, configuration, and installation of the device together with its installed hardware components," and "provides all security-sensitive resources for a device." SAMSUNG-1005, [0032].

92. TSS-MNO manages "[a]ll subscription-dependent and subscriber-related network provider services of a platform," e.g., "GSM, UMTS telephone, data services, or specialized location-based services." SAMSUNG-1005, [0026], [0033]. TSS-MNO is also "responsible for managing and protecting the subscriber-related portion of the vSIM credential, and performs the client-side network authentication of a subscriber." SAMSUNG-1005, [0033]. TSS-MNO "provides the vSIM core service (vSIM-CORE) for this purpose." SAMSUNG-1005, [0033]. For example, an MNO "prepares the subscriber-related portion of the vSIM credential for transmission to the vSIM-CORE," and once TSS-MNO has successfully performed and verified decryption of the vSIM credential, TSS-MNO's "vSIM-CORE seals the received vSIM credential on one or more valid

platform configurations."[8] SAMSUNG-1005, [0076]-[0077]. The vSIM-CORE is thus "configured to substitute essential functions (subscriber authentication) for the conventional SIM, but may also accommodate other authentication features." SAMSUNG-1005, [0033].

93. TSS-U "protects all user-related and private information, in particular the user's associated access authorization credential (user-related portion of the vSIM credential)." SAMSUNG-1005, [0034].

94. Each TSS includes "a logical unit comprising the trusted execution environment (TE-sigma) and the non-exchangeable security module (trusted module, TM) or the entity of the security module (TM-sigma) associated with the remote owner (RO) or stakeholder (sigma)." SAMSUNG-1005, [0031] ("Sigma" identifies the stakeholder, DO/User, MNO or DM). Each "TSS-sigma is always configured to sign and encrypt any given data," and "has access to a trusted service RTV-sigma," which "is responsible for verification, for example of defined system states based on reference data." SAMSUNG-1005, [0031].

[8] Within the context of cryptography, to "seal" means to provide confidentiality and integrity of data. SAMSUNG-1040, 280. Within the context of trusted storage, "sealing" means to encrypt data with a nonce (a number used once) that is known only to the trusted subsystem (therein ensuring the integrity of the data, i.e., the vSIM credential). SAMSUNG-1054, 4.

95. Once the vSIM has been installed, Schmidt explains that the "MTPs 200 and 300 are configured to implement a vSIM service which replaces the conventional smart card-based SIM card and its function." SAMSUNG-1005, [0030]. In fact, early telecommunication standards had contemplated vSIMs to entirely replace physical SIMS, explaining that "[a] virtual SIM can be used instead of, or as well as, a physical SIM." SAMSUNG-1063, 17. The MTP uses the vSIM credential for "subscriber authentication for a general network infrastructure." SAMSUNG-1005, [0030], [0134]-[0142], FIG. 11. Once the device is authenticated using the vSIM core, the MNO provides services, e.g., "GSM, UMTS telephone, data services, or specialized location-based services." SAMSUNG-1005, [0026].

96. In addition to "offering a substitute for the conventional SIM functions," Schmidt's system also provides "a mutual authentication between the MNO and the MTP," and "provides core network access to subscription-independent and/or non-subscriber-related services in a general communications domain, fine-grained function limitations such as SIM lock, and dynamic downgrade/upgrade of services." SAMSUNG-1005, [0112].

B. U.S. Pat. App. Pub. No. 2005/0101323 ("De Beer")

97. Similar to Schmidt, De Beer ("DB") describes a mobile telephone in "a cellular telecommunications system." SAMSUNG-1006, Abstract. Using data

stored in a SIM, DB's mobile telephone "select[s] a network (4) for registration and []perform[s] optim[ized] call routing to a call destination." *Id.* This approach provides "[g]reater control of the network selection and cost saving by avoiding roaming agreements." SAMSUNG-1006, Abstract. Further, when data for a particular network is not present on the SIM, *e.g.*, when the device is roaming, the device retrieves the relevant data from a control centre, as explained further below. SAMSUNG-1006, Abstract, [0004].

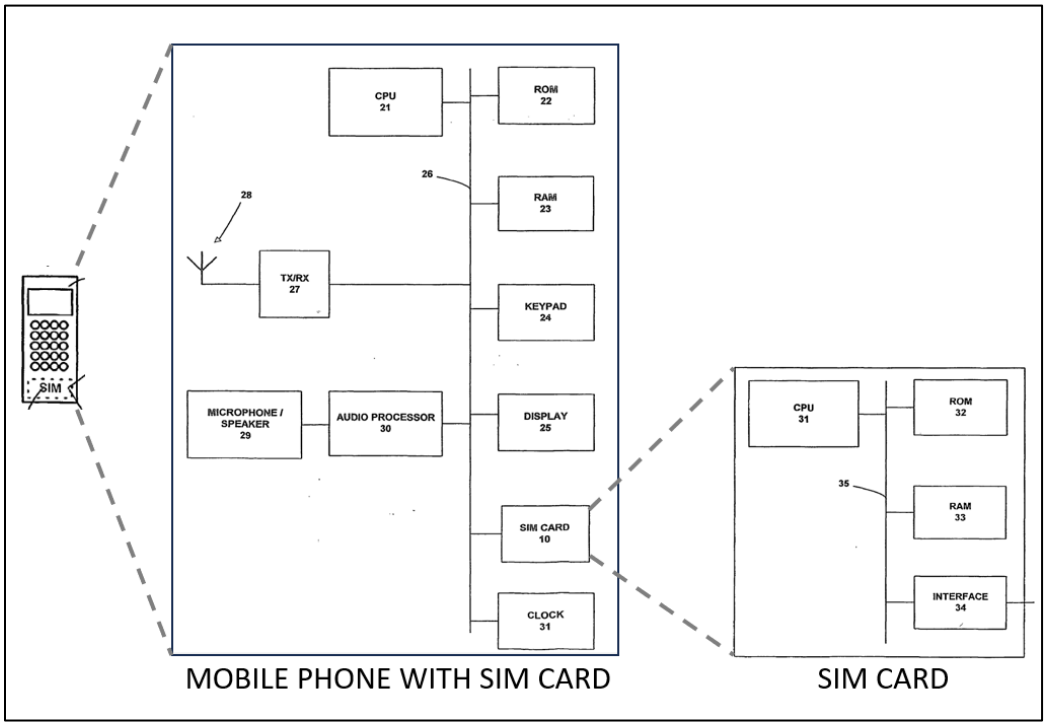
98. DB's system leverages a mobile telephone, which includes conventional components (e.g., CPU, ROM, RAM, display) and for wireless communication, includes a "transmitting and receiving circuit" that is "connected to an antenna." SAMSUNG-1006, [0041]-[0042], [0044].

99. The device further includes a SIM card, which includes "a processor 31 with a ROM 32 and RAM 33 formed of a flash memory so that the contents of the RAM persist when the SIM card is powered down." SAMSUNG-1006, [0043].

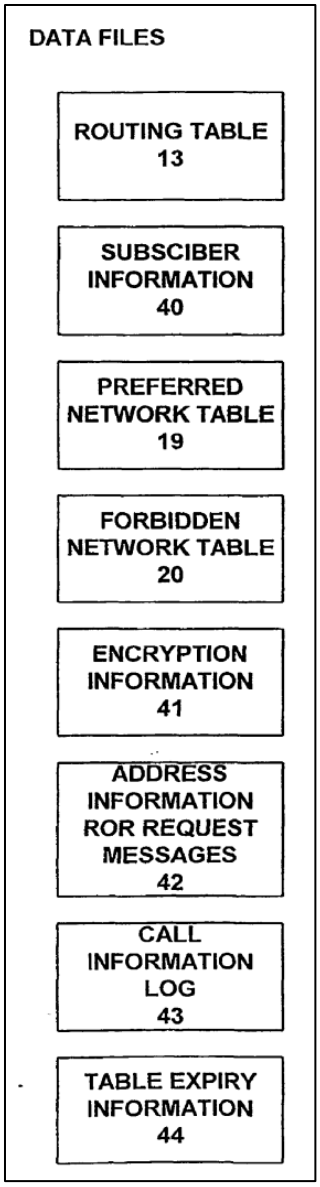
100. The SIM card stores data files (as shown below)—that guides device operation, including a routing table, subscriber information, preferred and forbidden network tables, call log, and table expiration. SAMSUNG-1006, [0041], [0046]-[0051], FIG. 4. A POSITA would have understood that the SIM card stores such data in the RAM (flash memory). SAMSUNG-1006, [0043]. Notably, SIM cards store persistent data in EEPROM (erasable, programmable read only

memory) or ROM (read-only memory), which can then be loaded into RAM for program execution. SAMSUNG-1042, 76.

101. DB's device and associated SIM card are illustrated below.



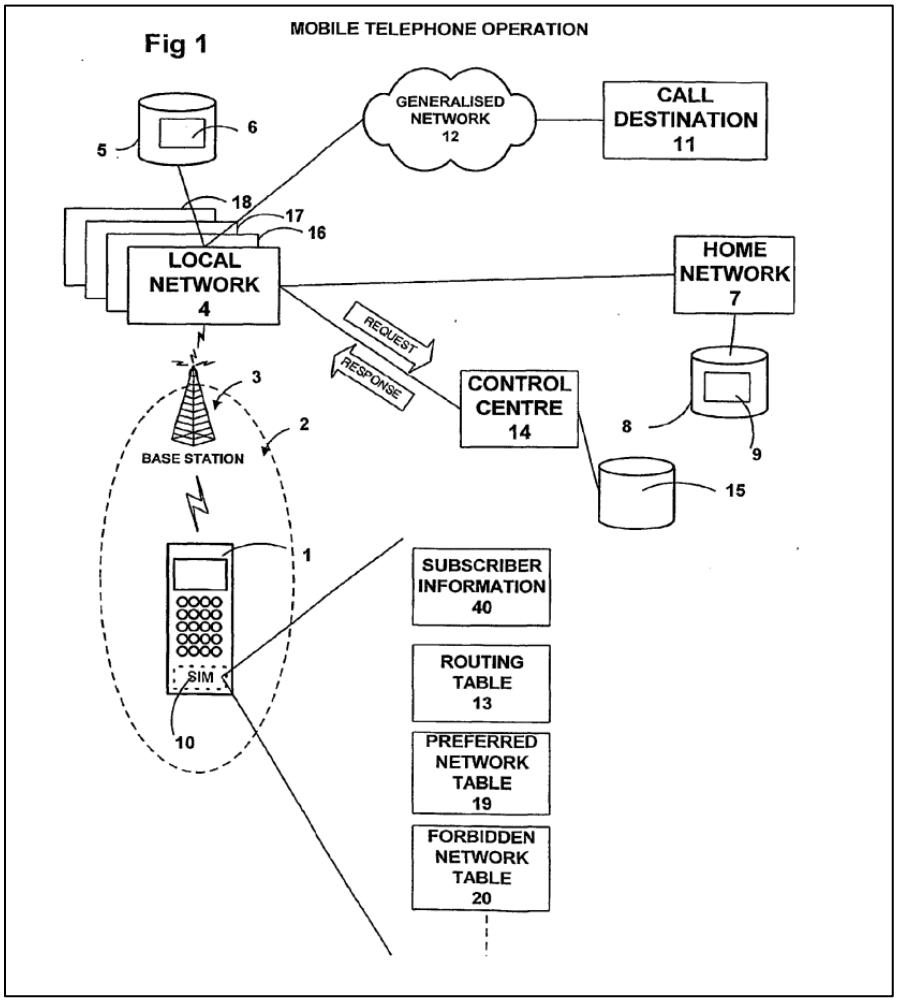
SAMSUNG-1006, FIGS. 1-3 (modified).



SAMSUNG-1006, FIG. 4.

102. As illustrated in FIG. 1 (reproduced below), when a device is outside its home network, it "register[s] with the local network 4 so that subsequent calls can be rapidly set up by the local network." SAMSUNG-1006, [0035]. "To commence the registration process, the mobile telephone 1 will typically need to

choose between a number of available networks including the local network 4 and additional networks 16, 17 and 18, any number of which may be detected as being available at the current location." *Id.*



SAMSUNG-1006, FIG. 1.

103. The mobile telephone 1 selects a network from among available networks using data in lookup tables stored in the SIM's memory—namely, "a preferred network table 19 which lists networks in order of preference" and "a forbidden network table 20 which lists those networks for which the subscriber

does not have authorisation from the home network 7 to complete registration." SAMSUNG-1006, [0036], [0046]. Once a network is selected, "[a]s part of the registration process, there is an exchange of information between the local network 4 and the home network 7 to establish the authenticity of the subscriber's proposed use of the network and to establish the manner in which calls are to be billed." SAMSUNG-1006, [0035].

104. After the device is registered, to optimize call routing, DB explains that "when a user enters a destination call number, an application of the mobile station is called to refer to a lookup table to retrieve stored data which enables the mobile station to perform least cost routing." SAMSUNG-1006, [0002]. The lookup table is stored on the SIM card's memory and is used by the device to select a network for registration and to perform optimized call routing to a call destination. SAMSUNG-1006, Abstract, [0003], [0046].

105. However, this "simplified scenario assumes that the current information stored in the SIM 10 is up to date and includes entries in the routing table 13, preferred network table 19 and forbidden network table 20 which are relevant to the currently available networks such as local network 4 and additional network 16 to 19." SAMSUNG-1006, [0038]. In practice, however, "[l]imitations on memory size and bandwidth for updating data to the SIM 10 prohibit the simultaneous maintenance of updated data covering all possible available networks

throughout the world for the GSM system," such that the information stored in the above-referenced lookup tables "is generally relevant only to the territory in which normal usage of the mobile station is anticipated." SAMSUNG-1006, [0003], [0039].

106. As a result, when the device roams from its home network, the "least cost routing function of the mobile station is [] typically unusable because of the lack of available relevant data within its memory." SAMSUNG-1006, [0004]. Thus, "[i]n the absence of stored data relevant to the currently available networks, the mobile station will typically register with whichever of the available networks presents the greatest signal strength,"—not according to the preferred and forbidden network lists. SAMSUNG-1006, [0005].

107. When the device is roaming away from its home network, the device registers with a local network, then determines whether new tables (including preferred and forbidden network lists, and call routing data) are required, and if so, uses the local network to retrieve up-to-date tables from a control centre. SAMSUNG-1006, [0051]-[0052], [0061], [0066], [0067]. Then, if the updated tables indicate that the device is connected to an unpreferred local network, the device re-registers on the preferred network according to the preferred and forbidden networks in the updated tables. SAMSUNG-1006, [0068]-[0069]. Once

connected, the device uses data in the routing table to determine routing information for outbound packets. SAMSUNG-1006, [0033]-[0034], [0053].

108. To obtain the new tables from the control centre, the device generates a request message that is "transmitted as an SMS (Short Message Service) message via the local network 4 to the control centre 14." SAMSUNG-1006, [0067]. Then, "[t]he control centre 14 responds by retrieving up-to-date tables from its database 15 and transmits a response message" in a SMS message that is transmitted "via the local network 4 to the mobile telephone 1." *Id.* The device receives the response message and updates the tables on the SIM with the received data. *Id.*

109. Even when the tables are present on the SIM, DB explains that the SIM table includes expiry information that "identif[ies] the maximum usable life of data such as the routing table," and beyond that life, the data are "expired and are no longer valid." SAMSUNG-1006, [0050], [0072]. When the device registers with its home network, if the "routing table has expired, or at least that relevant parts of the routing table relating to the registered network have expired and are no longer valid, a request message is generated at step 79 for an update of the routing table 13." SAMSUNG-1006, [0072]. DB explains that the device can determine that the data has expired by comparing the current time with the "time and date at which the validity expires," and/or the device "may output a message to the control centre 14 periodically in order to be informed whether the validity of the data has

expired." SAMSUNG-1006, [0108], [0110]. When the data is expired, a "request message is transmitted as an SMS message to the control centre 14 which responds by retrieving data from its database 15 and transmitting a response message in SMS format." SAMSUNG-1006, [0072]. Finally, "the routing table 13 is updated with the received data." SAMSUNG-1006, [0073].

110. DB's device additionally keeps a call log that stores "the duration and call destination of calls." SAMSUNG-1006, [0090]. The device periodically communicates the log data "to the control centre 14 by including call log information in the request message output by the message outputting means 104." SAMSUNG-1006, [0090], [0101]. The control centre can use the log "to verify billing information generated by networks within the generalised network 12 and by the local network 4." SAMSUNG-1006, [0090].

C. Schmidt-De Beer Combination

Overview

111. Schmidt describes a mobile device implementing a vSIM service that enables access to and use of a wireless cellular network communication. §IX.A. The vSIM service "replaces conventional smart card-based SIM card and its function." SAMSUNG-1005, [0030]; §IX.A. As explained above, telecommunication standards contemplated vSIMs replacing physical SIMS, e.g.,

explaining that "[a] virtual SIM can be used instead of, or as well as, a physical SIM." SAMSUNG-1063, 17.

112. While Schmidt describes techniques for implementing the vSIM service within a device's mobile trusted platform and explains that this service performs SIM card's functions of network use and access, it does not expressly describe details on how such conventional SIM-based function, e.g., of making calls and connecting to cellular networks, are performed.

113. In the same field of cellular network communications, DB describes implementation details regarding how these conventional SIM-based functions—including selecting a particular cellular network and routing calls efficiently to a destination—are performed using data stored in the SIM's memory. SAMSUNG-1006, Abstract; §IX.B.

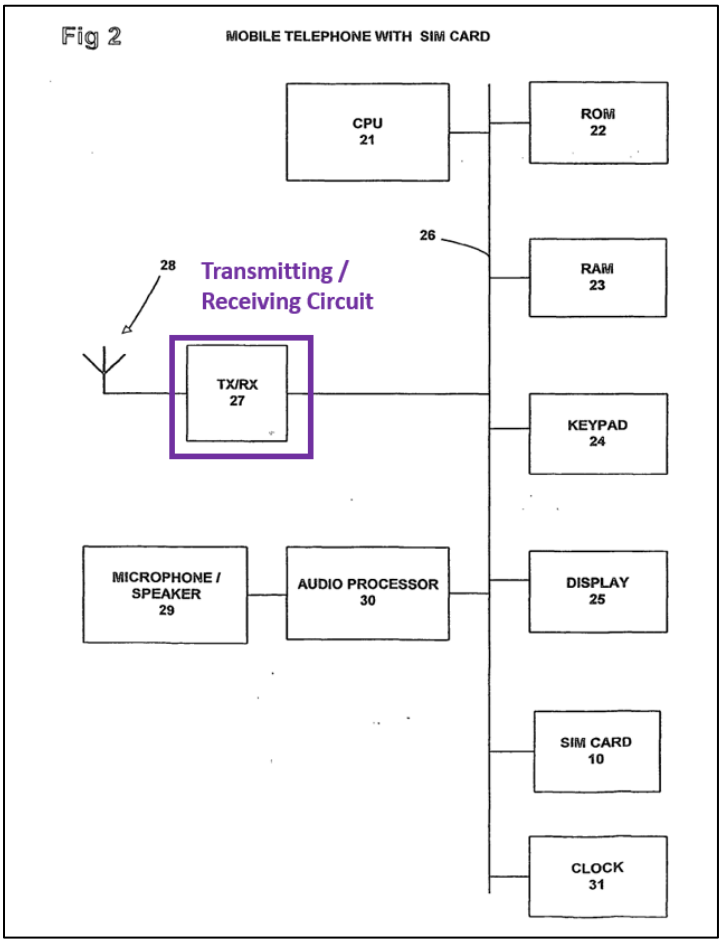
114. As explained further below, given that Schmidt's vSIM service replaces a SIM card and its associated functions, a POSITA would have found it obvious to combine Schmidt's and DB's teachings such that conventional SIM operations such as, e.g., network connection and call routing—as described in DB—would be performed using Schmidt's vSIM service and associated data.

Facilitating wireless network communications using a wireless modem

115. Both Schmidt and DB teach mobile devices that connect to and communicate with wireless cellular networks. §IX.A-B. A POSITA would have understood, or at least found it obvious, for such mobile devices to implement a modem to facilitate such wireless network communications.

116. In the relevant timeframe, it was well-known for a mobile device to implement a modem to enable wireless cellular network communications. For example, Taylor describes a "***wireless radio modem*** that may be incorporated into a host system … ***includes radio frequency modulation/demodulation circuitry*** employing electronic device elements that operate in a frequency range that minimizes the RF interference between the radio modem and the host system." SAMSUNG-1026, Abstract. Similarly, Schmidt and DB teach that mobile devices include transmission and receiver circuitry to facilitate wireless network communications. §IX.A-B. For example, Schmidt describes a wireless transmit/receive unit (WTRU) that includes a mobile trusted platform (MTP). SAMSUNG-1005, [0023]. In the WTRU, a "processor in association with software may be used to implement a radio frequency transceiver." SAMSUNG-1005, [0045]. DB similarly describes a mobile telephone with a "transmitting and receiving circuit," which is used, e.g., when "[t]he processor 21 initiates a call setup procedure with the local network 4 by outputting signals via the transmitter

circuit 27 which include the call routing information." SAMSUNG-1006, [0041]-[0042], [0076].



SAMSUNG-1006, FIG. 2 (annotated).

117. *Indeed*, a POSITA would have found it obvious for a computing device to use known networking components, such as a modem, to achieve the predictable result of facilitating network communications, as already contemplated by Schmidt and DB. Using a modem to enable a user device to communicate over the wireless cellular networks would have been a conventional and obvious way to

implement what each of Schmidt and DB describe, and is nothing more than utilizing familiar, known components (e.g., a modem including, e.g., a radio frequency transceiver of Schmidt, the TX/RX of DB) to achieve a predictable result of facilitating wireless cellular communications.

118. Thus, in view of Schmidt and DB's teachings of wireless network communication between mobile devices and a wireless cellular network, and the knowledge of a POSITA before the Critical Date (as evidenced by Taylor's above-cited disclosures as well as those of Schmidt and DB), a POSITA would have understood or found it obvious to implement Schmidt's mobile device to include a modem to facilitate the above-described network communications. A POSITA would have reasonably expected success in implementing the mobile device with a modem (including the above-described TX/RX or transceiver components) because this was a well-known, conventional way of achieving the wireless cellular communications that Schmidt and DB describe. For example, Alfano explains that:

- "Controller 106 is coupled to a radio modem 108 and an antenna 110". SAMSUNG-1034, [0028].
- "In most modern communication devices, controller 106 is embodied as a central processing unit (CPU) which runs operating system software in a memory compartment (not shown). Controller 106 will

normally control overall operation of wireless device 102, whereas signal processing operations associated with communication functions are typically performed in radio modem 108." SAMSUNG-1034, [0029].

- "Wireless device 402 includes a microprocessor 438, which is one implementation of controller 106 of FIG. 1, which controls overall operation of wireless device 402". SAMSUNG-1034, [0052].

119. Pattenden further explains that, "Radio modem device 104 generally includes a control block 108, a radio frequency (RF) transceiver 110, and an antenna 112. Control block 108 is coupled to interface 126 as well as to RF transceiver 110, which is coupled to antenna 112. Typically, control block 108 is embodied as a processor or central processing unit (CPU) which runs operating system software in a memory component." SAMSUNG-1035, [0018].

Securing transmissions from the modem

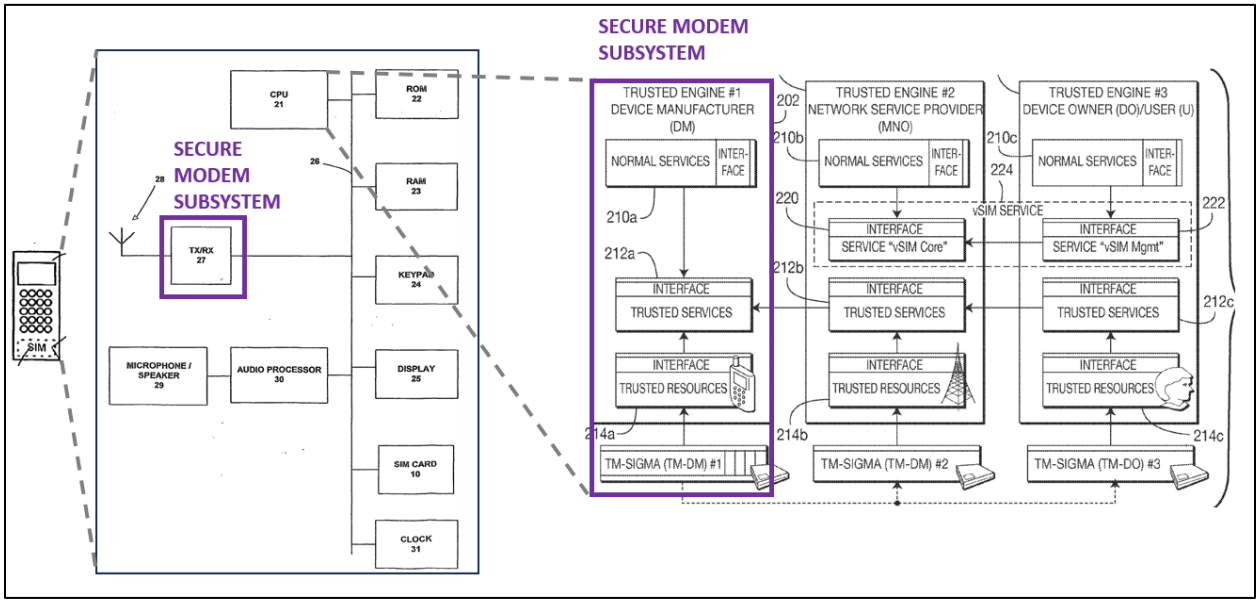
120. Schmidt explains that its vSIM architecture "is protected by a trusted operating system which is based on a permanently assigned trusted anchor and which supports multiple separate and trusted execution environments or sub systems." SAMSUNG-1005, [0025]. One such trusted execution environment is the "device manufacturer-trusted subsystem (TSS-DM)," which "controls all

internal and external communications and secures the communications channel." SAMSUNG-1005, Abstract, [0031]-[0032].

121. As explained in §IX.C (facilitating wireless network communication), the mobile device would implement a modem including components such as a transceiver (e.g., a TX/RX circuitry) that facilitate communications with a wireless cellular network. Because Schmidt teaches that TSS-DM "controls all internal and external communications and secures the communications channel," a POSITA would have understood or found obvious that the TSS-DM would control the communications that are transmitted/received via the above-described modem and its associated components. SAMSUNG-1005, [0032]. Indeed, in the relevant timeframe, it was well-known for a device to include logic to control the wireless cellular communications of a wireless modem via the device's modem (and its associated transceiver circuitry). For example, Alfano explains that "Wireless device 402 includes a microprocessor 438, which is one implementation of controller 106 of FIG. 1, which controls overall operation of wireless device 402" and "Controller 106 is coupled to a radio modem 108 and an antenna 110." SAMSUNG-1034, [0027], [0052].

122. A POSITA would have thus recognized that the TSS-DM (as executed by a processor, e.g., CPU of a device as disclosed in DB) and the above-described

wireless modem together make up a modem subsystem, as illustrated below.



SAMSUNG-1005, FIG-2 (modified), SAMSUNG-1006, FIGS. 1-2 (modified).

123. Additionally, because TSS-DM controls the communications and "secures" the channels used for such communication, a POSITA would have recognized that the TSS-DM together with the modem's transceiver circuitry, make up the combination device's secure modem subsystem. Indeed, further illustrating the secure aspects of the TSS-DM, Schmidt explains that an MTP "support[s] ***multiple protected, separate execution environments***"—one of which is the TSS-DM—where "[e]ach environment represents an area associated with a stakeholder." SAMSUNG-1005, [0030]. A POSITA would have recognized that using multiple TSSs, one for each stakeholder, isolates and protects data associated with the different stakeholders.

124. Specifically, Schmidt's FIG. 2 illustrates a user, network service provider, and device manufacturer—each of these stakeholders desire confidentiality and integrity guarantees over some portion of the data on the mobile device. For example, a POSITA would recognize that the MNO provides network access to a DO, and thus, the MNO TSS must correctly authenticate the DO to ensure they are indeed a valid subscriber to the network. For example, GSM networks contain Authentication Centers and Equipment Identity Registrars to, "serve for subscriber identification and authentication and for equipment registration." SAMSUNG-1023, 9. Contrarily, DOs often produce private information on their respective devices (such as personal photos), which they obviously wish to remain confidential to DMs and MNOs, and so on. By providing separate execution environments, each stakeholder is not only protected against potential threats created by other (adversarial) stakeholders, but are also insulated from errors originating from one TSS. For example, Madnick teaches "[i]f a single operating system's security fails, the VMM isolates this failure from other virtual machines."[9] SAMSUNG-1061, 11.

[9] While Madnick describes the benefits of isolation within the context of virtual machines, such benefits apply to technologies that provide isolation generally (e.g., secure execution environments).

125. Implementing the combination's secure modem subsystem would thus have been a conventional and obvious way to implement secure communications using a wireless modem and is nothing more than utilizing familiar, known components (e.g., a modem including RF circuitry of Schmidt and DB, together with TSS-DM of Schmidt) to achieve a predictable result of facilitating secure wireless cellular communications from the device.

126. A POSITA would have reasonably expected success in implementing such a secure modem subsystem given (1) Schmidt and DB's teachings of circuitry making up a modem enabling cellular network communications, (2) the common use of logic executed by a device to control communications using these hardware components, and (3) Schmidt's additional teachings of TSS-DM—i.e., a software-based trusted subsystem executed by a device processor—that provides one example of such conventional processing logic that controls network communications and additionally secures such communications.

Providing a secure partition in device memory that stores data conventionally stored in a physical SIM's memory

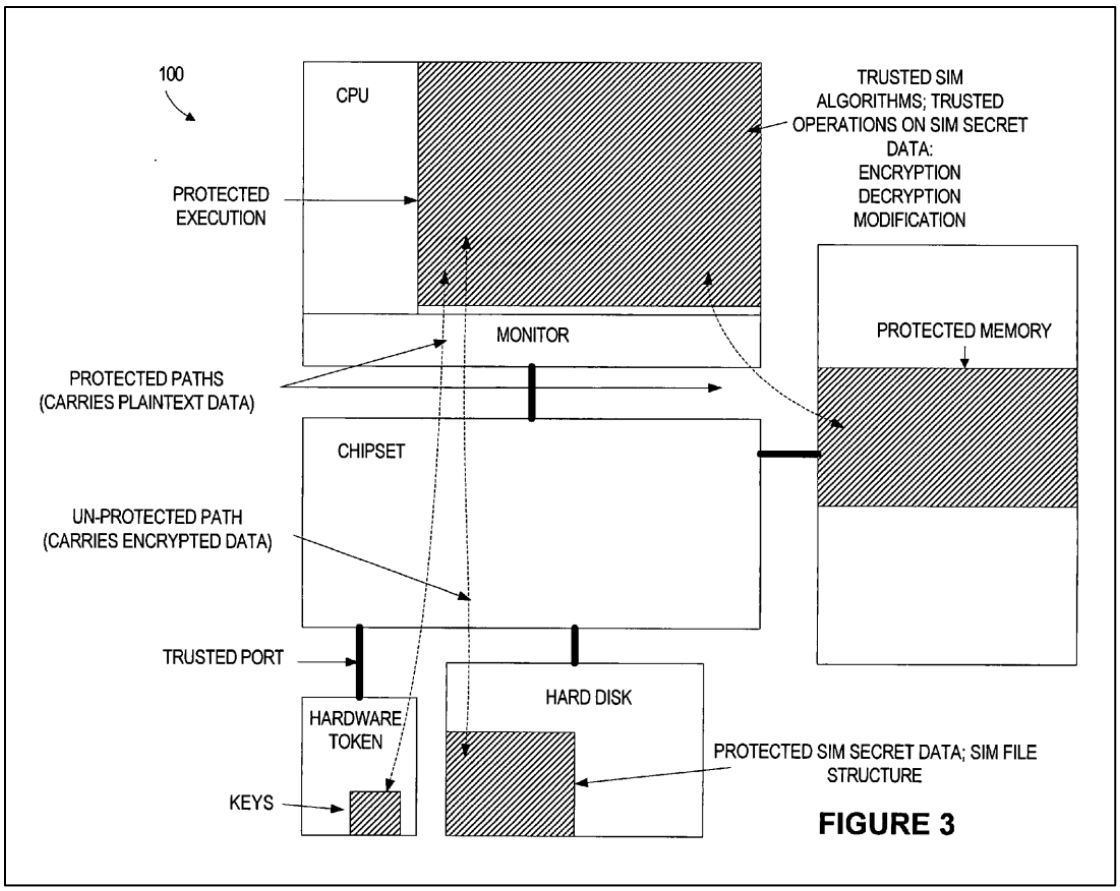
127. As explained in §IX.A *supra*, Schmidt's system would include a mobile device (e.g., a user equipment, cellular telephone, a PDA, or another user device capable of operating in a wireless environment) that implements a mobile trusted platform and which includes storage medium in the form of different types

of memory. *See* SAMSUNG-1005, [0023], [0143]-[0145]. Specifically, it is well-known that trusted platforms include memory that is partitioned into trusted and untrusted regions, e.g., as Scarlata explains: "[f]or example, a TPM may be used to protect data and to attest to the configuration of a platform," and "[t]he sub-components of a TPM may include an execution engine and secure non-volatile (NV) memory or storage." SAMSUNG-1067 [0003]. Additionally, the TrustZone Protection Controller, a hardware component within ARM processors that allow developers to create secure environments, "provides a software interface to set up memory areas as secure or non-secure." SAMSUNG-1059, 4.

128. As explained above (*see* §IX.A), the MTP includes multiple trusted subsystems (TSS) that are each configured to "store" information related to that subsystem. SAMSUNG-1005, [0005]. For example, the TSS-MNO "includes a vSIM core services unit, configured to ***store***, provide and process credential information relating to the MNO," and the "TSS-DO/TSS-U includes a vSIM management unit, configured to ***store***, provide and process credential information relating to the user of the MTP." *Id.* Schmidt further explains the MTP's architecture provides a "***protected storage***." SAMSUNG-1005, [0040], [0099]. Indeed, the "vSIM core service"—which is part of the TSS-MNO—is responsible for "the ***secure storage*** and use of subscribed data as well as subscriber authentication with the MNO." SAMSUNG-1005, [0033].

129. In the relevant timeframe, a POSITA would have recognized that providing a "protected storage" in a vSIM environment—as disclosed in Schmidt—offers some of the same security characteristics offered by a conventional SIM card. For example, Kasper explains that "[i]t is important … [that] vSIM services are at least as secure as traditional SIM-Cards," so "the platform must satisfy some generic SIM security characteristics, namely ***Protected Storage***, a tamper-resistant Isolated Execution Environment, User Authentication and Secure Channel." SAMSUNG-1029, 6. Kasper further explains that vSIM security characteristics include "that an adversary is not able to read, modify or destroy security-sensitive data or circumvent the access control mechanisms," and "prevent[ing] leakage of sensitive information" while ensuring that "required services are availab[le] and work as expected"). SAMSUNG-1029, 6. In addition, Bajikar explains that "the execution unit 146 may be capable of executing instructions to isolate open and protected partitions in on-chip (e.g. the cache memory 150) and off-chip memory (e.g. the main memory 120) and to control software access to protected memory." SAMSUNG-1066, [0027]. Bajikar further explains that the "main memory 120 may include both protected 154 and open 156 memory pages or partitions," and "[a]ccess to protected pages or partitions 154 in memory 120 is limited by the CPU 105 and/or the MCH 110 to specific trusted software and/or components as described in more detail herein, while access to

open pages or partitions in the memory 120 is according to conventional techniques." SAMSUNG-1066, [0035]. Bajikar's partitioned memory is illustrated in FIG. 3, reproduced below, which "shows, at a high level, various trusted paths and partitions that may be provided in the computing system 100 of one exemplary embodiment when a trusted execution environment has been established," where the "trusted areas are shaded." SAMSUNG-1066, [0046].



SAMSUNG-1066, FIG. 3.

130. For these reasons and the following additional reasons, a POSITA would have found it obvious to implement Schmidt's "protected storage" in the form of one or more secure memory partitions within SDD's on-device memory. Further, in the context of a mobile device, secure memory (e.g., flash memory) is secure storage. For example, Jobs describes a device that "may also include non-volatile memory, such as one or more magnetic disk storage devices, ***flash memory devices, or other non-volatile solid-state memory devices***." SAMSUNG-1062, [0097].

131. ***First***, as explained above, secure memory has significant security benefits that include, e.g., preventing circumvention of network access control mechanisms, preventing leakage of sensitive information, and ensuring proper operation of network services. SAMSUNG-1029, 6. For example, the TCG Mobile Trusted Module Specification discloses that TPMs "can manipulate data, provide evidence that they can be trusted to report the current state of the engine, and provide evidence about the current state of the engine." SAMSUNG-1031, 15. Moreover, the TCG Mobile Reference Architecture discloses that, "[t]he root key or its digest can be embedded in an RTS[10] (during manufacture, for example) if the

[10] Root-of-Trust-for-Storage (RTS) serves as a root of trust (or trust anchor) by storing sensitive information in a secure manner.

RTS has protected non-volatile memory. Alternatively, the root key or its digest can be loaded into the RTS during platform boot, before rogue software can execute on the platform. This enables the root key or its digest to be stored in protected non-volatile memory outside the RTS, and **loaded into protected volatile memory** inside the RTS every boot cycle," and thus, indicating the importance of secure ("protected") memory. SAMSUNG-1052, 29. Indeed, to provide the vSIM service that includes the same security benefits of a physical SIM, Schmidt's device is configured to provide "protected" or "secure" storage for storing SIM-related information (as explained above). SAMSUNG-1005, [0040], [0099]. Therefore, a POSITA would have understood that SDD includes secure memory.

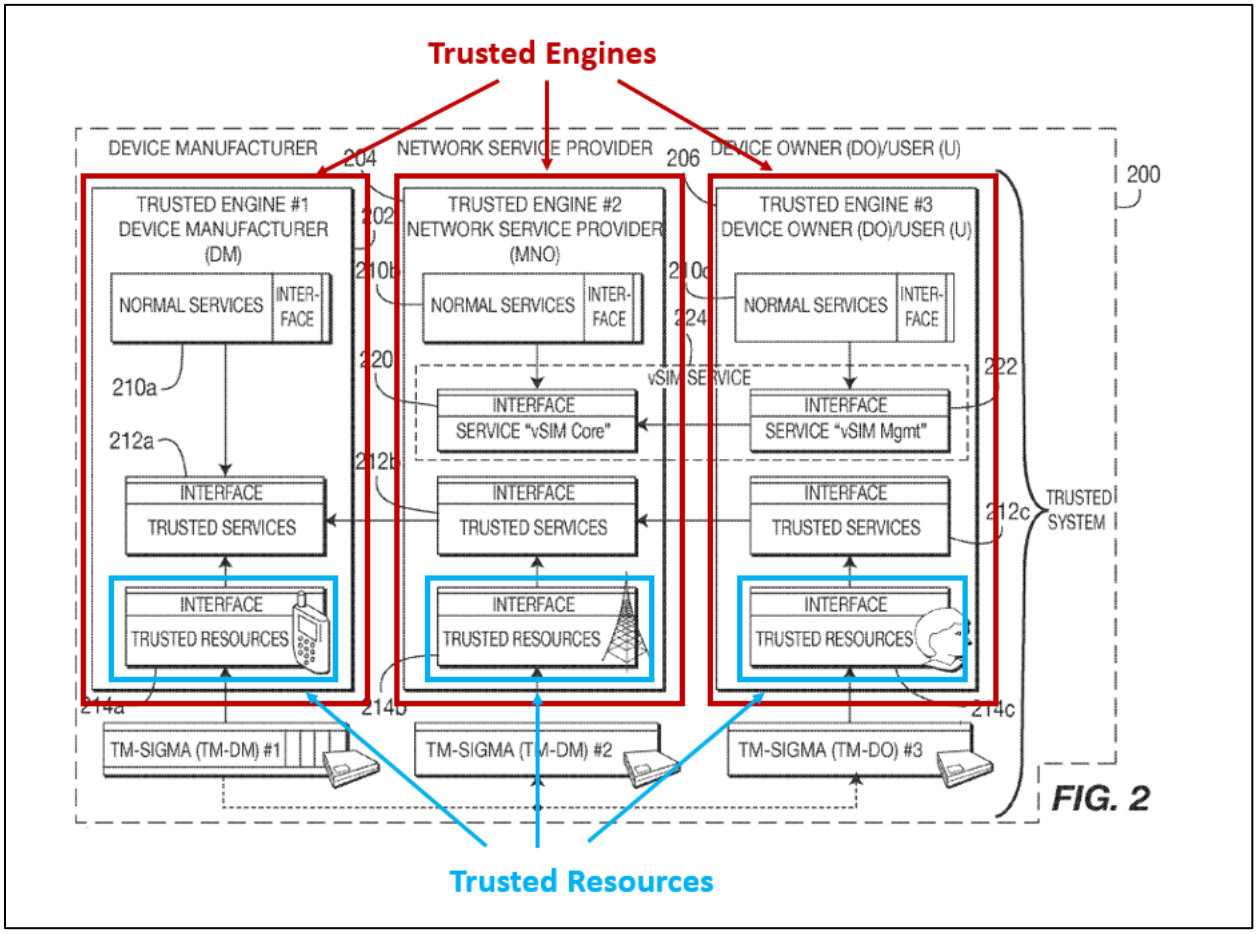
132. ***Second***, and relatedly, it was well-known in the relevant timeframe for device memory to include a secure memory partition to achieve such secure memory or protected storage within on-device memory. For example, Mittal explains that "execution units 211 may also be coupled to secure partition enforcement logic 218 which contains the logic to manage a secure partition in a memory or memories". SAMSUNG-1028, [0019]. Mittal further states that "[s]ecure memory partition 223 may be a section of physical memory or virtual memory." SAMSUNG-1028, [0020]. *See also* Mittal (SAMSUNG-1028) FIG. 2.

133. ***Third***, in the relevant timeframe, it was well-known for access to a secure memory partition to be limited to a secure execution environment and doing so, offered security benefits, including preventing unauthorized access to secure data, e.g., by misusing direct memory access and/or processor capabilities. For example, Mittal explains that:

> Securing execution includes ensuring the integrity of the execution and ensuring the privacy of code and data. Various types of threats may lead to a compromise of the integrity or privacy of a system. For example, malicious software may be able to exploit weaknesses in the operating system. Direct memory access devices may be able to read physical memory without processor support…. Attacks may also be made which take advantage of a processor's built-in debug mode or probe mode or which physically modify the connectivity of components in the system to observe and modify the communication between the components." SAMSUNG-1028, [0004]

134. ***Fourth***, Schmidt illustrates that each trusted engine (which are components of the trusted subsystems TSS-DM, TSS-MNO, TSS-DO/U) has access, via a dedicated interface, to a set of dedicated trusted resources.

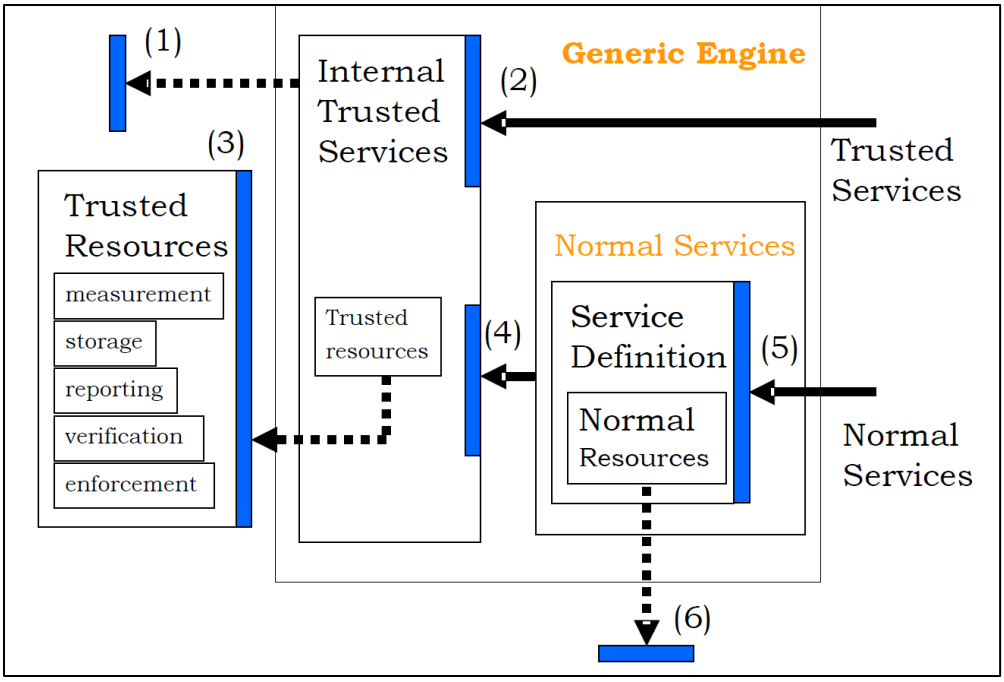
SAMSUNG-1005, [0037], FIG. 2.



SAMSUNG-1005, FIG. 2 (annotated)

135. In the relevant timeframe, it was well-known for access to trusted resources to be limited to a particular secure execution engine and to include secure storage.

136. For example, the TCG Mobile Reference Architecture illustrates that trusted resources are accessible only from within the engine. SAMSUNG-1030, 28, FIG. 3.



SAMSUNG-1030, FIG. 3.

137. Since Schmidt illustrates that the trusted resources (which would include protected/secure storage) in a trusted engine are accessed only by trusted services in that engine, a POSITA would have thus recognized or found obvious that access to a protected storage/secure memory partition would be limited to the corresponding trusted engine. SAMSUNG-1005, FIG. 2.

138. Thus, for the reasons described above, to achieve Schmidt's goal of providing "a more dynamic and ***concurrently secure*** software based solution to the SIM function," a POSITA would have been motivated to provide a secure partition in on-device memory to facilitate such protected and dedicated storage of subscriber and other similar SIM-related data, as contemplated by Schmidt. SAMSUNG-1005, [0004].

139. Trusted Platform Modules are one approach that provides secure storage through asymmetric cryptography. For example, TPMs contain private keys, embedded in tamper-resistant hardware, whose corresponding public key can be used to verify the authenticity of the data (i.e., a digital signature). SAMSUNG-1052, 37. Moreover, "shielded locations" are regions of memory in which the kernel of the operating system cannot read (without going through the API of the TPM). SAMSUNG-1052, 37. Using these mechanisms, TPMs can provide both confidentiality and integrity over data by serving as a "root of trust" and "shielded locations." SAMSUNG-1031, 16.

140. And, implementing such a secure memory partition as part of Schmidt's on-device memory would have been nothing more than implementing known methods/techniques (providing a secure memory partition for on-device memory) to known systems/devices (Schmidt's MTP/device that already contemplates a protected storage accessible by its TSSs) to achieve predictable results (a device with multiple TSSs and a memory with dedicated secure memory partitions, one which may store the SIM and subscriber related information).

141. A POSITA would have had a reasonable expectation of success in so implementing one or more secure memory partitions within memory of Schmidt's device. That's because Schmidt teaches that (1) the MTP includes a "protected storage" function and on-device memory, (2) TSS-MNO, via its vSIM core

service, is responsible for "secure storage and use of subscriber data as well as subscriber authentication with the MNO," and (3) it was well-known and conventional to use secure memory partitions to facilitate such secure storage within on-device memory (e.g., that is accessibly by a respective TSS). Such a combination would have also been well within a POSITA's capability to implement and would have involved a known and conventional implementation that achieves the MTP's disclosed secure data storage and access functions.

142. A POSITA would have also had multiple reasons to store data—conventionally stored in a physical SIM card–in one or more of the above-described secure memory partitions that would have been implemented in Schmidt's on-device memory.

143. For example, Schmidt discloses that the TSS-MNO's "vSIM core service is responsible for the ***secure storage*** and use of ***subscriber data as well as subscriber authentication*** with the MNO." SAMSUNG-1005, [0033]. A POSITA would have understood or at least found obvious that such "subscriber data" and "subscriber authentication" related information used in conjunction with a network operator (MNO) would include data conventionally stored in a physical SIM's memory that is used to access and use wireless services provided by a network operator. Further, as described above, storing subscriber data in secure memory prevents circumvention of network access control mechanisms and prevents

leakage of sensitive information. SAMSUNG-1029, 6. That is, the subscriber data would be stored in "shielded locations" which are protected by the TPM. SAMSUNG-1030, 37. Therefore, a POSITA would have understood that vSIM subscriber data is stored in the secure memory partition.

144. In a further example, in the relevant timeframe, DB disclosed a SIM's memory storing data used to connect to a cellular network and use its voice service (e.g., make calls using the connected-to network), such as, e.g., a routing table, preferred and forbidden network tables, and table expiry information. *See* SAMSUNG-1006, [0005], [0034], [0038], [0046], [0050]-[0051], FIG. 4. In addition, in the document "Characteristics of the USIM application," the 3rd Generation Partnership Project describes types of data store on a SIM including the Accumulated Call Meter (ACM) Maximum Value, USIM Service Table, Service Provider Name, Price per Unit and Currency Table, Cell Broadcast Message identifier selection, Access Control Class, Forbidden PLMNs, Cell Broadcast Message Identifier Range selection, Fixed Dialling Numbers, MSISDN, Short message service parameters, Short Message Status, etc. SAMSUNG-1025, 15-16, 19-22, 24-27, 32, 34-35, 39. Since these data fields relate to network connection and access, a POSITA would have understood that it was common for a SIM's memory to store data used to connect to a cellular network and to use its voice service.

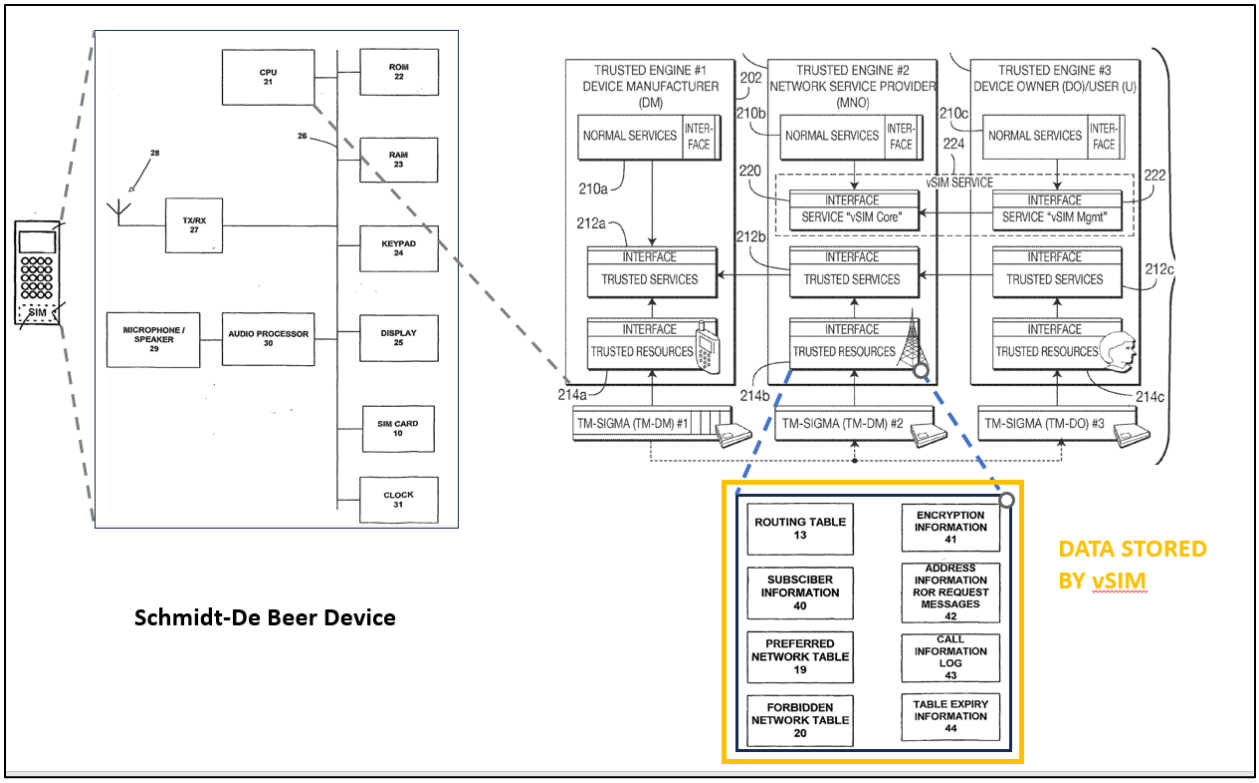
145. A POSITA would have had multiple reasons for the one or more above-described secure memory partitions to store SIM data such as, e.g., DB's lookup tables, given Schmidt's disclosure of secure storage of similar information and DB's disclosure of storage of such information in the SIM's dedicated memory. Indeed, providing secure storage of such information would further Schmidt's security goal of "prevent[ing] loss and escape of security-sensitive data, and ensur[ing] that all necessary services"—such as wireless network access and use of voice services—"are available and functional." SAMSUNG-1005, [0040].

146. Additionally, Schmidt teaches that its "vSIM service [] replaces the conventional smart card-based SIM card and its function." SAMSUNG-1005, [0030]. Therefore, to enable Schmidt's vSIM service to replace conventional SIM card function, it would have been obvious for this service to store data conventionally stored in a physical SIM's memory, including, e.g., a routing table, a preferred network table, a forbidden network table, table expiration information, as described in DB and as illustrated below. For example, Schmidt notes that "[a] vSIM platform must also ensure that only authorized subjects are able to access or manipulate protected data of the vSIM credential", where it is important to protect the vSIM credential data when "stored in the volatile or nonvolatile memory of the MTP." SAMSUNG-1005, [0040]. A POSITA would have understood that the vSIM credential would be protected in non-volatile memory (i.e., RAM) by

partitioning RAM into secure and insecure memory regions (as secure memory would only be accessed by trusted components, while insecure memory would be used by the system generally), which was conventional well before the Critical Date. For example, the ARM TrustZone Protection Controller "provides a software interface to the protection bits in a secure system in a Trustzone design" which "provides system flexibility to enable you to configure different areas of memory as secure or non-secure." SAMSUNG-1059, 3.

147. Such a combination would have amounted to implementing known methods/techniques (storage of SIM data in a secure on-device memory partition) to known systems/devices (Schmidt's vSIM-based MTP) to achieve predictable results (usage of vSIM services that are the same as those offered by a physical SIM).

148. A POSITA would have further expected reasonable success in such a combination given Schmidt's teaching of secure storage of data used to communicate with a network operator, and DB's express recognition of such data including the above-described lookup tables.



SAMSUNG-1005, FIG-2 (modified), SAMSUNG-1006, FIGS. 1-2 (modified).

Implementing roaming capability in Schmidt's vSIM-based environment

149. Schmidt explains that its MTP uses the vSIM service to access wireless cellular network services—similar to how a physical SIM facilitates connection and access to network services. SAMSUNG-1005, [0093]-[0109], FIG. 8. Additionally, as explained in §IX.C (secure partition), a POSITA would have found it obvious for the Schmidt-DB combination to leverage DB's teachings of data elements conventionally stored in SIM memory, and to store those elements within a secure memory partition on the combination's device.

150. Although Schmidt does not expressly describe how cellular services are used when Schmidt's device is roaming (i.e., away from its home network), a POSITA would have had multiple reasons to implement the device so as to facilitate use of network services while roaming and would have leveraged DB's teachings in this regard.

151. ***First***, in the relevant timeframe, it was well-known for devices communicating over wireless cellular network communications to support cellular network access and associated services while the device is roaming. For example, Nelson explains that when a "mobile station is operating in an area in which the primary service provider does not provide service, it may be desirable for the mobile station to obtain service from some secondary service provider, and in cases where "a mobile station obtains service from a service provider other than its primary service provider, that mobile station is ***roaming***." SAMSUNG-1027, 2:10-16. Nelson further explains that "[w]hen a mobile station determines that it can no longer obtain acceptable service from a primary service provider, the mobile station determines whether it is operating at the periphery of the primary service provider coverage area," and if so, "the mobile station is permitted to obtain service from a secondary service provider (i.e. roam)." SAMSUNG-1027, Abstract.

152. A POSITA would have been motivated to implement such conventional roaming functionality within a mobile device and in doing so, enabling device mobility away from the device's home network without interrupting access to wireless network services (e.g., making and receiving calls over a cellular network even when roaming).

153. ***Second***, DB describes a device that supports roaming and stores and updates data in its SIM's memory that is used to facilitate network access and communications while the device is roaming. SAMSUNG-1006, [0046]-[0051], [0066]-[0074]. DB explains that information stored on the SIM card "is generally relevant only to the territory in which normal usage of the mobile station is anticipated." SAMSUNG-1006, [0003]. Therefore, when the device roams from its home network, the "least cost routing function of the mobile station is [] typically unusable because of the lack of available relevant data within [the SIM's] memory." SAMSUNG-1006, [0004]. DB similarly explains that a "further problem arises from the usage in mobile stations of a preferred network table and forbidden network table [which are] generally stored in the SIM card." SAMSUNG-1006, [0005]. Therefore, a POSITA would have understood that this data may similarly become outdated when the combination's device is roaming. SAMSUNG-1006, [0004]-[0005].

154. To address these issues, DB describes that its device coordinates with a control centre to obtain updated information specific to the roamed-to region and updates the stored SIM data accordingly. SAMSUNG-1006, [0066]-[0074]. In particular, when away from its home network and after connecting with a local network, DB teaches that the device determines whether new tables are required, and if so, uses the local network to retrieve up-to-date tables from a control centre and stores them in the SIM's memory. SAMSUNG-1006, [0061], [0066], [0067]. Then, using the data in the updated lookup tables, DB's system accesses a preferred wireless network and performs least cost routing for calls. SAMSUNG-1006, [0068]-[0069], [0033]-[0034], [0053].

155. A POSITA would have thus been motivated to leverage DB's above-described teachings to overcome the issues with outdated SIM data, by obtaining and updating the lookup tables stored in secure memory and using that data to enable access to preferred wireless networks and to perform least cost routing of a call to its destination, including while the device is roaming. SAMSUNG-1006, [0046], [0075], [0087], [0097], [0099], [0112] (using data in updated routing table to perform call routing), SAMSUNG-1006, [0036], [0038], [0057], [0084], [0100] (using data in updated preferred and forbidden networks list to enable network access). For example, De Beer explains that "when an outgoing call to a call destination 11 is initiated by a call number input 108, the routing means intercepts

the call making process and provides a call output means 109 with routing information which will determine the route taken through the generalised network 12 between the local network 4 and the call destination 11." SAMSUNG-1006, [0087]. The "routing table 13 may include instructions for calls to certain call destinations 11 to be routed using a different protocol in which, instead of appending routing information to the outgoing call setup signals, an outgoing message, such as an SMS message is generated and forwarded to the control centre 14 to request routing information." SAMSUNG-1006, [0097].

156. ***Third***, implementing DB's teachings in combination with Schmidt would have amounted to nothing more than the use of a known technique (enabling conventional roaming functionality via DB's described teachings of updating lookup tables stored in the SIM and leveraging that data to facilitate network access and use while roaming) to improve similar devices (Schmidt's MTP) in a similar way and combining prior art elements according to known methods to yield the predictable results (as described above, e.g., network connectivity and least cost routing when a device is roaming).

157. A POSITA would have expected success in implementing DB's teachings related to roaming into Schmidt's device. The elements of the resulting combination device would each perform functions they had been known to perform prior to combination—the Schmidt-DB device providing for secure storage of

lookup tables in a secure memory partition and DB's additional teachings of services that update that data and use the updated data to facilitate network connectivity and call routing while the device is roaming. Moreover, combining these teachings would have required only routine programming knowledge well within the skill of a POSITA before the Critical Date. Schmidt already teaches that its TSS-MNO access securely stored data to interact with a network operator and thus, it would be straightforward to configure the TSS-MNO to interact with a network operator, such as the control centre, to obtain updated data (as described in DB) and to implement the additional functionality that uses this data to perform the above-described services (as also described in DB).

Schmidt-DB Combination

158. Schmidt-DB Device (SDD) refers to the above-described system that a POSITA would have been led to form based on Schmidt's and DB's teachings.

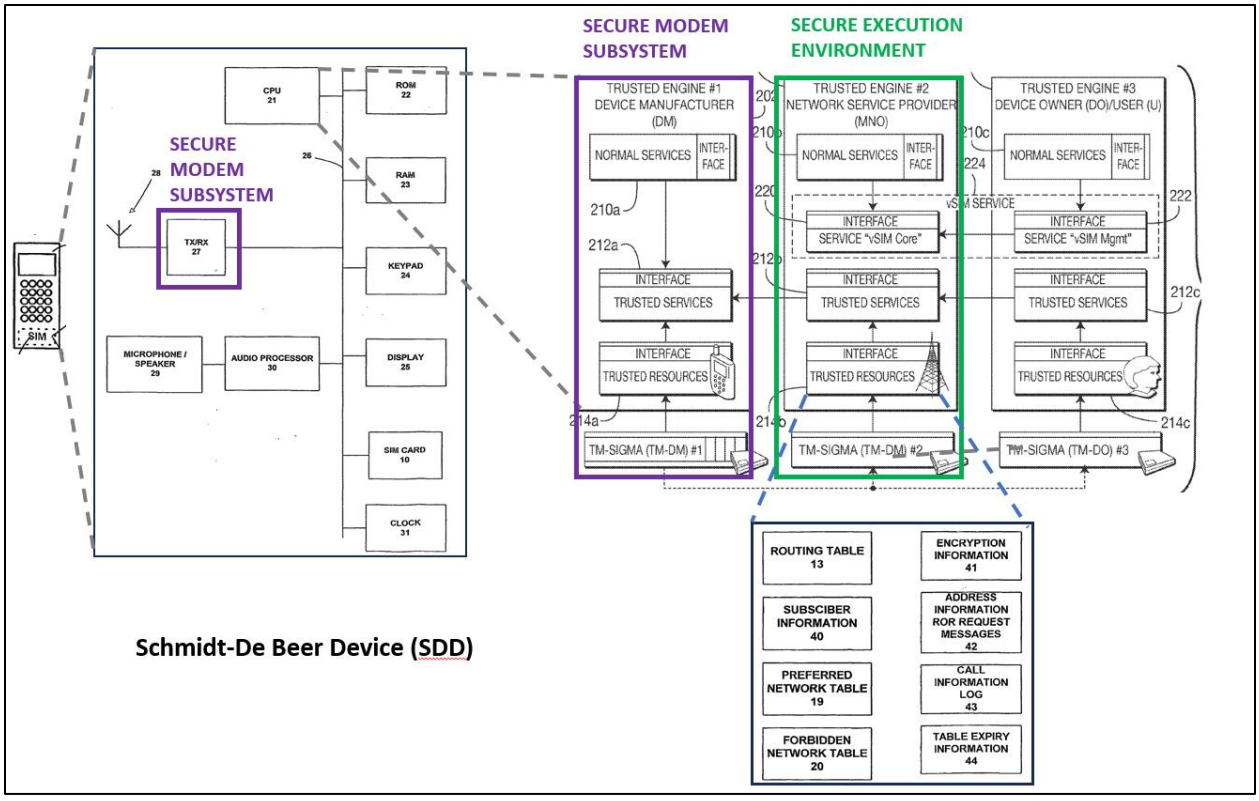
159. SDD implements a mobile device that, per Schmidt, includes a mobile trusted platform (MTP) with multiple trusted subsystems (TSS-DM, TSS-MNO, TSS-DO) and stores a vSIM credential. SAMSUNG-1005, [0002], [0023], [0029]-[0035], Abstract; *see* §IX.A.

160. SDD's mobile device further includes a wireless modem, including transceiver components, such as TX/RX, as disclosed in DB and Schmidt. SAMSUNG-1006, [0042], FIG. 2.

161. The wireless modem is secured by TSS-DM, which, per Schmidt, "***controls*** all internal and external communications and ***secures the communications channel***." SAMSUNG-1005, [0032]. Thus, SDD's wireless modem (including the transceiver components) and TSS-DM together facilitate communications of the device, and therefore form a secure modem subsystem.

162. SDD includes one or more secure memory partitions in on-device memory. SDD stores, in the one or more secure memory partitions, the vSIM credential (per Schmidt), as well as additional information conventionally stored on a physical SIM—which according to DB—can include a routing table, preferred network table, forbidden network table, etc. SAMSUNG-1006, [0046]-[0051], FIG. 4.

163. An example architecture of SDD, which leverages teachings of Schmidt and DB, is illustrated below:



SAMSUNG-1005, FIG-2 (modified), SAMSUNG-1006, FIGS. 1-2 (modified).

164. Additionally, as described above, SDD leverages DB's teachings related to roaming. For example, when away from its home network and after connecting with a local network, SDD determines whether new tables are required, and if so, uses the local network to retrieve up-to-date tables from a control centre and stores them in secure memory (per DB). SAMSUNG-1006, [0061], [0066], [0067]. Additionally, per DB, SDD is configured to update this data (which would be stored in a secure memory partition in SDD, and as I described above, secure memory partition were well-known) and use this data for network functions, such as connection to a preferred network and performing least cost routing to a call

destination. SAMSUNG-1006, [0052]-[0053], [0056]-[0059], [0068]; SAMSUNG-1059, 3. (Updating SIM data and using those data for network functions is described throughout the De Beer reference. SAMSUNG-1006, *generally*.)

165. In summary, and as I describe further in §X, SDD includes the trusted platform of Schmidt which provides a virtualized SIM that replaces a physical SIM card and its associated functions. §IX.C. SDD's trusted platform includes a SEE (TSS-MNO and associated TM-SIGMA) and secure or protected storage in the form of a secure memory partition that stores SIM-related data, including policy settings (e.g., routing table, preferred network table, forbidden network table conventionally stored on a physical SIM) that guide SDD's operation (e.g., determining to which network SDD connects and how traffic is routed on that network). From time-to-time and during operation of the device, SDD receives updated policy settings from a network service controller (control centre) over dedicated control channels, e.g., when SDD roams to a new location and/or when the policy settings expire.

D. U.S. Pat. App. Pub. No. 2004/0148237 ("Bittmann")

166. Bittmann describes techniques for "real time management of a communication network account" associated with a mobile device. SAMSUNG-1007, Abstract. In Bittmann, "an activity monitoring unit installed in or connected

to a communication device associated with the account" monitors "data activity of the communication device" and reports "on the data activity." SAMSUNG-1007, Abstract.

167. An "activity monitoring server utility" receives "reports on the data activity from the unit, rate[s] the data activity, and update[s] at least one allowance of the account based on a result of the rating." *Id.* The "rating of a voice event is typically based on rules related to the event (for example, the duration of the call, the distance between the two parties to the call, etc.) and/or related to the account (for example, the number of free minutes per period, discounts for multiple communication devices, etc.)." SAMSUNG-1007, [0002]. The "[p]ermitted activity for the account is changed if an allowance of the account reaches a predetermined restriction level." SAMSUNG-1007, Abstract.

168. Bittmann explains that "[r]ating data is difficult because data can be evaluated at different levels," e.g., "at the traffic level, the number of bytes and/or packets can be counted and rated" and "at the service level, the type of traffic can be determined and rated." SAMSUNG-1007, [0003].

169. In response, Bittmann's system "allows real time management of a communication network account, including real time change in the permitted activity of the account when necessary," and "the change in the permitted activity

may be the total blocking of all communication until credit for the account is re-established." SAMSUNG-1007, [0022]-[0023].

170. Bittmann's system (as depicted below) provides a communication device 110 that includes a monitoring unit that "monitors data activity of communication device 110" and "manages the account" of the device. SAMSUNG-1007, [0028]-[0029]. The monitoring unit monitors all data activity on the device or a subset of the data activity, such as, e.g., "web surfing, game-playing, emails, short message service (sms), voice over IP, faxing, transactions, etc." SAMSUNG-1007, [0031].

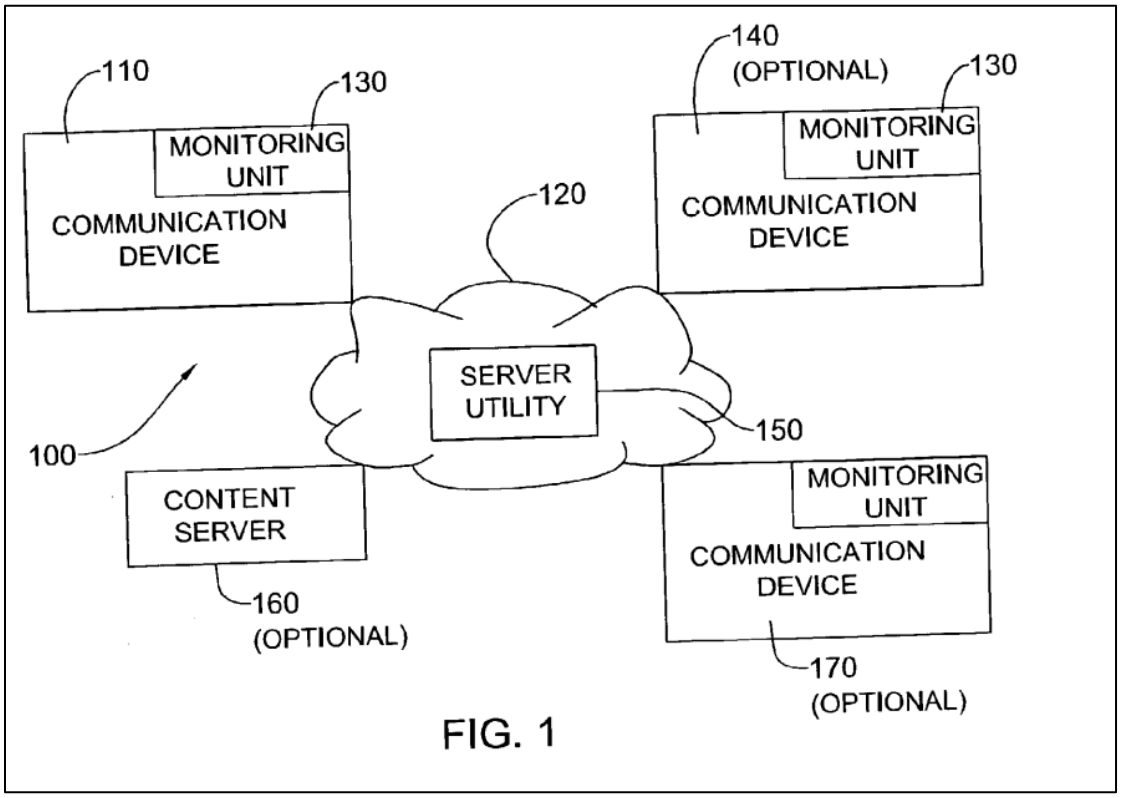


FIG. 1

SAMSUNG-1007, FIG. 1.

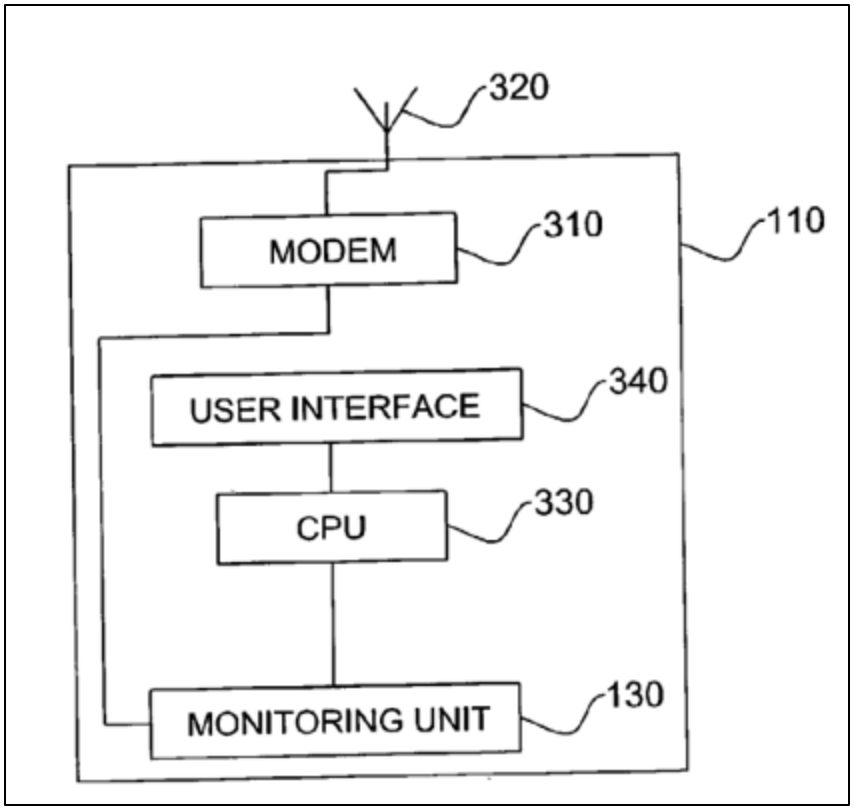
171. To "access the communication infrastructure, an account(s) associated with communication device 110 (and optionally 140) is established with the corresponding network operator(s)." SAMSUNG-1007, [0035]. In Bittmann, "one or more allowances are associated with each account," and although "one or more of the account allowances may not have associated restriction level(s), preferably at least one of the allowances has at least one associated restriction level." SAMSUNG-1007, [0037]. Then "[w]hen one or more of the allowances reaches the associated restriction level(s), activity in the account begins to be restricted." SAMSUNG-1007, [0037].

172. The device's monitoring unit sends data activity reports to the server utility, which rates "the data activity reported by the monitoring units." SAMSUNG-1007, [0042]. Such reports are transmitted "automatically in a manner not controlled by the user of communication device 110," which "ensures the integrity of activity data transfer to the server utility." SAMSUNG-1007, [0062]. The "transmission may periodically be initiated by monitoring unit 130, e.g., automatically after passage of a predefined time or according to a predefined set of rules or alternatively when unit 130 senses an off-peak period." SAMSUNG-1007, [0062].

173. When the "allowance reaches a pre-determined restriction level," the server restricts activity in the account. SAMSUNG-1007, [0045]. Restrictions can

be enforced by the monitoring unit or by the network, and can include "blockage of all data activity, blockage of certain types of data activity, blockage of non-free data activity, blockage of non-service related data activity (but allowing some or all service related data activity, for example data activity for replenishing the allowance), preventing all or some new data sessions from beginning (while allowing some or all current data sessions to complete), etc." SAMSUNG-1007, [0045], [0047].

174. As shown in FIG. 3A, Bittmann's monitoring unit can be coupled to the device's modem. SAMSUNG-1007, [0052], FIG. 3A. Bittmann explains that the "link between monitoring unit 130 and receiver/transmitter" of the device allows the device "to transmit stored activity data, through the cellular communication infrastructure, to server utility 150, preferably as out-of-band traffic." SAMSUNG-1007, [0053]. Additionally, "the link is configured so as to cause all data received by the associated communication device 110 or 140 to be intercepted by monitoring unit 130 prior to becoming available to the user of communication device 110 or 140." SAMSUNG-1007, [0053].



SAMSUNG-1007, FIG. 3A.

E. Schmidt-De Beer-Bittmann Combination

175. As explained in §IX.C, SDD is a mobile device that includes a secure execution environment and secure modem subsystem and that is configured to implement a vSIM service that provides the function of a conventional SIM.

176. Per DB, SDD connects to a "home" cellular network which in turn is associated with a service provider through a contractual relationship. SAMSUNG-1006, [0030], [0035]. Given that SDD facilitates use of services provided over a cellular network using the vSIM service, SDD would leverage DB teachings of

storing and tracking data related to the use of these services. For example, DB's device uses a call log, which is stored on the SIM, "for storing the duration and call destination of calls." SAMSUNG-1006, [0090], [0049], FIG. 4. The device periodically communicates this log data "to the control centre 14 by including call log information in the request message output by the message outputting means 104." SAMSUNG-1006, [0090], [0101]. The control centre can use the log "to verify billing information generated by networks within the generalised network 12 and by the local network 4." SAMSUNG-1006, [0090].

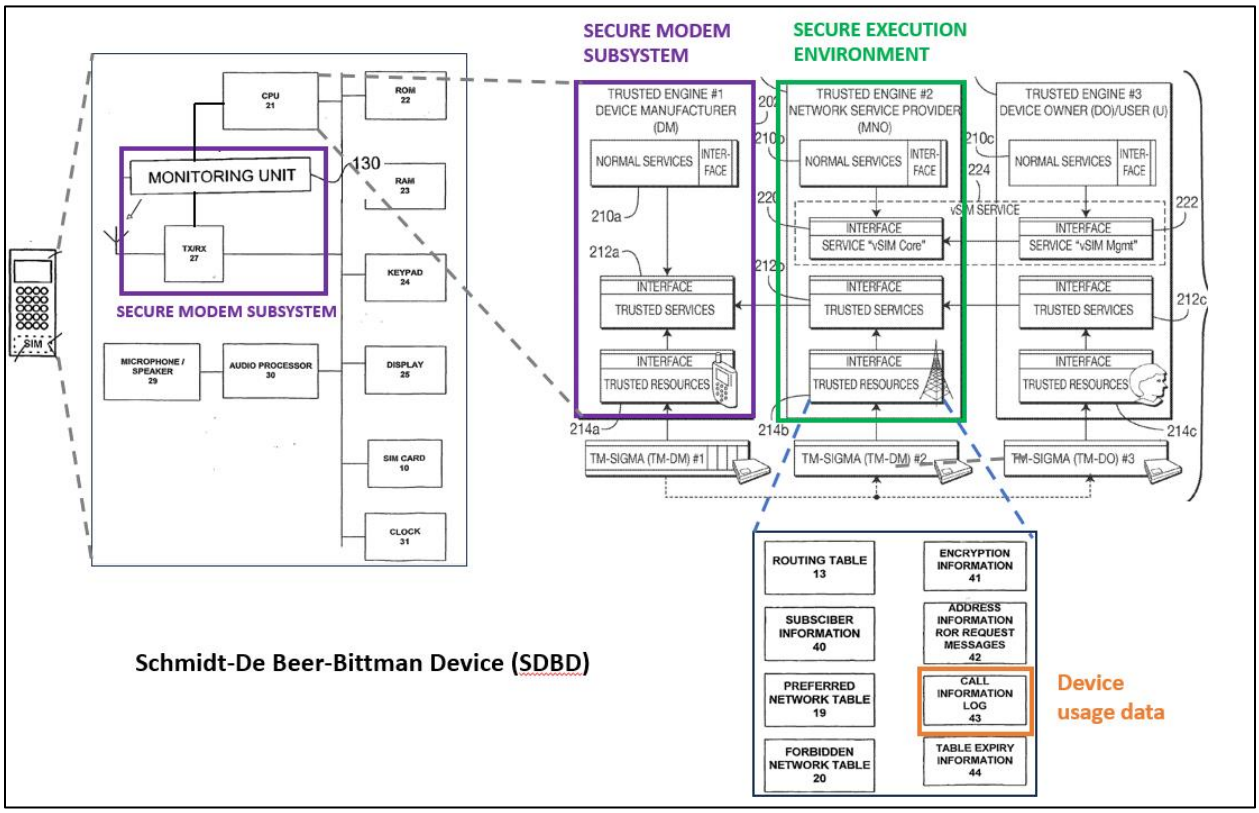
177. However, while DB explains that such data is captured and stored in a log, DB does not explicitly describe techniques for obtaining this log data.

178. A POSITA would have thus been motivated to look to references such as Bittmann, which describes a mobile device that includes a monitoring unit that monitors a device's network activity, provides reports to a server (similar to DB), and enforces service plan limits. §IX.D. The resulting Schmidt-DB-Bittmann device (SDBD) includes the components of SDD, enhanced by Bittmann's monitoring unit, which monitors device usage and enforces service plan limits. The monitoring unit would be included in the SDBD's secure modem subsystem, enabling it to "monitor[] data activity of communication device" and to "cause all data received by the associated communication device 110 or 140 to be intercepted by monitoring unit 130 prior to becoming available to the user of communication

device 110 or 140," per Bittmann. SAMSUNG-1007, [0028], [0031], [0053]. A POSITA would have understood that by including the monitoring unit in the modem subsystem, the monitoring unit has efficient access to all data transferred into and out of the device. Placing the monitoring unit in the modem subsystem ensures that the monitoring unit has access to all incoming and outgoing cellular data since such data necessarily traverses the cellular modem system (the component that sends and receives network data). Further, locating the monitoring unit in the modem subsystem simplifies the design of the monitoring unit by isolating the monitoring unit from data that is not incoming or outgoing – that is, the monitoring unit never "sees" data that need not be monitored, such as data transferred internally to the device. Excluding such data from monitoring also improves efficiency and conserves device resources by avoiding unnecessary work.

179. Bittmann itself describes this arrangement as a preferred embodiment, writing, "FIG. 3A shows cellular telephone 110 including a network interface 310 connected to an antenna 320. Network interface 310 can be for example a modem. Activity monitoring unit 130 links between a CPU 330 and network interface 310." SAMSUNG-1007, [0052]. Thus, Bittmann discloses that the monitoring unit is specifically placed to monitor data destined for a modem (and thus, is part of the modem subsystem). Also in the context of SDD,

which replaces the SIM card with a vSIM service, the call log data would be stored in SDD's secure memory partition since this secure memory partition replaces the secure memory partition of a physical SIM. SAMSUNG-1006, [0049], FIG. 4.



SAMSUNG-1005, FIG-2 (modified), SAMSUNG-1006, FIGS. 1-2 (modified); SAMSUNG-1007, FIG. 3A (modified).

180. In operation, SDBD performs the functions of SDD, including installing a vSIM and loading routing information. *See* §IX.C (Securing transmission from the modem). Additionally, to ensure compliance with SDBD's service plan, SDBD's monitoring unit monitors the device's inbound and outbound

traffic and stores the data in SDD's secure storage/memory partition. SAMSUNG-1006, [0049], FIG. 4; SAMSUNG-1007, [0028], [0031], [0053].

181. SDBD transmits data activity reports to a server, which rates "the data activity reported by the monitoring units." SAMSUNG-1007, [0042], [0062]. A POSITA would have understood that the Bittmann's server utility would execute on DB's control centre at least because both DB's control centre and Bittmann's server receive device usage data. For example, DB explains that "mobile stations may accumulate call log data to be included periodically in the request message for analysis at the control centre." SAMSUNG-1006, [0101]. Bittmann similarly explains that the device transmits "stored activity data, through the cellular communication infrastructure, to server utility 150, preferably as out-of-band traffic." SAMSUNG-1007, [0053].

182. A POSITA would have expected success in implementing a monitoring unit, as Bittmann teaches, into SDD. Such a combination would have required only routine programming knowledge well within the skill of a POSITA before the Critical Date. Indeed, this would have amounted to nothing more than the use of a known technique to improve similar devices – in each instance a communication device configured to monitor device operation (e.g., SDD's call logging per DB, and Bittmann's monitoring) – in a similar way and combining prior art elements according to known methods to yield the predictable results

described above. SAMSUNG-1006, [0049], [0076], [0092], [0101]-[0102]; §IX.C. For example, both SDD and Bittmann's device monitor and report on device function. SAMSUNG-1006, [0049], [0076], [0092], [0101]-[0102]; §IX.C. A POSITA would have further known that such device monitoring was common as of the Critical Date. Therefore, the combination of the techniques of Bittmann in SDD would require only routine programming knowledge.

183. Finally, the elements of the resulting SDBD would each perform functions they had been known to perform prior to the combination—SDD installs a vSIM in a secure execution environment and uses the vSIM to connect to cellular networks (per Schmidt), including while roaming (per DB), and Bittmann's monitoring unit monitors and reports device activity. §IXA-C; §IX.D. Further, SDBD's monitoring unit transmits data using SDD's modem subsystem in the same manner Bittmann's monitoring unit transmits data over a modem. SAMSUNG-1007, [0052]-[0053], [0055], FIG. 3A; §IX.C. For at least these reasons, a POSITA would have naturally expected success when incorporating Bittmann's teachings into SDD, as described above.

F. Smith, *Virtual Machines: Versatile Platforms for Systems and Processes* ("Smith")

184. Smith is a book from 2005 that explains "[v]irtual machine (VM) technologies have been developed in a number of contexts" and "enable new

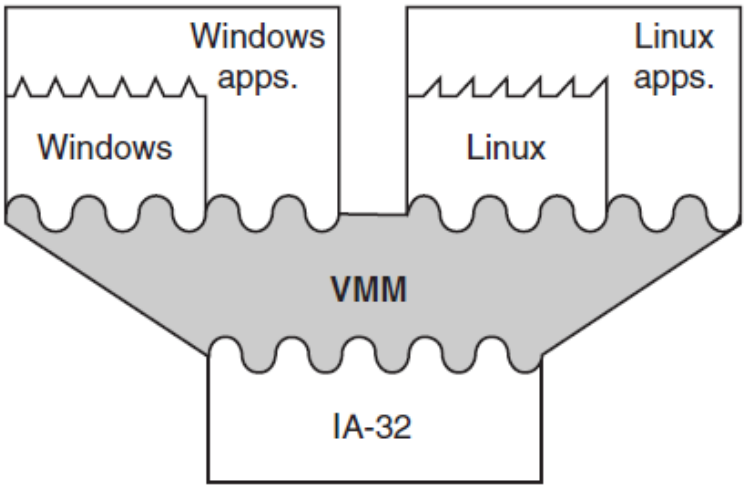
capabilities and to solve a variety of problems in interfacing major computer system components." SAMSUNG-1008, 8.

185. Smith describes various types of VMs, including a system VM, that "provide a complete system environment in which many processes, possibly belonging to multiple users, can coexist." SAMSUNG-1008, 25. Smith states that "[p]erhaps the most important feature of today's system VMs is that they provide a secure way of partitioning major software systems that run concurrently on the same hardware platform" such that "[s]oftware running on one guest system is isolated from software running on other guest systems."[11] SAMSUNG-1008, 26. Smith further explains that "[r]unning each application in its own virtual machine increases the robustness of the system," since erratic behavior "on a virtual machine" is "less likely to affect the operation of another application running on a different virtual machine." SAMSUNG-1008, 24.

186. In addition, Smith explains that VMs provide the "ability to support different operating systems simultaneously." SAMSUNG-1008, 26. Smith's FIG. 1.11 provides one example in which, on a single device, a Windows VM runs Windows applications and a Linux VM runs Linux applications. *Id*.

---

[11] Smith explains that "we usually refer to the underlying platform as the host and to the ***software that runs in the VM environment as the guest***." SAMSUNG-1008, 18.



SAMSUNG-1008, FIG. 1.11.

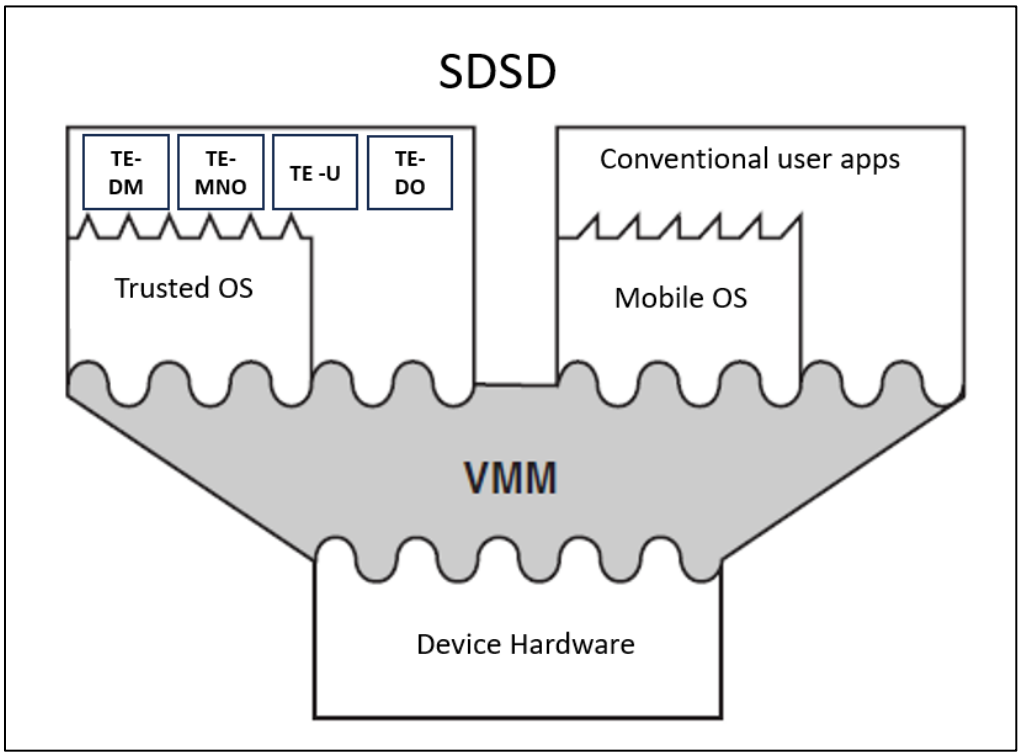
G. Schmidt-De Beer-Smith Combination

187. Per Schmidt, the "MTP operates a trusted operating system" (OS) that is loaded during "an initial startup process." SAMSUNG-1005, [0036], [0096]. A POSITA would understand or find obvious that mobile devices run user applications, e.g., e-mail, photo management, web browsing, etc., which would run in a conventional OS. SAMSUNG-1006, [0083]; SAMSUNG-1062, [0092] ("The device supports a variety of applications, such as one or more of the following: a telephone application, a video conferencing application, an e-mail application, an instant messaging application, a blogging application, a photo management application, a digital camera application, a digital video camera application, a web browsing application, a digital music player application, and/or a digital video player application."). However, while a POSITA would recognize that a mobile

device (e.g., SDD) includes a trusted OS (per Schmidt) and user applications, Schmidt does not provide implementation details describing how such apps would operate in parallel with and isolated from Schmidt's trusted OS and its TSSs.

188. A POSITA would have thus looked to references, such as Smith, that provide such implementation details and explain that VMs achieve such isolation of secure environments from generalized environments. For example, Smith explains that VMs provide the "ability to support different operating systems simultaneously," which is needed to run both Schmidt's TSSs and other applications on SDD. SAMSUNG-1008, 26. Further, as described above, Smith explains that "[p]erhaps the most important feature of today's system VMs is that they provide a secure way of partitioning major software systems that run concurrently on the same hardware platform" such that "[s]oftware running on one guest system is isolated from software running on other guest systems." SAMSUNG-1008, 26. Smith also explains that "[r]unning each application in its own virtual machine increases the robustness of the system," since erratic behavior "on a virtual machine" is "less likely to affect the operation of another application running on a different virtual machine." SAMSUNG-1008, 29. Thus, to increase the robustness of SDD, a POSITA would recognize that SDD's TSSs run in a VM that is separate from a VM running user apps.

189. The resulting Schmidt-DB-Smith device (SDSD) includes a Virtual Machine Monitor (VMM, per Smith),[12] that provides two VMs, one hosting a trusted OS and trusted engines (TSS-DM, TSS-MNO, etc.) (per Schmidt), and one hosting a second OS that runs conventional user applications, as illustrated below.



SAMSUNG-1008, FIG. 1.11(modified).[13]

[12] In System VMs, a VMM is the virtualizing software. SAMSUNG-1008, 17.

[13] SDSD further includes components such as TX/RX, multiple TM-SIGMAs, etc. These components are omitted from this figure for clarity.

190. The VMM provides an OS that is necessary to run conventional applications, per Smith, and since the MTP-related software runs in one VM apart from a second VM, erratic behavior of a conventional application is "less likely to affect the operation of" the MTP applications, which are "running on a different virtual machine," thereby improving device stability. SAMSUNG-1008, 29.

191. Schmidt also explains that the "system must also prevent loss and escape of security-sensitive data, and ensure that all necessary services are available and functional." SAMSUNG-1005, [0040]. Since Smith teaches that VMs isolate software running in a VM and "increase[] the robustness of the system," a POSITA would have been motivated to run Schmidt's MTP in a system VM, isolating the MTP, "prevent[ing] loss and escape of security-sensitive data and ensur[ing] that all necessary services are available and functional," even if other device applications, running outside the MTP malfunction. SAMSUNG-1005, [0040]; SAMSUNG-1008, 24, 26, 29.

192. A POSITA would have expected success in implementing an MTP in a VM. Such a combination would have required only routine programming knowledge well within the skill of a POSITA before the Critical Date. Indeed, this would have amounted to using a known technique (VMs) to improve operation of a known device (SDD). As taught by Smith, running software in a VM was well-

known long before the Critical Date. *See* SAMSUNG-1008, SAMSUNG-1012, *generally.*

193. Finally, the elements of the resulting SDSD each perform functions they performed prior to combination—Smith's environment provides VMs that isolate Schmidt's trusted OS from end-user applications, Schmidt's trusted OS downloads and manages the vSIM, and the device operates while roaming according to DB. A POSITA would have therefore expected success when combining Smith's teachings with SDD.

X. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '429 CLAIMS UNPATENTABLE

A. Ground 1A: Combination of Schmidt and De Beer Renders Obvious Claims 1-3 and 8-12

[1.1] A method of operating a wireless end-user device.

194. As explained below, SDD renders obvious a method of operating a wireless end-user device.

195. SDD is a wireless end-user device. Per Schmidt, SDD is a "wireless transmit/receive unit (WTRU)" that includes "a cellular telephone" and "any other type of user device capable of operating in a wireless environment." SAMSUNG-1005, [0023]. Similarly, DB teaches that a "mobile telephone (1) in a cellular telecommunications system uses" data stored in lookup tables (which would be stored in one or more secure memory partition—*see* §IX.C (providing a secure

partition) to "select a network (4) for registration and to perform optimise call routing to a call destination." SAMSUNG-1006, Abstract.

196. As explained in §IX.C, the methods of operating SDD include storing and updating the routing, preferred network and forbidden network tables in the device's secure memory partition. SAMSUNG-1005, [0030]; SAMSUNG-1006, [0038], [0066]-[0073], FIG. 4.

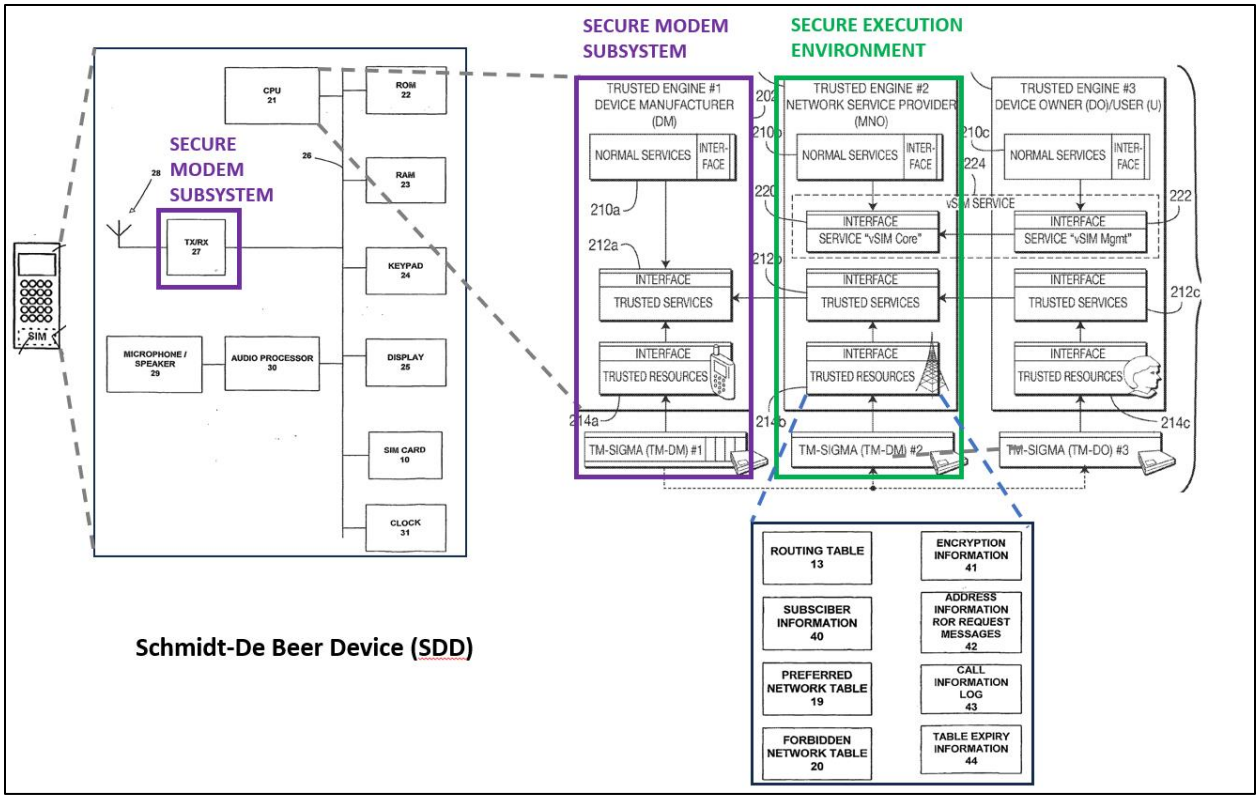
197. As explained in §IX.C (roaming), the methods further include using these tables to connect to appropriate networks and using services (e.g., making calls over these networks), e.g., using least cost routing as determined using the lookup tables (as explained in DB). SAMSUNG-1006, [0075]-[0077]. Additional details regarding the above-described methods for operating SDD are described with reference to [1.2]-[1.7] (incorporated here). *See also §VII.A.*

[1.2] connecting from a secure modem subsystem to a wireless cellular network;

198. As explained below, SDD's operation renders obvious connecting from a secure modem subsystem (e.g., the secure modem subsystem including SDD's radio frequency transceiver circuitry operating in conjunction with TSS-DM) to a wireless cellular network (e.g., local network, per DB). Specifically, a POSITA would recognize that devices with radio frequency transceivers would contain modems, as Jobs notes, "RF circuitry 108 may communicate with

networks, such as the Internet, also referred to as the World Wide Web (WWW), an intranet and/or a wireless network, such as a cellular telephone network, a wireless local area network (LAN) and/or a metropolitan area network (MAN), and other devices by wireless communication," which "may use any of a plurality of communications standards, protocols and technologies, including but not limited to Global System for Mobile Communications (GSM), …" SAMSUNG-1062, [0100]. Thus, radio frequency transceivers who communicate with cellular telephone networks through standards such as GSM (which Schmidt discloses: "While algorithms for the GSM standards A3 and A8 are shown below for purposes of example, similar techniques could be used with authentication algorithms of other wireless technologies as well." SAMSUNG-1005, [0095]) obviously contain modems to modulate digital signals into analog (radio) signals.

199. As explained in §IX.C (facilitating wireless communication, securing transmission), SDD includes a modem subsystem, which includes the TSS-DM and transceiver circuitry (e.g., TX-RX circuitry). Also, as explained in §IX.C (securing transmission), the TSS-DM together with the transceiver circuitry is a secure modem subsystem because TSS-DM secures the communication channels used for external communications from the MTP. SAMSUNG-1005, [0032].



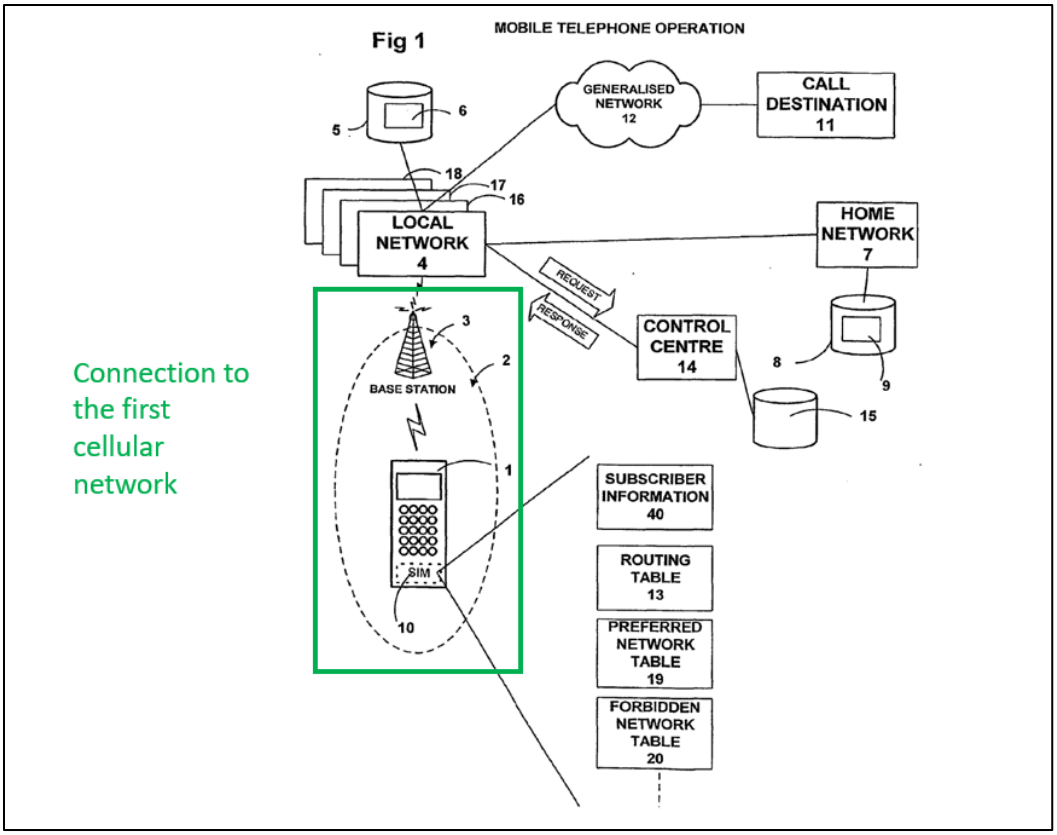
SAMSUNG-1005, FIG-2 (modified), SAMSUNG-1006, FIGS. 1-2 (modified).

200. SDD connects to the wireless cellular network from the secure modem subsystem. *See* §IX.C. Per Schmidt (and as described in [1.1]), SDD is a mobile device (e.g., a cellular telephone, PDA) which implements a "procedure for allowing access of a communication subscriber 802 to a ***cell based communication network***" (i.e., a wireless cellular network) "using the software based authorization credentials of the trusted mobile platform." SAMSUNG-1005, [0093], [0023]; *see* §IX.C. Additionally, per Schmidt, TSS-DM "generally controls all internal and external communications," and "all protocol messages of a TSS-sigma are

transmitted by the communications services of the TSS-DM 202 & 302 for the destination point thereof." SAMSUNG-1005, [0032].

201. Because TSS-DM controls ***all*** external communications of SDD, a POSITA would have understood that it also controls communications to a wireless cellular network (as further explained below). SAMSUNG-1005, [0032]. Further, because TSS-DM is part of SDD's secure modem subsystem, a POSITA would have understood that connections to the wireless cellular network are from SDD's secure modem subsystem. *See* §IX.C. Additionally, the wireless cellular network communications controlled by the TSS-DM would be transmitted or received by SDD's transceiver (e.g., the TX/RX circuitry). *See also §VII.C.*

202. Further, per Schmidt and DB, SDD connects from a secure modem subsystem to a wireless cellular network. SAMSUNG-1005, [0102]; SAMSUNG-1006, [0027], [0061]. This is illustrated in DB's following figure:



SAMSUNG-1006, FIG. 1 (annotated).

203. As DB explains, "the mobile telephone 1 is currently located within a cell 2 served by a base station 3 of a local network 4" such that "the term 'local' here being used in the context that the local network is ***accessible via cellular broadcast*** to the mobile telephone 1 in its current location." SAMSUNG-1006, [0027]. DB further explains that "[w]hen the mobile telephone 1 is turned on, it needs to register with the local network 4 so that subsequent calls can be rapidly set up by the local network." SAMSUNG-1006, [0035]. A POSITA would have understood that registering with the local network (which is a wireless cellular

network) is connecting to that network. De Beer further explains that "[d]uring the registration procedure, the mobile telephone 1 and local network 4 exchange identifying signals," which "allows the local network 4 to determine the identity of the subscribers [sic] home network 7 and home country." SAMSUNG-1006, [0061].

204. Thus, SDD leverages DB's and Schmidt's above-referenced teachings, such that during operation, SDD connects to a wireless cellular network (e.g., the local network that is accessible via cellular broadcast) from SDD's secure modem subsystem.

[1.3] connecting a first secure control channel from the secure modem subsystem through the wireless cellular network to a network service controller;

205. As explained below, SDD renders obvious connecting a first secure control channel (e.g., a channel over which an encrypted message is sent via SMS) from the secure modem subsystem (e.g., the TSS-DM operating in conjunction with the TX/RX) through the wireless cellular network (e.g., the local network) to a network service controller (e.g., the control centre).

206. The '429 Patent does not define the term "control channel" or for that matter, "channel." *See* SAMSUNG-1001. In the relevant field, a POSITA would have recognized that a "channel" is "a stream of information transmitted as part of a distinct communication, or conversation, or for a particular purpose or end use"

and "[o]ne channel may be distinguished from other channels by the time of occurrence of the transmission," among other factors. SAMSUNG-1022, 3. As I described in §VII.C, a POSITA would have further understood that a control channel is a channel over which control information is transmitted. For example, GSM defines "signaling channels" as "control channels," which "… offer a continuous, packet-oriented signaling service to [Mobile Stations] in order to enable them to send and receive messages at any time over the air interface to the [Base transceiver station]." SAMSUNG-1023, 12. Specifically, a POSITA would know that signaling information is control information as, "The control and management of cellular network demands a very high signaling effort." SAMSUNG-1023, 12.

207. Consistent with this understanding of channels and control channels, SDD renders obvious connecting a secure control channel through the wireless cellular network to a network service controller. SAMSUNG-1006, [0067].

208. As explained in §IX.C (roaming), SDD leverages DB's teachings of obtaining updated lookup tables including data regarding preferred and forbidden networks, and routing information—e.g., by requesting and receiving such information via an SMS message sent over a control channel. Per DB, after registering with the local network, SDD determines "from the MCC of the registered network whether there has been a change in the country code indicating

that the subscriber has moved to a location in a new country." SAMSUNG-1006, [0066]. If SDD determines "that the country code is new, then it is determined that a request message must be generated in order to obtain new versions of the routing table 13, preferred network table 19 and the forbidden network table 20," and a "request message is generated at step 72 and ***transmitted as an SMS (Short Message Service) message via the local network 4***" (i.e., wireless cellular network") ***and*** "***to the control centre*** 14" (i.e., network services controller). SAMSUNG-1006, [0067].

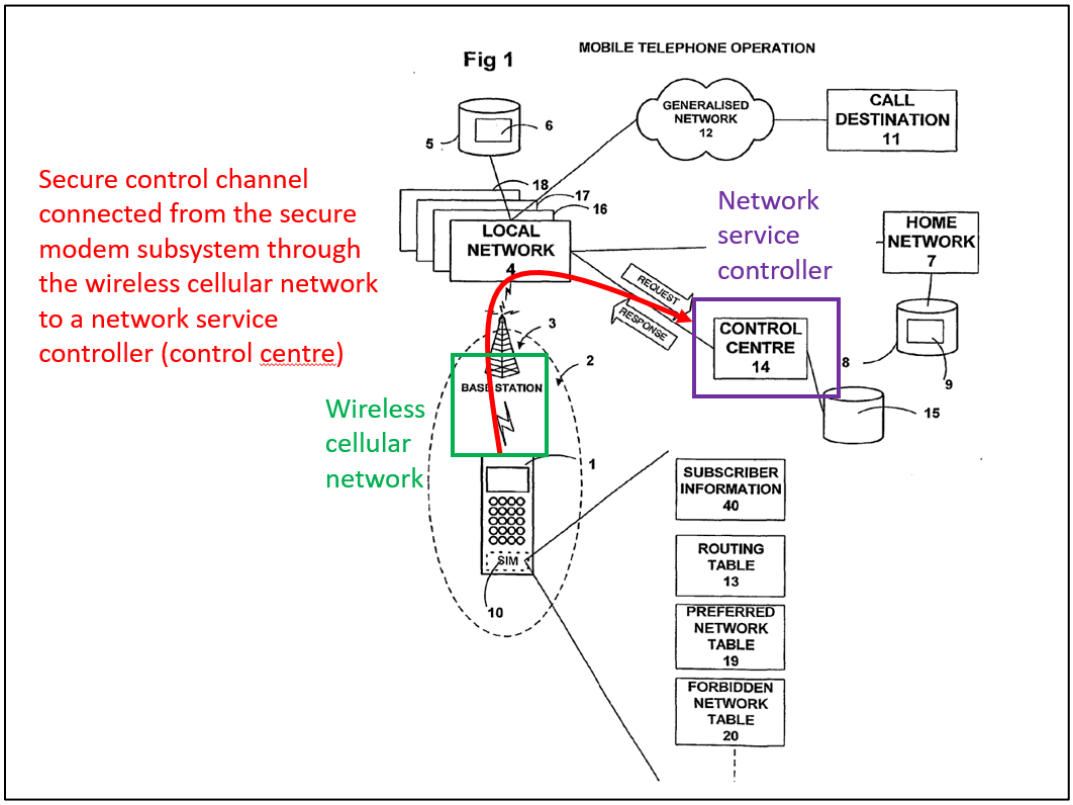
209. A POSITA would have understood that a network service controller controls network services, and because DB's control centre controls network services (e.g., by providing routing tables that are used to access a network and its services), it is a network service controller. For example, Bauer explains that "[m]any communication networks include a ***network service controller***," which "manages the communication network by establishing the dedicated communication links, performing diagnostics on switches and/or links within the network, and configuring the switches and/or links." SAMSUNG-1033, 1:23-30. Additionally, the '429 patent explains that "service control policies, for example, can be set by the service controller," which is a function that is performed by SDD's control centre. SAMSUNG-1001, 14:56-58. Moreover, since DB's control centre controls network services (e.g., by providing routing tables that are

used to access a network and its services), it is a network service controller. SAMSUNG-1033, 1:23-30.

210. The SMS messages to the control centre include control information and are distinct from data messages that are sent via SMS and displayed to the user. For example, per DB, such "SMS messages" sent and received by the device "[are] transparent to the user of the mobile telephone 1" and constitute "a special type of SMS message … which [is not] displayed in the display 25 of the mobile telephone." SAMSUNG-1006, [0080]. These messages include requests for information or the actual information (e.g., routing table 13, preferred network table 19 and the forbidden network table 20), which control how the device accesses a network and therefore constitute control information. Thus, these special SMS messages include control information that are used to control the device, and it follows that the channel over which they are sent would be a control channel.

211. Further still, a POSITA would have understood or found obvious that the above-described special SMS message would be transmitted over a control channel. In the relevant timeframe, it was well-known for such SMS messages to be sent over control channels. For example, Minborg explains that "[i]n the GSM standard, ***SMS messages can be transmitted over a Stand-alone Dedicated Control Channel*** (SDCCH)." SAMSUNG-1020, [0005]. Weiser, as another

example, similarly explains that "***SDCCH sub-channels*** can be used to carry control, ***SMS*** and Wireless Applications Protocol (WAP) traffic." SAMSUNG-1021, [0306].



SAMSUNG-1006, FIG. 1 (annotated).

212. It would have therefore been obvious to utilize such well-known control channels to facilitate delivery of control information included in the special SMS message and this would have been nothing more than implementing known methods/techniques (use of a dedicated control channel, as taught in references like Minborg and Weiser) to known systems/devices (e.g., mobile devices of the type taught in Schmidt and/or DB) to achieve predictable results (transmission of

control information in the special SMS message, as contemplated by DB). Another reason motivating the use of a dedicated control channel for delivery and receipt of the above-described control information is to reduce traffic on data channels -- channels are for delivery of data communications. A POSITA would have had a reasonable expectation of success in implementing a dedicated channel for delivery of the special SMS message given (1) common use of control channels for delivery of control information and (2) well-known dedicated control channels that are regularly used in cellular network communications for transmission of the type of SMS messages (as DB teaches).

213. SDD further renders obvious that the control channel includes a connection from the secure modem subsystem to the control centre (i.e., a network service controller) and is secure. For example, per Schmidt, TSS-DM (which is part of SDD's secure modem subsystem) "controls all internal and external communications and ***secures the communications channel***." SAMSUNG-1005, [0032]. A POSITA would have understood that "s*ecuring a communications channel*" means making a channel secure between two endpoints, where 'secure' means providing confidentiality and integrity of the communications (through cryptography). For example, as Merkle teaches, "[s]ecure communications takes place between two indiviudals when they communicate privately in spite of efforts by a third person to learn what is being communicated. … The general method

uses this key as a parameter, and will perform a particular transformation on messages for a particular key. Because Z does not know this key, he cannot perform the particular transformation, and thus cannot encrypt or decrypt messages." SAMSUNG-1058, 2. In other words, the above-described control channel, includes a communication channel from the secure modem subsystem through the local network (i.e., the wireless cellular network) and to the control centre (i.e., the network services controller) and is secured.

214. Note that, as described in [1.4], SDD's control channels further include a connection from the SDD's SEE to the secure modem subsystem. Thus, data for the first and second control channels pass from the SEE (including TSS-MNO) via the secure modem subsystem (including TSS-DM), to the network service controller. In other words, each of the first and second control channels includes an internal connection from the TSS-MNO to the TSS-DM and an external connection from TSS-DM (and via the modem's transceiver circuitry) to the control centre—which together form the respective control channels (as further described with reference to [1.4] below). As I explain in further detail below (in reference to [1.4]), it was common in networked systems for communication between certain on-device applications and external components to traverse intermediate components, e.g., the modem. Thus, in view of the above, it would

have been obvious for the above-described first secure control channel to provide a connection from the secure modem subsystem to a network service controller.

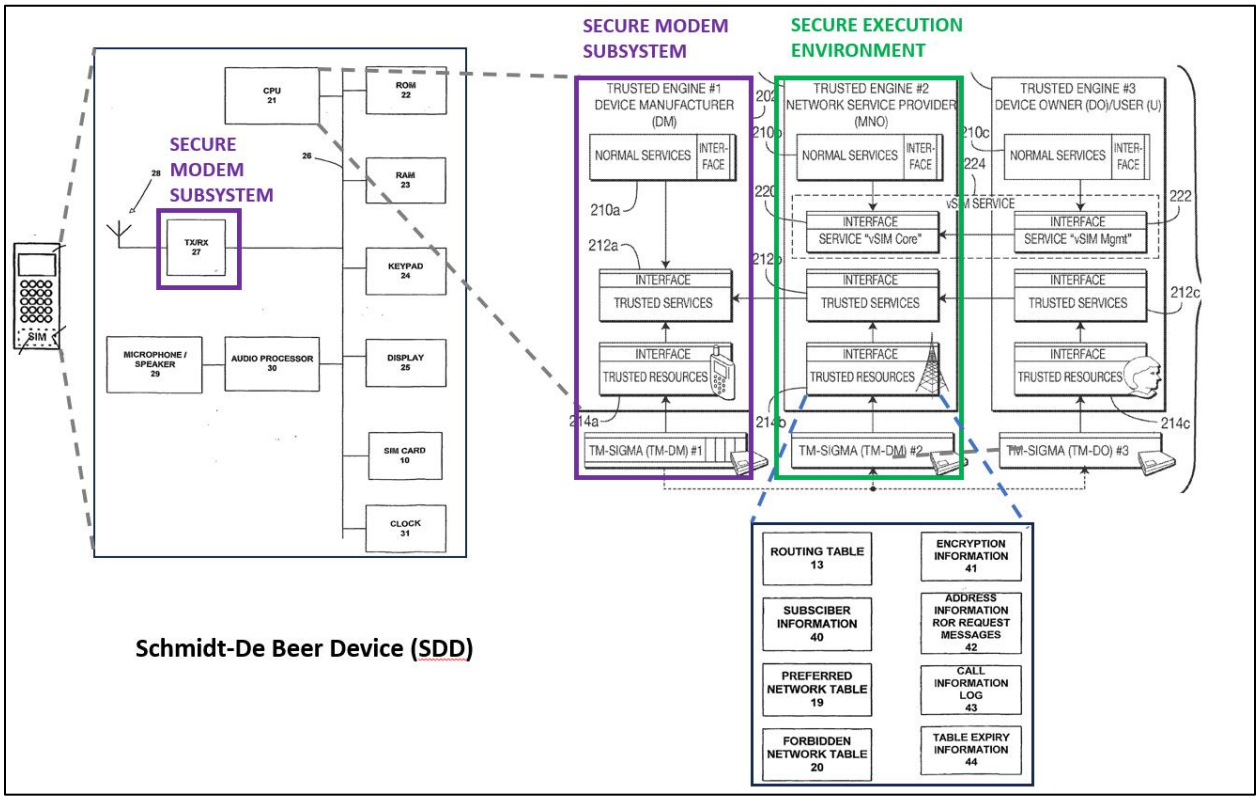
[1.4] connecting a second secure control channel from a secure execution environment, separately secure from the secure modem subsystem, through the secure modem subsystem and the wireless cellular network to the network service controller;

215. As explained below, SDD renders obvious connecting a second secure control channel (e.g., a channel established at a later time, such as the next day, over which an encrypted message is sent via SMS) from a secure execution environment (e.g., TSS-MNO), separately secure from the secure modem subsystem, through the secure modem subsystem (e.g., TSS-DM operating in conjunction with the TX/RX) and the wireless cellular network (e.g., the local network) to the network service controller (e.g., control centre).

216. In SDD, a mobile trusted platform includes multiple trusted subsystems (TSSs), including TSS-MNO, a secure execution environment. Per Schmidt, each TSS includes a "***trusted execution environment*** (TE-sigma) and the non-exchangeable security module (trusted module, TM)." SAMSUNG-1005, [0031]. Each TSS is also "configured to sign and ***encrypt any given data***" and "has access to a trusted service RTV-sigma," which "is responsible for verification, for example of defined system states based on reference data." *Id.*

217. Additionally, TSS-MNO is a trusted subsystem/execution environment that "is responsible for managing and protecting the subscriber-

related portion of the vSIM credential, and performs the client-side network authentication of a subscriber." SAMSUNG-1005, [0033].



SAMSUNG-1005, FIG-2 (modified), SAMSUNG-1006, FIGS. 1-2 (modified).

218. SDD connects a second secure control channel to the network services controller. As explained in §IX.C (roaming) and in [1.3] above, SDD leverages DB's teachings of obtaining updated lookup tables from the control centre. Per DB, if a device lacks a soft reset facility, "the application must rely upon initiating re-registration ***when the user next turns off and on the power to the apparatus***." SAMSUNG-1006, [0065]. Therefore, a POSITA would have recognized that when a user reboots the phone (in the same location), the registration process

repeats—thus resulting in the connection of a second channel. Specifically, a POSITA would have understood that, after a sufficient passage of time, the first control channel would be destroyed, conserving systems resources. For example, to keep a TCP connection alive, the connected computers can send keep-alive packets "when no data or acknowledgement packets have been received for the connection within an interval." SAMSUNG-1064, 101. Sending and receiving such packets consumes resource, which is wasteful for a connection that is otherwise dormant. Therefore, the second channel differs temporally from the first, and thus, "[o]ne channel may be distinguished from other channels by the ***time of occurrence*** of the transmission," among other factors. SAMSUNG-1022, 3. *See also* §VII.C.

219. During registration, SDD "determine[s] … whether the routing table 13 is still valid by comparing current date and time information provided by clock 31 with an expiry date field included in the routing table" (the latter specifying the expiration or maximum usable life of the data in the routing table). SAMSUNG-1006, [0050], [0072]. If "it is determined that the routing table has expired, or at least that relevant parts of the routing table relating to the registered network have expired and are no longer valid, a ***request message is generated at step 79 for an update of the routing table 13***." SAMSUNG-1006, [0072].

220. The "request message is transmitted as an SMS message to the control centre 14 which responds by retrieving data from its database 15 and transmitting a response message in SMS format" that includes the updated routing table 13. SAMSUNG-1006, [0072]-[0073].

221. As explained above with reference to element [1.3] (incorporated here), a POSITA would have understood or found obvious that the SMS message from SDD includes control information and would be sent over a control channel (e.g., a dedicated channel such as a SDCCH).

222. The claim does not specify that the "first control channel" is distinct from the "second control channel." Nevertheless, even if the claim was interpreted as such, a POSITA would have recognized or found obvious that the control channel used for transmission of the above-described control information would be a separate channel from the first control channel, described above for element [1.3].

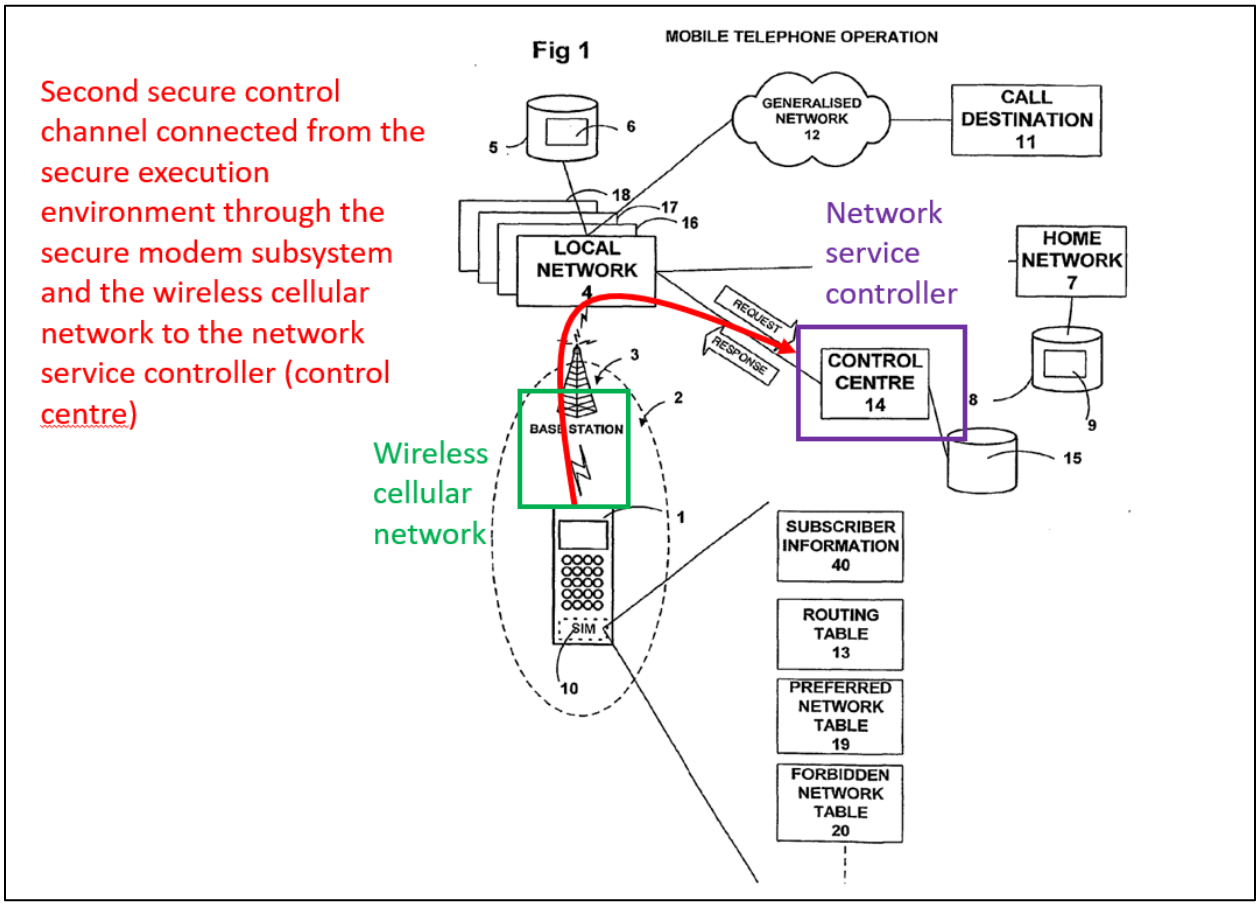
223. As an initial matter, the second control channel is at least temporally distinct (e.g., existing on a different day) from the first control channel. For example, as described above, to conserve resources, a "channel" was understood to be "a stream of information transmitted as part of a distinct communication, or conversation, or for a particular purpose or end use" and "[o]ne channel may be

distinguished from other channels ***by the time of occurrence of the transmission***," among other factors. SAMSUNG-1022, 3.

224. Additionally, a POSITA would recognize that GSM does indeed support temporal channel differentiation through Time Division Multiple Access (TDMA) communication techniques: "Thus the sequence of time slots assigned to a mobile station represents the physical channels of a TDMA system. In each time slot, the mobile station transmits a data burst. The period assigned to a time slot for a mobile station thus also determines the number of TDMA channels on a carrier frequency." SAMSUNG-1022, 3.

225. Additionally, or alternatively, a POSITA would have recognized or found obvious that this control channel would be physically or logically distinct from the "first control channel" identified with reference to element [1.3]. As explained for element [1.3], a dedicated control channel (e.g., SDCCH) may be used for sending and receiving the above-described information. Such dedicated channels are released and/or torn down after their use, such that, at a later time a new dedicated channel—with updated channel properties—is connected. SAMSUNG-1022, 3. Therefore, a POSITA would have understood or found obvious that, when SDD is powered off (e.g., overnight) and subsequently restarted in the same location, SDD will connect through the same local network (wireless

cellular network) via a second secure control channel to the control centre (network service controller) to obtain an updated routing table.



SAMSUNG-1006, FIG. 1 (annotated).

226. Additionally, SDD connects the above-described second secure control channel to the network services controller from the secure execution environment. In particular, SDD's registration process includes a connection from TSS-MNO because, per Schmidt, "[a]ll subscription-dependent and subscriber-related network provider services of a platform are allocated to the TSS-MNO." SAMSUNG-1005, [0033]. A POSITA would have recognized that the above-

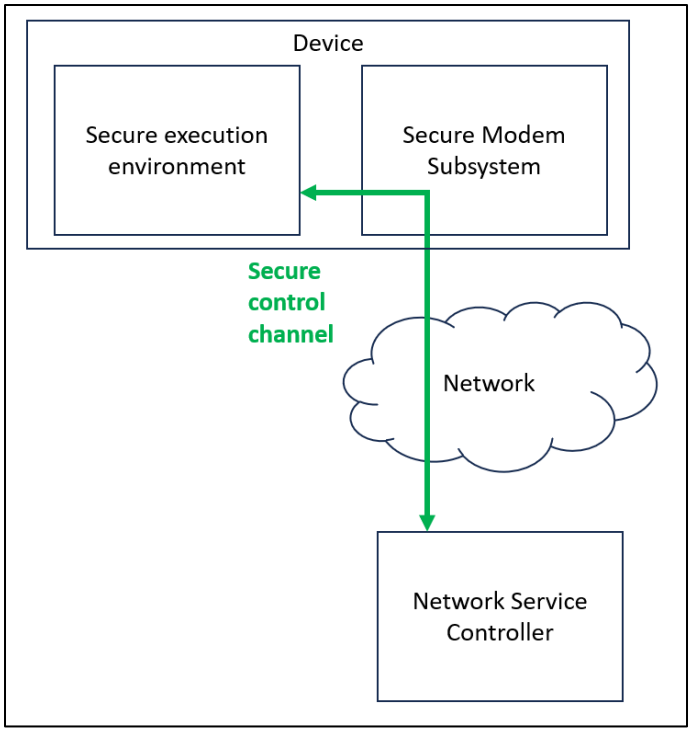
described registration process while the device is roaming—per DB—is both subscription-dependent and subscriber-related. SAMSUNG-1005, [0033]. A POSITA would have understood that the owner of the device ("DO," per Schmidt) purchases a service plan from a provider (therefore making it subscriber-dependent) and the service plan defines the capabilities and costs of the service plan (therefore making it subscription dependent). For example, Jobs explains that "[u]sers of portable communication devices (e.g., mobile telephones, handhelds, media players, personal digital assistants (PDAs), BlackBerry™, pocket PCs, Smart Phones, etc.) typically enter into service contracts with service providers for voice and/or data services," and "[s]ervice plans can provide data services, voice services or a combination of voice and data services often referred to as 'bundled' services." SAMSUNG-1038, [0002]. Therefore, in the context of SDD's architecture, the connection of the second control channel would be from from SDD's secure execution environment (TSS-MNO)[14] via the secure modem subsystem (since its TSS-DM component "controls all internal and external

[14] As described above, the secure execution environment includes TSS-MNO and that associated TM-SIGMA. For brevity, in places throughout this document, I list only the TSS-MNO component of the secure execution environment.

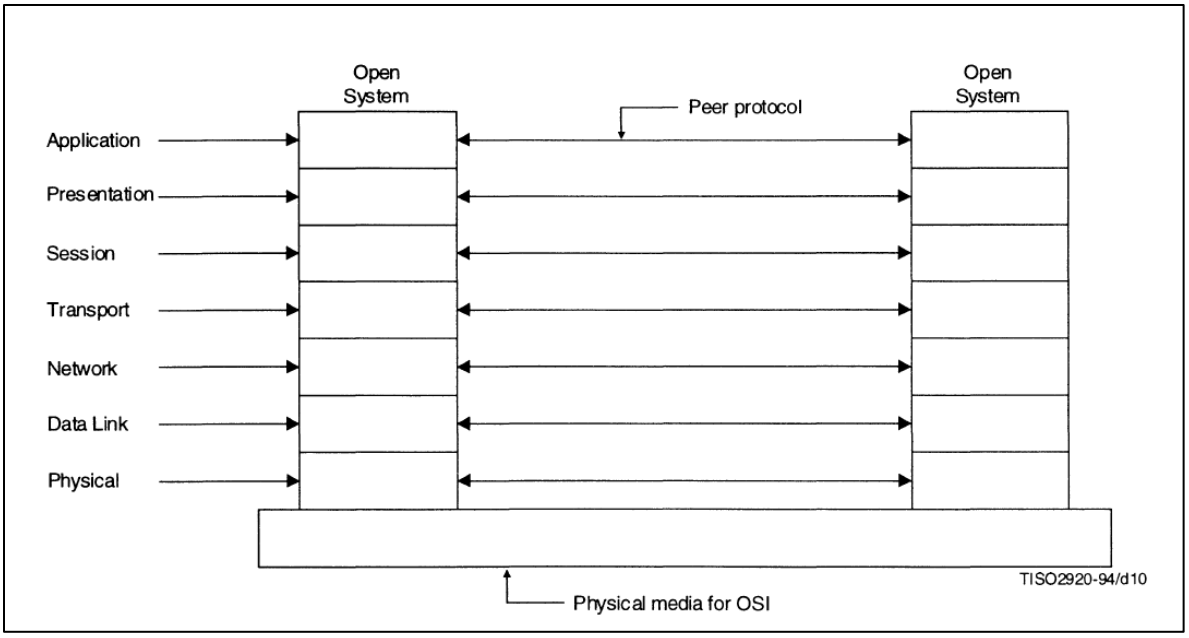
communications"), to the network service controller (control centre). SAMSUNG-1005, [0032].

227. Note that while element [1.3] describes the first secure control channel as being "from the secure modem subsystem through the wireless cellular network to a network service controller" and element [1.4] describes the second secure control channel as being from "a secure execution environment ... through the secure modem subsystem and the wireless cellular network to the network service controller," a POSITA would have understood that these limitations can describe a configuration in which all control channels run from the secure execution environment, through the secure modem subsystem to the network service controller.

228. For example, in my illustration below, a POSITA would have understood that the control channel (green arrow) connects the device to the network service controller, connects the secure execution environment to the network service controller and connects the secure modem subsystem to the network service controller.



229. In fact, it was (and is) common in networking for channels to span multiple components. Consider, for example, the OSI model (illustrated below), which includes 7 layers ranging from the Application layer down to the Physical layer. SAMSUNG-1068, 34. In such cases, a POSITA would have understood that there is a channel from the application layer at one system to the application layer of the other system, a channel from the presentation layer at one system to the presentation layer of the other system, ..., and from the physical layer at one system to the physical layer at the other. Additionally, since data within a system flows "down" the layers, there is a connection from the application layer at one system, through the presentation layers (and all lower layers at the system) to the other system, then up through the layers at the other system.



SAMSUNG-1068, Figure 11.

230. The OSI document further explains that "[n]ot all open systems provide the initial source or final destination of data. When the physical media for OSI do not link all open systems directly, some open systems act only as relay open systems, passing data to other open systems," as illustrated below. SAMSUNG-1068, 34. In such cases, a POSITA would have recognized that there are connections (at each layer) between the two open systems, and (at the relevant layers) from each individual open system and the relay open system.

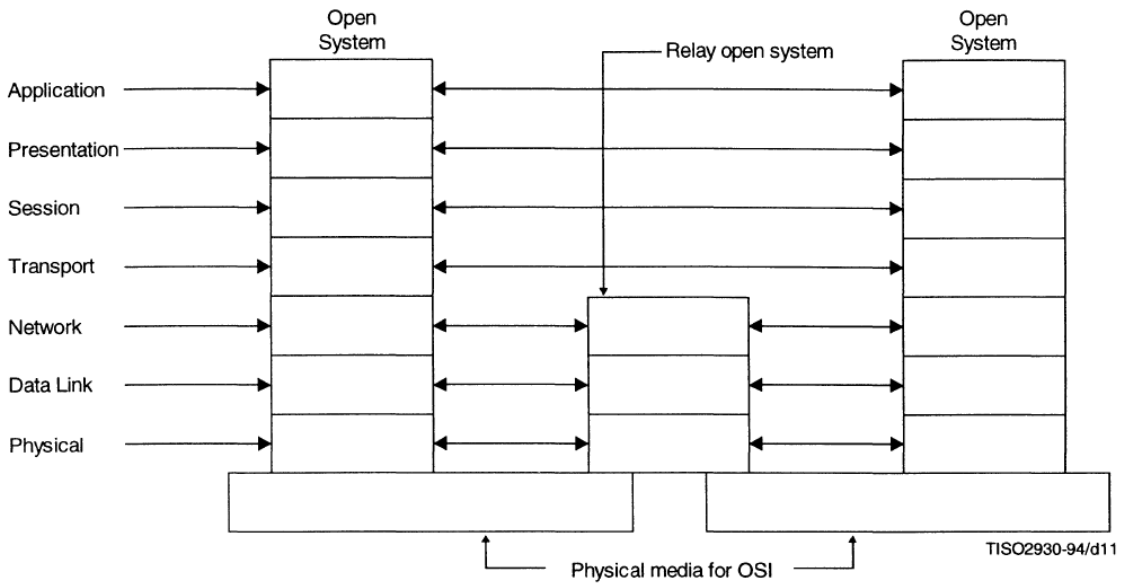


Figure 12 – Communication involving relay open systems

SAMSUNG-1068, Figure 12.

231. For at least these reasons, a POSITA would have understood that it was conventional in networking for connections among numerous components (both hardware and software components) to exist, even when describing the same end-to-end connection, e.g., presentation layer to presentation layer in the OSI model or secure execution environment (via the secure modem subsystem) to the network service controller.

232. As with the first secure control described above with reference to element [1.3] above, this second control channel is also secure because (1) per Schmidt, TSS-MNO encrypts communications it sends and (2) TSS-DM (which is

part of the secure modem subsystem) "controls all internal and external communications"—such as the communication channel including the second control channel—and "***secures [this] communications channel***." SAMSUNG-1005, [0032].

233. Finally, SDD's secure execution environment (TSS-MNO) is separately secure from the secure modem subsystem (including SDD's transceiver circuitry operating in conjunction with TSS-DM). For example, per Schmidt, the device includes "three ***separate*** trusted sub systems" and "multiple protected***,*** ***separate*** execution environments." SAMSUNG-1005, [0028], [0030]. Therefore, SDD's secure execution environment (TSS-MNO) is separate from the secure modem subsystem (which includes TSS-DM). Further, they are separately secure because each trusted subsystem "is always configured to sign and encrypt any given data." SAMSUNG-1005, [0031].

[1.5] receiving at the secure execution environment, via the second secure control channel, one or more messages from the network service controller, the one or more messages comprising one or more service policy settings.

234. As explained below, SDD renders obvious receiving at the secure execution environment (e.g., TSS-MNO), via the second secure control channel, one or more messages comprising one or more service policy settings (e.g., a response message including routing table updates) from the network service controller (e.g., control centre).

235. As described in [1.4], when the routing table has expired, SDD transmits a "request message … as an SMS message to the control centre 14," which "responds by retrieving data from its database 15 and transmitting a response message in SMS format." SAMSUNG-1006, [0072]. The response message includes an updated routing table, and SDD's routing table is updated with the received data. SAMSUNG-1006, [0073].

236. A POSITA would have recognized or found obvious that the request and response messages, which are both SMS messages, would use the same control channel. As described above, while it is resource inefficient to maintain a dormant channel over long periods, it is also inefficient to tear-down and reconnect a channel for each use of the channel. For example, establishing a TCP connection requires a "three-way handshake" and handling numerous potential error conditions. SAMSUNG-1065, 31-37. Therefore, in cases where a request and response are sent in quick succession, it is resource efficient to use the same channel for both the request and response messages.

237. The "routing information" includes service policy settings such as "routing table 13, preferred network table 19 and forbidden network table 20." SAMSUNG-1006, [0055]. As I describe further in the sections on claims 8 and 9, a POSITA would have understood that the routing table, preferred network table and forbidden network table are policy settings because they constrain the device's

use of the network. For example, Stone explains that "[a] simple view of policy in regard to networks is that policy constrains communications." SAMSUNG-1036, 1. Put differently, a "policy" is a set of rules or parameters that must be complied with for a system or user to use a network. For example, as Jude describes, "[i]n practice, [policy-based network management] manifests itself as a set of rules that define the relationships among: a set of network conditions[;] [p]otential responses to those conditions[;] [and] [t]he devices that will implement those responses." SAMSUNG-1057, 2. Routing tables and network tables are policies by definition, as they define rules to enforce network behaviors to optimize performance, security, or both. Specifically, routing tables define where information must be sent for one device to send (i.e., "route") information to another device. As Malhotra discusses, "[s]imilarily, a routing table must contain at least two pieces of information: the destination network and the next hop toward that destination." SAMSUNG-1056, 2. As a routing table is a collection of rules that a device must follow to send information across the network, it is therefore a policy setting. Preferred/forbidden network tables, as the names imply, define the networks that mobile devices should and should not connect to (for example, a device may contain networks on its forbidden list that are for specific countries when roaming). SAMSUNG-1006, [0036]. Clearly, such network tables are a collection of rules and therefore are policy settings. *See also* §VII.B,

238. Further, since the routing information, preferred network table and forbidden network table are subscription and subscriber dependent, and since a POSITA would have understood that "[a]ll subscription-dependent and subscriber-related network provider services of a platform are allocated to the TSS-MNO," a POSITA would have understood or found obvious that the policy setting are received by TSS-MNO, and therefore by the SEE (of which TSS-MNO is a component). SAMSUNG-1005, [0033].

[1.6] storing the one or more service policy settings in a secure memory partition accessible only from the secure execution environment, and

239. As explained below, SDD renders obvious storing the one or more service policy settings (e.g., updated routing table entries received from the control centre) in a secure memory partition accessible only from the secure execution environment (e.g., TSS-MNO).

240. As explained in §IX.C (secure partition, roaming), SDD includes a secure memory partition in its on-device memory and stores therein lookup tables including routing information (which are policy settings, as explained in [1.5] and §VII.B). *See* SAMSUNG-1006, [0046], [0067], FIG. 4. As described above, secure memory partitions were well-known as of the Critical Data. For example, the ARM TrustZone Protection Controller "provides a software interface to the protection bits in a secure system in a Trustzone design" which "provides system

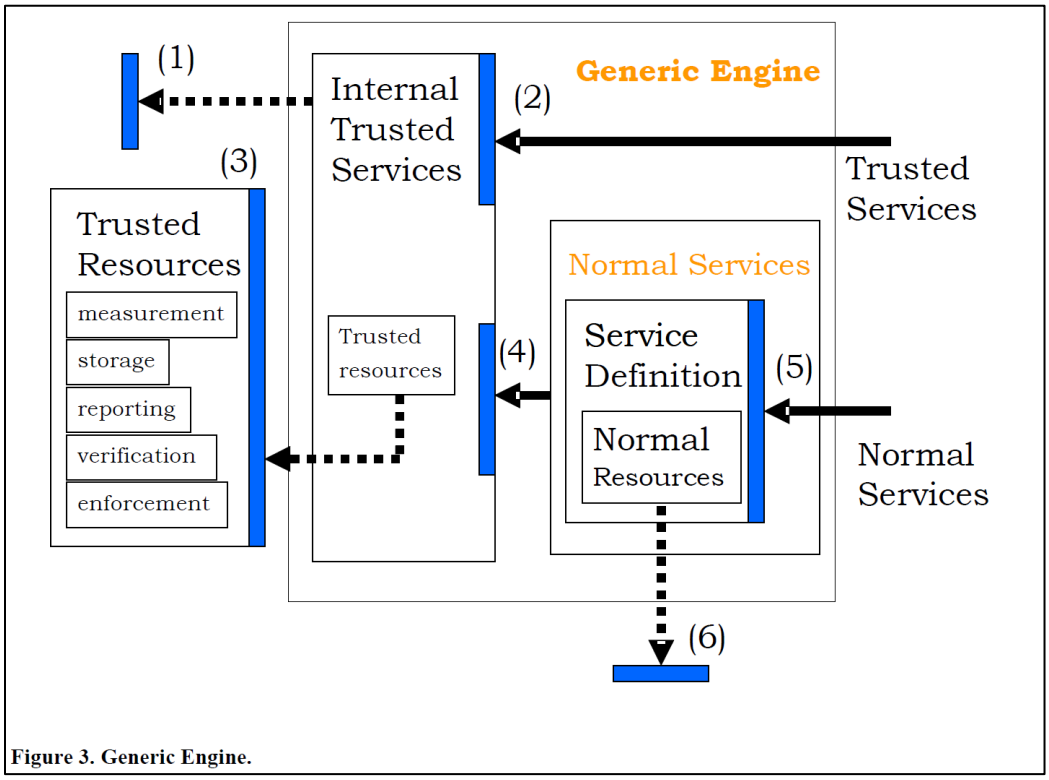
flexibility to enable you to configure different areas of memory as secure or non-secure." SAMSUNG-1059, 3.

241. Additionally, per DB and as explained in §IX.C (secure partition, roaming), when SDD receives the updated routing information (i.e., the one or more service policy setting), it stores/updates this information in the secure memory partition. Per DB, when the mobile terminal requests updated routing tables (*see* analysis for [1.4] *supra*), "[t]he control centre 14 responds by retrieving up-to-date tables from its database" and transmits them in "a response message via the local network 4 to the mobile telephone 1" where the existing "***tables 13, 19 and 20 are updated with the received data***." SAMSUNG-1006, [0046], [0067], FIG. 4. Because SDD includes a secure memory partition where this information is stored (*see* §IX.C (secure partition)), a POSITA would have understood or found obvious that the lookup tables (including the routing information) stored in this secure memory partition, are updated and stored therein using the updated information received from the control centre.

242. Further, SDD's policy settings (e.g., routing table, preferred network table and forbidden network table) stored in a secure memory partition are accessible only from the secure execution environment (TSS-MNO). As Schmidt explains, "TSS-MNO includes a vSIM core services unit, configured to ***store***, provide and process credential information relating to the MNO" and this vSIM

core "perform[s] the SIM functions related to the MNO." SAMSUNG-1005, [0005], [0029]. TSS-MNO further "is responsible for managing and ***protecting the subscriber-related portion of the vSIM credential.***" SAMSUNG-1005, [0033].

243. Additionally, Schmidt discloses that each TSS, including TSS-MNO, has its own dedicated set of trusted resources—which a POSITA would have understood or found obvious as including trusted/secure storage. For example, the Trusted Computed Group Mobile Reference architecture includes a "reference engine" with trusted resources, including storage. SAMSUNG-1030, 28.

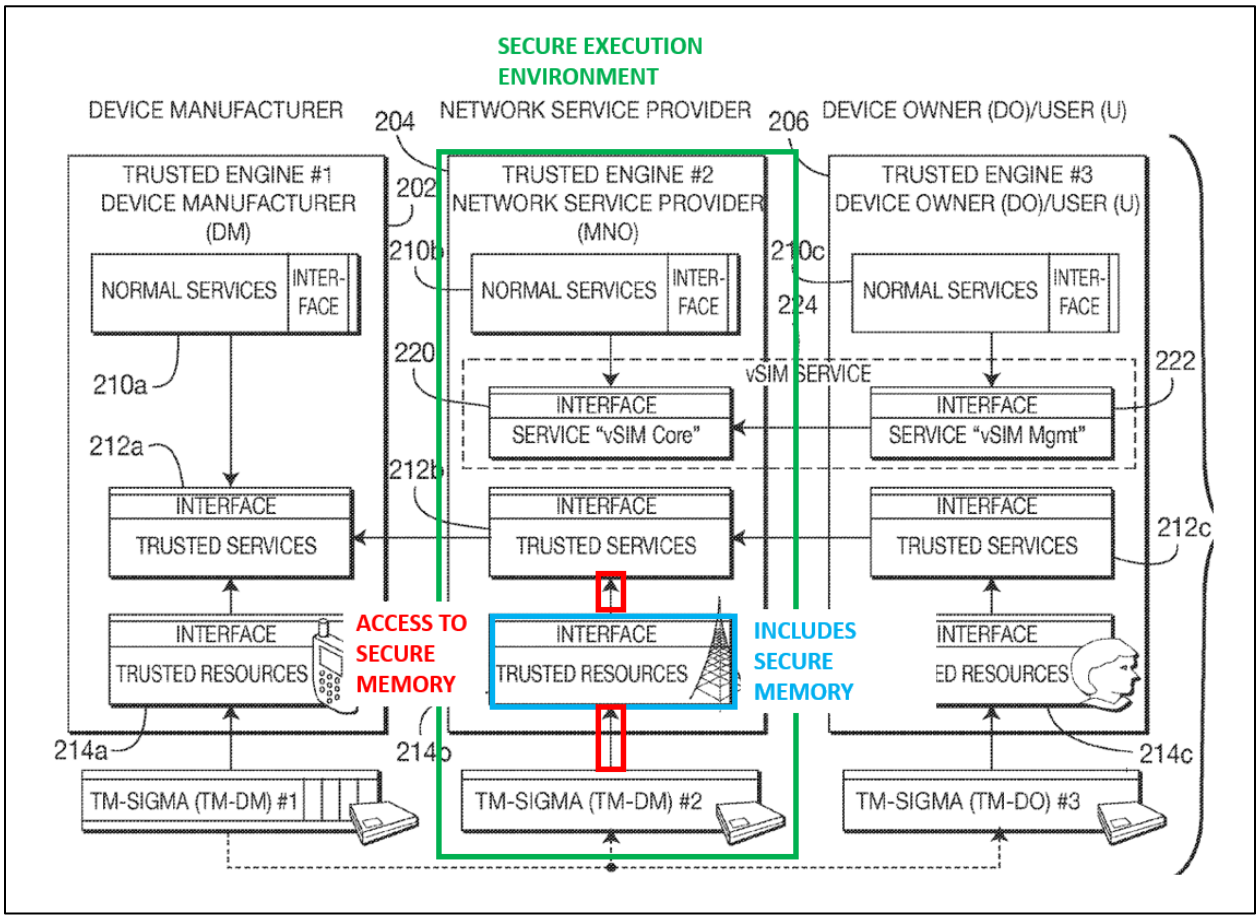


SAMSUNG-1030, Figure 3.

244. Thus, a POSITA would have understood that trusted resources in the context of a trusted subsystem includes a protected storage in the form of dedicated storage, such as a secure memory partition corresponding to the trusted subsystem. SAMSUNG-1030, 28.

245. The trusted resources (including trusted storage) of TSS-MNO are accessible only from TSS-MNO (secure execution environment). For example, Schmidt's FIG. 2 demonstrates that the TSS-MNO's trusted resources (which include secure memory) are available only through the "interface" to the "trusted resources" within TSS-MNO, accessible by "trusted services" and the "trusted entity of the security module." SAMSUNG-1005, FIG. 2, [0028], [0037]. These interfaces are an emergent property of the design of secure execution environments in that data that crosses over a "trust boundary" (i.e., data originating from untrusted services) should be scrutinized for correctness and authenticity, while data that is within the trust boundary can be, by definition, assumed to be non-adversarial (i.e., trusted) services. As Gasser teaches, "In any effort to plan for security features, it is crucial to establish a clear understanding of the *system boundary* and define the threats (originating outside the boundary) against which the system must defend itself" and "[t]he security-relevant components implement the internal controls. Separating the two types of components is an imaginary boundary called the *security perimeter*." SAMSUNG-1055, 1-3. Additionally,

given that Schmidt explains that each TSS is separate and isolated from other TSSs, a POSITA would have understood or found obvious that the trusted resources of a particular TSS, such as TSS-MNO, would not be accessible by any other TSS or other system component.



SAMSUNG-1005, FIG. 2 (annotated).

[1.7] enforcing, at least in part from the secure execution environment, a network service profile comprising the one or more service policy settings, to control the wireless end-user device use of a service on the wireless cellular network.

246. As explained below, SDD renders obvious enforcing, at least in part from the secure execution environment (e.g., TSS-MNO), a network service profile (e.g., data files, per DB) comprising the one or more service policy settings (e.g., routing table, preferred network table and forbidden network table, per DB), to control the wireless end-user device use of a service on the wireless cellular network (e.g., voice and/or data use on the local network and generalized networks, per DB).

247. The '429 specification does not define the term "network service profile" and thus, this term should be accorded its plain and ordinary meaning. In the relevant timeframe, a POSITA would have understood that a network service profile is a collection of information that is used to control the "interactions between the mobile telephone and the current network." SAMSUNG-1037, Abstract. Consistent with this understanding, the policy settings stored in SDD's secure memory (e.g., routing table, preferred network table and forbidden network table, as explained in §IX.C (secure partition) and in [1.5]-[1.6]) would be understood as a network service profile because they represent a collection of information that is used to control the interactions between the mobile telephone and the current network (e.g., access to the network and manner in which a call is

routed to a destination over the network). SAMSUNG-1006, [0033]-[0034], [0036].

248. Additionally, and consistent with an example embodiment described in the '429 specification, a POSITA would have recognized or found obvious that the policy settings stored in SDD's secure memory (e.g., routing table, preferred network table and forbidden network table, as explained in §IX.C (secure partition) and in [1.5]-[1.6]) are policy settings and therefore are included in, or associated with, a network service profile. SAMSUNG-1006, [0046], FIG. 4. For example, the abstract of the '429 patents teaches that a network service profile includes service policy settings that are associated with a service plan that provides access to the service on the wireless network. SAMSUNG-1001, Abstract.

249. For example, DB explains that the routing table is used to choose a call route with minimum cost, such that call routing and cost for completing a call provide access to a service (e.g., voice calling) on a service plan (with associated cost for use of such a service, e.g., voice calling or data services). SAMSUNG-1006, Abstract, [0034], [0097]-[0098]; *see* analysis for [2] (explaining that network service profile including its policy settings are associated with a service plan). *See also* §VII.B.

250. Additionally, DB explains that the forbidden network table "lists those networks for which the subscriber does ***not have authorisation*** from the home

network 7 to complete registration." SAMSUNG-1006, [0036]. A POSITA would have recognized that such authorization to access (or not access) a network is also related to the service plan because a service plan enables access to a network and to services on the network. For example, Jobs explains that:

> *"Service plans can provide data services, voice services or a combination of voice and data services often referred to as 'bundled' services. The service plans typically allocate limited amounts of minutes, bandwidth or storage based on the price of the plan." SAMSUNG-1038, [0002].*

251. Similarly, DB explains that, in "selecting a network for registration purposes, the mobile telephone 1 refers to a preferred network table 19 which lists networks in order of preference." SAMSUNG-1006, [0036]. DB further explains that "the list of available networks is compared with the preferred network table 19 which has entries for a number of mobile network codes in order of preference," and "[i]f one or more of the MNCs in the available network list is found in the preferred network table 19, the preferred network is identified and at step 63 ***the preferred network is selected for registration***." SAMSUNG-1006, [0058].

252. As explained below, SDD's secure execution environment (TSS-MNO) enforces, at least in part, the network service profile to control the device's use of a service on the wireless cellular network. For example, per DB, SDD

would enforce call routing to a call destination using at least the updated routing table (policy setting included in the network service profile), thereby controlling the use of a voice calling service on the wireless cellular network. For example, DB states that "the connection path to the call destination 11 [is] determined in accordance with a preferred route." SAMSUNG-1006, [0032]. DB further explains that when the device initiates a call, "[t]he connection path utilized" for the call "generally presents a number of available options depending for example on the interconnect facilities available to the local network," and the "mobile telephone 1 has ***a call routing facility*** which allows routing information to be accessed" and "added to a user defined call number." SAMSUNG-1006, [0032]-[0033]. In this manner, "a setup procedure initiated via the local network 4 results in the connection path to the call destination 11 being ***determined in accordance with a preferred route***." SAMSUNG-1006, [0032].

253. Additionally, per DB, the "preferred network table 19 [] lists networks in order of preference" and the forbidden network table lists "those networks for which the subscriber does not have authorisation from the home network 7 to complete registration." SAMSUNG-1006, [0036]. As explained above, the preferred network table is enforced by the device, which determines "[i]f one or more of the MNCs in the available network list is found in the preferred network table 19, the preferred network is identified and at step 63 ***the preferred network is***

selected for registration." SAMSUNG-1006, [0058]. The forbidden network table is enforced at the device which compares "each network in the list [of available networks] with the forbidden network table 20 and any networks which are excluded are removed from the list of available networks." SAMSUNG-1006, [0057].

254. Further, DB explains that when "the country code is new, then it is determined that a request message must be generated in order to obtain new versions of the routing table 13, preferred network table 19 and the forbidden network table 20." SAMSUNG-1006, [0067]. Then the "local network [the wireless cellular network] with which the mobile telephone is now registered is then compared at step 74 with the updated preferred network table 19 and forbidden network table 20," and if "it is determined that another one of the available networks has a higher level of preference in the list, a process of re-registration is initiated at step 75 in order to replace the currently registered network with the preferred network which then becomes the 'local network' referred to above." SAMSUNG-1006, [0068]. DB further explains that "it may be determined at step 74 that the currently registered network is listed in the forbidden network table 20, in which case step 75 similarly follows to force re-registration." SAMSUNG-1006, [0069]. Thus, SDD enforces service policies to control SDD use of the local network, by dropping access to the local network

(therefore disallowing access to the service over the local network) if the local network is forbidden or not preferred.

255. Therefore, because SDD leverages the above teachings in DB, the routing information, preferred network table and forbidden network table are used by SDD to enforce policies used to control the wireless end-user device use of a network service (e.g., telephony, data), e.g., by selecting a least-cost route, using a preferred network and/or avoiding forbidden networks. Thus, SDD enforces service policies to control SDD use of the local network ["the wireless cellular network"], e.g., by determining routing over the network.

256. In DB, routing is performed by the SIM processor. SAMSUNG-1006, [0052]-[0053]. Since SDD has no physical SIM, and therefore no separate SIM processor (processor 31 in DB's FIG. 3), such processes are performed by SDD's trusted services. SAMSUNG-1006, [0043], FIG. 3.

257. As I explained in [1.5], the routing information, preferred network table and forbidden network table are subscription and subscriber dependent. Therefore, a POSITA would have understood or found obvious that SDD's enforcement is performed, at least in part, by TSS-MNO, and therefore by the SEE (of which TSS-MNO is a component). SAMSUNG-1005, [0033]. Indeed, such an implementation, which would be straightforward to implement (in view of DB's disclosures) and amounts to implementing of known techniques to a known system

to achieve predictable—would ensure the security benefits provided by a SIM processor are maintained in the context of the SDD system where the trusted services, including those of TSS-MNO, providing the same security benefits.

258. In summary, Schmidt teaches that the secure execution environment (TSS-MNO) is responsible for "managing and protecting" the vSIM data (including the network service profile) and "performs the SIM functions related to the MNO." SAMSUNG-1005, [0033]. In view of Schmidt and De Beer, a POSITA would have thus understood or found obvious that the TSS-MNO (i.e., a component of the secure execution environment) would access this stored information (since only TSS-MNO has access to the data) from its dedicated memory partition and would be the entity responsible, at least in part, for the above-described enforcement of the network constraints defined by the data in the stored lookup tables to enable, e.g., network access and least cost call routing.

[2] The method of claim 1, wherein the network service profile is associated with a service plan that provides for access to the service on the wireless cellular network.

259. SDD renders obvious that the network service profile (as described in [1.7]) is associated with a service plan that provides for access to the service on the wireless cellular network.

260. The '429 specification does not define a "service plan." SAMSUNG-1001, *generally*. However, a POSITA would understand that a service plan "can

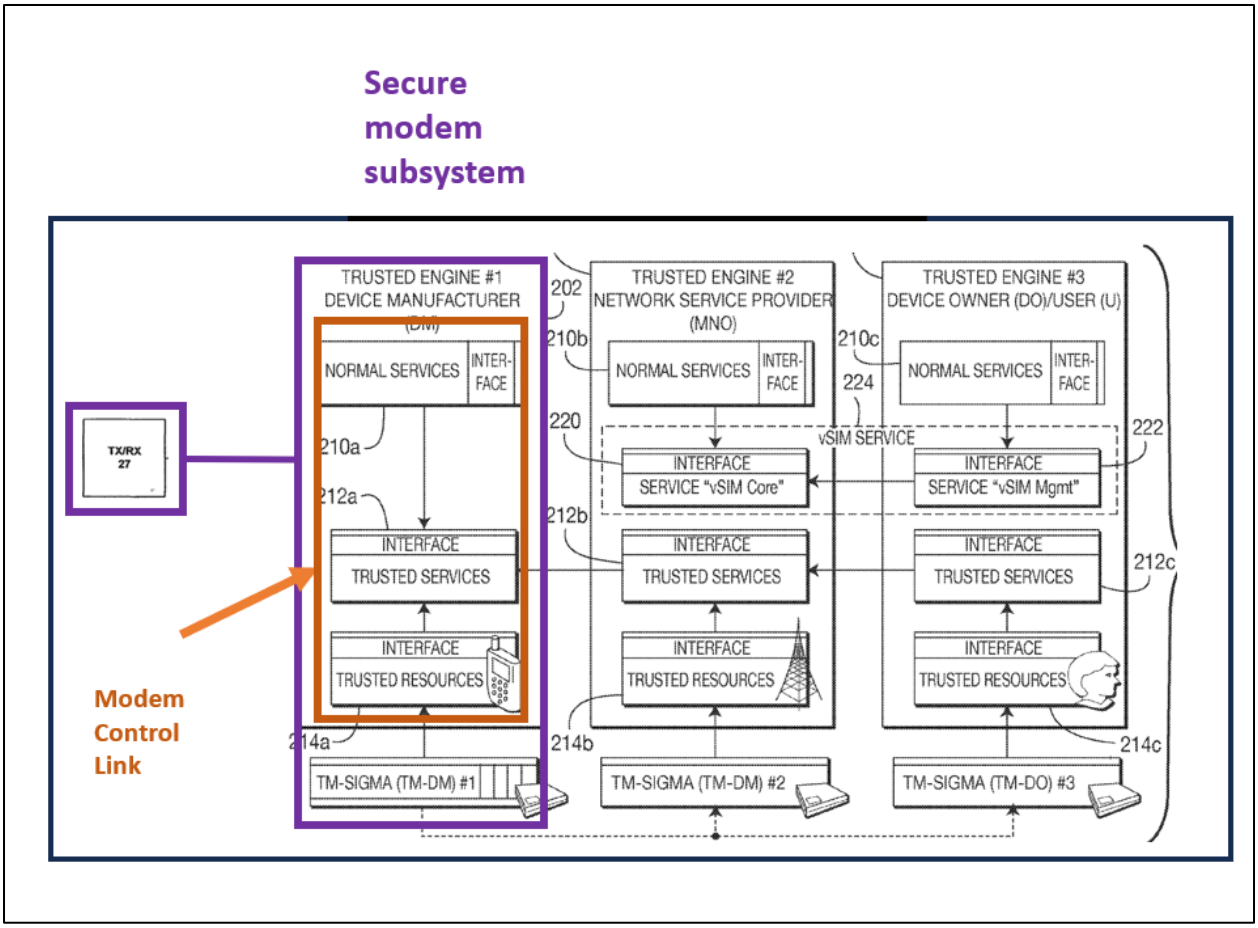
provide data services, voice services or a combination of voice and data services often referred to as 'bundled' services," and defines pricing for these services, e.g., as explained by Jobs. SAMSUNG-1038, [0002],

261. Consistent with this understanding of service plan, and in view of DB's teachings, SDD's device would subscribe to a service plan that provides access to services (e.g., voice and data services) for certain defined pricing and uses stored policy settings to facilitate access to such services. As DB teaches, a "home network 7 is operated by a home service provider with whom a subscriber using the mobile telephone 1 has in this example ***a contractual relationship***." SAMSUNG-1006, [0030]. DB further explains that the routing table is used to choose a call route with minimum cost, such that call routing and cost for completing a call provide access to a service (e.g., voice calling) on a service plan (with associated cost for use of such a service). SAMSUNG-1006, Abstract, [0034], [0097]-[0098]. Additionally, DB explains that the forbidden network table "lists those networks for which the subscriber ***does not have authorisation*** from the home network 7 to complete registration." SAMSUNG-1006, [0036]. A POSITA would have recognized that such authorization to access (or not access a network) is also related to the service plan because such authorization is related to network access.

262. Moreover, as explained in [1.7], SDD's device includes a network service profile that includes policy settings. Because the device would subscribe to a service plan and use the same policy settings to control access to services (as described in [1.7]) included in the service plan, a POSITA would have understood that the network service profile (which includes one or more policy settings) in SDD is associated with a service plan that provides for access to services (e.g., voice calling, data services) on the wireless cellular network. *See* analysis for [1.7].

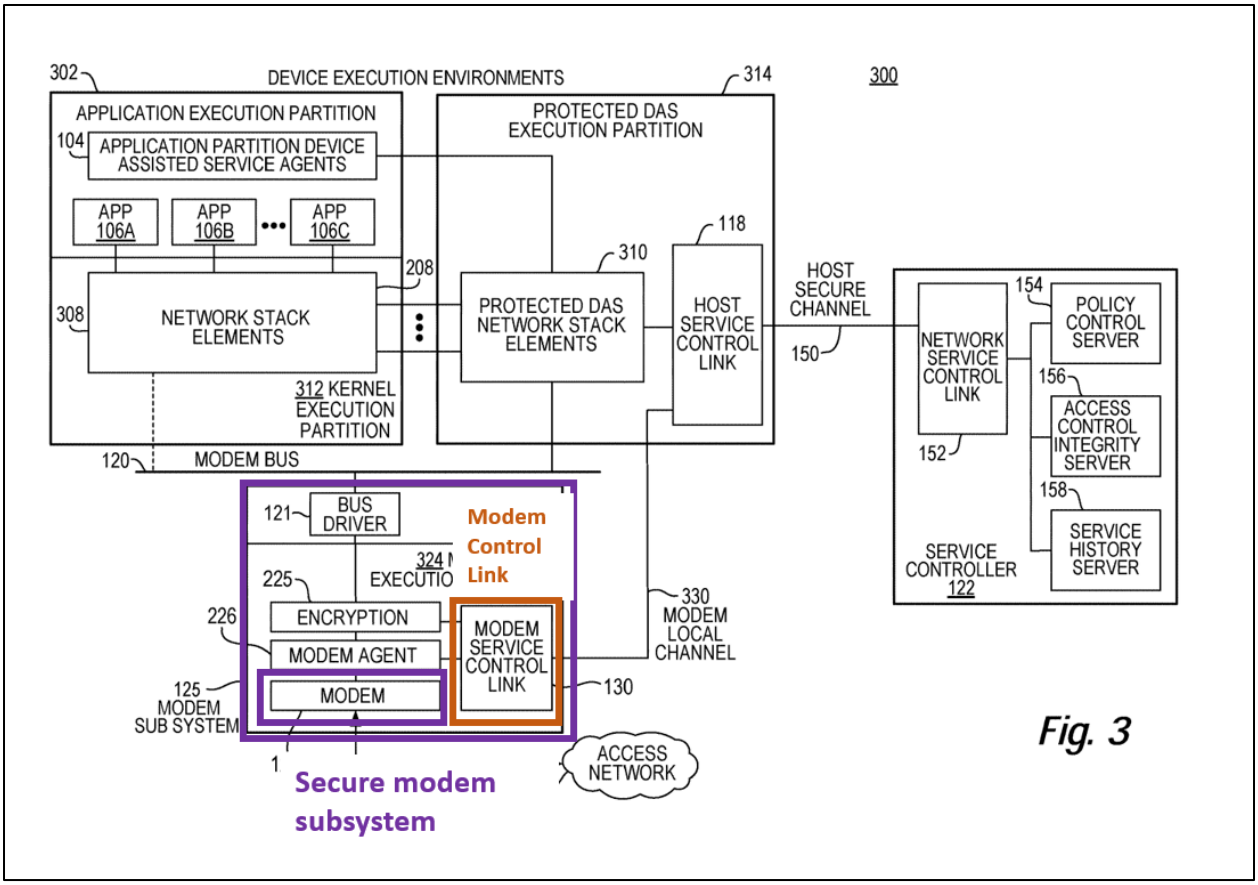
[3.1] The method of claim 1, wherein the secure modem subsystem comprises a modem control link and a modem local channel, and the first secure control channel connects the modem control link to the network service controller through the modem local channel, and

263. In SDD, as illustrated below, the secure modem subsystem comprises a modem control link, coupled to the physical modem (TX/RX) in the secure modem subsystem. SAMSUNG-1005, [0032]; SAMSUNG-1006, [0042].



SAMSUNG-1005, FIG. 2 (excerpts, annotated); SAMSUNG-1006, FIG. 2 (excerpts, annotated).

264. This structure is analogous to the '429 Patent's embodiment of FIG. 3 embodiment (reproduced below) in the '429 patent in which the modem control link ("modem service control link") and the physical modem ("modem") are components of the modem subsystem. SAMSUNG-1001, 10:29-48.

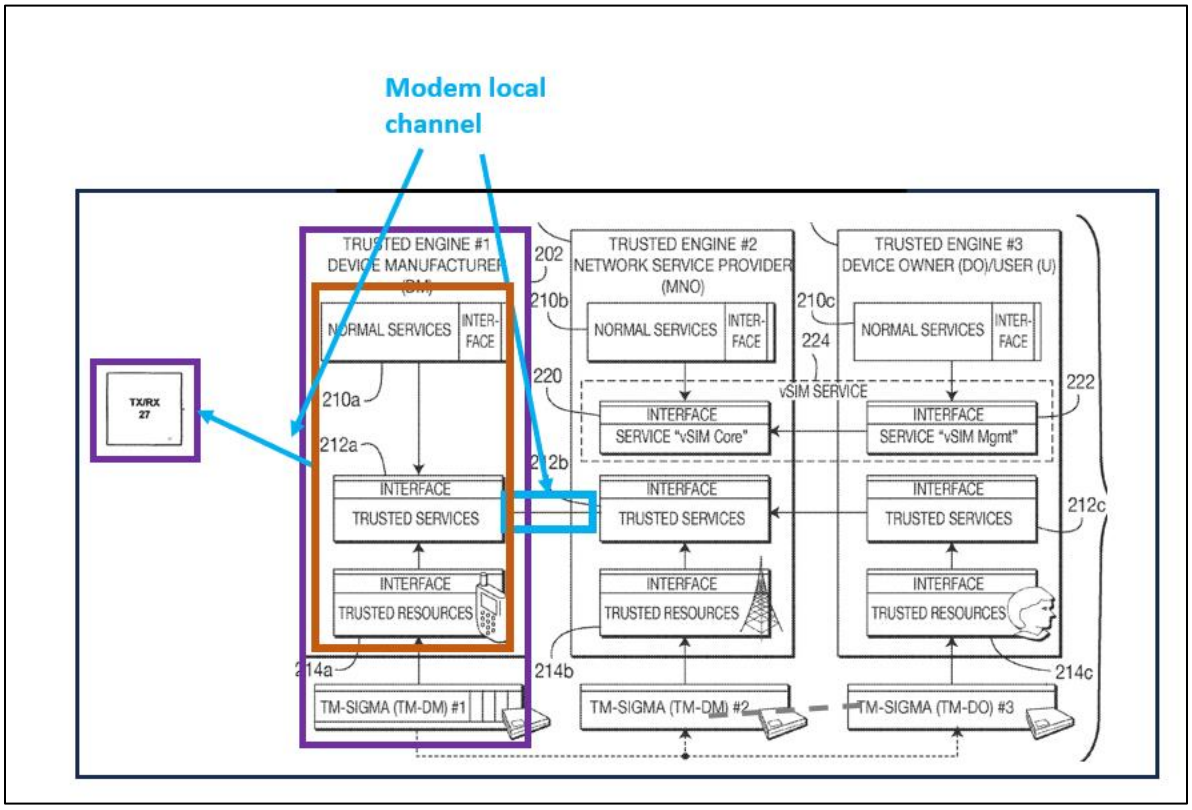


SAMSUNG-1001, FIG. 3 (annotated).

265. As shown below, SDD's secure modem subsystem further comprises a modem local channel that couples the modem control link to TSS-MNO and TX/RX – that is, components that are ***local*** to the device. Including local interfaces to a component was (and is) a conventional design technique.

266. A POSITA would have understood that the modem subsystem includes this modem local channel since TSS-DM "controls all internal and external communications and secures the communications channel," and therefore interchanges data both with TSS-MNO, which is allocated "[a]ll subscription-

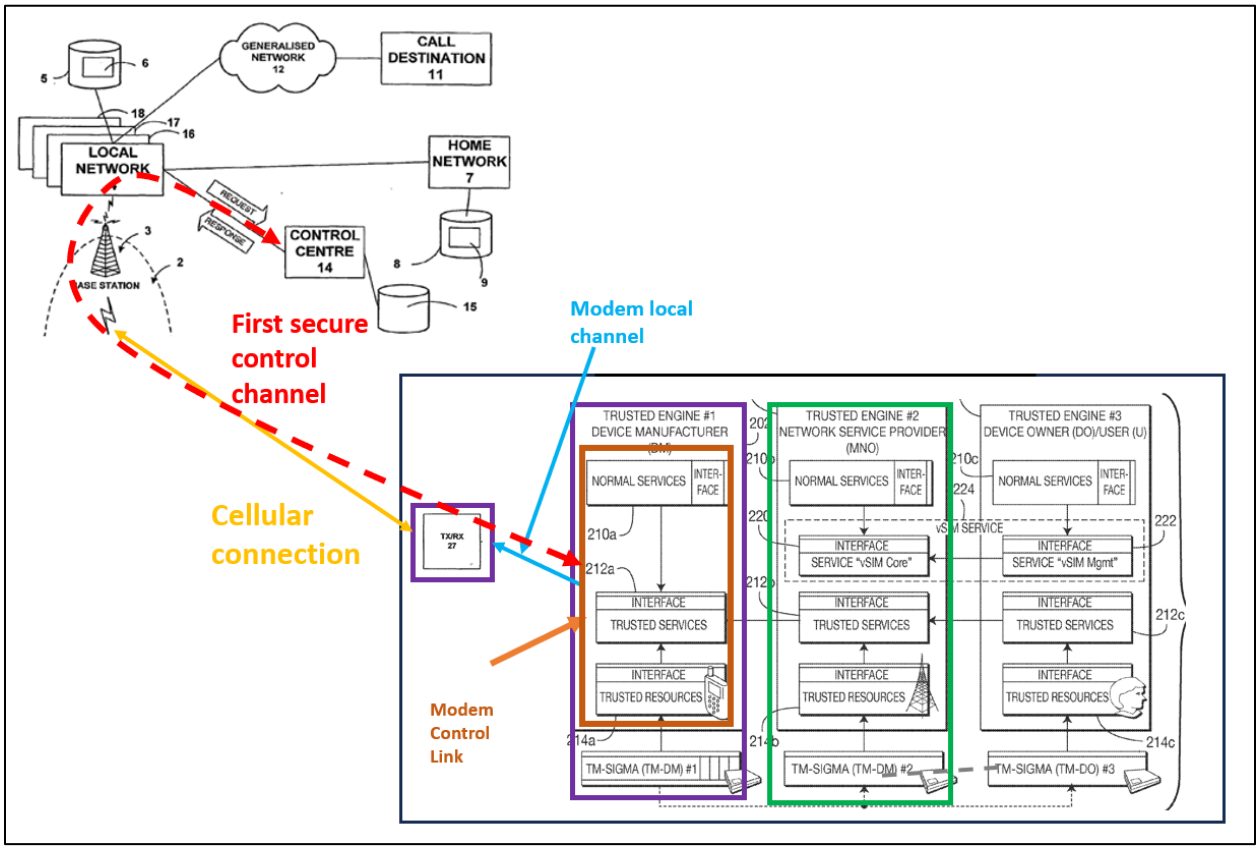
dependent and subscriber-related network provider services," and the TX/RX, the physical hardware used to send/receive cellular data. SAMSUNG-1005, [0032]-[0033]; SAMSUNG-1006, [0042].



SAMSUNG-1005, FIG. 2 (excerpts, annotated); SAMSUNG-1006, FIG. 2 (excerpts, annotated)

267. Additionally, the first secure control channel connects the modem control link to the network service controller through the modem local channel. *See* SAMSUNG-1001, FIG. 3 and associated description (describing similar functionality). As described in [1.3]-[1.6], the control channels facilitate transmission of policy settings (and requests for the same) between the secure

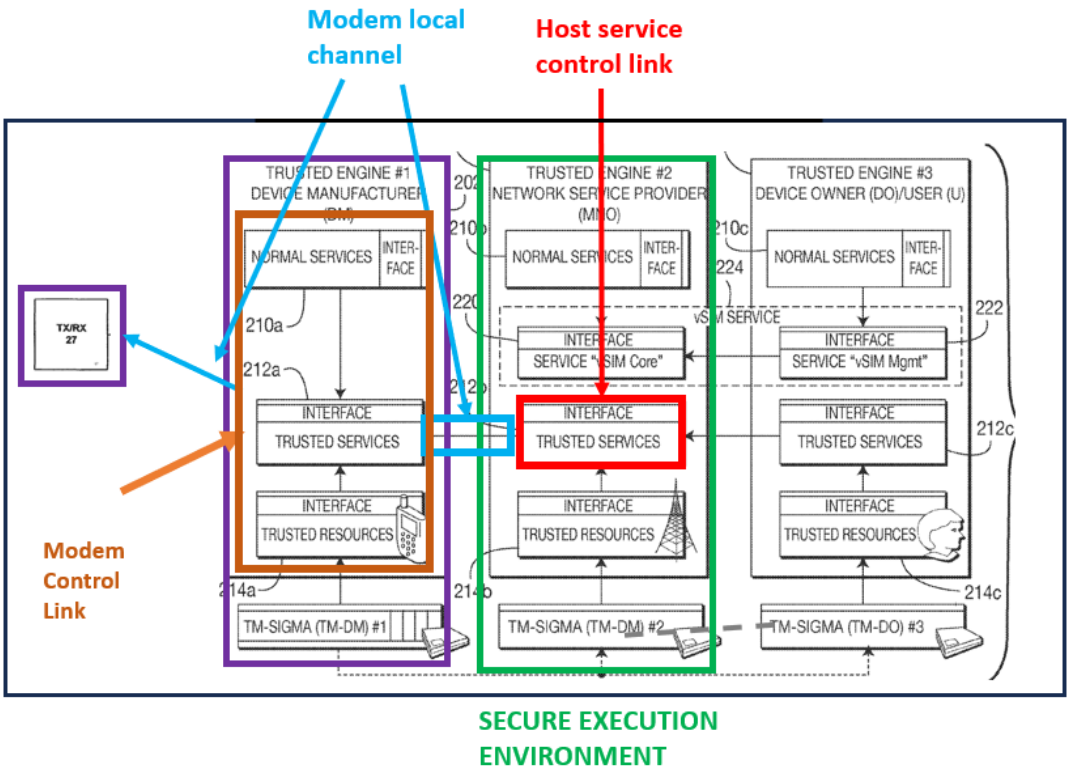
modem subsystem (which includes the transceiver circuitry and TSS-DM) and the network service controller (control centre). It follows then that this control channel connects the modem control link (in TSS-DM, which controls all communication of SDD) to/from the network service controller (i.e., control centre) and such a connection would be via the modem local channel that connects the modem control link to the transceiver (TX/RX) circuitry, as described above. SAMSUNG-1005, [0032]; SAMSUNG-1006, [0042]. *See also* §VII.C,



SAMSUNG-1005, FIGS. 2 (excerpts, annotated); SAMSUNG-1006, FIGS. 1, 2 (excerpts, annotated).

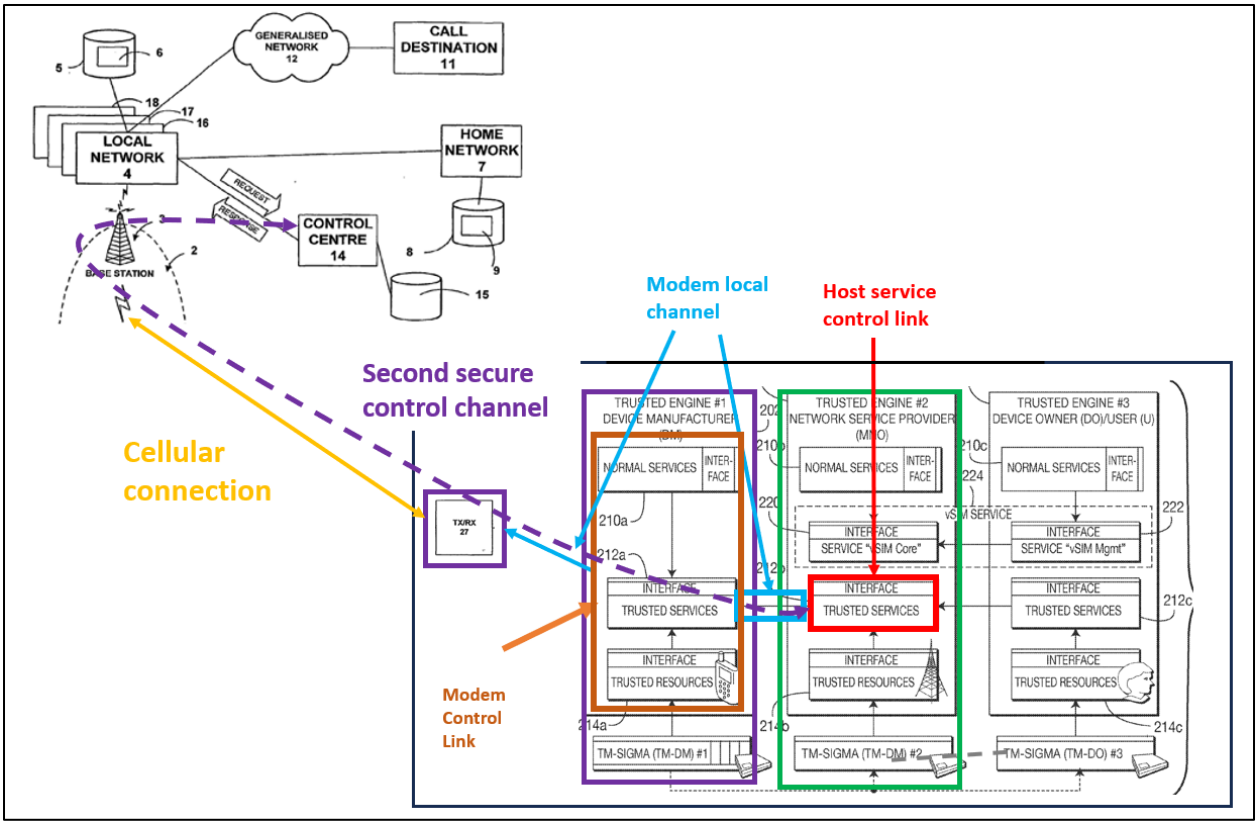
[3.2] wherein the secure execution environment comprises a host service control link, the second secure control channel coupled to the host service control link, the modem local channel providing secure communication between the modem control link and the host service control link.

268. In SDD, the SEE (TSS-MNO/TM-SIGMA) comprises a host service control link that "facilitates communication with a host secure channel." SAMSUNG-1001, 6:9-11; §IX.C. As illustrated in Schmidt's FIG. 2, TSS-MNO's trusted services interface (host service control link) couples TSS-MNO and TSS-DM, and since TSS-DM controls all external communication, a POSITA would have understood that TSS-MNO's trusted services interface facilitates communication with the secure control channels (via TSS-DM to the control centre, e.g., to retrieve policy settings). SAMSUNG-1005, FIG. 2, [0032]; see [1.4]-[1.6].



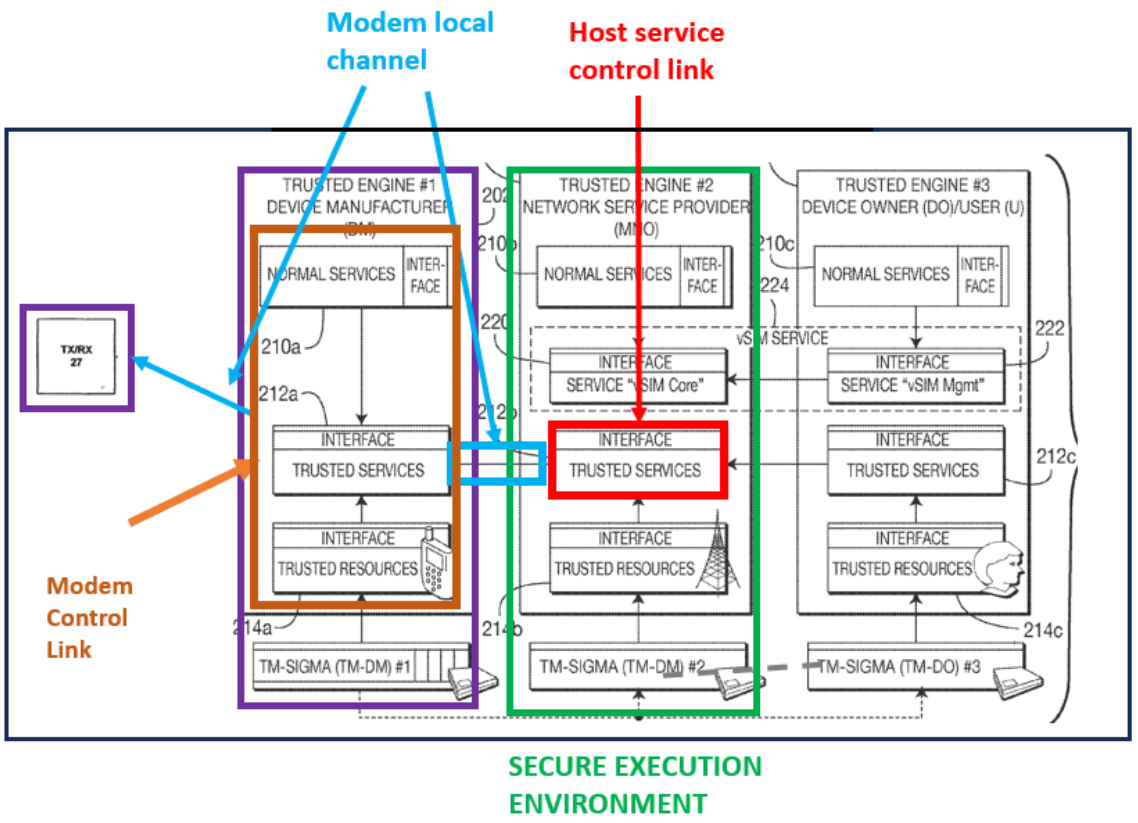
SAMSUNG-1005, FIG. 2 (annotated); SAMSUNG-1006, FIG. 2 (excerpt).

269. In SDD, the second secure control channel is coupled to the host service control link. As explained in [1.4]-[1.6], SDD's TSS-MNO facilitates communication to the control centre (network service controller), e.g., to retrieve policy settings, which occurs over the first and second secure control channels. SAMSUNG-1005, [0033]; *see* [1.4]-[1.6]. Because TSS-MNO's trusted services interface (host service control link) couples TSS-MNO and TSS-DM, and TSS-DM controls all external communication, the second secure control channel is coupled to the host service control link. SAMSUNG-1005, [0032]. *See also* §VII.C.



SAMSUNG-1005, FIG. 2 (annotated); SAMSUNG-1006, FIGS. 1, 2 (annotated).

270. In SDD, as illustrated below, the modem local channel provides secure communication between the modem control link (e.g., in TSS-DM) and the host service control link (TSS-MNO's trusted services interface). Since each "TSS-sigma is always configured to sign and encrypt any given data," a POSITA would have understood that communication between the modem control link and the host service control link is secure (encrypted). SAMSUNG-1005, [0031].



SAMSUNG-1005, FIG. 2 (annotated); SAMSUNG-1006, FIG. 2 (excerpt, annotated).

[8] The method of claim 1, wherein the one or more service policy settings include an access control setting, a traffic control setting, and/or an admission control setting.

271. SDD's service policy settings (as described above in claim 1) include traffic control settings. In SDD, the routing table specifies traffic control settings that are used to determine a connection path to a call destination. SAMSUNG-1006, [0032]-[0033], [0087]. As DB explains, "when an outgoing call to a call destination 11 is initiated," the device "intercepts the call making process and

provides a call output means 109 with ***routing information*** which will determine the route taken through the generalised network 12 between the local network 4 and the call destination 11." SAMSUNG-1006, [0087]. Because the routing information controls the route taken by traffic through the network, a POSITA would have understood that the routing information is a traffic control setting (e.g., that controls how traffic flows through the network).

272. In addition, SDD leverages DB's teachings (as described in §IX.C (roaming)), which provide that the "connection path utilised for any given call generally presents a number of available options depending for example on the interconnect facilities available to the local network 4," and the "***mobile telephone 1 has a call routing facility which allows routing information to be accessed from the SIM card 10 and added to a user defined call number such that a setup procedure initiated via the local network 4 results in the connection path to the call destination 11 being determined in accordance with a preferred route***." SAMSUNG-1006, [0032]. DB further explains that to "achieve this routing function, the ***mobile telephone 1 has stored in its SIM card 10 a routing table 13 in the form of a look up table which allows routing information to be extracted rapidly and with minimal processing whenever a user initiates a call.***" SAMSUNG-1006, [0033].

273. Further, per DB, SDD's service policy settings include a forbidden network table used to enforce access control settings when selecting a network for registration purposes. SAMSUNG-1006, [0036], [0046]. As explained in DB, "a forbidden network table 20 … lists those networks for which the subscriber does not have authorisation from the home network 7 to complete registration." SAMSUNG-1006, [0036]. DB further explains that "any networks which are excluded are removed from the list of available networks." SAMSUNG-1006, [0057]. Therefore, per DB, in SDD, access to a forbidden network is controlled (disallowed) at the device (SDD) based on the forbidden network table (a policy setting). SAMSUNG-1006, [0036], [0057]; §IX.C (roaming). Further, because the network access is controlled using the forbidden network table, these service policy settings are access control settings. *See also* §VII.B.

[9] The method of claim 1, wherein the one or more service policy settings include a network or device management communication setting.

274. Per DB, SDD's service policy settings include network management communication settings. As explained for claim 8, SDD leverages DB's teachings of storing and using a routing table (network management communication setting) to determine a connection path to a call destination. SAMSUNG-1006, [0032]-[0033], [0087]. In SDD, "when an outgoing call to a call destination 11 is initiated," the device "intercepts the call making process and provides a call output means 109 with ***routing information*** which will determine the route taken through

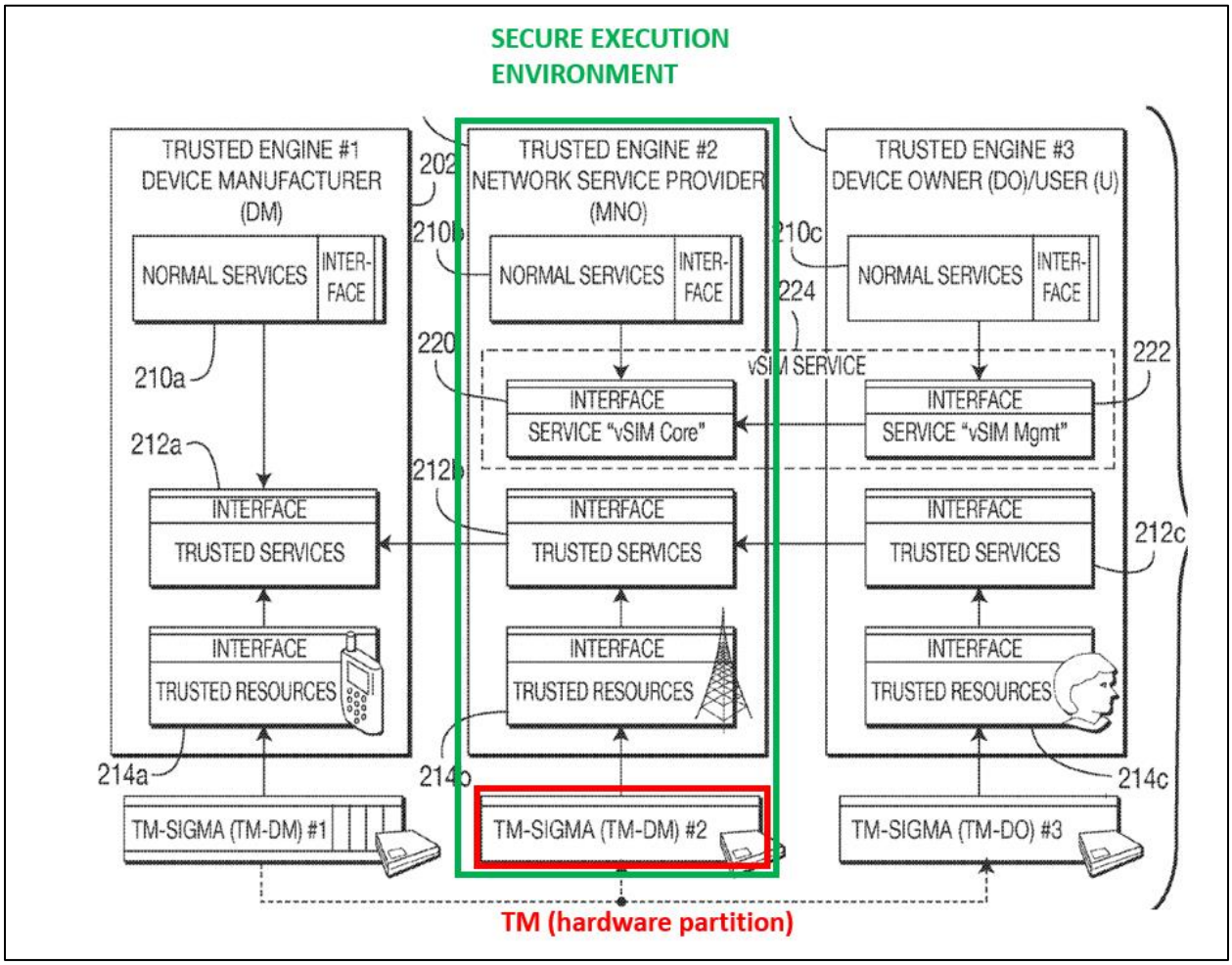
the generalised network 12 between the local network 4 and the call destination 11." SAMSUNG-1006, [0087].

275. A POSITA would have understood or find obvious that a policy setting used to determine a preferred route is a network management communication setting because it manages how the device communicates over the network, e.g., by defining a route. In more detail, the preferred route is related to communications since a route is a path over which devices exchange information – that is, *communicate* with one another. Policies that govern the selection of a route are network management communication settings because "the connection path" (that is, the route) "to the call destination 11 [is] determined in accordance with a preferred [network] route," which is determined based on the routing table policy setting. SAMSUNG-1006, [0032]. *See also* §VII.B.

[10] The method of claim 1, wherein the secure execution environment is implemented at least in part as a hardware partition.

276. In SDD, the secure execution environment is implemented at least in part as a hardware partition. For example, Schmidt explains that the "MTP in general, is a mobile platform having a non-exchangeable security module (trusted module, TM) permanently associated with the ***hardware platform***." SAMSUNG-1005, [0036]. A POSITA would have understood that the TM is a hardware partition. Further, per Schmidt, the secure execution environment includes a TM

(TM-SIGMA (TM-DM) #2), as illustrated below. SAMSUNG-1005, [0031], [0037], FIG. 2.



SAMSUNG-1005, FIG. 2 (annotated).

277. From these disclosures, a POSITA would have understood or found obvious that the secure execution environment is implemented at least in part as a hardware partition. For example, Schmidt teaches that the TM-SIGMA is a "non-exchangeable security module" that is "permanently associated with the hardware platform." SAMSUNG-1005, [0031], [0036]. A POSITA would understand that a

security module that is permanently associated with hardware is, at least in part, implemented in hardware. Specifically, a POSITA would have understood that Schmidt's system includes a hardware security module—a physical computing device that performs a variety of security-related functions, such as managing cryptography keys, accelerating cryptography operations (i.e., encryption and decryption), among other functions, as described in the NIST publication, "Security Requirements for Cryptographic Modules. SAMSUNG-1049, 13. As I described in Section IX.A, a trust anchor can provide a chain of trust to authenticate an entity (be it a website in the context of networks or a specific kernel version in the context of systems)—it is establishing this chain of trust that allows Schmidt to define subsystems that contain components that "trust" one another. A security module, rooted in hardware, is arguably the most secure component to serve as the root of trust, given that hardware is more tamperproof than software (as tampering hardware requires physical access to the hardware security module). SAMSUNG-1054, 1-3.

[11] The method of claim 1, wherein the secure execution environment is implemented at least in part as a software partition.

278. In SDD, the secure execution environment is implemented at least in part as a software partition. Schmidt explains that TSS-MNO is implemented as one of multiple separate and isolated trusted subsystems—i.e., in separate partitions implemented in software—within MTP/device. SAMSUNG-1005,

[0036], [0054]. Given this disclosure, a POSITA would have recognized that the TSS-MNO (secure execution environment) is implemented at least in part as a software partition.

[12] The method of claim 1, wherein the secure execution environment is implemented at least in part in a virtual machine executed on a processor.

279. In SDD, the secure execution environment (TSS-MNO) is implemented at least in part in a virtual machine executed on a processor. For example, Schmidt explains that the "MTP operates a trusted operating system," and the "trusted software layer supports multiple separate trusted subsystems (TSS-SIGMA) with a protected and insulated execution and memory function." SAMSUNG-1005, [0036]. As described above, SDD's secure execution environment includes a TSS-SIGMA, TSS-MNO. §IX.C (Schmidt-DB combination). A POSITA would have understood that "multiple separate trusted subsystems [] with a protected and insulated execution and memory function" together make up virtual machines. SAMSUNG-1005, [0036]. A POSITA would have understood that a virtual machine is a software based computer that functions like a computer, e.g., a computing environment dedicated to providing a virtual SIM service that mimics a traditional computing module such as a SIM card. For example, Smith-2005 notes that, "[i]n constrast, a system VM provides a complete, persistent system environment that supports an operating system along with its many user processes. It provides the guest operating system with access to virtual

hardware resources, including networking, I/O, and perhaps a graphical user interface along with a processor and memory." SAMSUNG-1067, 3. In other words, Smith-2005 discloses that virtual machines provide the operating systems they run access to (virtualized) hardware resources, including a processor. In fact, Smith-2005 states that a "virtual machine can support individual processes or ***a complete system***" and that "[t]he concept of virtualization can be applied not only to subsystems such as disks but ***to an entire machine***." SAMSUNG-1067, 1-2. Therefore, Smith-2005 discloses that virtual machines run on processors. A POSITA would have therefore recognized that the secure execution environment (TSS-MNO) is executed at least in part on a virtual machine.

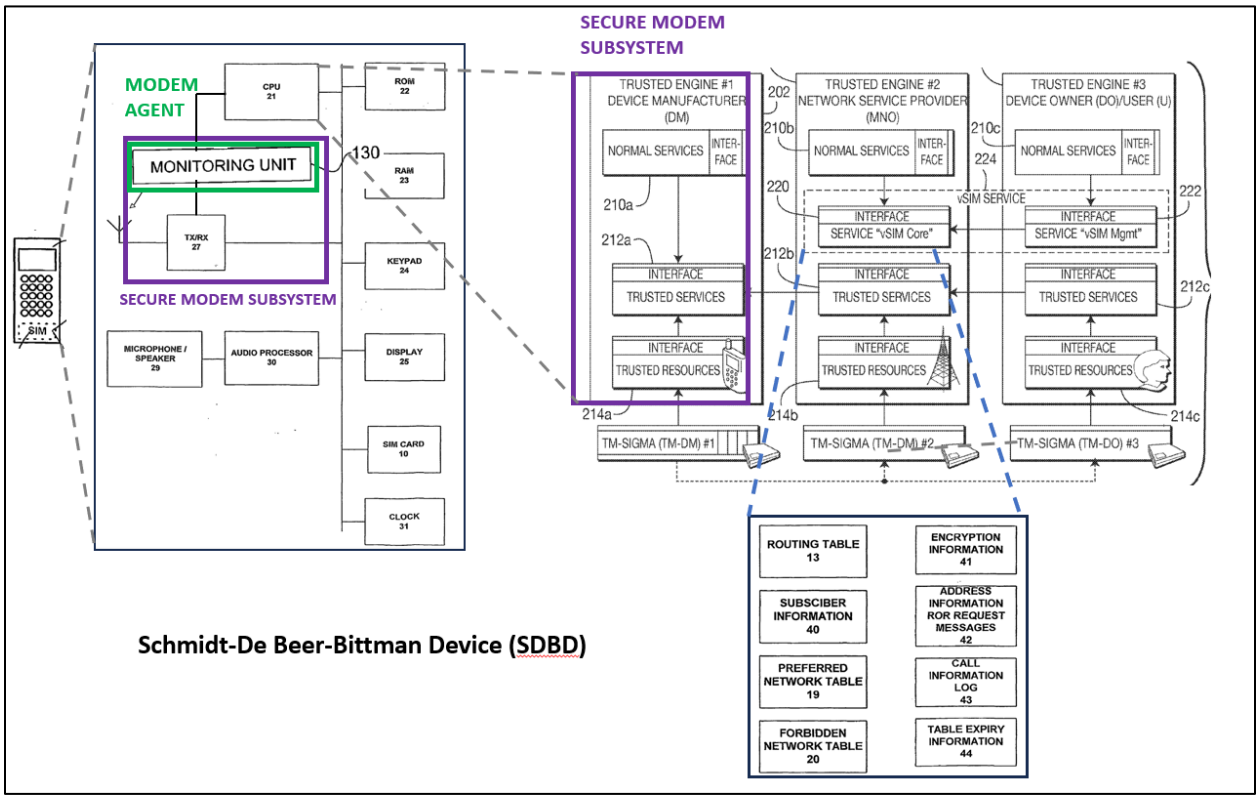
280. Further, the above-described virtual machine is executed at least in part on hardware. For example, Schmidt explains that the "methods or flow charts provided herein may be implemented in a computer program, software, or firmware incorporated in a computer-readable storage medium for ***execution by a general purpose computer or a processor***." SAMSUNG-1005, [0143].

B. Ground 1B: Combination of Schmidt, De Beer, and Bittmann Renders Obvious Claims 4-7

[4] The method of claim 1, wherein the secure modem subsystem further comprises a modem agent accessible only by the network service controller through the first secure control channel.

281. SDBD's secure modem subsystem includes a modem agent (activity monitoring unit, per Bittmann), enabling SDBD to monitor "data transferred to

and/or from device." §IX.E; SAMSUNG-1007, [0031]. As Bittmann explains, the "activity monitoring unit 130" "links between a CPU … and a network interface," and "monitors data activity of [the] communication device." SAMSUNG-1007, [0028], [0052].



SAMSUNG-1005, FIG-2 (modified), SAMSUNG-1006, FIGS. 1-2 (modified); SAMSUNG-1007, FIG. 3A (modified).

282. The secure modem subsystem, and therefore the monitoring unit (modem agent) is only accessible by the network service controller (control centre) through the first secure control channel (the control channel between TSS-DM and control centre, as described above with reference to [1.3]). For example, per

Schmidt, TSS-DM "controls all internal and external communications." SAMSUNG-1005, [0032]. Therefore, the network services controller (control centre) accesses the modem agent only through the secure control channel via TSS-DM. A POSITA would further understand or find obvious that the modem agent is accessible to the network service controller only through the first control channel. That's because, when the first control channel is active, that channel is the only dedicated connection between the control centre and the secure modem subsystem, including the modem agent (monitoring unit). (As described in [1.3] and [1.4], only one control channel is active at a time – that is, the first and second control channels differ based on time of occurrence. SAMSUNG-1022, 3.) *See also* §VII.C.

[5] The method of claim 4, wherein the modem agent comprises a service measurement point for use of the service.

283. SDBD's modem agent (e.g., monitoring unit, per Bittmann) comprises a service measurement point for use of the service on the device. SAMSUNG-1007, [0028]-[0029], [0031]. As Bittmann explains, the "monitoring unit 130 monitors all data activity of" the device and includes "some or all of the data transferred to and/or from device 110 over communication network 120, for example some or all data transferred between devices 110 and 140, some or all data transferred between devices 110 and 170, some or all data transferred between

device 110 and content server 160, etc." SAMSUNG-1007, [0031]. Bittmann further explains that "[e]xamples of the monitored data activity include inter-alia one or more of the following: web surfing, game-playing, emails, short message service (sms), voice over IP, faxing, transactions, etc." SAMSUNG-1007, [0031].

284. A POSITA would have recognized or found obvious that SDBD's modem agent would comprise the monitoring unit (service measurement point) because the modem agent has efficient access to all cellular service data (and only cellular data) transferred into and out of the device, thereby improving efficiency and conserving device resources.

285. Therefore, a POSITA would have recognized that the monitoring unit (modem agent) is a service measurement point for services on the device (e.g., web surfing, SMS, voice). SAMSUNG-1007, [0031].

286. And as explained in [1.7], the service used by the device includes voice and/or other data services.

[6] The method of claim 5, further comprising the modem agent communicating a first report of the use of the service to the network service controller through the first secure control channel.

287. As described in [5], SDBD's modem agent (monitoring unit) monitors data activity of the device. SAMSUNG-1007, [0031]; §X.B.[5]. And, as explained in §IX.C and §X.A.[1.6], data conventionally stored on a physical SIM would be stored in secure memory partition in SDBD. Therefore, in SDBD, a

POSITA would understand or find obvious that the monitored data, which is also conventionally stored on the SIM (per DB), would be stored in the dedicated vSIM protected storage in the form of a secure memory partition (which as explained above would only be accessible by the TSS-MNO). SAMSUNG-1005, [0030]; SAMSUNG-1006, [0049], FIG. 4.

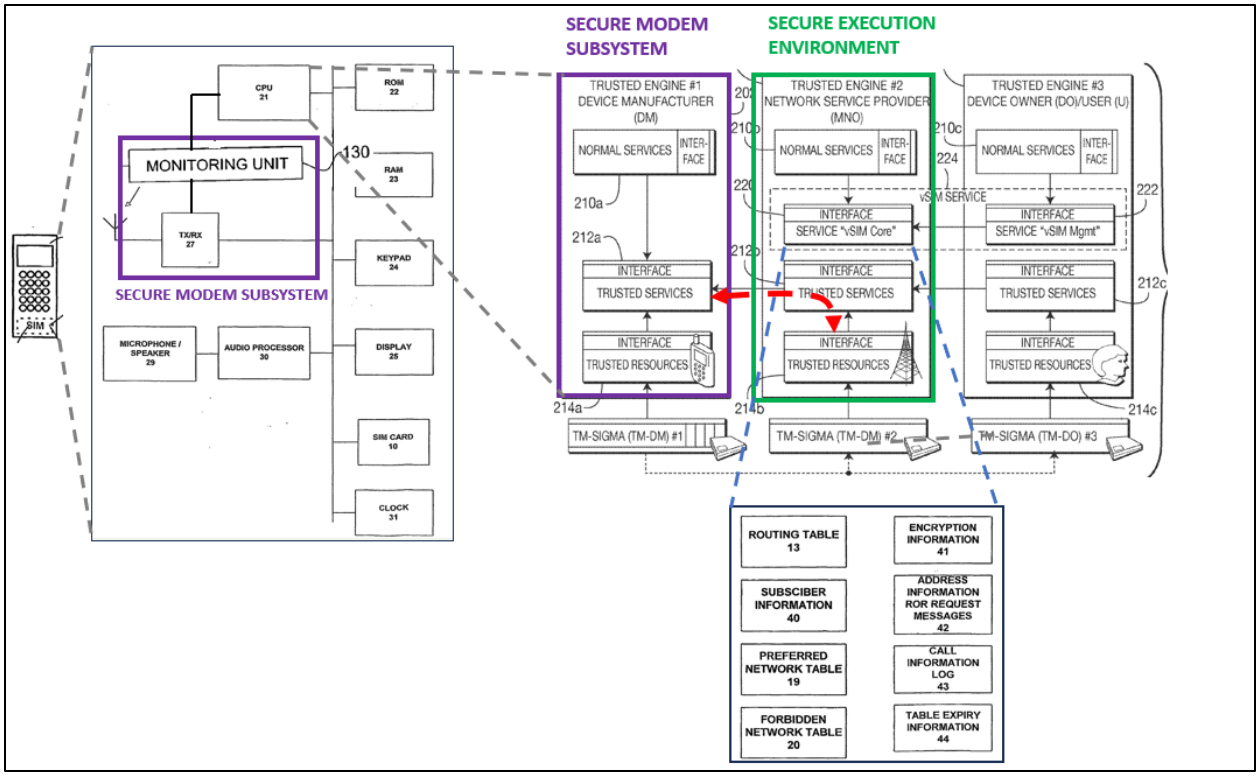
288. In SDBD, the monitored call log data would be communicated from the device to the control centre. Per DB, the call log "is ***periodically communicated to the control centre***." SAMSUNG-1006, [0090]. Bittmann similarly explains that the monitoring unit reports device data activity to a server, which manages the account of the device, e.g., to limit data activity if an account's allowance is exceeded. SAMSUNG-1007, [0029], [0037], [0043], [0046].

289. Additionally, a POSITA would understand or find obvious to implement SDBD's system so that the monitored call log data is communicated from the TSS-MNO to the monitoring agent, and then from the monitoring agent to the control centre. As explained above, in SBDB, the call log that would be stored in SDBD's secure memory partition is only accessible via the TSS-MNO. SAMSUNG-1005, [0028], FIG 2. Additionally, per Schmidt, TSS-MNO is responsible for "[a]ll subscription-dependent and subscriber-related network provider services," (SAMSUNG-1006, [0049]) which would include provision of call log data (conventionally stored on a SIM, per De Beer) to the network

controller, e.g., for billing or other associated functions related to use of network services. SAMSUNG-1005, [0033]; SAMSUNG-1006, [0049].

290. Given these disclosures, a POSITA would recognize or find obvious that SDBD's system would be implemented so that either (1) the monitoring unit requests the call log data from the TSS-MNO, which then communicates this requested data to the monitoring unit, or (2) the TSS-MNO communicates this data to the monitoring unit without being prompted to do so. Either implementation would be straightforward to implement and would be a predictable solution to facilitate provision of data—which is only accessible by TSS-MNO—to the network service controller, via the monitoring unit in the secure modem subsystem.

291. Further, since in SDBD there is no connection from the secure modem subsystem to the trusted resources secure execution, a POSITA would have understood or found obvious that SDBD's secure modem subsystem, including the monitoring agent, has access to the call log data ***only*** through the secure execution environment's trusted services, as illustrated in the dotted red line below. SDBD's secure modem subsystem cannot access the call log data directly since SDBD provides no such access.



SAMSUNG-1005, FIG-2 (modified), SAMSUNG-1006, FIGS. 1-2 (modified); SAMSUNG-1007, FIG. 3A (modified).

292. Subsequently, per DB and Bittmann, this monitored call log would be communicated from the monitoring unit (i.e., the modem agent), via the secure modem subsystem's components, to the control centre (i.e., the network service controller). *See, e.g.*, SAMSUNG-1007, [0042] (sending "data activity reports ***from monitoring units***," which are part of SDBD's secure modem subsystem), [0053] ("[t]he link between monitoring unit 130 and receiver/transmitter" allows "unit 130 to transmit stored activity data"); SAMSUNG-1006, [0090].

293. Additionally, in SDBD, the data activity report would be communicated by the monitoring unit through the first secure control channel. For

example, Bittmann explains that "[t]he link between monitoring unit 130 and receiver/transmitter" allows "unit 130 to transmit stored activity data, through the cellular communication infrastructure, to server utility 150, preferably as ***out-of-band traffic***." SAMSUNG-1007, [0053]. A POSITA would understand that control channels, including SDCCH, transmits traffic out-of-band. *See also* §VII.C.

294. Moreover, because SDBD would have already established a first control channel (e.g., SDCCH) between the device and the control centre, a POSITA would understand or find obvious that, when transmitting stored activity data out-of-band to the control centre, SDBD would use the same first control channel because that would have been conventional and straightforward, and would improve efficiency and conserve resources. *See* analysis for [1.3] *supra.*

295. For these reasons, the TSS-MNO of SDBD's SEE communicates a first report of the use of the service to the modem agent (monitoring unit in the secure modem subsystem), which in turn would communicate the report to the network service controller (control centre) through the first secure control channel.

[7] The method of claim 6, further comprising the secure execution environment separately communicating a second report of the monitored use of the service through the second secure control channel.

296. As described in [6], SDBD would periodically communicate monitored call logs/usage reports (i.e., the monitored use of the service) from the

SEE (including TSS-MNO) through the secure modem subsystem (including the monitoring unit and TX/RX) to the control centre (network services controller). *See* [6], *supra.*

297. Moreover, as explained in [6], at a first time, SDBD would communicate a first report over the first secure control channel. At a later time (e.g., on the next day), there would be a second secure control channel with the control centre, and SDBD would communicate a second report of monitored use through that second secure control channel. Specifically, as explained in [1.4], the second control channel is established at a later time from the first secure control channel, such as the next day. Therefore, when SDBD communicates the report (the "call log ... is ***periodically communicated to the control centre***"), a POSITA would understand or find obvious that the report is transmitted over the second secure control channel, which is the only control channel available with the control centre at that time. *See* [1.4]; SAMSUNG-1006, [0090].

298. Therefore, in SDBD, the SEE (TSS-MNO/TM-SIGMA) separately communicates a second report (at a later time than the first report) of the monitored use of the service (via the secure modem subsystem) to the network service controller and using the second secure control channel (the only channel available at that later time). *See also* §VII.C.

C. Ground 1C: Schmidt in view of DB and Smith renders claims 10-12 obvious

[10] The method of claim 1, wherein the secure execution environment is implemented at least in part as a hardware partition.

299. In SDD, the SEE (TSS-MNO, TM-SIGMA) is implemented at least in part as a hardware partition. §X.A.[1.4]. Smith explains that the "virtual machine is implemented as a combination of a real machine and virtualizing software." SAMSUNG-1008, 18. The virtualizing software can "partition a single large hard disk into a number of smaller virtual disks," such that the "virtual disks are mapped to a real disk by implementing each of the virtual disks as a single large file on the real disk." SAMSUNG-1008, 14. As described above, TSS-MNO (part of the SEE) includes trusted resources, including trusted storage, which is a hardware partition (created by the VMM) of SDSD's physical storage. SAMSUNG-1030, 28. §X.A.[1.6].

300. Thus, a POSITA would have understood that the SEE is implemented in part as a hardware partition (a trusted storage partition in TSS-MNO). SAMSUNG-1005, [0033].

[11] The method of claim 1, wherein the secure execution environment is implemented at least in part as a software partition.

301. In SDSD, the MTP is implemented as a VM, which is a software partition. *See* §IX.F-G. A VM is a software partition at least since VMs "provide a secure way of partitioning major software systems that run concurrently on the

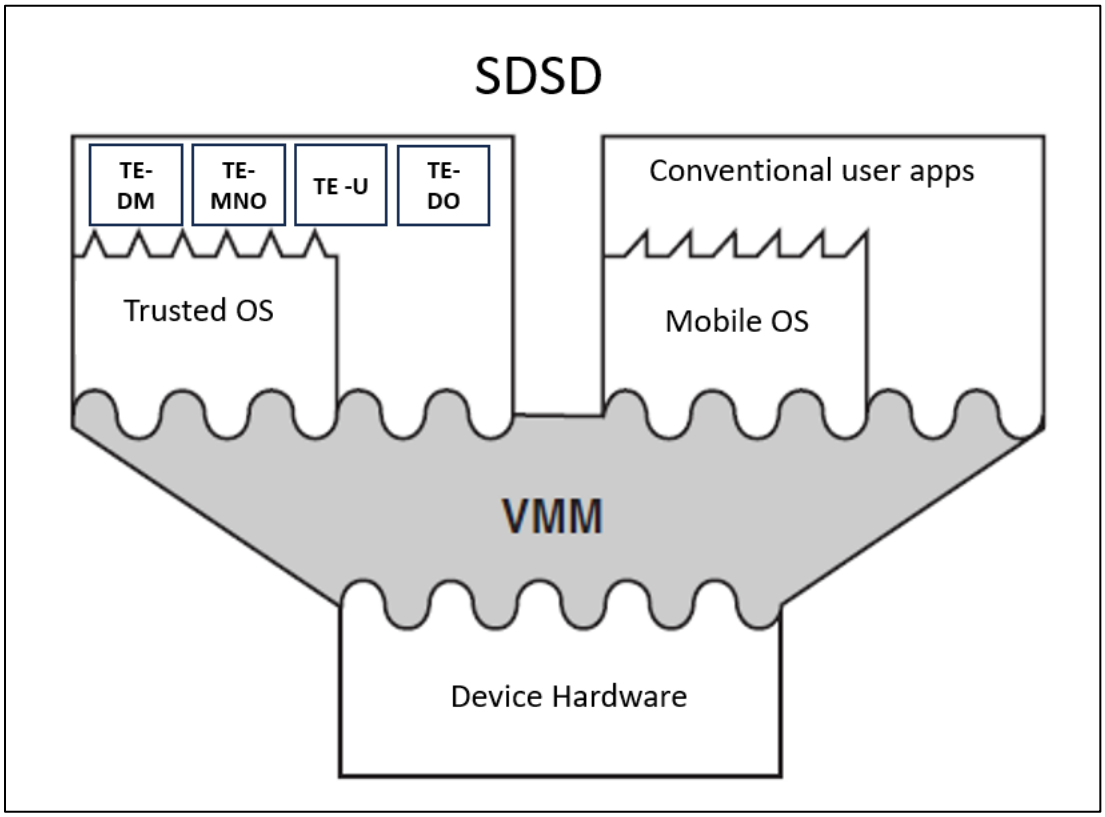
same hardware platform" such that "[s]oftware running on one guest system is isolated from software running on other guest systems. SAMSUNG-1008, 24.

[12] The method of claim 1, wherein the secure execution environment is implemented at least in part in a virtual machine executed on a processor.

302. SDSD renders [12] obvious.

303. In SDSD, the MTP, which includes the SEE (TSS-MNO, TM-SIGMA).

304. The System VM executes on a processor that is device hardware, e.g., the IA-32 hardware platform, which includes a processor. SAMSUNG-1008, 25, FIG. 1.11.



SAMSUNG-1008, FIG. 1.11(modified).

XI. CONCLUSION

305. For all the reasons I have noted in the foregoing paragraphs, claims 1-30 of the ’429 Patent are obvious in view of the references discussed above. ’429

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

APPENDIX A

Patrick Drew McDaniel

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

ACADEMIC AND RESEARCH APPOINTMENTS

Tsun-Ming Shih Professor of Computer Sciences, 2022-Present
University of Wisconsin-Madison, Madison, WI

William L. Weiss Professor of Information and Communications Technology 2017-2022
Computer Science and Engineering, Pennsylvania State University, University Park, PA

Distinguished Professor 2016-2017
Computer Science and Engineering, Pennsylvania State University, University Park, PA

Professor 2011-2015
Computer Science and Engineering, Pennsylvania State University, University Park, PA

Associate Professor 2007-2011
Computer Science and Engineering, Pennsylvania State University, University Park, PA

Hartz Family Career Development Assistant Professor 2004-2007
Computer Science and Engineering, Pennsylvania State University, University Park, PA

Adjunct Professor 2003-2009
Stern School of Business, New York University, New York, NY

Senior Research Staff Member 2001-2004
AT&T Labs - Research, Florham Park, NJ

RESEARCH LEADERSHIP APPOINTMENTS

Director, National Science Foundation, Center for Trustworthy Machine Learning 2018-present
Participants: Penn State, Stanford, UC Berkeley, UC San Diego, Univ. of Wisconsin, Univ. of Virginia

Director, Institute for Networking and Security Research 2016-2022
College of Engineering, Pennsylvania State University, University Park, Pennsylvania

Program Manager, Cyber-Security Collaborative Research Alliance (CRA) 2013-2018
College of Engineering, Pennsylvania State University, University Park, Pennsylvania

Co-Director, Systems and Internet Infrastructure Laboratory 2004-2022
College of Engineering, Pennsylvania State University, University Park, Pennsylvania

EDUCATION

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

AFFILIATIONS

Association for Computing Machinery (ACM), *Fellow*

The Institute of Electrical and Electronics Engineers (IEEE), *Fellow*

American Association for the Advancement of Science (AAAS), *Fellow*

USENIX Advanced Computing Systems Association (USENIX)

STUDENTS

Past PhD Students

- *Ryan Sheatsley*, Spring 2024, now **Post-doc**, University of Wisconsin-Madison

- *Z. Berkay Celik*, Spring 2019, now **Assistant Professor**, Purdue University
- *Nicolas Papernot*, Spring 2018, now **Assistant Professor**, University of Toronto
- *Wenhui Hu*, Fall 2016, now **Senior Member of Technical Staff**, Oracle
- *Devin Pohly*, Spring 2016, now **Assistant Professor**, Wheaton College
- *Damien Octeau*, Summer 2014, now **Software Engineer in Security**, Google
- *Steve McLaughlin*, Spring 2014, now **Senior Software Engineer**, Samsung Research America
- *Thomas Moyer*, Summer 2011, now **Assistant Professor**, University of North Carolina-Charlotte
- *William Enck*, Spring 2011, now **Professor**, North Carolina State University
- *Kevin Butler*, Summer 2010, now **Professor**, University of Florida
- *Machigar Ongtang*, Summer 2010, now **Assistant Professor**, Dhurakij Pundit University
- *Patrick Traynor*, Spring 2008, now **John and Mary Lou Dasberg Preeminent Chair, Professor**, University of Florida, co-advisor
- *Fr. Boniface Hicks*, Fall 2007, now **Assistant Professor**, St. Vincent College

Current PhD Students

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

Past Masters Students

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

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

Past Post-Docs

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

TEACHING

University of Wisconsin-Madison, College of Letters and Science

- **CompSci 642 - Intro to Information Security** - Fall 2023, Fall 2024
- **CompSci 839 - Emerging Trends in Systems Security and Privacy** - Spring 2025

Pennsylvania State University, College of Engineering

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

New York University, Stern School of Business

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

HONORS, AWARDS, AND KEYNOTE ADDRESSES

Most Influential Paper of PLDI 2014, *for the paper "FlowDroid: Precise Context, Flow, Field, Object-sensitive and Lifecycle-aware Taint Analysis for Android Apps" , Presented annually to the author(s) of a paper presented at the PLDI held 10 years prior to the award year, June 2024.*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Keynote Addresses

1. Securitys Role in Achieving Sustainability, 29th ACM Conference on Computer and Communications Security (CCS), Los Angeles, CA, November, 2022.

2. Security, Game Theory, and Their Role in Achieving Sustainability, Conference on Decision and Game Theory for Security, Pittsburgh, PA, October, 2022.

3. Prognosticating the Future of IoT Security, 2022 IEEE SafeThings Workshop, San Francisco, CA, May 2022.

4. The Challenges of Machine Learning in Adversarial Settings. Triangle Area Privacy and Security Day, Durham, NC, October, 2019.

5. The Challenges of Machine Learning in Adversarial Settings. 2019 Subversion and Assurance of AI Workshop, US National Reconnaissance Office, Washington, DC, March, 2019.

6. Attacks, Defenses, and Impacts of Machine Learning in Adversarial Settings. 2017 Conference on Security and Privacy in Communication Networks (SecureComm), Niagara Falls, Canada, October, 2017.

7. Tracing the Arc of Smartphone Application Security. 2017 ACM on International Workshop on Security And Privacy Analytics. Scottsdale, AZ, March, 2017.

8. Tracing the Arc of Smartphone Application Security. 12th International Conference on Information Systems Security, Jaipur, India, December, 2016.

9. The 25th International Conference on Computer Communication and Networks (ICCCN 2016), August, 2016, Waikoloa, Hawaii.

10. Learning from Ourselves: Where are we and where can we go in mobile systems security?. Mobile Security Technologies (MOST) 2016 Workshop, IEEE Computer Society Security and Privacy Workshops, San Jose, CA, May, 2016.

11. Eight Years of Mobile Smartphone Security. Center for Secure and Dependable Systems (CSDS) Cybersecurity Symposium, Coeur d'Alene, April, 2016.

12. The Importance of Measurement and Decision Making to a Science of Security, 2015 IEEE Conference on Communications and Network Security (CNS), September 2015, Florence, Italy.

13. The Importance of Measurement and Decision Making to a Science of Security. 3rd International Symposium on Resilient Cyber Systems, Philadelphia, PA, August, 2015.

14. The Importance of Measurement and Decision Making to a Science of Security, 2015 Symposium And Bootcamp on the Science of Security (Hotsos), April 2015, University of Illinois at Urbana-Champaign

15. Security and Science of Agility, ACM Workshop on Moving Target Defense (MTD 2014), November 2014, Scottsdale, AZ

16. A Secondary Internet Revolution: How the Smart Device has Changed the Information Security Landscape, IEEE New Technology Industry Seminar (NTIS '13), Everett WA, August, 2013

17. Permission-based Application Governance; A Step Forward or Backward?, 26th Annual WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'12), Paris, France, July 2012.

18. Scalable Integrity-Guaranteed AJAX, The 14th Asia-Pacific Web Conference (APWeb), Kunming, China, April 2012.

19. Security Challenges and Solutions in Mobile Smartphone Applications, IEEE Computer Security Foundations (CSF 2011), Abbaye des Vaux de Cernay, France, June 2012.

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

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

Distinguished Lectures

1. Adversarial Machine Learning: A 10-year Perspective, NSF ACTION AI Institute Distinguished Lecture Series, Virtual, December, 2024.

2. Adversarial Machine Learning: A 10-year Perspective, University of Illinois, Champaign-Urbana, Champaign, IL, November, 2024.

3. The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, University of California, Los Angeles, Los Angeles, CA, December, 2023.

4. The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, Michigan State University, Lansing, MI, November, 2023.

5. The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective. Computer Science Department, Temple University, Philadelphia, PA, February, 2022.

6. The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective. Computer Science Department, University of Wisconsin-Madison, Madison, WI, February, 2020.

7. Shutterstock Distinguished Lecture: The Challenges of Machine Learning in Adversarial Settings. Computer Science Department, Stonybrook University, Stonybrook, NY, December, 2019.

8. Distinguished Blockchain Lecture: The Challenges of Machine Learning in Adversarial Settings. Cylab Security and Privacy Institute, Carnegie Mellon University, Pittsburgh, PA, December, 2019.

9. Distinguished Speaker Series: The Challenges of Machine Learning in Adversarial Settings. Department of Computer Science, University at Buffalo, Buffalo, NY, November, 2018.

10. Samuel D. Conte Distinguished Lecture Series: The Challenges of Machine Learning in Adversarial Settings. Department of Computer Science, Purdue University, West Lafeyette, Indiana, November, 2018.

11. The Challenges of Machine Learning in Adversarial Settings. Department of Software and Information Systems, University of North Carolina at Charlotte, Charlotte, NC, February, 2018.

12. Tracing the Arc of Smartphone Application Security. Celebrating 50 Years of Computer Science @ NC State, North Carolina State University, Raleigh, NC, October, 2017.

13. Tracing the Arc of Smartphone Application Security. Computer Science Department and the Electrical and Computer Engineering Department Seminar Series, Colorado State University, Fort Colins, CO, October, 2017.

14. Tracing the Arc of Smartphone Application Security. Rochester Institute of Technology, College of Computing and Information Sciences, Rochester, NY, September, 2017.

15. Tracing the Arc of Smartphone Application Security, University of Texas-Dallas Department of Computer Science, Dallas, TX, May 2017.

16. Tracing the Arc of Smartphone Application Security. Rochester Institute of Technology, College of Computing and Information Sciences, Rochester, NY, May 2017.

17. Tracing the Arc of Smartphone Application Security. University of California-Irvine, Computer Science Department, Irvine CA, March, 2017.

18. Tracing the Arc of Smartphone Application Security. The Ohio State University, Department of Computer Science and Engineering, Columbus, OH, March, 2017.

19. Tracing the Arc of Smartphone Application Security. Virginia Technical University, Department of Computer Science, Blacksburg, VA, March, 2017.

20. Six Years of Mobile Smartphone Security, CISPA Distinguished Lecture Series, Max Planck Institute/Saarland University, Saarbrucken Germany, July, 2015.

21. Six Years of Mobile Smartphone Security. Technische Universtat Darmstadt, Darmstadt Germany, July, 2015.

22. Security Challenges and Solutions in Mobile Smartphone Applications. Computer and Information Science Department, University of Oregon, Eugene, OR, April, 2011.

23. Security Challenges and Solutions in Mobile Smartphone Applications. Department of Software Information Systems College of Computing and Informatics, UNC Charlotte, Charlotte, NC, December, 2010.

RESEARCH SUPPORT

co-PI, *MURI: Cohesive and Robust Human-Bot Cybersecurity Teams*, Army Research Office, *$6,000,0000* (PSU award $739,527), 07/01/2021-06/30/2026, Collaborators: Many.

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

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

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

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

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

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

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

PI, *Models for Enabling Continuous Reconfigurability of Secure Missions (MACRO) Cyber-Security Collaborative Research Alliance (CRA)*, Army Research Laboratory, *$24.1 million ($48.2 million with renewal at 12/17)*,

9/20/2013-9/19/2023 (renewed at 5 years), Collaborators: PSU, Carnegie Mellon, Indiana, UC Davis, UC Riverside, ARL, CERDEC.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PROFESSIONAL ACTIVITIES

Editorial Positions, Panels, and Boards

IEEE Technical Committee on Security and Privacy
- *Chair*–January 2014-January 2016
- *Vice Chair*–January 2012-December 2014

ACM Transactions on Internet Technology (TOIT)
- *Editor in Chief*–September 2007-December 2012
- *Associate Editor*–April 2004-August 2007

IEEE Security and Privacy Magazine
- *Area Editor, Secure Systems*–January 2009-2015

IEEE Transactions on Computers (TC)
- *Associate Editor*–August 2008-2014

ACM Transactions on Information and System Security (TISSEC)
- *Associate Editor*–May 2007-May 2012

IEEE Transactions on Software Engineering (TSE)
- *Associate Editor*–January 2007-April 2012
- *Guest Editor, Special Issue on Topics in Security*–Fall 2006-April 2012

IEEE Transactions on Parallel and Distributed Systems (TPDS)
- *Guest Editor, Special Issue on Trust, Security and Privacy in Parallel and Distributed Systems*–Fall 2012

Elsevier Journal of Computer Networks
- *Guest Editor, Special Issue on Web Security*–Fall 2003-Spring 2005

Encyclopedia of Cryptography and Security
- *Editorial Board Member*–Fall 2002-Spring 2005

Journal of Defense Modeling and Simulation
- *Guest Editor, Special Issue on Cyber Risk and Vulnerability Estimation*–Winter 2018-

Other Professional Activities

IEEE Workshop on the Internet of Safe Things (SafeThings)
- *Steering Committee*–2022-present

Helmholtz Center for Information Security (CISPA), Scientific Advisory Board
- *Member*–2019-present

Ohio University College of Engineering, Board of Vistors
- *Member*–2018-present

Penn State CISO Advisory Board
- *Member*–2016-2022

Member, Technical Guideline Development Committee, U.S. Election Assistance Commission
- *Member*–2010-2011

Natural Sciences and Engineering Research Council of Canada, Internetworked Systems Security Network
- *Scientific Advisory Board*–2008-2013

Technology for Cyber Physical System Security Forum, Cyber Security Research and Development, (Senators Joseph I. Lieberman and Susan Collins, Chairs)
- *Speaker and Participant*–September 2008

ACM Student Organization Advisor
- *Penn State Computer Science and Engineering Department*–2006-2012

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

President's National Security Telecommunications Advisory Panel

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

Abusable Technologies Awareness Center (ATAC)

- *Panelist*–October 2003-2010

AT&T IP Services Security Council

- *Member*–June 2003-August 2004

AT&T Internet Intellectual Property Review Team

- *Member*–September 2001-May 2002

ACM SIGCOMM Student Travel Grant Committee

- *Member*–August 2005

National Science Foundation, Grant Review Panel

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

Department of Energy SciDAC Review Panel

- *Member*–2001

Conference and Workshop Participation

IEEE Symposium on Security and Privacy

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

USENIX Security Symposium

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

ACM Conference on Computer and Communications Security (CCS)

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

IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)

- *Founding Program Co-Chair*–2023

IEEE European Symposium on Security and Privacy

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

International Conference on Privacy, Security and Trust (PST)

- *Steering Committee*–2019-

International Conference on Learning Representations (ICLR)

- *Program Committee*–2024

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

- *Program Committee*–2017

Network and Distributed System Security Symposium (NDSS)

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

Annual Computer Security Applications Conference (ACSAC)

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

Financial Cryptography

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

Computer Security Foundations Symposium (CSF)

- *Program Committee*–2011, 2021

European Symposium on Research in Computer Security (ESORICS)
- *Program Committee*–2004, 2005, 2021

ACM Symposium of SDx Research 2021 (SOSR)
- *Program Committee*–2021

International Symposium on Engineering Secure Software and Systems (ICISSP)
- *Program Committee*–2015

IEEE Conference on Communications and Network Security (CNS)
- *Program Committee*–2015, 2017

ACM Annual International Conference on Mobile Computing and Networking (MobiCom)
- *Program Committee*–2010, 2011, 2012
- *Program Committee, Distinguished Member*–2021

ACM Annual International Conference on Mobile Systems, Applications, and Services (MobiSys)
- *Program Committee*–2012

ACM Symposium on Access Control Models and Technologies (SACMAT)
- *Program Committee*–2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2011

ACM Conference on ASIA Computer and Communications Security (ASIA CCS)
- *Program Committee*–2008

ACM Conference on Electronic Commerce (ACM EC)
- *Program Committee*–2005

EAI International Conf. on Security and Privacy in Communication Networks (SecureComm)
- *Program Committee*–2020

International Conference on Applied Cryptography and Network Security (ACNS)
- *Program Committee*–2006

ACM Annual Digital Forensics Conference
- *Program Committee*–2012

IEEE Workshop on the Internet of Safe Things
- *Program Committee*–2019, 2022

ACM Workshop on Moving Target Defense (MTD)
- *Program Committee*–2015, 2016

IEEE ICNP Workshop on Secure Network Protocols (NPSec)
- *Program Committee*–2005, 2006

Conference on Decision and Game Theory for Security (GameSec)
- *Program Committee*–2012, 2018

ACM Symposium on Applied Computing (SAC)
- *Program Committee, Information Security Research and Applications* –2010

USENIX Annual Technical Conference
- *Program Committee*–2002, 2003

World Wide Web Conference (WWW)
- *Security and Privacy Track Vice-Chair*–2005
- *Security and Privacy Track Deputy Vice-Chair*–2004
- *Program Committee*–2003, 2007, 2010, 2011

Intl. Conference on Emerging Trends in Information and Communication Security (ETRICS)
- *Program Committee*–2006

International Conference On Distributed Computing Systems (ICDCS)
- *Program Committee*–2011

IEEE INFOCOM
- *Program Committee*–2007

IEEE GLOBECOM

- *Program Committee*–2010

Military Communications Conference (MILCOM)
- *Program Committee*–2015, 2016, 2017, 2018, 2019, 2021, 2022

The Five Nines Workshop on Designing and Managing High Availability Internet Services (INM)
- *Program Committee*–2007

International Conference on Information Systems Security (ICISS)
- *Steering Committee*–2007
- *Program Co-Chair*–2007
- *Program Committee*–2005, 2006, 2009, 2011

International Conference on Parallel Processing
- *Program Committee-Network Security*–2003

USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)
- *Program Committee*–2010

ACM Workshop on Networking, Systems, Applications on Mobile Handhelds (MobiHand)
- *Program Committee*–2009

ACM Workshop on Cloud Computing Security
- *Program Committee*–2009, 2010

ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)
- *Program Committee*–2011, 2012, 2013

International Workshop on Security in Software Engineering
- *Founding General Co-Chair*–2007

USENIX Workshop On Offensive Technology (WOOT)
- *Program Committee*–2007

ACM Storage Security and Survivability Workshop
- *Program Committee*–2006

ACM SIGCOMM Workshop on Internet Network Management
- *Program Committee*–2006, 2007

Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec)
- *Program Committee*–2006, 2007, 2008

Workshop on Workshop on Telecommunications Infrastructure Protection and Security (TIPS)
- *General Chair*–2009

USENIX Workshop on Hot Topics in Security (HotSec)
- *Program Chair*–2011
- *Program Committee*–2007, 2008, 2009, 2010, 2012

ACM Workshop TPC on Security and Privacy in Smartphones and Mobile Devices
- *Program Committee*–2011

International Workshop on Security (IWSEC)
- *Program Committee*–2006

International Workshop on Systems and Network Security (SNS)
- *Program Committee*–2005, 2006

COLLABORATORS (Last 48 Months)

Bolor-Erdene Zolbayar , Ahmed Abdou, Stefan Achleitner, Hidayet Aksu, Leonardo Babun, Paul Barford, Novella Bartolini, Yohan Beugin, Hoak, Blaine, Christopher Burchard, Quinn Burke, Z. Berkay Celik, Kamalika Chaudhuri, Muhao Chen, Adrien Cosson, Kyle Denney, Genannt Dohmann, Kyle Domico, Matthew Durbin, Pauley, Eric, David Evans, Jean-Charles Noirot Ferrand, Felix Freiling, Anshul Gandhi, Rahul George, Kanad Ghose, Kartik Gopalan, Ryan Guide, Amy Hasan, Ting He, Blaine Hoak, Thorsten Holz, Junjie Hu, Syed Rafiul Hussain, Alban Héon, Trent Jaeger, Somesh Jha, Rachel King, Engin Kirda, Farinaz Koushanfar, Srikanth V. Krishnamurthy, Daniel E. Krych, Domico, Kyle, Thomas La Porta, Dongyoon Lee, Jiazhao Li, Kunyang Li, Yiquan Li, Bo

Li, Yixuan Li, Azaree Lintereur, David Yu Liu, Zhenhua Liu, David Liu, Andrea Matwyshyn, Patrick McDaniel, Patrick Mcdaniel, Fidan Mehmeti, Shuai Mu, Yujin Nam, Namitha Nambiar, Michael Norris, Kyle Ostrowski, Nicolas Papernot, McDaniel, Patrick, Eric Pauley, Jonathan Petit, Jingyuan Qi, Xiangyu Qi, Burke, Quinn, Konrad Rieck, Tajana Rosing, Sheatsley, Ryan, Ahmad-Reza Sadeghi, Alejandro Andrade Salazar, Ryan Sheatsley, Tyler Shipp, Amit Kumar Sikder, Anand Sivasubramaniam, Wenjia Song, Indra Spiecker, Michael Swift, Gang Tan, Sanchal Thakkar, Selcuk Uluagac, Prasanna Venkatesh, Gunjan Verma, Bimal Viswanath, Jiongxiao Wang, Michael J. Weisman, Chaowei Xiao, Ya Xiao, Tian Xie, Danfeng Yao, Beugin, Yohan, Mingli Yu, Erez Zadok, Danfeng Zhang, Shulin Zhao, Minxuan Zhou, Sencun Zhu, Shitong Zhu, Bolor-Erdene Zolbayarn

CASES (Expert Witness, last 4 years)

Certain Mobile Phones, Components Thereof, and Products Containing Same, ITC Inv. No. 337-TA-1375, and In the Matter of Certain Electronic Devices, Including Mobile Phones, Tablets, Laptops, Components Thereof, and Products Containing the Same, Expert for Expert for the defense (Lenovo), International Trade Court, Case no. No. 337-TA-1375; No. 337-TA-1376; No. 5:23- cv-569; No. 5:23-cv-570.

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

Inter Partes Review, Expert for Expert for Apple Inc., United States Patent and Trademark Office, Case no. Patent No 10,929,512.

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

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

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

Inter Partes Review, Expert for Expert for Samsung Electronics Co., Ltd., United States Patent and Trademark Office, Case no. Patent Nos 9,277,433 and 9,521,578.

Inter Partes Review, Expert for Expert for Dropbox Inc., United States Patent and Trademark Office, Case no. Patent Nos 8,484,260 and 8,296,338.

Finjan, LLC. v. SonicWall Inc., Expert for Expert for SonicWall, Northern District of California, Case no. Case No. 5:17-cv-04467-BLF-VKD.

WebRoot, INC. and OpenText, Inc. v Kaspersky Lab, Trent Micro, Sophos LTD., Crowdstrike Holdings, INC, and Forcepoint, LCC., Expert for Expert for the Plaintiff, Western District of Texas, Case no. 6:22-CV-00243-ADA-DTG, 6:22-CV-00239-ADA-DTG, 6:22-CV-00240-ADA-DTG, 6:22-CV-00241-ADA-DTG, FORCEPOINT, LLC, and 6:22-CV-00342-ADA-DTG.

INDUSTRIAL EXPERIENCE

Software Developer 1994-1995
Applied Innovation, Inc., Columbus, OH

Project Manager 1993-1994
Primary Access Corporation, San Diego, CA

Software Developer 1991-1993
Primary Access Corporation, San Diego, CA

Software Developer 1989
Integrated Technologies, Inc., Muncie, IN

PUBLICATIONS

Books and Book Chapters

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

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

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

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

Patrick McDaniel, *Computer and Network Authentication*, Handbook of Information Security, John Wiley and Sons, September, 2004. Eds. Hossein Bidgoli.

Patrick McDaniel, *IPsec*, Encyclopedia of Information Security, Kluwer, 2003. Eds. Hossein Bidgoli.

Patrick McDaniel, *Policy*, Encyclopedia of Information Security, Kluwer, 2003. Eds. Hossein Bidgoli.

Patrick McDaniel, *Authentication*, The Internet Encyclopedia, John Wiley and Sons, 2002.

Journal Articles

Quinn Burke and Yohan Beugin and Blaine Hoak and Rachel King and Eric Pauley and Ryan Sheatsley and Mingli Yu and Ting He and Thomas La Porta and Patrick McDaniel, *Securing Cloud File Systems with Shielded Execution*, IEEE Transactions on Dependable and Secure Computing (TDSC), September, 2024.

Mingli Yu and Quinn Burke and Thomas La Porta and Patrick McDaniel, *Stealthy Misreporting Attacks Against Load Balancing*, IEEE/ACM Transactions on Networking (TON), 2024.

Anshul Gandhi and Dongyoon Lee and Zhenhua Liu and Shuai Mu and Erez Zadok and Kanad Ghose and Kartik Gopalan and David Yu Liu and Syed Rafiul Hussain and Patrick McDaniel, *Metrics for Sustainability in Data Centers*, SIGENERGY Energy Inform. Rev., New York, NY, USA, ACM, 3, 3, 40–46, October, 2023.

Quinn Burke and Patrick McDaniel and Thomas La Porta and Mingli Yu and Ting He, *Misreporting Attacks Against Load Balancers in Software-Defined Networking*, Mobile Networks and Applications, Springer, 2023.

Tian Xie and Sanchal Thakkar and Ting He and Patrick McDaniel and Quinn Burke, *Joint Caching and Routing in Cache Networks with Arbitrary Topology*, IEEE Transactions on Parallel and Distributed Systems, May, 2023.

Ya Xiao and Wenjia Song and Jingyuan Qi and Bimal Viswanath and Patrick McDaniel and Danfeng Yao, *Specializing Neural Networks for Cryptographic Code Completion Applications*, IEEE Transactions on Software Engineering, IEEE, 2023.

Matthew Durbin and Ryan Sheatsley and Patrick McDaniel and Azaree Lintereur, *Experimental tests of Gamma-ray Localization Aided with Machine-learning (GLAM) capabilities*, Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment, 1038, 2022.

Amit Kumar Sikder and Leonardo Babun and Z. Berkay Celik and Hidayet Aksu and Patrick McDaniel and Engin Kirda and Selcuk Uluagac, *Who's Controlling My Device? Multi-User Multi-Device-Aware Access Control System for Shared Smart Home Environment*, ACM Transactions on Internet of Things, Association for Computing Machinery, May, 2022.

Michael Norris and Z. Berkay Celik and Prasanna Venkatesh and Shulin Zhao and Patrick McDaniel and Anand Sivasubramaniam and Gang Tan, *IoTRepair: Flexible Fault Handling in Diverse IoT Deployments*, ACM Transactions on Internet of Things, ACM, 2022.

Tian Xie and Namitha Nambiar and Ting He and Patrick McDaniel, *Attack Resilience of Cache Replacement Policies: A Study Based on TTL Approximation*, IEEE/ACM Transactions on Networking, 2022.

Quinn Burke and Fidan Mehmeti and Rahul George and Kyle Ostrowski and Trent Jaeger and Thomas La Porta and Patrick Mcdaniel, *Enforcing Multilevel Security Policies in Unstable Networks*, IEEE Transactions on Network and Service Management, IEEE, June, 2022.

Ryan Sheatsley and Nicolas Papernot and Michael J. Weisman and Gunjan Verma and Patrick McDaniel, *Adversarial Examples for Network Intrusion Detection Systems*, Journal of Computer Security (JCS), IOS Press, January, 2022.

Quinn Burke and Patrick McDaniel and Thomas La Porta and Mingli Yu and Ting He, *Misreporting Attacks Against Load Balancers in Software-Defined Networking*, Mobile Networks and Applications, Springer, 2021.

Daniel E. Krych and Patrick McDaniel, *Exposing Android Social Applications: Linking Data Leakage to Privacy Policies*, Journal of Cyber Security Technology, Taylor & Francis, 5, 3-4, 2021.

Alejandro Andrade Salazar and Ryan Sheatsley and Jonathan Petit and Patrick McDaniel, *Physics-based Misbehavior Detection System for V2X Communications*, SAE International Journal of Connected and Automated Vehicles, SAE International, June, 2021.

Mingli Yu and Tian Xie and Ting He and Patrick McDaniel and Quinn Burke, *Flow Table Security in SDN: Adversarial Reconnaissance and Intelligent Attacks*, IEEE/ACM Transactions on Networking, 29, 6, 1063-6692, December, 2021.

Leonardo Babun and Kyle Denney and Z. Berkay Celik and Patrick McDaniel and Selcuk Uluagac, *A Survey on IoT Platforms: Communication, Security, and Privacy Perspectives*, Computer Networks, 192, 19, June, 2021.

Ryan Sheatsley and Matthew Durbin and Azaree Lintereur and Patrick McDaniel, *Improving Radioactive Material Localization by Leveraging Cyber-Security Model Optimizations*, IEEE Sensors, 21, 8, April, 2021.

Stefan Achleitner and Quinn Burke and Patrick McDaniel and Trent Jaeger and Thomas La Porta and Srikanth V. Krishnamurthy, *MLSNet: A Policy Complying Multilevel Security Framework for Software Defined Networking*, IEEE Transactions on Network and Service Management, 18, 1, March, 2021.

Dan Boneh and Andrew J. Grotto and Patrick McDaniel and Nicolas Papernot, *Preparing for the Age of Deepfakes and Disinformation*, Stanford HAI Policy Brief, 2020.

Dan Boneh and Andrew J. Grotto and Patrick McDaniel and Nicolas Papernot, *How Relevant Is the Turing Test in the Age of Sophisbots?*, IEEE Security & Privacy Magazine, 17, 64-71, Nov/Dec, 2019.

Z. Berkay Celik and Patrick McDaniel and Thomas Bowen, *Malware Modeling and Experimentation through Parameterized Behavior*, Journal of Defense Modeling and Simulation (JDMS), 15, 1, 31-48, 2017.

Z. Berkay Celik and Earlence Fernandes and Eric Pauley and Gang Tan and Patrick McDaniel, *Program Analysis of Commodity IoT Applications for Security and Privacy: Opportunities and Challenges*, ACM Computing

Surveys (CSUR), ACM, 42, 4, 2019.

Z. Berkay Celik and Patrick McDaniel and Gang Tan and Leonardo Babun and Selcuk Uluagac, *Verifying IoT Safety and Security in Physical Spaces*, IEEE Security & Privacy Magazine, IEEE, 17, 5, 30-37, 2019.

Ahmed Atya and Zhiyun Qian and Srikanth V. Krishnamurthy and Thomas La Porta and Patrick McDaniel and Lisa Marvel, *Catch Me if You Can: Malicious Co-Residency on the Cloud*, IEEE/ACM Transactions on Networking, 27, 2, April, 2019.

Ian Goodfellow and Patrick McDaniel and Nicolas Papernot, *Making machine learning robust against adversarial inputs*, Communications of the ACM, ACM, 61, 7, 56-6, June/July, 2018.

Dave Tian and Kevin Butler and Joseph Choi and Patrick McDaniel and Padma Krishnaswamy, *Securing ARP/NDP From the Ground Up*, IEEE Transactions on Information Forensics and Security, 12, 9, 2131-2143, April, 2017.

Stefan Achleitner and Thomas La Porta and Patrick McDaniel and Shridatt Sugrim and Srikanth V. Krishnamurthy and Ritu Chada, *Deceiving Network Reconnaissance Unsing SDN-based Virtual Topologies*, IEEE Transactions on Network and Service Management, Special Issue on Advances in Management of Softwarized Networks, 14, 4, July, 2017.

Chaz Lever and Robert Walls and Yacin Nadji and David Dagon and Patrick McDaniel and Manos Antonakakis, *Dawn of the Dead Domain: Measuring the Exploitation of Residual Trust in Domains*, IEEE Security & Privacy Magazine (Secure Systems issue column), April, 2017.

Patrick McDaniel and Nicolas Papernot and Z. Berkay Celik, *Machine Learning in Adversarial Settings*, IEEE Security & Privacy Magazine, 14, 3, May/June, 2016.

Patrick McDaniel and Ananthram Swami, *The Cyber Security Collaborative Research Alliance:Unifying Detection, Agility, and Risk in Mission-Oriented Cyber Decision Making*, CSIAC Journal, Army Research Laboratory (ARL) Cyber Science and Technology, 5, 1, January, 2017.

Damien Octeau and Daniel Luchaup and Somesh Jha and Patrick McDaniel, *Composite Constant Propagation and its Application to Android Program Analysis*, IEEE Transactions on Software Engineering, 42, 11, 999-1014, 2016.

Steven Arzt and Siegfried Rasthofer and Christian Fritz and Eric Bodden and Alexandre Bartel and Jacques Klein and Yves Le Traon and Damien Octeau and Patrick McDaniel, *FlowDroid: Precise Context, Flow, Field, Object-sensitive and Lifecycle-aware Taint Analysis for Android Apps*, ACM SIGPLAN Notices, 49, 6, 259-269, June, 2014.

Alexander Kott and Ananthram Swami and Patrick McDaniel, *Security Outlook: Six Cyber Game Changers for the Next 15 Years*, IEEE Computer, 47, 12, 104-106, 2014.

Zhenfu Cao and Keqiu Li and Xu Li and Patrick McDaniel and Radha Poovendran and Guojun Wang and Yang Xiang, *Guest Editors' Introduction: Special Issue on Trust, Security, and Privacy in Parallel and Distributed Systems*, IEEE Transactions on Parallel and Distributed Systems, 25, 2, 279-28, 2014.

Patrick McDaniel and Brian Rivera and Ananthram Swami, *Toward a Science of Secure Environments*, IEEE Security & Privacy Magazine, 12, 4, July/August, 2014.

William Enck and Peter Gilbert and Seungyeop Han and Vasant Tendulkar and Byung-Gon Chun and Landon Cox and Jaeyeon Jung and Patrick McDaniel and Anmol Sheth, *TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*, ACM Transactions on Computer Systems (TOCS), 32, 2, June, 2014.

William Enck and Peter Gilbert and Byung-Gon Chun and Landon Cox and Jaeyeon Jung and Patrick McDaniel and Anmol Sheth, *TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*, Communications of the ACM, 57, 3, March, 2014.

Machigar Ongtang and Stephen McLaughlin and William Enck and Patrick McDaniel, *Semantically Rich Application-Centric Security in Android*, Security and Communication Networks, 5, 6, 658-673, 2012.

Patrick McDaniel, *Bloatware Comes to the Smartphone*, IEEE Security & Privacy Magazine, 10, 4, July/August, 2011.

Thomas Moyer and Kevin Butler and Joshua Schiffman and Patrick McDaniel and Trent Jaeger, *Scalable Web Content Attestation*, IEEE Transactions on Computers, 61, 5, 686–699, April, 2011.

Patrick McDaniel, *Data Provenance and Security*, IEEE Security & Privacy Magazine, 9, 3, March/April, 2011.

Joshua Schiffman and Thomas Moyer and Trent Jaeger and Patrick McDaniel, *Network-based Root of Trust for Installation*, IEEE Security & Privacy Magazine, 40-48, Jan/Feb, 2011.

Kevin Butler and Stephen McLaughlin and Thomas Moyer and Patrick McDaniel, *New Security Architectures Based on Emerging Disk Functionality*, IEEE Security and Privacy Magazine, 8, 5, October, 2010.

Patrick McDaniel and William Enck, *Not So Great Expectations: Why Application Markets Haven't Failed Security*, IEEE Security & Privacy Magazine, 8, 5, 76–78, September/October, 2010.

Patrick Traynor and Chaitrali Amrutkar and Vikhyath Rao and Trent Jaeger and Patrick McDaniel and Thomas La Porta, *From Mobile Phones to Responsible Devices*, Journal of Security and Communication Networks (SCN), 4, 6, 719 – 726, June, 2011.

Patrick Traynor and Kevin Butler and William Enck and Kevin Borders and Patrick McDaniel, *malnets: Large-Scale Malicious Networks via Compromised Wireless Access Points*, Journal of Security and Communication Networks (SCN), 2, 3, 102-113, March, 2010.

Matthew Pirretti and Patrick Traynor and Patrick McDaniel and Brent Waters, *Secure Attribute-Based Systems*, Journal of Computer Security (JCS), 18, 5, 799–837, 2010.

Boniface Hicks and Sandra Rueda and Luke St. Clair and Trent Jaeger and Patrick McDaniel, *A Logical Specification and Analysis for SELinux MLS Policy*, ACM Transactions on Information and System Security (TISSEC), 13, 26, 2010.

Kevin Butler and Toni Farley and Patrick McDaniel and J. Rexford, *A Survey of BGP Security Issues and Solutions*, Proceedings of the IEEE, 2010, 1, 100-122, January, 2010.

Kevin Butler and Sunam Ryu and Patrick Traynor and Patrick McDaniel, *Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems*, IEEE Transactions on Parallel and Distributed Systems (TPDS), 20, 12, 1803-1815, December, 2009.

Patrick McDaniel and Stephen McLaughlin, *Security and Privacy Challenges in the Smart Grid*, IEEE Security & Privacy Magazine (Secure Systems issue column), 7, 3, 75-77, May/June, 2009.

Patrick Traynor and William Enck and Patrick McDaniel and Thomas La Porta, *Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks*, IEEE/ACM Transactions on Networking (TON), 17, 1, 40-53, February, 2009.

William Enck and Machigar Ongtang and Patrick McDaniel, *Understanding Android Security*, IEEE Security & Privacy Magazine, 7, 1, 50–57, January/February, 2009.

William Enck and Thomas Moyer and Patrick McDaniel and Shubho Sen and Panagiotis Sebos and Sylke Spoerel and Albert Greenberg and Yu-Wei Sung and Sanjay Rao and William Aiello, *Configuration Management at Massive Scale: System Design and Experience*, IEEE Journal on Selected Areas in Communications (JSAC), 27, 3, 323-335, 2009.

Heesook Choi and William Enck and Jaesheung Shin and Patrick McDaniel and Thomas La Porta, *ASR: Anonymous and Secure Reporting of Traffic Forwarding Activity in Mobile Ad Hoc Networks*, Wireless Networks (WINET), ACM/Kluwer, 15, 4, 525-539, May, 2009.

Patrick Traynor and William Enck and Patrick McDaniel and Thomas La Porta, *Exploiting Open Functionality in SMS-Capable Cellular Networks*, Journal of Computer Security, 16, 6, 713-742, Febraury, 2009.

Patrick Traynor and Michael Chien and Scott Weaver and Boniface Hicks and Patrick McDaniel, *Non-Invasive Methods for Host Certification*, ACM Transactions on Information and System Security (TISSEC), 11, 3, 2008.

Patrick McDaniel and Bashar Nuseibeh, *Guest Editorial: Special Issue on Software Engineering for Secure Systems*, IEEE Transactions on Software Engineering, 34, 1, 3–4, 2008.

Wesam Lootah and William Enck and Patrick McDaniel, *TARP: Ticket-based Address Resolution Protocol*, Computer Networks, Elsevier, 51, 15, 4322–4337, October, 2007.

Patrick McDaniel and Avi Rubin, *Guest Editoral: Special Issue on Web Security*, Computer Networks, Elsevier, 22, 2, 2005.

Patrick McDaniel and Atul Prakash, *Enforcing Provisioning and Authorization Policy in the Antigone System*, Journal of Computer Security, 14, 6, 483–511, November, 2006.

Patrick McDaniel and Atul Prakash, *Methods and Limitations of Security Policy Reconciliation*, ACM Transactions on Information and System Security (TISSEC), Association for Computing Machinery, 9, 3, 259-291, August, 2006.

Patrick McDaniel and William Aiello and Kevin Butler and JohnIoannidis, *Origin Authentication in Interdomain Routing*, Journal of Communication Networks, Elsevier, 50, 16, 2953-2980, November, 2006.

Matthew Pirretti and Sencun Zhu and VijaykrishnanNarayanan and Patrick McDaniel and Mahmut Kandemir and Richard Brooks, *The Sleep Deprivation Attack in Sensor Networks: Analysisand Methods of Defense*, International Journal of Distributed Sensor Networks, 2, 3, 267-287, June, 2005.

Simon Byers and Lorrie Cranor and Eric Cronin and DaveKormann and Patrick McDaniel, *Analysis of Security Vulnerabilities in the Movie Productionand Distribution Process*, Telecommunications Policy, 28, 8, 619-644, August, 2004.

Conference Publications

Blaine Hoak and Ryan Sheatsley and Patrick McDaniel, *Err on the Side of Texture: Texture Bias on Real Data*, IEEE Secure and Trustworthy Machine Learning Conference (SaTML 2025), IEEE, April, 2025. Copenhagen, Denmark.

Eric Pauley and Kyle Domico and Blaine Hoak and Ryan Sheatsley, Ryan and Quinn Burke and Yohan Beugin and Engin Kirda and Patrick McDaniel, *Secure IP Address Allocation at Cloud Scale*, 2025 Network and Distributed Systems Security Symposium (NDSS), Internet Society, February, 2025. San Diego, CA.

Quinn Burke and Ryan Sheatsley and Rachel King and Owen Hines and Michael Swift and Patrick McDaniel, *On Scalable Integrity Checking For Secure Cloud Disks*, 23rd USENIX Conference on File and Storage Technologies (FAST '25), USENIX Association, February, 2025.

Jiongxiao Wang and Jiazhao Li and Yiquan Li and Xiangyu Qi and Junjie Hu and Yixuan Li and Patrick McDaniel andMuhao Chen and Bo Li and Chaowei Xiao, *Mitigating Fine-tuning based Jailbreak Attack with Backdoor Enhanced Safety Alignment*, Proceedings of Conference on Neural Information Processing Systems (NeurIPS), December, 2024.

Yohan Beugin and Patrick McDaniel, *Interest-disclosing Mechanisms for Advertising are Privacy-Exposing (not Preserving)*, Proceedings on Privacy Enhancing Technologies (PETS), July, 2024. (**The Andreas Pfitzmann Best Student Paper Award (runner-up)**)

Blaine Hoak and Patrick McDaniel, *Explorations in Texture Learning*, 12th International Conference on Learning Representations, Tiny Papers Track (ICLR), May, 2024.

Tian Xie and Sanchal Thakkar and Ting He and Novella Bartolini and Patrick McDaniel, *Host-based Flow Table Size Inference in Multi-hop SDN*, Proceedings of the IEEE GLOBECOM, IEEE, December, 2023. Kuala Lumpur, Malaysia.

Eric Pauley and Paul Barford and Patrick McDaniel, *The CVE Wayback Machine: Measuring Coordinated Disclosure from Exploits Against Two Years of Zero-Days*, Proceedings of the ACM 2023 Internet Measurement Conference (IMC), October, 2023. Montreal, Canada. (**runner up-best paper award**)

Mingli Yu and Quinn Burke and Thomas La Porta and Patrick McDaniel, *mMLSnet: Multilevel Security Network With Mobility*, Proceedings of the Military Communications Conference (MILCOM), IEEE, October, 2023. Boston, MA.

Ryan Guide and Eric Pauley and Yohan Beugin and Ryan Sheatsley and Patrick McDaniel, *Characterizing the Modification Space of Signature IDS Rules*, MILCOM 2023 - 2023 IEEE Military Communications Conference (MILCOM), IEEE, October, 2023. Boston, MA.

Eric Pauley and Paul Barford and Patrick McDaniel, *DScope: A Cloud-Native Internet Telescope*, 32nd USENIX Security Symposium (USENIX Security 23), USENIX Association, August, 2023. Anaheim, CA.

Ryan Sheatsley and Blaine Hoak and Eric Pauley and Patrick McDaniel, *The Space of Adversarial Strategies*, 32nd USENIX Security Symposium (USENIX Security 23), USENIX Association, August, 2023.

Eric Pauley and Gang Tan and Danfeng Zhang and Patrick McDaniel, *Performant Binary Fuzzing without Source Code using Static Instrumentation*, Conference on Communications and Network Security (CNS), IEEE, October, 2022.

Patrick McDaniel, *Keynote Address: Sustainability is a Security Problem (extended abstract)*, Proceedings of the ACM Conference on Computer and Communications Security (CCS), ACM, November, 2022.

Kyle Domico and Ryan Sheatsley and Yohan Beugin and Quinn Burke and Patrick McDaniel, *A Machine Learning and Computer Vision Approach to Geomagnetic Storm Forecasting*, Machine Learning in Heliophysics (ML-Helio), AGU, November, 2022.

Tian Xie and Sanchal Thakkar and Ting He and Patrick Mcdaniel and Quinn Burke, *Joint Caching and Routing in Cache Networks with Arbitrary Topology*, Proceedings of the International Conference on Distributed Computing Systems (ICDCS), July, 2022.

Yohan Beugin and Quinn Burke and Blaine Hoak and Ryan Sheatsley and Eric Pauley and Gang Tan and Syed Rafiul Hussain and Patrick McDaniel, *Building a Privacy-Preserving Smart Camera System*, Proceedings on Privacy Enhancing Technologies (PETS), July, 2022.

Eric Pauley and Ryan Sheatsley and Blaine Hoak and Quinn Burke and Yohan Beugin and Patrick McDaniel, *Measuring and Mitigating the Risk of IP Reuse on Public Clouds*, 2022 IEEE Symposium on Security and Privacy

(IEEE S&P), IEEE, May, 2022. San Francisco, CA.

Ahmed Abdou and Ryan Sheatsley and Yohan Beugin and Tyler Shipp and Patrick McDaniel, *HoneyModels: Machine Learning Honeypots*, Proceedings of the Military Communications Conference (MILCOM), IEE, November, 2021.

Ryan Sheatsley and Blaine Hoak and Eric Pauley and Yohan Beugin and Michael J. Weisman and Patrick McDaniel, *On the Robustness of Domain Constraints*, Proceedings of the ACM Conference on Computer and Communications Security (CCS), ACM, November, 2021.

Tian Xie and Ting He and Patrick McDaniel and Namitha Nambiar, *Attack Resilience of Cache Replacement Policies*, IEEE International Conference on Computer Communications (INFOCOM), IEEE, May, 2021.

Adrien Cosson and Amit Kumar Sikder and Leonardo Babun and Z. Berkay Celik and Patrick McDaniel and Selcuk Uluagac, *Sentinel: A Robust Intrusion Detection System for IoT Networks Using Kernel-Level System Information*, In 6th ACM/IEEE Conference on Internet of Things Design and Implementation (IoTDI), April, 2021.

Matthew Durbin and Ryan Sheatlsey and Patrick McDaniel and Azaree Lintereur, *A Multi-Step Machine Learning Approach to Directional Gamma Ray Detection*, 2020 IEEE Nuclear Science Symposium and Medical Imaging Conference (NSS/MIC), October, 2020.

Sayed M. Saghaian and Thomas La Porta and Simone Silvestri and Patrick McDaniel, *Improving Robustness of a Popular Probabilistic Clustering Algorithm Against Insider Attacks*, International Conference on Security and Privacy in Communication Networks (SecureComm 2020), EAI, October, 2020.

Quinn Burke and Patrick McDaniel and Thomas La Porta and Mingli Yu and Ting He, *Misreporting Attacks in Software-Defined Networking*, International Conference on Security and Privacy in Communication Networks (SecureComm 2020), EAI, October, 2020.

Amit Kumar Sikder and Leonardo Babun and Z. Berkay Celik and Abbas Acar and Hidayet Aksu and Patrick McDaniel and Engin Kirda and Selcuk Uluagac, *KRATOS: Multi-User Multi-Device-Aware Access Control System for the Smart Home*, 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '20), ACM, July, 2020.

Mingli Yu and Ting He and Patrick McDaniel and Quinn Burke, *Flow Table Security in SDN: Adversarial Reconnaissance and Intelligent Attacks*, IEEE INFOCOM, IEEE Conference on Computer Communications, June, 2020. Beijing, China.

Michael Norris and Z. Berkay Celik and Prasanna Venkatesh and Shulin Zhao and Patrick McDaniel and Anand Sivasubramaniam and Gang Tan, *IoTRepair: Systematically addressing device faults in commodity IoT*, In 5th ACM/IEEE Conference on Internet of Things Design and Implementation (IoTDI), April, 2020.

Raquel Alvarez and Jake Levenson and Ryan Sheatsley and Patrick McDaniel, *Application Transiency: Towards a Fair Trade of Personal Information for Application Services*, Proceedings of the EAI Conference on Security and Privacy in Communication Networks (SecureComm), October, 2019. Orlando, FL.

Giuseppe Petracca and Yuqiong Sun and Ahmad-Atamli Reineh and Jens Grossklags and Patrick McDaniel and Trent Jaeger, *EnTrust: Regulating Sensor Access by Cooperating Programs via Delegation Graphs*, Proceedings of the 28th USENIX Security Symposium, Augus, 2019. Santa Clara, CA.

Matthew Durbin and Ryan Sheatsley and Christopher Balbier and Tristan Grieve and Patrick McDaniel and Azaree Lintereur, *Development of Machine Learning Algorithms for Directional Gamma Ray Detection*, Proceedings of the Institute of Nuclear Materials Management Annual Meeting (INMM), July, 2019. Palm Desert, CA. (**J. D. Williams student paper award, Nuclear Security and Physical Protection division**)

Z. Berkay Celik and Abbas Acar and Hidayet Aksu and Abbas Acar and Ryan Sheatsley and Selcuk Uluagac and Patrick McDaniel, *Curie: Policy-based Secure Data Exchange*, ACM Conference on Data and Applications Security (CODASPY), March, 2019. Dallas, TX.

Z. Berkay Celik and Gang Tan and Patrick McDaniel, *IoTGuard: Dynamic Enforcement of Security and Safety Policy in Commodity IoT*, Network and Distributed System Security Symposium (NDSS), February, 2019. San Diego, CA.

Dang Tu Nguyen and Chengyu Song and Zhiyun Qian and Srikanth V. Krishnamurthy and Edward J. M. Colbert and Patrick McDaniel, *IoTSan: Fortifying the Safety of IoT Systems*, Proceedings of the 14th International Conference on emerging Networking EXperiments and Technologies (CoNEXT '18), December, 2018.

Z. Berkay Celik and Leonardo Babun and Amit Kumar Sikder and Hidayet Aksu and Gang Tan and Patrick McDaniel and Selcuk Uluagac, *Sensitive Information Tracking in Commodity IoT*, Proceedings of the 27th USENIX Security Symposium, August, 2018. Baltimore, MD.

Rauf Izmailov and Shridatt Sugrim and Ritu Chadha and Patrick McDaniel and Ananthram Swami, *Enablers Of Adversarial Attacks in Machine Learning*, Proceedings of the Military Communications Conference (MILCOM), IEEE, October, 2018.

Sayed M. Saghaian and Thomas La Porta and Trent Jaeger and Z. Berkay Celik and Patrick McDaniel, *Mission-oriented Security Model, Incorporating Security Risk, Cost and Payout*, Proceedings of EAI SECURECOMM 2018, August, 2018. (**best paper award**)

Z. Berkay Celik and Patrick McDaniel and Gang Tan, *Soteria: Automated IoT Safety and Security Analysis*, USENIX Annual Technical Conference (USENIX ATC), July, 2018. Boston, MA.

Z. Berkay Celik and Patrick McDaniel and Rauf Izmailov and Nicolas Papernot and Ryan Sheatsley and Raquel Alvarez and Ananthram Swami, *Detection under Privileged Information*, ACM Asia Conference on Computer and Communications Security (ASIACCS), June, 2018.

Florian Tramer and Alexey Kurakin and Nicolas Papernot and Ian Goodfellow and Dan Boneh and Patrick McDaniel, *Ensemble Adversarial Training: Attacks and Defenses*, International Conference on Learning Representations (ICLR), 2018. Vancouver, Canada.

Nicolas Papernot and Patrick McDaniel and Arunesh Sinha and Michael Wellman, *SoK: Security and Privacy in Machine Learning*, Security and Privacy (EuroS&P), 2018 IEEE European Symposium on on Security and Privacy (EuroS&P), IEEE, April, 2018. London, UK.

Chun-Ming Lai and Xiaoyun Wang and Yunfeng Hong and Yu-Cheng Lin and Felix Wu and Patrick McDaniel and Hasan Cam, *Attacking Strategies and Temporal Analysis Involving Facebook Discussion Groups*, 13th IEEE International Conference on Network and Service Management, November, 2017. Tokyo, Japan.

Kathrin Grosse and Nicolas Papernot and Praveen Manoharan and Michael Backes and Patrick McDaniel, *Adversarial Examples for Malware Detection*, 22nd European Symposium on Research in Computer Security (ESORICS '17), September, 2017. Oslo, Norway.

Z. Berkay Celik and David Lopez-Paz and Patrick McDaniel, *Patient-Driven Privacy Control through Generalized Distillation*, Proceedings of the Privacy-Aware Computing (PAC), IEEE, 2017.

Abbas Acar and Z. Berkay Celik and Hidayet Aksu and Selcuk Uluagac and Patrick McDaniel, *Achieving Secure and Differentially Private Computations in Multiparty Settings*, Proceedings of the Privacy-Aware Computing (PAC), IEEE, 2017.

Vaibhav Rastogi and Drew Davidson and Lorenzo De Carli and Somesh Jha and Patrick McDaniel, *Cimplifier: Automatically Debloating Containers*, 11Th Joint Meeting of the European Software Engineering Conference and

the Acm Sigsoft Symposium on the Foundations of Software Engineering, September, 2017. Paderborn, Germany.

Yunfeng Hong and Yongjian Hu and Chun-Ming Lai and Felix Wu and Iulian Neamtiu and Yu Paul and Patrick McDaniel and Hasan Cam and Gail-Joon Ahn, *Defining and Detecting Environment Discrimination in Android Apps*, The 13th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 17), October, 2017.

Nicolas Papernot and Patrick McDaniel and Ian Goodfellow and Somesh Jha and Z. Berkay Celik and Ananthram Swami, *Practical Black-Box Attacks against Machine Learning*, ACM Asia Conference on Computer and Communications Security (ASIACCS) 2017, April, 2017.

Stefan Achleitner and Thomas La Porta and Trent Jaeger and Patrick McDaniel, *Adversarial Network Forensics in Software Defined Networking*, ACM Symposium on SDN Research (SOSR), ACM, April, 2017. (**best student paper award**)

Stefan Achleitner and Thomas La Porta and Patrick McDaniel and Srikanth V. Krishnamurthy and Alexander Poylisher and Constantin Serban, *Stealth Migration: Hiding Virtual Machines on the Network*, IEEE International Conference on Computer Communications (INFOCOM), IEEE, 2017.

Ahmed Atya and Zhiyun Qian and Srikanth V. Krishnamurthy and Thomas La Porta and Patrick McDaniel and Lisa Marvel, *Malicious Co-Residency on the Cloud: Attacks and Defense*, IEEE International Conference on Computer Communications (INFOCOM), IEEE, 2017.

Nathaniel Lageman and Eric Kilmer and Robert Walls and Patrick McDaniel, *BinDNN: Resilient Function Matching Using Deep Learning*, 2016 International Conference on Security and Privacy in Communication Networks (SECURECOMM), October, 2016.

Z. Berkay Celik and Nan Hu and Yun Li and Nicolas Papernot and Patrick McDaniel and Jeff Rowe and Robert Walls and Karl Levitt and Novella Bartolini and Thomas La Porta and Ritu Chadha, *Mapping Sample Scenarios to Operational Models*, Proceedings of the Military Communications Conference (MILCOM), IEEE, 2016.

Nicolas Papernot and Patrick McDaniel and Ananthram Swami and Richard Harang, *Crafting Adversarial Input Sequences for Recurrent Neural Networks*, Proceedings of the Military Communications Conference (MILCOM), IEEE, 2016.

Michael Backes and Sven Bugiel and Erik Derr and Patrick McDaniel and Damien Octeau and Sebastian Weisgerber, *On Demystifying the Android Application Framework: Re-Visiting Android Permission Specification Analysis*, Proceedings of the 25th USENIX Security Symposium, August, 2016.

Devin Pohly and Patrick McDaniel, *Modeling Privacy and Tradeoffs in Multichannel Secret Sharing Protocols*, 46th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), June, 2016.

Chaz Lever and Robert Walls and Yacin Nadji and David Dagon and Patrick McDaniel and Manos Antonakakis, *Domain-Z: 28 Registrations Later*, Proceedings of the 37th IEEE Symposium on Security and Privacy, May, 2016. San Francisco, CA.

Yasemin Acar and Michael Backes and Sven Bugiel and Sascha Fahl and Patrick McDaniel and Matthew Smith, *SoK: Lessons Learned From Android Security Research For Appified Software Platforms*, Proceedings of the 37th IEEE Symposium on Security and Privacy, May, 2016. San Francisco, CA.

Nicolas Papernot and Patrick McDaniel and Xi Wu and Somesh Jha and Ananthram Swami, *Distillation as a Defense to Adversarial Perturbations Against Deep Neural Networks*, Proceedings of the 37th IEEE Symposium on Security and Privacy, May, 2016. San Francisco, CA.

Charles Huber and Scott Brown and Patrick McDaniel and Lisa Marvel, *Cyber Fighter Associate: A Decision Support System for Cyber Agility*, Proceedings of the 50th Annual Conference on Information Sciences and Sys-

tems (CISS), March, 2016. Princeton, NJ.

Nicolas Papernot and Patrick McDaniel and Somesh Jha and Matthew Fredrikson and Z. Berkay Celik and Ananthram Swami, *The Limitations of Deep Learning in Adversarial Settings*, Proceedings of the 1st IEEE European Symposium on Security and Privacy, IEEE, 2016. Saarbrucken, Germany.

Damien Octeau and Somesh Jha and Matthew Dering and Patrick McDaniel and Alexandre Bartel and Li Li and Jacques Klein and Yves Le Traon, *Combining Static Analysis with Probabilistic Models to Enable Market-Scale Android Inter-Component Analysis*, Proceedings of the 43rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL), January, 2016. St. Petersburg, Florida, USA.

Devin Pohly and Patrick McDaniel, *MICSS: A Realistic Multichannel Secrecy Protocol*, IEEE Global Communications Conference (GLOBECOM), December, 2015. San Diego, CA.

Robert Walls and Eric Kilmer and Nathaniel Lageman and Patrick McDaniel, *Measuring the Impact and Perception of Acceptable Advertisements*, Proceedings of the ACM 2015 Internet Measurement Conference (IMC), October, 2015. Tokyo, Japan.

Nicolas Papernot and Patrick McDaniel and Robert Walls, *Enforcing Agile Access Control Policies in Relational Databases using Views*, Proceedings of the Military Communications Conference (MILCOM), October, 2015. Tampa, FL.

Alessandro Oltramari and Lorrie Cranor and Robert Walls and Patrick McDaniel, *Computational Ontology of Network Operations*, Proceedings of the Military Communications Conference (MILCOM), October, 2015. Tampa, FL.

Z. Berkay Celik and Robert Walls and Patrick McDaniel and Ananthram Swami, *Malware Traffic Detection using Tamper Resistant Features*, Proceedings of the Military Communications Conference (MILCOM), October, 2015. Tampa, FL.

Devin Pohly and Charles Sestito and Patrick McDaniel, *Adaptive Protocol Switching Using Dynamically Insertable Bumps in the Stack*, Proceedings of the Military Communications Conference (MILCOM), October, 2015. Tampa, FL.

Azeem Aqil and Ahmed Atya and Trent Jaeger and Srikanth V. Krishnamurthy and Karl Levitt and Patrick McDaniel and Jeff Rowe and Ananthram Swami, *Detection of Stealthy TCP-based DoS Attacks*, Proceedings of the Military Communications Conference (MILCOM), October, 2015. Tampa, FL.

Daniel E. Krych and Stephen Lange-Maney and Patrick McDaniel and William Glodek, *Investigating Weaknesses in Android Certificate Security*, SPIE 9478, Modeling and Simulation for Defense Systems and Applications X, May, 2015.

Damien Octeau and Daniel Luchaup and Matthew Dering and Somesh Jha and Patrick McDaniel, *Composite Constant Propagation: Application to Android Inter-Component Communication Analysis*, Proceedings of the 37th International Conference on Software Engineering (ICSE), May, 2015. Florence, Italy.

Li Li and Alexandre Bartel and Tegawende Bissyande and Jacques Klein and Yves Le Traon and Steven Arzt and Siegfried Rasthofer and Eric Bodden and Damien Octeau and Patrick McDaniel, *IccTA: Detecting Inter-Component Privacy Leaks in Android Apps*, Proceedings of the 37th International Conference on Software Engineering (ICSE), May, 2015. Florence, Italy.

Jing Tian and Kevin Butler and Patrick McDaniel and Padma Krishnaswamy, *Securing ARP From the Ground Up*, CODASPY '15: Proceedings of the 5th ACM Conference on Data Application and Security and Privacy, March, 2015. San Antonio, TX, USA.

Alessandro Oltramari and Lorrie Cranor and Robert Walls and Patrick McDaniel, *Building an Ontology of Cyber Security*, Proc. Intl. Conference on Semantic Technologies for Intelligence, Defense, and Security (STIDS), November, 2014.

Matthew Dering and Patrick McDaniel, *Android Market Reconstruction and Analysis*, Proceedings of the Military Communications Conference (MILCOM), October, 2014. Baltimore, MD.

Wenhui Hu and Damien Octeau and Patrick McDaniel and Peng Liu, *Duet: Library Integrity Verification for Android Applications*, Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), July, 2014. Oxford, United Kingdom.

Steven Arzt and Siegfried Rasthofer and Christian Fritz and Eric Bodden and Alexandre Bartel and Jacques Klein and Yves Le Traon and Damien Octeau and Patrick McDaniel, *FlowDroid: Precise Context, Flow, Field, Object-sensitive and Lifecycle-aware Taint Analysis for Android Apps*, Proceedings of the 35th Conference on Programming Language Design and Implementation (PLDI), June, 2014. Edinburgh, UK.

Phillip Koshy and Diana Koshy and Patrick McDaniel, *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*, Proceedings of Financial Cryptography 2014, International Financial Cryptography Association (IFCA), February, 2014. Christ Church, Barbado.

Stephen McLaughlin and Devin Pohly and Patrick McDaniel and Saman Zonouz, *A Trusted Safety Verifier for Process Controller Code*, Proc. ISOC Network and Distributed Systems Security Symposium (NDSS), February, 2014. San Diego, CA.

Damien Octeau and Patrick McDaniel and Somesh Jha and Alexandre Bartel and Eric Bodden and Jacques Klein and Yves Le Traon, *Effective Inter-Component Communication Mapping in Android with Epicc: An Essential Step Towards Holistic Security Analysis*, Proceedings of the 22th USENIX Security Symposium, August, 2013. Washington, DC.

Devin J. Pohly and Stephen McLaughlin and Patrick McDaniel and Kevin Butler, *Hi-Fi: Collecting High-Fidelity Whole-System Provenance*, Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC), December, 2012. Orlando, Florida.

Stephen McLaughlin and Patrick McDaniel, *SABOT: Specification-based Payload Generation for Programmable Logic Controllers*, 19th ACM Conference on Computer and Communications Security (CCS), October, 2012.

Weining Yang and Ninghui Li and Yuan Qi and Wahbeh Qardaji and Stephen McLaughlin and Patrick McDaniel, *Minimizing Private Data Disclosures in the Smart Grid*, 19th ACM Conference on Computer and Communications Security (CCS), October, 2012.

Eun Kyoung Kim and Patrick McDaniel and Thomas La Porta, *A Detection Mechanism for SMS Flooding Attacks in Cellular Networks*, Proceedings of the 8th International Conference on Security and Privacy in Communication Networks (SECURECOMM 2012), September, 2012. Padua, Italy.

Damien Octeau and Somesh Jha and Patrick McDaniel, *Retargeting Android Applications to Java Bytecode*, 20th International Symposium on the Foundations of Software Engineering (FSE), November, 2012. Research Triangle Park, NC. (**best artifact award**)

Thomas Moyer and Trent Jaeger and Patrick McDaniel, *Scalable Integrity-Guaranteed AJAX*, Proceedings of the 14th Asia-Pacific Web Conference (APWeb), April, 2012. Kunming, China. (*Invited Paper*)

Patrick McDaniel and Stephen McLaughlin, *Structured Security Testing in the Smartgrid*, Proceedings of 5th International Symposium on Communications, Control, and Signal Processing, May, 2012. Rome, Italy. (*Invited Paper*)

Stephen McLaughlin and Patrick McDaniel and William Aiello, *Protecting Consumer Privacy from Electric Load Monitoring*, The 18th ACM Conference on Computer and Communications Security (CCS), October, 2011. Chicago, IL.

William Enck and Damien Octeau and Patrick McDaniel and Swarat Chaudhuri, *A Study of Android Application Security*, Proceedings of the 20th USENIX Security Symposium, August, 2011. San Francisco, CA.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Kells: A Protection Framework for Portable Data*, Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC), December, 2010. Austin, TX.

Stephen McLaughlin and Dmitry Podkuiko and Adam Delozier and Sergei Miadzvezhanka and Patrick McDaniel, *Multi-vendor Penetration Testing in the Advanced Metering Infrastructure*, Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC), December, 2010. Austin, TX.

Machigar Ongtang and Kevin Butler and Patrick McDaniel, *Porscha: Policy Oriented Secure Content Handling in Android*, Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC), December, 2010. Austin, TX.

Patrick Traynor and Joshua Schiffman and Thomas La Porta and Patrick McDaniel and Abhrajit Ghosh and Farooq Anjum, *Constructing Secure Localization Systems with Adjustable Granularity*, IEEE Global Communications Conference (GLOBECOM), December, 2010. Miami, FL.

William Enck and Peter Gilbert and Byung-Gon Chun and Landon Cox and Jaeyeon Jung and Patrick McDaniel and Anmol Sheth, *TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*, Proceedings of the 9th USENIX Symposium on Operating Systems Design and Implementation (OSDI), October, 2010. Vancouver, BC.

Toby Ehrenkranz and Jun Li and Patrick McDaniel, *Realizing A Source Authentic Internet*, Proceedings of the 6th International ICST Conference on Security and Privacy in Communications Networks (Securecomm), September, 2010. Singapore.

Boniface Hicks and Sandra Rueda and David King and Thomas Moyer and Joshua Schiffman and Yogesh Sreenivasan and Patrick McDaniel and Trent Jaeger, *An Architecture for Enforcing End-to-End Access Control over Web Applications*, Proceedings of the Fifteenth ACM Symposium on Access Control Models and Technologies (SACMAT 2010), 163-172, June, 2010. Pittsburgh, PA.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Disk-Enabled Authenticated Encryption*, Proceedings of the 26th IEEE Symposium on Massive Storage Systems and Technologies (MSST), May, 2010.

Machigar Ongtang and Stephen McLaughlin and William Enck and Patrick McDaniel, *Semantically Rich Application-Centric Security in Android*, Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC), 340-349, December, 2009. Honolulu, Hawaii. (**best paper**)

Thomas Moyer and Kevin Butler and Joshua Schiffman and Patrick McDaniel and Trent Jaeger, *Scalable Asynchronous Web Content Attestation*, Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC), 95-104, December, 2009. Honolulu, Hawaii.

Joshua Schiffman and Thomas Moyer and Christopher Shal and Trent Jaeger and Patrick McDaniel, *Justifying Integrity Using a Virtual Machine Verifier*, Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC), 83-92, December, 2009. Honolulu, Hawai.

William Enck and Machigar Ongtang and Patrick McDaniel, *On Lightweight Mobile Phone App Certification*, Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS), 235-245, November, 2009.

Patrick Traynor and Michael Lin and Machigar Ongtang and Vikhyath Rao and Trent Jaeger and Thomas La Porta and Patrick McDaniel, *On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core*, Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS), 223-234, November, 2009.

William Enck and Patrick McDaniel and Trent Jaeger, *PinUP: Pinning User Files to Known Applications*, Proceedings of the 24th Annual Computer Security Applications Conference (ACSAC), December, 2008.

William Enck and Kevin Butler and Thomas Richardson and Patrick McDaniel and Adam Smith, *Defending Against Attacks on Main Memory Persistence*, Proceedings of the 24th Annual Computer Security Applications Conference (ACSAC), December, 2008.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Rootkit-Resistant Disks*, Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS), November, 2008. Alexandria, VA.

Patrick Traynor and Kevin Butler and William Enck and Patrick McDaniel, *Realizing Massive-Scale Conditional Access Systems Through Attribute-Based Cryptosystems*, ISOC Network & Distributed System Security Symposium (NDSS), February, 2008. San Diego, CA.

Luke St. Clair and Joshua Schiffman and Trent Jaeger and Patrick McDaniel, *Establishing and Sustaining System Integrity via Root of Trust Installation*, 23rd Annual Computer Security Applications Conference (ACSAC), 19-29, December, 2007. Miami, FL.

Boniface Hicks and Tim Misiak and Patrick McDaniel, *Channels: Runtime System Infrastructure for Security-typed Languages*, 23rd Annual Computer Security Applications Conference (ACSAC), 443-452, December, 2007. Miami, FL.

Dhananjay Bapat and Kevin Butler and Patrick McDaniel, *Towards Automated Privilege Separation*, Proceedings of 2nd International Conference onInformation Systems Security (short paper), December, 2007. Delhi, India.

Lisa Johansen and Kevin Butler and Michael Rowell and Patrick McDaniel, *Email Communities of Interest*, Fourth Conference on Email and Anti-Spam (CEAS 2007, August, 2007. Mountain View, California.

Patrick Traynor and Patrick McDaniel and Thomas La Porta, *On Attack Causality in Internet-Connected Cellular Networks*, Proceedings of the 16th USENIX Security Symposium, 1–16, August, 2007. Boston, MA.

Boniface Hicks and Sandra Rueda and Trent Jaeger and Patrick McDaniel, *From Trusted to Secure: Building and Executing Applications that Enforce System Security*, Proceedings of the USENIX Annual Technical Conference, June, 2007. Santa Clara, CA.

William Enck and Patrick McDaniel and Shubho Sen and Panagiotis Sebos and Sylke Spoerel and Albert Greenberg and Sanjay Rao and William Aiello, *Configuration Management at Massive Scale: System Design and Experience*, Proceedings of the USENIX Annual Technical Conference, June, 2007. Santa Clara, CA.

Boniface Hicks and Sandra Rueda and Luke St. Clair and Trent Jaeger and Patrick McDaniel, *A Logical Specification and Analysis for SELinux MLS*, 12th ACM Symposium on Access Control Models andTechnologies (SACMAT), ACM, June, 2007. Sophia Antipolis, France.

Anusha Sriraman and Kevin Butler and Patrick McDaniel and Padma Raghavan, *Analysis of IPv4 Address Space Delegation Structure*, 12th IEEE Symposium on Computers and Communications (ISCC), July, 2007. Aveiro, Portugal.

Heesook Choi and Thomas La Porta and Patrick McDaniel, *Privacy Preserving Communication in MANETs*, Proceedings of Fourth Annual IEEE CommunicationsSociety Conference on Sensor, Mesh, and Ad Hoc Communications andNetworks (SECON 07), June, 2007. San Diego, CA.

Sophie Qiu and Patrick McDaniel and Fabian Monrose, *Toward Valley-Free Inter-domain Routing*, Proceedings of 2007 IEEE International Conference onCommunications (ICC 2007), June, 2007. Glasgow, Scottlan.

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

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

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

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

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

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

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

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

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

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

Patrick McDaniel and Shubho Sen and Oliver Spatscheck andJacobus Van der Merwe and William Aiello and Charles Kalmanek, *Enterprise Security: A Community of Interest Based Approach*, Proceedings of Network and Distributed Systems Security2006 (NDSS), February, 2006. San Diego, CA.

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

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

William Enck and Patrick Traynor and Patrick McDaniel andThomas La Porta, *Exploiting Open Functionality in SMS-Capable Cellular Networks*, Proceedings of the 12th ACM Conference on Computer and Communication-

sSecurity (CCS), 393–404, May, 2005. Alexandria, VA.

Matthew Pirretti and Sencun Zhu and VijaykrishnanNarayanan and Patrick McDaniel and Mahmut Kandemir and Richard Brooks, *The Sleep Deprivation Attack in Sensor Networks: Analysisand Methods of Defense*, Proceedings of the Innovations and CommercialApplications of Distributed Sensor Networks Symposi, October, 2005. Bethesda, Maryland. (**best paper**)

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

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

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

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

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

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

Geoff Goodell and William Aiello and Tim Griffin and John Ioannidis and Patrick McDaniel and Avi Rubin, *Working Around BGP: An Incremental Approach to ImprovingSecurity and Accuracy of Interdomain Routing*, Proceedings of Network and Distributed Systems Security2003 (NDSS), Internet Society, 75-8, February, 2003. San Diego, CA.

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

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

Hugh Harney and Andrea Colegrove and Patrick McDaniel, *Principles of Policy in Secure Groups*, Proceedings of Network and Distributed Systems Security2001 (NDSS), Internet Society, 125-13, February, 2001. San Diego, CA.

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

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

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

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

Workshop Papers

Yujin Nam and Rachel King and Quinn Burke and Minxuan Zhou and Patrick McDaniel and Tajana Rosing, *Efficient Host Intrusion Detection using Hyperdimensional Computing*, Proceedings of the 2024 IEEE International Conference on Big Data workshop Cyber Threat Intelligence and Hunting, IEEE, December, 2024.

Rachel King and Quinn Burke and Yohan Beugin and Blaine Hoak and Kunyang Li and Eric Pauley and Ryan Sheatsley and Patrick McDaniel, *ParTEETor: A System for Partial Deployments of TEEs within Tor*, Proceedings of the 23rd Workshop on Privacy in the Electronic Society (WPES), ACM, October, 2024. Salt Lake City, UT, USA.

Yohan Beugin and Patrick McDaniel, *A Public and Reproducible Assessment of the Topics API on Real Data*, SecWeb 2024 Workshop, IEEE Security and Privacy Workshops (SPW), May, 2024.

Kunyang Li and Kyle Domico and Jean-Charles Noirot Ferrand and Patrick McDaniel, *The Efficacy of Transformer-Based Adversarial Attacks in Security Domains*, Workshop on Artificial Intelligence for Cyber (MILCOM 2023, October, 2023. Boston, MA.

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

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

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

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

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

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

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

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

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

Patrick McDaniel and Trent Jaeger and Thomas La Porta and Nicolas Papernot and Robert Walls and Alexander Kott and Lisa Marvel and Ananthram Swami and Prasant Mohapatra and Srikanth V. Krishnamurthy and

Iulian Neamtiu, *Security and Science of Agility*, First ACM Workshop on Moving Target Defense (MTD 2014), November, 2014. Scottsdale, AZ.

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

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

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

Thomas La Porta and Patrick McDaniel and Karl Rauscher and Jun Shu, *The Impact of Supply Chain on Information and Communications Technology Security*, In the 1st Workshop on Workshop on Telecommunications Infrastructure Protection and Security, December, 2009. Honolulu, Hawaii.

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

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

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

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

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

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

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

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

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

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

Vancouver, B.C., Canada.

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

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

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

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

William Aiello and Charles Kalmanek and Patrick McDaniel andShubho Sen and Oliver Spatscheck and Jacobus Van der Merwe, *Analysis of Communities Of Interest in Data Networks*, Passive and Active Measurement Workshop 2005, March, 2005. Boston, M.

Simon Byers and Lorrie Cranor and David Kormann andPatrick McDaniel, *Searching for Privacy: Design and Implementation of aP3P-Enabled Search Engine*, Proceedings of 2004 Workshop on Privacy EnhancingTechnologies (PETS), May, 2004. Toronto, Canad.

Hao Wang and Somesh Jha and Patrick McDaniel and MironLivn, *Security Policy Reconciliation in Distributed ComputingEnvironments*, Proceedings of 5th International Workshop on Policiesfor Distributed Systems and Networks (Policy 2004), IEEE Computer Society Press, 137-146, June, 2004. Yorktown Heights, N.

Simon Byers and Lorrie Cranor and Eric Cronin and DaveKormann and Patrick McDaniel, *Analysis of Security Vulnerabilities in the Movie Productionand Distribution Process*, Proceedings of 2003 ACM Workshop on Digital RightsManagement, ACM, October, 2003. Washington, DC, also appeared in Telecommunications PolicyResearch Conference – September 2003.

Patents

U.S. Patent No. 7,873,350, Patrick McDaniel and Martin Strauss, *End-to-end secure wireless communication for requesting a more secure channel*, January, 2011.

U.S. Patent No. 7,975,044, Oliver Spatscheck and Subhabrata Sen and Jacobus Van der Merwe and Patrick McDaniel, *Automated disambiguation of fixed-serverport-based applications from ephemeral applications*, July, 2011.

U.S. Patent No. 8,175,580, Patrick McDaniel and Martin Strauss, *End-to-end secure wireless communication for requesting a more secure channel*, May, 2012.

U.S. Patent No. 8,453,227, William Aiello and Charles Kalmanek and William Leighton III and Patrick McDaniel and Subhabrata Sen and Oliver Spatscheck and Jacobus Van der Merwe, *Reverse firewall with self-provisioning*, May, 2013.

U.S. Patent No. 8,732,293, Patrick McDaniel and Subhabrata Sen and Oliver Spatscheck and Jacobus Van der Merwe, *System and method for tracking individuals on a data network using communities of interest*, May, 2014.

U.S. Patent No. 8,813,213, William Aiello and Charles Kalmanek and William Leighton III and Patrick McDaniel and Subhabrata Sen and Oliver Spatscheck and Jacobus Van der Merwe, *Reverse firewall with self-provisioning*, August, 2014.

Other Publications

Patrick McDaniel and Farinaz Koushanfar, *NSF Secure and Trustworthy Computing 2.0 Vision Statement*, Public Report, August, 2023.

Patrick McDaniel and Thorsten Holz and Indra Spiecker and Genannt Dohmann and Christopher Burchard and Ahmad-Reza Sadeghi and Konrad Rieck and Kamalika Chaudhuri and Somesh Jha and Andrea Matwyshyn and David Evans and Felix Freiling and Amy Hasan, *Cybersecurity and Machine Learning: Vision Document, Report on the joint NSF/DFG Cybersecurity and Machine Learning Research Workshop*, Public Report, National Science Foundation/Deutsche Forschungsgemeinschaf, December, 2021.

Patrick McDaniel and John Launchbury, *Artificial Intelligence and Cybersecurity: Opportunities and Challenges 2019 Technical Workshop Report*, Public Report, Networking and Information Technology Research and Development Subcommittee, Machine Learning and Artificial Intelligence Subcommittee, and the Special Cyber Operations Research and Engineering Subcommittee of the National Science and Technology Council, 2020.

Patrick McDaniel and Avi Rubin, *Conference Proceedings*, 2008 IEEE Symposium on Security and Privacy, IEEE, May, 2008. Oakland, CA.

Patrick McDaniel and Kevin Butler and William Enck and Harri Hursti and Stephen McLaughlin and Patrick Traynor and Matthew Blaze and Adam Aviv and Pavol Cerny and Sandy Clark and Eric Cronin and Gaurav Shah and Micah Sherr and Giovanni Vigna and Richard Kemmerer and David Balzarotti and Greg Banks and Marco Cova and Viktoria Felmetsger and William Robertson and Fredrik Valeur and Joseph Lorenzo Hall and Laura Quilter, *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing*, Ohio Secretary of State, Public Report, 2007.

Patrick McDaniel and Shyam K. Gupta, *Conference Proceedings*, The Third International Conference Information Systems Security, Springer, December, 2007. Delhi, India.

Birgit Pfitzmann and Patrick McDaniel, *Conference Proceedings*, 2007 IEEE Symposium on Security and Privacy, IEEE, May, 2007. Oakland, CA.

Patrick McDaniel, *Conference Proceedings*, The 14th USENIX Security Symposium, USENIX, August, 2005. Baltimore, MD.

Patrick McDaniel, *Policy Evolution: Autonomic Environmental Security*, Software Engineering Research Center Showcase, USA, December, 2004.

Hugh Harney and Uri Meth and Andrea Colegrove and AngelaSchuett and Patrick McDaniel and Gavin Kenny and HaithamCruickshank and Sunil Iyengar, *GSAKMP (Draft)*, Internet Research Task Force, August, 2003.

Patrick McDaniel and Atul Prakash, *A Flexible Architecture for Security Policy Enforcement*, Proceedings of DARPA Information SurvivabilityConference and Exposition III, Research Summaries, 234-239, April, 2003.

Jim Irrer and Atul Prakash and Patrick McDaniel, *Antigone: Policy-Based Secure Group Communications Systems and AMirD: Antigone-Based Secure File Mirroring System*, Proceedings of DARPA Information SurvivabilityConference and Exposition III, Demo Summaries, 44-4, April, 2003.

Patrick McDaniel and Sugih Jamin, *Windowed Key Revocation in Public Key Infrastructures*, NASA Tech Briefs, 55, August, 2002.

Patrick McDaniel and Atul Prakash, *Antigone Secure Group Communication System*, NASA Tech Briefs, 2001.

Patrick McDaniel, *Policy Management in Secure Group Communication*, PhD Thesis, University of Michigan, Ann Arbor, MI, August, 2001.

Patrick McDaniel and Hugh Harney and Andrea Colegrove andAtul Prakash and Peter Dinsmore, *Multicast Security Policy Requirements and Building Blocks(Draft)*, Internet Research Task Force, Secure MulticastResearch Group (SMuG), November, 2000.

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

Patrick McDaniel and Hugh Harney and Peter Dinsmore and Atul Prakash, *Multicast Security Policy (Draft)*, Internet Research Task Force, Secure MulticastResearch Group (SMuG), June, 2000.

Patrick McDaniel, *8th USENIX Security Symposium Conference Summaries,Potpourri Session*, USENIX Login Magazine, 9-12, November, 1999.

Patrick McDaniel, *The Analysis of D_i, a Detailed Design Metric on LargeScale Software*, Masters Thesis, Ball State University, Muncie, IN, June, 1991.

Technical Reports

Blaine Hoak and Patrick McDaniel, *On Synthetic Texture Datasets: Challenges, Creation, and Curation*, Technical Report 2409.10297 cs.CV, arXiv preprint, 2024.

Rachel King and Quinn Burke and Yohan Beugin and Blaine Hoak and Kunyang Li and Eric Pauley and Ryan Sheatsley and Patrick McDaniel, *ParTEETor: A System for Partial Deployments of TEEs within Tor*, Technical Report 2408.14646, arXiv preprint, August, 2024.

Quinn Burke and Ryan Sheatsley and Rachel King and Michael Swift and Patrick McDaniel, *Cloud Storage Integrity at Scale: A Case for Dynamic Hash Trees*, Technical Report 2405.03830, arXiv preprint, May, 2024.

Alban Héon and Ryan Sheatsley and Quinn Burke and Blaine Hoak and Eric Pauley and Yohan Beugin and Patrick McDaniel, *Systematic Evaluation of Geolocation Privacy Mechanisms*, Technical Report 2309.06263, arXiv preprint, September, 2023.

Yohan Beugin and Patrick McDaniel, *Interest-disclosing Mechanisms for Advertising are Privacy-Exposing (Not Preserving)*, Technical Report 2306.03825, arXiv preprint, May, 2023.

Quinn Burke and Yohan Beugin and Blaine Hoak and Rachel King and Eric Pauley and Ryan Sheatsley and Mingli Yu and Ting He and Thomas La Porta and Patrick McDaniel, *Securing Cloud File Systems using Shielded Execution*, Technical Report 2305.18639, arXiv preprint, May, 2023.

Yohan Beugin and Quinn Burke and Blaine Hoak and Ryan Sheatsley and Eric Pauley and Gang Tan and Syed Rafiul Hussain and Patrick McDaniel, *Privacy-Preserving Protocols for Smart Cameras and Other IoT Devices*, Technical Report 2208.09776, arXiv preprint, August, 2022.

Pauley, Eric and Domico, Kyle and Hoak, Blaine and Sheatsley, Ryan and Burke, Quinn and Beugin, Yohan and McDaniel, Patrick, *EIPSIM: Modeling Secure IP Address Allocation at Cloud Scale*, Technical Report arXiv:2210.14999, arXiv preprint, 2022.

Bolor-Erdene Zolbayarn and Ryan Sheatsley and Patrick McDaniel and Michael J. Weisman and Sencun Zhu and Shitong Zhu and Srikanth V. Krishnamurthy, *Generating Practical Adversarial Network Traffic Flows using NIDSGAN*, Technical Report arXiv:2203.06694, arXiv preprint, March, 2022.

Ryan Sheatsley and Blaine Hoak and Eric Pauley and Yohan Beugin and Michael J. Weisman and Patrick McDaniel, *On the Robustness of Domain Constraints*, Technical Report arXiv:2105.08619, arXiv preprint, 2021.

Ryan Sheatsley and Nicolas Papernot and Michael J. Weisman and Gunjan Verma and Patrick McDaniel, *Adversarial Examples in Constrained Domains*, Technical Report arXiv:2011.01183, arXiv preprint, 2020.

Stefan Achleitner and Quinn Burke and Patrick McDaniel and Trent Jaeger and Thomas La Porta and Srikanth V. Krishnamurthy, *MLSNet: A Policy Complying Multilevel Security Framework for Software Defined Networking*, Technical Report INSR-500-TR-0500-2019, Institute of Networking and Security Research, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, January, 2019.

Michael Norris and Z. Berkay Celik and Patrick McDaniel and Gang Tan and Prasanna Venkatesh and Shulin Zhao and Anand Sivasubramaniam, *IoTRepair: Systematically Addressing Device Faults in Commodity IoT (Extended Paper)*, Technical Report arXiv:2002.07641, arXiv preprint, 2020.

Amit Kumar Sikder and Leonardo Babun and Z. Berkay Celik and Abbas Acar and Hidayet Aksu and Patrick McDaniel and Engin Kirda and Selcuk Uluagac, *KRATOS: Multi-User Multi-Device-Aware Access Control System for the Smart Home*, Technical Report arXiv:1911.10186, arXiv preprint, 2020.

Leonardo Babun and Z. Berkay Celik and Patrick McDaniel and Selcuk Uluagac, *Real-time Analysis of Privacy-(un)aware IoT Applications*, Technical Report arXiv:1911.10461, arXiv preprint, 2019.

Dan Boneh and Andrew J. Grotto and Patrick McDaniel and Nicolas Papernot, *How Relevant is the Turing Test in the Age of Sophisbots?*, Technical Report arXiv:1909.00056, arXiv preprint, 2019.

Chun-Ming Lai and Xiaoyun Wang and Jon W. Chapman and Yu-Cheng Lin and Yu-Chang Ho and Felix Wu and Patrick McDaniel and Hasan Cam, *More or Less? Predict the Social Influence of Malicious URLs on Social Media*, Technical Report arXiv:1812.02978, arXiv preprint, 2018.

Dang Tu Nguyen and Chengyu Song and Zhiyun Qian and Srikanth V. Krishnamurthy and Edward J. M. Colbert and Patrick McDaniel, *IoTSan: Fortifying the Safety of IoT Systems*, Technical Report arXiv:1810.09551, arXiv preprint, 2018.

Z. Berkay Celik and Earlence Fernandes and Eric Pauley and Gang Tan and Patrick McDaniel, *Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities*, Technical Report arXiv:1809.06962, arXiv preprint, 2018.

Giuseppe Petracca and Jens Grossklags and Patrick McDaniel and Trent Jaeger, *Regulating Access to System Sensors in Cooperating Programs*, Technical Report arXiv:1808.05579, arXiv preprint, 2018.

Z. Berkay Celik and Patrick McDaniel and Gang Tan, *Soteria: Automated IoT Safety and Security Analysis*, Technical Report arXiv:1805.08876, arXiv preprint, 2018.

Nicolas Papernot and Patrick McDaniel, *Deep k-Nearest Neighbors: Towards Confident, Interpretable and Robust Deep Learning*, Technical Report arXiv:1803.04765, arXiv preprint, 2018.

Z. Berkay Celik and Leonardo Babun and Amit Kumar Sikder and Hidayet Aksu and Gang Tan and Patrick McDaniel and Selcuk Uluagac, *Sensitive Information Tracking in Commodity IoT*, Technical Report arXiv:1802.08307, arXiv preprint, 2018.

Chun-Ming Lai and Xiaoyun Wang and Yunfeng Hong and Yu-Cheng Lin and Felix Wu and Patrick McDaniel and Hasan Cam, *Attacking Strategies and Temporal Analysis Involving Facebook Discussion Groups*, Technical Report arXiv:1802.04500, arXiv preprint, 2017.

Abbas Acar and Z. Berkay Celik and Hidayet Aksu and Selcuk Uluagac and Patrick McDaniel, *Achieving Secure and Differentially Private Computations in Multiparty Settings*, Technical Report arXiv:1707.01871, arXiv preprint, 2017.

Florian Tramer and Alexey Kurakin and Nicolas Papernot and Ian Goodfellow and Dan Boneh and Patrick McDaniel, *Ensemble Adversarial Training: Attacks and Defenses*, Technical Report arXiv:1705.07204, arXiv preprint, 2017.

Nicolas Papernot and Patrick McDaniel, *Extending Defensive Distillation*, Technical Report arXiv:1705.05264, arXiv preprint, 2017.

Florian Tramer and Nicolas Papernot and Ian Goodfellow and Dan Boneh and Patrick McDaniel, *The Space of Transferable Adversarial Examples*, Technical Report arXiv:1704.03453, arXiv preprint, 2017.

Z. Berkay Celik and Hidayet Aksu and Abbas Acar and Ryan Sheatsley and Selcuk Uluagac and Patrick McDaniel, *Curie: Policy-based Secure Data Exchange*, Technical Report arXiv:1702.08342, arXiv preprint, 2017.

Kathrin Grosse and Praveen Manoharan and Nicolas Papernot and Michael Backes and Patrick McDaniel, *On the (Statistical) Detection of Adversarial Examples*, Technical Report arXiv:1702.06280, arXiv preprint, 2017.

Z. Berkay Celik and David Lopez-Paz and Patrick McDaniel, *Patient-Driven Privacy Control through Generalized Distillation*, Technical Report arXiv:1611.08648, arXiv preprint, 2017.

Nicolas Papernot and Patrick McDaniel and Arunesh Sinha and Michael Wellman, *Towards the Science of Security and Privacy in Machine Learning*, Technical Report arXiv:1611.03814, arXiv preprint, 2016.

Nicolas Papernot and Ian Goodfellow and Ryan Sheatsley and Reuben Feinman and Patrick McDaniel, *cleverhans v1.0.0: an adversarial machine learning library*, Technical Report arXiv:1610.0076, arXiv preprint, 2016.

Nicolas Papernot and Patrick McDaniel, *On the Effectiveness of Defensive Distillation*, Technical Report arXiv:1607.05113, arXiv preprint, 2016.

Kathrin Grosse and Nicolas Papernot and Praveen Manoharan and Michael Backes and Patrick McDaniel, *Adversarial Perturbations Against Deep Neural Networks for Malware Classification*, Technical Report arXiv:1606.04435, arXiv preprint, 2016.

Nicolas Papernot and Patrick McDaniel and Ian Goodfellow, *Transferability in Machine Learning: from Phenomena to Black-Box Attacks using Adversarial Samples*, Technical Report arXiv:1605.07277, arXiv preprint, 2016.

Nicolas Papernot and Patrick McDaniel and Ananthram Swami and Richard Harang, *Crafting Adversarial Input Sequences for Recurrent Neural Networks*, Technical Report arXiv:1604.08275, arXiv preprint, 2016.

Z. Berkay Celik and Patrick McDaniel and Rauf Izmailov and Nicolas Papernot and Ryan Sheatsley and Raquel Alvarez and Ananthram Swami, *Detection under Privileged Information*, Technical Report arXiv:1603.09638, arXiv preprint, 2016.

Vaibhav Rastogi and Drew Davidson and Lorenzo De Carli and Somesh Jha and Patrick McDaniel, *Towards Least Privilege Containers with Cimplifier*, Technical Report arXiv:1602.08410, arXiv preprint, 2016.

Nicolas Papernot and Patrick McDaniel and Ian Goodfellow and Somesh Jha and Z. Berkay Celik and Ananthram Swami, *Practical Black-Box Attacks against Machine Learning*, Technical Report arXiv:1602.02697, arXiv preprint, 2016.

Nicolas Papernot and Patrick McDaniel and Somesh Jha and Matthew Fredrikson and Z. Berkay Celik and Ananthram Swami, *The Limitations of Deep Learning in Adversarial Settings*, Technical Report arXiv:1511.07528, arXiv preprint, 2015.

Nicolas Papernot and Patrick McDaniel and Xi Wu and Somesh Jha and Ananthram Swami, *Distillation as a Defense to Adversarial Perturbations against Deep Neural Networks*, Technical Report arXiv:1511.04508, arXiv

preprint, 2015.

Alexander Kott and Ananthram Swami and Patrick McDaniel, *Six Potential Game-Changers in Cyber Security: Towards Priorities in Cyber Science and Engineering*, Technical Report arXiv:1511.00509, arXiv preprint, 2015.

Li Li and Alexandre Bartel and Jacques Klein and Yves Le Traon and Steven Arzt and Siegfried Rasthofer and Eric Bodden and Damien Octeau and Patrick McDaniel, *I know what leaked in your pocket: uncovering privacy leaks on Android Apps with Static Taint Analysis*, Technical Report arXiv:1404.7431, arXiv preprint, 2014.

Devin Pohly and Patrick McDaniel, *Modeling Privacy and Tradeoffs in Multichannel Secret Sharing Protocols*, Technical Report NAS-TR-0188-2016, Institute of Networking and Security Research, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, January, 2016.

Nicolas Papernot and Patrick McDaniel and Somesh Jha and Matthew Fredrikson and Z. Berkay Celik and Ananthram Swami, *The Limitations of Deep Learning in Adversarial Settings*, Technical Report NAS-TR-0172-2014, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, October, 2016.

Wenhui Hu and Damien Octeau and Patrick McDaniel and Peng Liu, *Duet: Library Integrity Verification for Android Applications*, Technical Report NAS-TR-0172-2014, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2016.

Devin Pohly and Stephen McLaughlin and Patrick McDaniel and Kevin Butler, *Hi-Fi: Collecting High-Fidelity Whole-System Provenance*, Technical Report NAS-TR-0160-2012, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2016.

Damien Octeau and Somesh Jha and Patrick McDaniel, *Retargeting Android Applications to Java Bytecode*, Technical Report NAS-TR-0150-2011, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, September, 2011.

Stephen McLaughlin and Patrick McDaniel, *Protecting Consumer Privacy from Electric Load Monitoring*, Technical Report NAS-TR-0147-2011, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, March, 2011.

William Enck and Patrick McDaniel, *Federated Information Flow Control for Mobile Phones*, Technical Report NAS-TR-0136-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, July, 2010.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Kells: A Protection Framework for Portable Data*, Technical Report NAS-TR-0134-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2010.

Stephen McLaughlin and Dmitry Podkuiko and Adam Delozier and Sergei Miadzvezhanka and Patrick McDaniel, *Multi-vendor Penetration Testing in the Advanced Metering Infrastructure*, Technical Report NAS-TR-0133-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2010.

Machigar Ongtang and Kevin Butler and Patrick McDaniel, *Porscha: Policy Oriented Secure Content Handling in Android* , Technical Report NAS-TR-0132-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2010.

Joshua Schiffman and Thomas Moyer and Hayawardh Vijayakumar and Trent Jaeger and Patrick McDaniel, *Seeding Clouds with Trust Anchors*, Technical Report NAS-TR-0127-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, April, 2010.

William Enck and Machigar Ongtang and Patrick McDaniel, *TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*, Technical Report NAS-TR-0120-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2010.

Joshua Schiffman and Thomas Moyer and Christopher Shal and Trent Jaeger and Patrick McDaniel, *Justifying Integrity Using a Virtual Machine Verifier*, Technical Report NAS-TR-0119-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, August, 2010.

Machigar Ongtang and Stephen McLaughlin and William Enck and Patrick McDaniel, *Semantically Rich Application-Centric Security in Android*, Technical Report NAS-TR-0116-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2010.

Stephen McLaughlin and Dmitry Podkuiko and Patrick McDaniel, *Energy Theft in the Advanced Metering Infrastructure*, Technical Report NAS-TR-0115-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2010.

Kevin Butler and Stephen McLaughlin and Thomas Moyer and Joshua Schiffman and Patrick McDaniel and Trent Jaeger, *Firma: Disk-Based Foundations for Trusted Operating Systems*, Technical Report NAS-TR-0114-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, April, 2010.

William Enck and Machigar Ongtang and Patrick McDaniel, *On Lightweight Mobile Phone App Certification*, Technical Report NAS-TR-0113-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, April, 2010.

Patrick Traynor and Michael Lin and Machigar Ongtang and Vikhyath Rao and Thomas La Porta and Patrick McDaniel, *On Cellular Botnets: Measuring the Impact of Malicious Devices on the Network Core*, Technical Report NAS-TR-0110-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, March, 2010.

Boniface Hicks and Sandra Rueda and Yogesh Sreenivasan and Guruprasad Jakka and David King and Trent Jaeger and Patrick McDaniel, *An Architecture for Enforcing End-to-End Security Over Web Applications*, Technical Report NAS-TR-0104-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, January, 2009.

Joshua Schiffman and Thomas Moyer and Christopher Shal and Trent Jaeger and Patrick McDaniel, *No Node Is an Island: Shamon Integrity Monitoring Approach*, Technical Report NAS-TR-0103-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2009.

Patrick Traynor and Michael Lin and Machigar Ongtang and Vikhyath Rao and Trent Jaeger and Thomas La Porta and Patrick McDaniel, *On Cellular Botnets: Measuring the Impact of Malicious Devices on the Network Core*, Technical Report NAS-TR-0099-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, Novemeber, 2008.

Kevin Butler and Stephen McLaughlin and Thomas Moyer and Patrick McDaniel and Trent Jaeger, *SwitchBlade: Policy-Driven Disk Segmentation*, Technical Report NAS-TR-0098-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, November, 2008.

Thomas Moyer and Kevin Butler and Joshua Schiffman and Patrick McDaniel and Trent Jaeger, *Scalable Asynchronous Web Content Attestation*, Technical Report NAS-TR-0095-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA,

September, 2008.

William Enck and Machigar Ongtang and Patrick McDaniel, *Automated Cellphone Application Certification in Android (or) Mitigating Phone Software Misuse Before It Happens*, Technical Report NAS-TR-0094-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, September, 2008.

Boniface Hicks and Sandra Rueda and Luke St. Clair and Trent Jaeger and Patrick McDaniel, *A Logical Specification and Analysis for SELinux MLS Policy*, Technical Report NAS-TR-0091-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, July, 2008.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Rootkit-Resistant Disks*, Technical Report NAS-TR-0089-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, April, 2008.

Patrick Traynor and Joshua Schiffman and Thomas La Porta and Patrick McDaniel and Abhrajit Ghosh and Farooq Anjum, *Constructing Secure Localization Systems with Adjustable Granularity*, Technical Report NAS-TR-0084-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, December, 2007.

Stephen McLaughlin and Kevin Butler and William Enck and Patrick McDaniel, *Genbd - A Generic Block Device*, Technical Report NAS-TR-0082-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, November, 2007.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Non-Volatile Memory and Disks: Avenues for Policy Architectures*, Technical Report NAS-TR-0074-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, June, 2007.

William Enck and Sandra Rueda and Joshua Schiffman and Yogesh Sreenivasan and Luke St. Clair and Trent Jaeger and Patrick McDaniel, *Protecting Users From "Themselves"*, Technical Report NAS-TR-0073-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, June, 2007.

Dhananjay Bapat and Kevin Butler and Patrick McDaniel, *Towards Automated Privilege Separation*, Technical Report NAS-TR-0071-2007, Network and Security Research Center, Department of Computer Science and Engineering,Pennslyvania State University, University Park, PA, USA, May, 2007.

Patrick Traynor and Kevin Butler and William Enck and Patrick McDaniel, *Realizing Massive-Scale Conditional Access Systems Through Attribute-Based Cryptosystems*, Technical Report NAS-TR-0070-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, May, 2007.

Luke St. Clair and Joshua Schiffman and Trent Jaeger andPatrick McDaniel, *Establishing and Sustaining System Integrity viaRoot of Trust Installation*, Technical Report NAS-TR-0067-2007, Network and Security Research Center, Department of Computer Science and Engineering,Pennslyvania State University, University Park, PA, USA, April, 2007.

Boniface Hicks and David King and Patrick McDaniel, *Jifclipse: Development Tools for Security-Typed Language*, Technical Report NAS-TR-0065-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, April, 2007.

William Enck and Patrick McDaniel and Trent Jaeger, *Protecting User Files by Reducing Application Access*, Technical Report NAS-TR-0063-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2007.

Boniface Hicks and Sandra Rueda and Trent Jaeger andPatrick McDaniel, *A Logical Specification and Analysis for SELinux MLSPolicy*, Technical Report NAS-TR-0058-2007, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, January, 2007.

Boniface Hicks and Sandra Rueda and Trent Jaeger andPatrick McDaniel, *From Trusted to Secure: Building and ExecutingApplications that Enforce System Security*, Technical Report NAS-TR-0061-2007, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, January, 2007.

Lisa Johansen and Kevin Butler and William Enck andPatrick Traynor and Patrick McDaniel, *Grains of SANs: Building Storage Area Networks fromMemory Spots*, Technical Report NAS-TR-0060-2007, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, January, 2007.

Patrick Traynor and Vikhyath Rao and Trent Jaeger andPatrick McDaniel and Thomas La Porta, *From Mobile Phones to Responsible Devices*, Technical Report NAS-TR-0059-2007, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, January, 2007.

Anusha Sriraman and Kevin Butler and Patrick McDaniel andPadma Raghavan, *Analysis of the IPv4 Address Space Delegation Structure*, Technical Report NAS-TR-0057-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, December, 2006.

Luke St. Clair and Joshua Schiffman and Trent Jaeger andPatrick McDaniel, *Sum of the Parts: Composing Trust from Validation Primitives*, Technical Report NAS-TR-0056-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, November, 2006.

Sophie Qiu and Patrick McDaniel and Fabian Monrose, *Toward Valley-Free Inter-domain Routing*, Technical Report NAS-TR-0054-2006, Network and Security Research Center, Department of Computer Science and Engineeering, Pennsylvania State University, University Park, PA, USA, October, 2006.

Boniface Hicks and Sandra Rueda and Trent Jaeger andPatrick McDaniel, *Integrating SELinux with Security-typed Languages*, Technical Report NAS-TR-0052-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, October, 2006.

Patrick Traynor and William Enck and Patrick McDaniel andThomas La Porta, *Mitigating Attacks on Open Functionality in SMS-CapableNetworks*, Technical Report NAS-TR-0051-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, October, 2006.

Patrick Traynor and Kevin Butler and William Enck and Kevin Borders and Patrick McDaniel, malnets*: Large-Scale Malicious Networks via Compromised Wireless Access Points*, Technical Report NAS-TR-0048-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, September, 2006.

Boniface Hicks and Sandra Rueda and Trent Jaeger and Patrick McDaniel, *Breaking Down the Walls of Mutual Distrust: Security-typed Email Using Labeled IPsec*, Technical Report NAS-TR-0049-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, September, 2006.

Sunam Ryu and Kevin Butler and Patrick Traynor and Patrick McDaniel, *Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems*, Technical Report NAS-TR-0043-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, August, 2006.

Wesam Lootah and William Enck and Patrick McDaniel, *TARP: Ticket-based Address Resolution Protocol (extended version)*, Technical Report NAS-TR-0046-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, August, 2006.

Patrick McDaniel, *Understanding Equivalance in High-Level and Information Flow Policy*, Technical Report NAS-TR-0042-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, July, 2006.

Trent Jaeger and Patrick McDaniel and Luke St. Clair and Ramon Caceres and Reiner Sailer, *Shame on Trust in Distributed Systems*, Technical Report RC239664 (W0605-129), IBM Research Division, Yorktown Heights, NY, May, 2006.

Lisa Johansen and Kevin Butler and Michael Rowell and Patrick McDaniel, *Email Communities of Interest*, Technical Report NAS-TR-0040-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, May, 2006.

Boniface Hicks and Kiyan Ahmadizadeh and Patrick McDaniel, *From Languages to Systems: Understanding PracticalApplication Development in Security-typed Languages*, Technical Report NAS-TR-0035-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, April, 2006.

Boniface Hicks and David King and Patrick McDaniel andMichael Hicks, *Trusted Declassification: High-level policy for asecurity-typed language*, Technical Report NAS-TR-0033-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, March, 2006.

Matthew Pirretti and Patrick Traynor and PatrickMcDaniel and Brent Waters, *Secure Attribute-Based Systems*, Technical Report NAS-TR-0028-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, February, 2006.

William Enck and Kevin Butler and Thomas Richardson andPatrick McDaniel, *Securing Non-Volatile Main Memory*, Technical Report NAS-TR-0029-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, February, 2006.

Luke St. Clair and Lisa Johansen and William Enck andMatthew Pirretti and Patrick Traynor and Patrick McDaniel andTrent Jaeger, *Password Exhaustion: Predicting the End of Password Usefulness*, Technical Report NAS-TR-0030-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2006.

Heesook Choi and Patrick McDaniel and Thomas La Porta, *Privacy Preserving Communication in MANETs*, Technical Report NAS-TR-0031-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, December, 2005.

Matthew Pirretti and Vijaykrishnan Narayanan and PatrickMcDaniel and Bharat Madan, *SLAT: Secure Localization with Attack Tolerance*, Technical Report NAS-TR-0024-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, August, 2005.

Patrick Traynor and Michael Chien and Scott Weaver andBoniface Hicks and Patrick McDaniel, *Non-Invasive Methods for Host Certification*, Technical Report NAS-TR-0025-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, September, 2005.

Sophie Qiu and Patrick McDaniel and Fabian Monrose andAvi Rubin, *Characterizing Address Use Structure and Stabillity ofOrigin Advertizement in Interdomain Routing*, Technical Report NAS-TR-0018-2005, Network

and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, July, 2005.

Hosam Rowaihy and William Enck and Patrick McDaniel andThomas La Porta, *Limiting Sybil Attacks in Structured Peer-to-Peer Networks*, Technical Report NAS-TR-0017-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, July, 2005.

Boniface Hicks and Patrick McDaniel and Ali Hurson, *Information Flow Control in Database Security: A CaseStudy for Secure Programming with Jif*, Technical Report NAS-TR-0011-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, Uni versity Park, PA, USA, April, 2005.

Wesam Lootah and William Enck and Patrick McDaniel, *TARP: Ticket-Based Address Resolution Protocol*, Technical Report NAS-TR-0010-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, June, 2005.

Patrick Traynor and Kevin Butler and William Enck andJennifer Plasterr and Scott Weaver and John van Bramer and PatrickMcDaniel, *Privacy-Preserving Web-Based Email*, Technical Report NAS-TR-0009-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, June, 2005.

William Enck and Patrick Traynor and Patrick McDaniel andThomas La Porta, *Exploiting Open Functionality in SMS-Capable Cellular Networks*, Technical Report NAS-TR-0007-2005, Network and Security Center, Department of Computer Science, Pennsylvania State University, May, 2005.

Boniface Hicks and David King and Patrick McDaniel, *Declassification with Cryptographic Functions in aSecurity-Typed Language*, Technical Report NAS-TR-0004-2005, Network and Security Center, Department of Computer Science, Pennsylvania State University, January, 2005.

William Aiello and Kevin Butler and Patrick McDaniel, *Path Authentication in Interdomain Routing*, Technical Report TR NAS-TR-0002-2004, Network and Security Center, Department of Computer Science and Engineering, Penn State University, November, 2004.

Dan Pei and William Aiello and Anna Gilbert and PatrickMcDaniel, *Origin Disturbances in BGP*, Technical Report TD-62TJJF8, AT&T Labs - Research, Florham Park, NJ, July, 2004.

Kevin Butler and Toni Farley and Patrick McDaniel andJennifer Rexford, *A Survey of BGP Security Issues and Solutions*, Technical Report TD-5UGJ33, AT&T Labs - Research, Florham Park, NJ, February, 2004.

Patrick McDaniel and Atul Prakash, *Securing Distributed Applications Using a Policy-based Approach*, Technical Report TD-5UDKVD, AT&T Labs - Research, Florham Park, NJ, December, 2003.

William Aiello and John Ioannidis and Patrick McDaniel, *Origin Authentication in Interdomain Routing*, Technical Report TD-5QHG2G, AT&T Labs - Research, Florham Park, NJ, August, 2003.

Eric Cronin and Sugih Jamin and Tal Malkin and PatrickMcDaniel, *On the Performance, Feasibility, and Use of Forward SecureSignatures*, Technical Report TD-5QHGBK, AT&T Labs - Research, Florham Park, NJ, August, 2003.

Simon Byers and Lorrie Cranor and Eric Cronin and DaveKormann and Patrick McDaniel, *Analysis of Security Vulnerabilities in the Movie Productionand Distribution Process*, Technical Report TD-5N6SJ4, AT&T Labs - Research, Florham Park, NJ, August, 2003.

Patrick McDaniel, *On Context in Authorization Policy*, Technical Report TD-5JCJCK, AT&T Labs - Research, Florham Park, NJ, January, 2003.

Patrick McDaniel and Atul Prakash, *An Architecture for Security Policy Enforcement*, Technical Report TD-5C6JFV, AT&T Labs - Research, Florham Park, NJ, July, 2002.

Patrick McDaniel and Atul Prakash, *Methods and Limitations of Security Policy Reconciliation*, Technical Report TD57-PAW, AT&T Labs - Research, Florham Park, NJ, February, 2002.

Patrick McDaniel and Atul Prakash, *Ismene: Provisioning and Policy Reconciliation in SecureGroup Communication*, Technical Report CSE-TR-438-00, Electrical Engineering and Computer Science, Universityof Michigan, December, 2000.

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

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

Patrick McDaniel and Sugih Jamin, *Windowed Certificate Revocation*, Technical Report CSE-TR-413-99, Electrical Engineering and Computer Science, Universityof Michigan, November, 1999.

Patrick McDaniel and Atul Prakash and Peter Honeyman, *Antigone: A Flexible Framework for Secure Group Communication*, Technical Report 99-2, Center for Information Technology Integration, September, 1999.

Patrick McDaniel and Avi Rubin, *A Response to "Can We Eliminate Certificate RevocationLists?"*, Technical Report 99.8.1, AT&T Labs - Research, Florham Park, NJ, August, 1999.

Andrew Adamson and Charles J. Antonelli and Kevin Coffman andPatrick McDaniel and Jim Rees, *Secure Distributed Virtual Conferencing: Multicast orBust*, Technical Report 99-1, Center for Information Technology Integration, January, 1999.

Patrick McDaniel and Sugih Jamin, *Windowed Key Revocation in Public Key Infrastructures*, Technical Report CSE-TR-376-98, Electrical Engineering and Computer Science, Universityof Michigan, , 1998.

Patrick McDaniel and Sugih Jamin, *A Scalable Key Distribution Hierarchy*, Technical Report CSE-TR-366-98, Electrical Engineering and Computer Science, Universityof Michigan, , 1998.

Patrick McDaniel and Peter Honeyman and Atul Prakash, *Lightweight Secure Group Communication*, Technical Report 98-2, Center for Information Technology Integration,University of Michigan, April, 1998.

Wayne Zage and Delores Zage and Patrick McDaniel and IrshadKhan, *Evaluating Design Metrics on Large-Scale Software*, Technical Report SERC-TR-106-P, Software Engineering Resource Center, PurdueUniversity, September, 1991.

PUBLIC SPEAKING

Adversarial Machine Learning: A 10-year Perspective, NSF ACTION AI Institute Distinguished Lecture Series, Virtual, December, 2024.

Adversarial Machine Learning: A 10-year Perspective, University of Illinois, Champaign-Urbana, Champaign, IL, November, 2024.

Security and its Role in Achieving Sustainability, Workshop on the Architecture of Green Energy Systems: The Underlying Problem and Its Challenge, Institute for Mathematical and Statistical Innovation, University of Chicago, Chicago, IL, June, 2024.

The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, University of California, Los Angeles, Los Angeles, CA, December, 2023.

The Security of AI (what organizations need to know), TEDxUWMadison, Madison, WI, November, 2023.

The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, Michigan State University, Lansing, MI, November, 2023.

The Security of AI (what organizations need to know), Greater Madison Chamber of Commerce, Madison, WI, September, 2023.

Security's Role in Achieving Sustainability, Center for Sustainability and the Global Environment, Madison, WI, February, 2023.

Security's Role in Achieving Sustainability, 29th ACM Conference on Computer and Communications Security (CCS), Los Angeles, CA, November, 2022.

Security, Game Theory, and Their Role in Achieving Sustainability, Conference on Decision and Game Theory for Security, Pittsburgh, PA, October, 2022.

NSF Funding: Why, What and How, School of Computer, Data & Information Sciences, UW-Madison, Madison, WI, October, 2022.

Prognosticating the Future of IoT Security, 2022 IEEE SafeThings Workshop, San Francisco, CA, May, 2022.

The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, Temple University, Philadelphia, PA, March, 2022.

The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, CACR Security Speaker Series, Indiana University, Online, August, 2021.

The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, Robustness of AI Systems to Adversarial Attacks (RAISA3), Online, August, 2020.

The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, Computer Science Department, University of Wisconsin-Madison, Madison, WI, February, 2020.

The Challenges of Machine Learning in Adversarial Settings, Computer Science Department, Stonybrook University, Stonybrook, NY, December, 2019.

The Challenges of Machine Learning in Adversarial Settings, Cylab Security and Privacy Institute, Carnegie Mellon University, Pittsburgh, PA, December, 2019.

The Challenges of Machine Learning in Adversarial Settings, S2ERC, Ball State University, Muncie, IN, November, 2019.

The Challenges of Machine Learning in Adversarial Settings, Triangle Area Privacy and Security Day, Durham, NC, October, 2019.

AI-Cybersecurity Workshop Briefing to the NITRD and MLAI Subcommittees, NITRD and MLAI Subcommittees Quarterly Meeting, Washington, DC, July, 2019.

Workshop on the Security and Privacy of Machine Learning, Workshop on the Security and Privacy of Machine Learning, International Conference on Machine Learning, Long Beach, CA, June, 2019.

The Challenges of Machine Learning in Adversarial Settings, 2019 Subversion and Assurance of AI Workshop, US National Reconnaissance Office, Washington, DC, March, 2019.

The Challenges of Machine Learning in Adversarial Settings, National Science Foundation, Alexandria, VA, March, 2019.

Convergence of AI and IoT, Intelligence Community Studies Board, Division on Engineering and Physical Sciences, The National Academy of Sciences/Engineering, Washington, DC, February, 2019.

Tracing the Arc of Smartphone Application Security, Duke University, Durham, NC, February, 2019.

The Challenges of Machine Learning in Adversarial Settings, Department of Computer Science, University at Buffalo, Buffalo, NY, November, 2018.

The Challenges of Machine Learning in Adversarial Settings, Department of Computer Science, Purdue University, West Lafeyette, Indiana, November, 2018.

The Challenges of Machine Learning in Adversarial Settings, Computer Science Department, Indiana University of Pennsylvania, Indiana, PA, October, 2018.

The Challenges of Machine Learning in Adversarial Settings, Penn State University Alumni Association, University Park, PA, September, 2018.

The Challenges of Machine Learning in Adversarial Settings, Department of Software and Information Systems, University of North Carolina at Charlotte, Charlotte, NC, February, 2018.

Tracing the Arc of Smartphone Application Security, School of Electrical and Computer Engineering, Georgia Tech University, Atlanta, GA, December, 2017.

Tracing the Arc of Smartphone Application Security, Department of Electrical Engineering and Computer Science, Ohio University, Athens, OH, October, 2017.

Attacks, Defenses, and Impacts of Machine Learning in Adversarial Settings, 2017 Conference on Security and Privacy in Communication Networks (SecureComm), Niagara Falls, Canada, October, 2017.

Attacks, Defenses, and Impacts of Machine Learning in Adversarial Settings, Celebrating 50 Years of Computer Science @ NC State, North Carolina State University, Raleigh, NC, October, 2017.

Tracing the Arc of Smartphone Application Security, Computer Science Department and the Electrical and Computer Engineering Department Seminar Series, Colorado State University, Fort Collins, CO, October, 2017.

Tracing the Arc of Smartphone Application Security, Rochester Institute of Technology, College of Computing and Information Sciences, Rochester, NY, September, 2017.

Tracing the Arc of Smartphone Application Security, University of Texas-Dallas, Department of Computer Science, Dallas, TX, May, 2017.

Tracing the Arc of Smartphone Application Security, 2017 ACM on International Workshop on Security And Privacy Analytics, Scottsdale, AZ, March, 2017.

Tracing the Arc of Smartphone Application Security, The Ohio State University, Department of Computer Science and Engineering, Columbus, OH, March, 2017.

Tracing the Arc of Smartphone Application Security, University of California-Irvine, Computer Science Department, Irvine, CA, March, 2017.

Tracing the Arc of Smartphone Application Security, Virginia Technical University, Department of Computer Science, Blacksburg, VA, March, 2017.

Tracing the Arc of Smartphone Application Security, 12th International Conference on Information Systems Security , Jaipur, India, December, 2016.

Tracing the Arc of Smartphone Application Security, University of Michigan, Ann Arbor, Ann Arbor, MI, November, 2016.

Machine Intelligence in Adversarial Settings, Developing a Normative Framework for Cyberwarfare, United States Naval Academy, Annapolis, MD, September, 2016.

Eight Years of Mobile Smartphone Security, University of Pittsburgh, Pittsburgh, PA, September, 2016.

Eight Years of Mobile Smartphone Security, New Jersey Institute of Technology, Newark, NJ, September, 2016.

Setting a Cyber-Security Baseline for Physical Systems: Terminology, Technologies, and Goals, Pacific Northwest Clean Water Association, webinar, August, 2016.

The Limitations of Machine Learning in Adversarial Settings, 25th International Conference on Computer Communication and Networks (ICCCN 2016), Waikoloa, HI, August, 2016.

Learning from Ourselves: Where are we and where can we go in mobile systems security?, Mobile Security Technologies (MOST) 2016 Workshop, IEEE Computer Society Security and Privacy Workshops, San Jose, CA, May, 2016.

Eight Years of Mobile Smartphone Security, Center for Secure and Dependable Systems (CSDS) Cybersecurity Symposium, Coeur d'Alene, April, 2016.

Eight Years of Mobile Smartphone Security, University of Idaho, Moscow, ID, April, 2016.

Army Installation 2035: Cyber Challenges and Opportunities, US Department of Defense, Arlington, VA, April, 2016.

The Limitations of Machine Learning in Adversarial Settings, Florida Institute on National Security Assured Autonomy Workshop, Fort Myers, FL, February, 2016.

SABOT: Specification-based Payload Generation for Programmable Logic Controllers, Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) , San Francisco, CA, February, 2016.

Seven Years of Mobile Smartphone Security, Computer and Information Sciences Department, Temple University, Philadelphia, PA, January, 2016.

Seven Years of Mobile Smartphone Security, Massachusetts Institute of Technology–Lincoln Labs, Lexington, MA, January, 2016.

Six Years of Mobile Smartphone Security, Information Trust Institute, University of Illinois at Urbana-Champaign, Urbana-Champaign, IL, September, 2015.

The Importance of Measurement and Decision Making to a Science of Security, 2015 IEEE Conference on Communications and Network Security, Florence, Italy, September, 2015.

The Importance of Measurement and Decision Making to a Science of Security, 3rd International Symposium on Resilient Cyber Systems, Philadelphia, PA, August, 2015.

Six Years of Mobile Smartphone Security, CISPA Distinguished Lecture Series, Max Planck Institute/Saarland University, Saarbrucken Germany, July, 2015.

Six Years of Mobile Smartphone Security, Technische Universtat Darmstadt, Darmstadt Germany, July, 2015.

Estimating Attack Intent and Mission Impact From Detection Signals, Workshop on Cyber Attack Detection, Forensics and Attribution forAssessment of Mission Impact, NATO Science and Technology Organization, Information Systems Technology Panel, Istanbul, Turkey, June, 2015.

The Importance of Measurement and Decision Making to a Science of Security, 2015 Symposium And Bootcamp on the Science of Security (Hotsos), University of Illinois at Urbana-Champaign, April, 2015.

Security and Science of Agility, First ACM Workshop on Moving Target Defense (MTD 2014), Scottsdale, AZ, November, 2014.

Evaluating Mobile Smartphone Security: The First Five Years, Computer Science Colloquium Series, Harvard School of Engineering and Applied Sciences, Harvard University, Boston, MA, October, 2014.

A Secondary Internet Revolution: How the Smart Device has Changed the Information Security Landscape, IEEE New Technology Industry Seminar (NTIS '13), Everett, WA, August, 2013.

Geotargeting: Mobile Device Privacy and Security, National Academy of Sciences, Washington DC, February, 2013.

Authentication and Web Security, Security and Privacy in IT-EMTM 604 Guest Lecture, University of Pennsylvania, Philadelphia, PA, February, 2013.

The Realities of Voting: A Retrospective of Ten Years of Information Security and Electronic Voting Systems, 2012 Information Assurance Day, Computer Science Department, Indiana University of Pennsylvania, Indiana, PA, November, 2012.

Permission-based Application Governance; A Step Forward or Backward?, 26th Annual WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'12), Paris, France, July, 2012.

Evaluating Mobile Smartphone Security: The First Four Years, Carnegie Mellon University, Pittsburgh, PA, April, 2012.

Scalable Integrity-Guaranteed AJAX, The 14th Asia-Pacific Web Conference (APWeb), Kunming, China, April, 2012.

Evaluating Mobile Smartphone Application Security, Singapore Management University, Singapore, September, 2011.

Evaluating Mobile Smartphone Application Security, Computer Security Foundations Symposium, Florham Park, NJ, July, 2011.

Security Challenges and Solutions in Mobile Smartphone Applications, Computer Security Foundations Symposium, Domaine de l'Abbaye des Vaux de Cernay, France, June, 2011.

Security Challenges and Solutions in Mobile Smartphone Applications, Computer and Information Science Department, University of Oregon, Eugene, OR, April, 2011.

Identifying (and Addressing) Security and Privacy Issues in Smart Electric Meters, Center for Non-Linear Studies, Los Alamos, NM, February, 2011.

Security Challenges and Solutions in Mobile Smartphone Applications, Department of Software Information SystemsCollege of Computing and Informatics, UNC Charlotte, Charlotte, NC, December, 2010.

Security Challenges and Solutions in Mobile Smartphone Applications, Computer Science Department, Indiana University of Pennsylvania, Indiana, PA, December, 2010.

Security Challenges and Solutions in Mobile Smartphone Applications, Computer Science Department, Georgetown University, Washington D.C., November, 2010.

Security Challenges and Solutions in Mobile Smartphone Applications, Networking and Security Research Center, ComputerScience and Engineering, Pennsylvania State University, University Park, PA, October, 2010.

Security Challenges and Solutions in Mobile Smartphone Applications, Security Day Seminar, Penn State University, University Park, PA, October, 2010.

The Changing Vulnerability Landscape, Association for Computing Machinery, Penn State Student Chapter, University Park, PA, September, 2010.

The Changing Vulnerability Landscape, ExxonMobil, Falls Church, VA, March, 2010.

The Impact of Supply Chain on Information and Communications Technology Security, The 1st Workshop on Telecommunications Infrastructure Protection and Security, Honolulu, HI, December, 2000.

Energy Theft in the Advanced Metering Infrastructure, Networking and Security Research Center, ComputerScience and Engineering, Pennsylvania State University, State College, PA, October, 2009.

Secure Provenance in High-End Computing Systems, NSF HECURA FSIO PI Meeting, Arlington, VA, August, 2009.

Missing Glue: Architectural Support for Security Annotations, National Science Foundation Security Driven Architecture Workshop, Arlington, VA, July, 2009.

Scalable Integrity-Justified Content Provenance, NSERC ISSNet Workshop, Ottawa, Canada, June, 2009.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

lseb: Testing Large Scale BGP Security in ReplayableNetwork Environments, NSF/DETER Community Workshop, Arlington, VA, June, 2006.

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

JifClipse: Extending Developer Tools for Security-TypedLanguages, Software Engineering Research Center SpringShowcase, Shaumburg, IL, June, 2006.

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

Information Flow Revisited: Software Engineering toProvable Security, Network Center of Excellence, Motorola Labs, Shaumburg, IL, May, 2006.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Analysis of Security Vulnerabilities in the MovieProduction and Distribution Process, Ball State University, Muncie, IN, April, 2004.

Origin Authentication in Interdomain Routing, Computer Science Department, University of Illinois, Champaign, IL, March, 2004.

Origin Authentication in Interdomain Routing, Computer Science and Engineering Department,University of Minnesota, Minneapolis, MN, March, 2004.

Origin Authentication in Interdomain Routing, Computer Science Department, Johns Hopkins University, Baltimore, MD, March, 2004.

Origin Authentication in Interdomain Routing, Department of Computer Science, University ofMassachusetts - Amherst, Amherst, MA, March, 2004.

Origin Authentication in Interdomain Routing, Computer Science and Engineering Department, PennState University, University Park, PA, March, 2004.

Origin Authentication in Interdomain Routing, School of Electrical Engineering and ComputerScience, Oregon State University, Corvallis, OR, February, 2004.

Origin Authentication in Interdomain Routing, Computer Science Department, NorthwesternUniversity, Evanston, IL, February, 2004.

Origin Authentication in Interdomain Routing, Computer Science Department, SUNY-Stony Brook, Stony Brook, NY, February, 2004.

Attack Profiling and Simulation in Interdomain Routing, P2INGS Quarterly Meeting, Tempe, AZ, February, 2004.

Analysis of Security Vulnerabilities in the MovieProduction and Distribution Process, AT&T Finance Lunch, Morristown, NJ, January, 2004.

Origin Authentication in Interdomain Routing, AT&T IP Security Conference, Middletown, NJ, November, 2003.

Origin Authentication in Interdomain Routing, 10th ACM Conference on Computer and CommunicationsSecurity (CCS), Washington, DC, October, 2003.

Origin Authentication in Interdomain Routing, Computer Science Department, Stevens Institute ofTechnology, Hoboken, NJ, October, 2003.

Origin Authentication in Interdomain Routing, Computer Science Department, Arizona State University, Mesa, AZ, September, 2003.

Analysis of Security Vulnerabilities in the MovieProduction and Distribution Process, 31st Technology Policy Research Conference (TPRC), Arlington, VA, September, 2003.

On Context in Authorization Policy, 8th ACM Symposium on Access Control Models andTechnologies, Como, Italy, June, 2003.

The Antigone Project, DARPA Principal Investigator Meeting, San Antonio, TX, January, 2003.

Methods and Limitations of Security Policy Reconciliation, 2002 IEEE Symposium on Security and Privacy, Oakland, CA, May, 2002.

Policy Management in Distributed Systems, Cigital, Washington, DC, April, 2002.

Antigone: Policy Management in Secure Group Communication, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, April, 2001.

Antigone: Policy Management in Secure Group Communication, Computer Science Department, University of Wisconsin, Madison, MD, April, 2001.

Antigone: Policy Management in Secure Group Communication, Computer Science Department, University of Maryland, College Park, MD, April, 2001.

Antigone: Policy Management in Secure Group Communication, Computer Science Department, University of North Carolina, Chapel Hill, Chapel Hill, NC, April, 2001.

Antigone: Policy Management in Secure Group Communication, Computer Science Department, Johns Hopkins University, Baltimore, MD, March, 2001.

Antigone: Policy Management in Secure Group Communication, AT&T Shannon Laboratory, Florham Park, NJ, February, 2001.

Antigone: Policy Management in Secure Group Communication, Telcordia Applied Research Laboratory, Morristown, NJ, February, 2001.

Policy Problem Area 3 - Overview and Requirements, Internet Engineering Task Force MSEC BOF, San Diego, CA, December, 2000.

Multicast Security Policy Requirements and Building Blocks, Quarterly Secure Multicast Research Group Meeting (SMuG), San Diego, CA, December, 2000.

Antigone: Implementing Policy in Secure Multiparty Communication, Systems Design and Implementation (SDI) / Laboratoryfor Computer Systems (LCS) seminar series, School of ComputerScience, Carnegie Mellon University, Pittsburgh, PA, November, 2000.

Secure Group Communication in Antigone 2.0, 11th Annual IPoCSE Research Symposium, Ann Arbor, MI, October, 2000.

Antigone Secure Group Communication, Bi-Annual DARPA Visit, Software System Research Laboratory, Ann Arbor, MI, September, 2000.

Problem Area 3: Policy, Quarterly Secure Multicast Research Group Meeting (SMuG), Pittsburgh, PA, July, 2000.

Windowed Certificate Revocation, IEEE INFOCOM 2000, Tel Aviv, Israel, March, 2000.

A Response to 'Can We Eliminate Certificate Revocation Lists?', Financial Cryptography 2000, Anguilla, British West Indies, February, 2000.

Multicast Security Policy Definition, Quarterly Secure Multicast Research Group Meeting (SMuG), Washington, DC, November, 1999.

Antigone: A Flexible Framework for Secure Group Communication, Quarterly Secure Multicast Research Group Meeting (SMuG, NAI Labs, Baltimore, MD, September, 1999.

Antigone: A Flexible Framework for Secure Group Communication, 10th Annual IPoCSE Research Symposium, Ann Arbor, MI, September, 1999.

Antigone: A Flexible Framework for Secure Group Communication, 8th USENIX Security Symposium, Washington, DC, August, 1999.

Antigone: A Flexible Framework for Secure Group Communication, IBM Watson Security Seminar, Westchester County, NY, July, 1999.

Windowed Revocation in Public Key Infrastructures, Department of Electrical Engineering and ComputerScience, University of Michigan, Ann Arbor, MI, September, 1998.

Scalable Key Distribution Hierarchy, 9th Annual IPoCSE Research Symposium, Ann Arbor, MI, March, 1998.

JavaLauncher Applet Platform, NASA, Kennedy Space Center Security Seminar, Kennedy Space Center, FL, January, 1998.

Secure High Performance Group Communication, Directed StudyDefense, Department of Electrical Engineering and ComputerScience, University of Michigan, Ann Arbor, MI, September, 1997.