Filed on behalf of: VirnetX Inc.
By:
Joseph E. Palys
Paul Hastings LLP
875 15th Street NW
Washington, DC 20005
Telephone: (202) 551-1996
Facsimile: (202) 551-0496
E-mail: josephpalys@paulhastings.com

Naveen Modi
Paul Hastings LLP
875 15th Street NW
Washington, DC 20005
Telephone: (202) 551-1990
Facsimile: (202) 551-0490
E-mail: naveenmodi@paulhastings.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner

v.

VIRNETX INC.
Patent Owner

Case IPR2015-00812
Patent 8,850,009

Declaration of Fabian Monrose, Ph.D.

Table of Contents

I, FABIAN MONROSE, declare as follows:

I. Introduction

1. I have been retained by VirnetX Inc. ("VirnetX") for this *inter partes* review proceeding. I understand that this proceeding involves U.S. Patent No. 8,850,009 ("the '009 patent"). I understand the '009 patent is assigned to VirnetX and that it is part of a family of patents that stems from U.S. provisional application nos. 60/106,261 ("the '261 application"), filed on October 30, 1998, and 60/137,704 ("the '704 application"), filed on June 7, 1999. I understand that the '009 patent is a continuation of U.S. application no. 13/903,788 filed May 28, 2013 ("the '788 application"), which is a continuation of U.S. application no. 13/336,790 filed December 23, 2011 (now U.S. Patent No. 8,458,341, "the '341 patent"), which is a continuation of U.S. application no. 13/049,552 filed March 16, 2011 ("the '552 application), which is a continuation of U.S. application no. 11/840,560 filed August 17, 2007 (now U.S. Patent No. 7,921,211, "the '211 patent"), which is a continuation of U.S. application no. 10/714,849 filed November 18, 2003 (now U.S. Patent No. 7,418,504 ("the '504 patent), which is a continuation of U.S. application no. 09/558,210 filed April 26, 2000 ("the '210 application," abandoned). And I understand the '210 application is a continuation-in-part of U.S. application no. 09/504,783 filed February 15, 2000 (now U.S. Patent 6,502,135, "the '135 patent"), and that the '135 patent is a continuation-in-

part of U.S. application no. 09/429,643 (now U.S. Patent No. 7,010,604) filed October 29, 1999, which claims priority to the '261 and '704 applications.

II. Resources Consulted

2. I have reviewed the '009 patent, including claims 1-8, 10-20, and 22-25. I have also reviewed the Petition for *Inter Partes* Review (Paper No. 1) filed with the U.S. Patent and Trademark Office ("Office") by Apple Inc. on March 2, 2015 (Paper No. 1, the "Petition"). I have also reviewed the Patent Trial and Appeal Board's ("Board") decision to institute *inter partes* review (Paper No. 8, the "Decision") of September 11, 2015.

3. I understand that in this proceeding the Board instituted review of the '009 patent on one ground: obviousness of claims 1-8, 10-20, and 22-25 over *Beser* and RFC 2401. I have reviewed the exhibits and other documentation supporting the Petition that are relevant to the Decision and the instituted grounds, and any other material that I reference in this declaration.

III. Background and Qualifications

4. I have a great deal of experience and familiarity with computer and network security, and have been working in this field since 1993 when I entered the Ph.D. program at New York University.

5. I am currently a Professor of Computer Science at the University of North Carolina at Chapel Hill. I also hold an appointment as the Director of

Computer and Information Security at the Renaissance Computing Institute (RENCI). RENCI develops and deploys advanced technologies to facilitate research discoveries and practical innovations. To that end, RENCI partners with researchers, policy makers, and technology leaders to solve the challenging problems that affect North Carolina and our nation as a whole. In my capacity as Director of Computer and Information Security, I lead the design and implementation of new platforms for enabling access to, and analysis of, large and sensitive biomedical data sets while ensuring security, privacy, and compliance with regulatory requirements. At RENCI, we are designing new architectures for securing access to data (e.g., using virtual private networks and data leakage prevention technologies) hosted among many different institutions. Additionally, I serve on RENCI's Security, Privacy, Ethics, and Regulatory Oversight Committee (SPOC), which oversees the security and regulatory compliance of technologies, designed under the newly-formed Data Science Research Program and the Secure Medical Research Workspace.

6. I received my B.Sc. in Computer Science from Barry University in May 1993. I received my MSc. and Ph.D. in Computer Science from the Courant Institute of Mathematical Sciences at New York University in 1996 and 1999, respectively. Upon graduating from the Ph.D. program, I joined the Systems Security Group at Bell Labs, Lucent Technologies. There, my work focused on the

analysis of Internet Security technologies (e.g., IPsec and client-side authentication) and applying these technologies to Lucent's portfolio of commercial products. In 2002, I joined the Johns Hopkins University as Assistant Professor in the Computer Science department. I also served as a founding member of the Johns Hopkins University Information Security Institute (JHUISI). At JHUISI, I served a key role in building a center of excellence in Cyber Security, leading efforts in research, education, and outreach.

7. In July of 2008, I joined the Computer Science department at the University of North Carolina (UNC) Chapel Hill as Associate Professor, and was promoted to Full Professor four years later. In my current position at UNC Chapel Hill, I work with a large group of students and research scientists on topics related to cyber security. My former students now work as engineers at several large companies, as researchers in labs, or as university professors themselves. Today, my research focuses on applied areas of computer and communications security, with a focus on traffic analysis of encrypted communications (e.g., Voice over IP); Domain Name System (DNS) monitoring for performance and network abuse; network security architectures for traffic engineering; biometrics and client-to-client authentication techniques; computer forensics and data provenance; runtime attacks and defenses for hardening operating system security; and large-scale

empirical analyses of computer security incidents. I also regularly teach courses in computer and information security.

8. I have published over 75 papers in prominent computer and communications security publications. My research has received numerous awards, including the Best Student Paper Award (IEEE Symposium on Security & Privacy, July, 2013), the Outstanding Research in Privacy Enhancing Technologies Award (July, 2012), the AT&T Best Applied Security Paper Award (NYU-Poly CSAW, Nov., 2011), and the Best Paper Award (IEEE Symposium on Security & Privacy, May, 2011), among others. My research has also received corporate sponsorship, including two Google Faculty Research Awards (2009, 2011) for my work on network security and computer forensics, as well as an award from Verisign Inc. (2012) for my work on DNS.

9. I am the sole inventor or a co-inventor on three issued US patents and four pending patent applications, nearly all of which relate to network and systems security. Over the past 12 years, I have been the lead investigator or a co-investigator on grants totaling nearly nine million US dollars from the National Science Foundation (NSF), the Department of Homeland Security (DHS), the Department of Defense (DoD), and industry. In 2014, I was invited to serve on the Information Science and Technology (ISAT) study group for the Defense Advanced Research Projects Agency (DARPA). During my three year

appointment, I will assist DARPA by providing continuing and independent assessment of the state of advanced information science and technology as it relates to the U.S. Department of Defense.

10. I have chaired several international conferences and workshops, including for example, the USENIX Security Symposium, which is the premier systems-security conference for academics and practitioners alike. Additionally, I have also served as Program Chair for the USENIX Workshop on Hot Topics in Security, the Program Chair for the USENIX Workshop on Large-scale Exploits & Emergent Threats, the local arrangements Chair for the Financial Cryptography and Data Security Conference, and the General Chair of the Symposium on Research in Attacks and Defenses. As a leader in the field, I have also served on numerous technical program committees including the Research in Attacks, Intrusions, and Defenses Symposium (2012, 2013), USENIX Security Symposium (2013, 2005-2009), Financial Cryptography and Data Security (2011, 2012), Digital Forensics Research Conference (2011, 2012), ACM Conference on Computer and Communications Security (2009-2011, 2013), IEEE Symposium on Security and Privacy (2007, 2008), ISOC Network & Distributed System Security (2006—2009), International Conference on Distributed Computing Systems (2005, 2009, 2010), and USENIX Workshop on Large-scale Exploits and Emergent Threats (2010-2012).

11. From 2006 to 2009, I served as an Associate Editor for IEEE Transactions on Information and Systems Security (the leading technical journal on cyber security), and currently serve on the Steering Committee for the USENIX Security Symposium.

12. My curriculum vitae, which is appended, details my background and technical qualifications. Although I am being compensated at my standard rate of $450/hour for my work in this matter, the compensation in no way affects the statements in this declaration.

IV. Level of Ordinary Skill

13. I am familiar with the level of ordinary skill in the art with respect to the inventions of the ’009 patent as of what I understand is the patent’s early-2000 priority date. Specifically, based on my review of the technology, the educational level of active workers in the field, and drawing on my own experience, I believe a person of ordinary skill in art at that time would have had a master’s degree in computer science or computer engineering, as well as two years of experience in computer networking with some accompanying exposure to network security. My view is consistent with VirnetX’s view that a person of ordinary skill in the art requires a master’s degree in computer science or computer engineering and approximately two years of experience in computer networking and computer security. I have been asked to respond to certain opinions offered by Dr. Roberto

Tamassia, consider how one of ordinary skill would have understood certain claim terms, and consider how one of ordinary skill in the art would have understood the references mentioned above in relation to the claims of the '009 patent. My findings are set forth below.

V. Claim Terms

14. I understand that in an *inter partes* review proceeding, the claims of a patent are construed under the broadest reasonable interpretation in light of the specification. I also understand that the parties have proposed constructions for certain terms of the '009 patent. Unless otherwise noted, I have used Patent Owner's proposed constructions in my analysis. In my opinion, Patent Owner's proposed constructions are consistent with the specification. To the extent Patent Owner has not proposed a construction for a term, I understand that term to have its plain and ordinary meaning from the perspective of one of ordinary skill in the art in light of the specification. I have applied that understanding in my analysis.

A. "Encrypted Communication Link" Phrases (Claims 1, 2, 8, 11, 14, 15, and 23)

15. I understand that the parties and the Board have put forth the following constructions for purposes of this proceeding:

VirnetX's Proposed Construction	Apple's Proposed Construction	Decision's Construction
A direct communication link that is encrypted	A transmission path that restricts access to data, addresses, or other	No construction proposed

	information on the path at least by using encryption	

16. One of ordinary skill in the art would understand that the ’009 patent describes encrypted communications that are direct between a first and second device. For instance, in one embodiment, the ’009 patent describes the link between an originating TARP terminal and a destination TARP terminal as direct. (*See, e.g.,* Ex. 1003, 10:16-25, Fig. 2; *see also id.* at 34:13-20 (describing a variation of the TARP embodiments as including a direct communication link); 38:42-45 (describing the embodiment of Figure 24 in which a first computer and second computer are connected directly).) The ’009 patent similarly describes direct encrypted communications in later embodiments as well. (*See, e.g., id.* at 40:45-48, 41:39-42 (describing a virtual private network as being direct between a user’s computer and target), 42:49-53, 43:42-46 (describing a load balancing example in which a virtual private network is direct between a first host and a second host), 49:44-46, 49:55-67 (describing a secure communication link that is direct between a first computer and a second computer), Figs. 24, 26, 28, 29, 33.)

17. In each of these embodiments, the ’009 patent specification discloses that the link traverses a network (or networks) through which it is simply passed or routed via various network devices such as Internet Service Providers, firewalls, and routers. (*See, e.g., id.* at Figs. 2, 24, 28, 29, 33.)

B. "Provisioning Information" (Claims 1 and 14)

18. I understand that the parties and the Board have put forth the following constructions for purposes of this proceeding:

VirnetX's Proposed Construction	Apple's Proposed Construction	Decision's Construction
Information that is used to establish an encrypted communication link	Information that enables communication in a virtual private network, where the virtual private network uses encryption	No construction proposed

19. In my opinion, Patent Owner's construction is consistent with the general notion that provisioning refers to setting up or establishing a connection or service. One dictionary explains that provisioning is "[s]etting up a telecommunications service for a particular customer," and that "[c]ommon carriers provision circuits by programming their computers to switch customer lines into the appropriate networks." (Ex. 2007 at 6, *McGraw-Hill Computer Desktop Encyclopedia* (9th ed. 2001).) Applying these principles to provisioning in the context of the '009 patent, encrypted communications channel provisioning refers to setting up or establishing an encrypted communication channel. Thus, in the context of the '009 patent, the "provisioning information" is "information that is used to establish an encrypted communications channel."

20. In my opinion, in the context of the '009 patent, one of ordinary skill in the art would not understand provisioning information to encompass any and all

information that merely "enables or aids in" communication using an encrypted communications channel, as that information may have nothing to do with provisioning. For example, information that simply enabled or aided in communication using an encrypted communications channel would encompass source and destination information for individual packets of data that are traveling over a pre-existing channel. One of ordinary skill in the art would not have understood a channel to be provisioned every time a data packet is sent across it.

C. "VPN Communication Link" (Claim 8)

21. I understand that the parties and the Board have put forth the following constructions for purposes of this proceeding:

VirnetX's Proposed Construction	Apple's Proposed Construction	Board's Construction
A communication path between two devices in a virtual private network	A transmission path between two devices that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping	No construction proposed

1. A "VPN Communication Link" Does Not Exist Outside of a Virtual Private Network

22. The '009 patent discloses that a VPN communication link is a communication path between computers in a virtual private network. When a secure domain name service (SDNS) receives a query for a secure network address, it "accesses VPN gatekeeper 3314 for establishing a VPN communication link between software module 3309 [at the querying computer 3301] and secure server 3320." (Ex. 1003 at 52:7-9.) Then, "VPN gatekeeper 3314 provisions computer 3301 and secure web server computer 3320 . . . thereby creating the VPN" between the devices. (Ex. 1001 at 52:10-13, emphasis added.) Notably, the secure server 3320 "can only be accessed through a VPN communication link." (Ex. 1001 at 52:9-10.)

2. "Authentication" and "Address Hopping" Alone Do Not Result in a "Virtual Private Network Communication Link"

23. Petitioner's proposed construction is technically incorrect. Of the obfuscation methods in the proposed construction—authentication, encryption, and address hopping—only encryption restricts access to "data, addresses, or other information on the path," as required by the first portion of the construction. The other techniques alone do not "hide information on the path," as Petitioner's construction requires.

24. In my opinion, authentication merely ensures the recipient that a message originated from the expected sender, which is consistent with the definition of authentication in a dictionary the '009 patent refers to. (Ex. 2008 at 3, Glossary for the Linux FreeS/WAN Project.) Authentication does not prevent an eavesdropper from accessing data transmitted over an unsecure communication link. The specification is also consistent with my understanding, as it describes at least one scenario where an authenticated transmission occurs "in the clear"—i.e., over an unsecured communication link:

> SDNS [secure domain name service] 3313 can be accessed through secure portal 3310 "in the clear", that is, without using an administrative VPN communication link. In this situation, secure portal 3310 preferably authenticates the query using any well-known technique, such as a cryptographic technique, before allowing the query to proceed to SDNS [3313].

(Ex. 1003 at 52:21-26.)

25. Address hopping alone also does not provide the claimed security, as there is nothing inherent in moving from address to address that hides information on the path or precludes an eavesdropper from reading the details of a communication. This is why the '009 patent discloses embodiments that use encryption in conjunction with address hopping to protect, for example, the next address in a routing scheme from being viewed by eavesdroppers. (*See, e.g.*, Ex.

1003 at 3:40-54, stating in part that "[e]ach TARP packet's true destination is concealed behind a layer of encryption generated using a link key.") It is the encryption that hides information on the path while moving from address to address. (*See, e.g.*, Ex. 1003 at 3:20-4:44.)

26. While authentication and address hopping may be used in conjunction with encryption as an "obfuscation method," this fact does not make them sufficient by themselves to "hide information on the path," as Petitioner's construction requires.

3. A "Virtual Private Network Communication Link" Must Be Direct

27. In my opinion, one of skill would understand that a "virtual private network communication link" in the context of the '009 patent describes a "direct" link, as discussed above in Section V.A.

4. A VPN Requires a Network of Computers

28. In my opinion, the Petitioner's construction eliminates the "network" from a virtual private network and a virtual private network communication link. One of ordinary skill in the art would understand the plain meaning of a VPN communication link to mean that the link must exist in a VPN and therefore must be between computers in a network. Consistent with my understanding, in describing a VPN, the '009 patent refers to the "FreeS/WAN" project, which has a glossary of terms. (Ex. 1003 at 40:7 and bibliographic data showing references

cited.) The FreeS/WAN glossary defines a VPN as "a network which can safely be used as if it were private, even though some of its communication uses insecure connections. All traffic on those connections is encrypted." (Ex. 2008 at 24, Glossary for the Linux FreeS/WAN Project.) According to this glossary, a VPN includes at least the requirement of a "network of computers."

29. The specification further describes a VPN as including multiple "nodes." (*See, e.g.*, Ex. 1003 at 17:36-40, referring to "each node in the network" and "vastly increasing the number of distinctly addressable nodes," 22:11, "nodes on the network"; *see also id.* 19:61-63, 19:24:59.) More specifically, the network allows "each node . . . to communicate with other nodes in the network." (Ex. 1003 at 17:40-42.) So a device within a VPN is able to communicate with the other devices within that same VPN. In addition, the specification distinguishes point-to-point queries from those carried on a VPN communication link, stating that they occur "without using an administrative VPN communication link." (*See, e.g.*, Ex. 1003 at 52:21-23, 26-29.)

5. A VPN Requires Encryption

30. In my opinion, in view of the specification, a virtual private network requires encryption. For instance, the '009 patent specification's "TARP" embodiments describe a "unique two-layer encryption format" where "[e]ach TARP packet's true destination address is concealed behind a layer of encryption"

(first layer) and "[t]he message payload is hidden behind an inner layer of encryption" (second layer). (Ex. 1003 at 3:21-23.) In addition, the FreeS/WAN glossary of terms in the '009 patent's prosecution history explains that a VPN is "a network which can safely be used as if it were private, even though some of its communication uses insecure connections. All traffic on those connections is encrypted." (Ex. 2008 at 24, Glossary for the Linux FreeS/WAN Project.) Another contemporaneous computing dictionary also states that "VPNs enjoy the security of a private network via access control and encryption . . . ." (Ex. 2007 at 8, *McGraw-Hill Computer Desktop Encyclopedia* (9th ed. 2001).)

D. Other Terms

31. I understand that the parties and Board have provided the following constructions for purposes of this proceeding. I agree that the claim language encompasses the features described in each of VirnetX's constructions.

"Domain Name Service (DNS) Request" (Claims 1, 12-14, 24 and 25)		
VirnetX's Proposed Construction	Apple's Proposed Construction	Board's Construction
A request for a resource corresponding to a domain name	A request for a resource corresponding to a domain name	No construction proposed

"Interception of the DNS Request" (Claims 1, 12-14, 24, and 25)		
VirnetX's Proposed Construction	Apple's Proposed Construction	Board's Construction
No construction necessary; alternatively, receiving a request to look up an internet protocol address and, apart from resolving it into an address, performing an evaluation on it related to establishing an encrypted communication link	Receiving a DNS request pertaining to a first entity at another entity	No construction proposed
"Secure Communications Service" (Claims 1-3, 10, 12, 14-16, 22, and 24)		
VirnetX's Proposed Construction	Apple's Proposed Construction	Board's Construction
The functional configuration of a network device that enables it to participate in a secure communications link with another network device	The functional configuration of a network device that enables it to participate in a secure communications link with another computer or device	No construction proposed
"Indication" (Claims 1, 10, 14, and 22)		
VirnetX's Proposed Construction	Apple's Proposed Construction	Board's Construction
No construction necessary	Something that shows the probable presence or existence or nature of	No construction proposed
"Domain Name" (Claims 7 and 20)		
VirnetX's Proposed Construction	Apple's Proposed Construction	Board's Construction
A name corresponding to a network address	A name corresponding to an IP address	No construction proposed

"Modulation" (Claims 4, 5, 17, and 18)		
VirnetX's Proposed Construction	Apple's Proposed Construction	Board's Construction
No construction necessary, alternatively, the process of encoding data for transmission over a medium by varying a carrier signal.	The process of encoding data for transmission over a medium by varying a carrier signal	No construction proposed

VI. *Beser* and RFC 2401

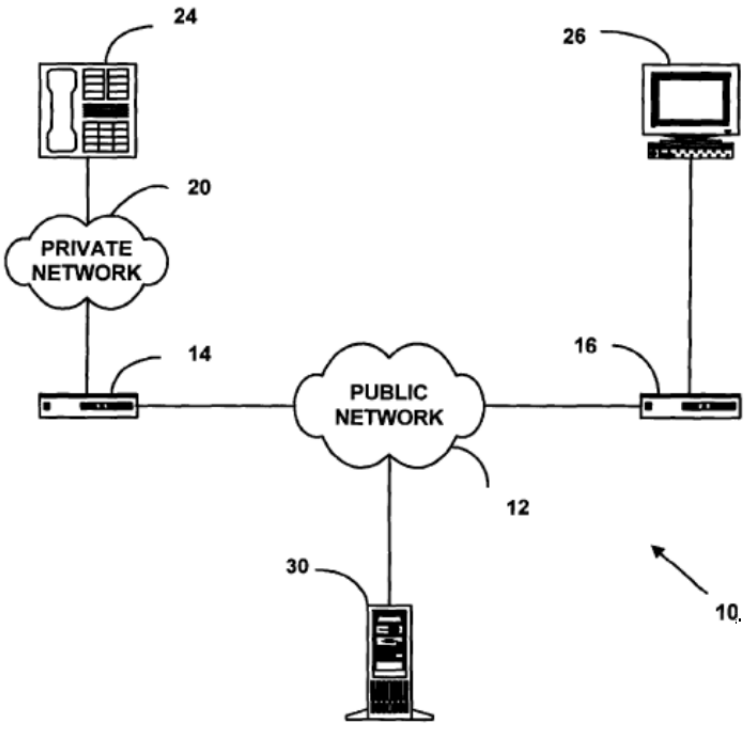
A. *Beser*'s Disclosure

32. *Beser* "relates to communications in data networks," (Ex. 1007 at 1:8-9), and the fact that "the Internet is not a very secure network," (*id.* at 1:26-27). Prior art methods attempted to secure communications by "encrypt[ing] the information inside the IP packets before transmission." (*Id.* at 1:54-56.) *Beser* teaches that this method is not secure because a determined hacker could accumulate enough packets from a source to decrypt the message. (*Id.* at 1:56-58.) Nor, as *Beser* teaches, is this method practicable, especially in the context of voice and audio data, because encryption at the source and decryption at the destination are computationally intensive. (*Id.* at 1:58-67, 2:8-17.) *Beser* therefore identifies a need for a more secure system that prevents a hacker from intercepting media flow without the computational burden associated with encryption. (*Id.* at 2:36-40.)

33. Instead of using encryption, *Beser* teaches a "tunneling association" that hides the originating and terminating ends of the tunnel during

communications on a public network. (*Id.* at 3:1-9.) Because the source is hidden, hackers are prevented from intercepting communications, resulting in "increase[d] [] security of communication *without an increased computational burden*." (*Id.* at 2:36-40, 3:4-9 (emphasis added).) One of ordinary skill in the art would have understood that *Beser* teaches away from encryption and that its proposed solution avoids encryption.

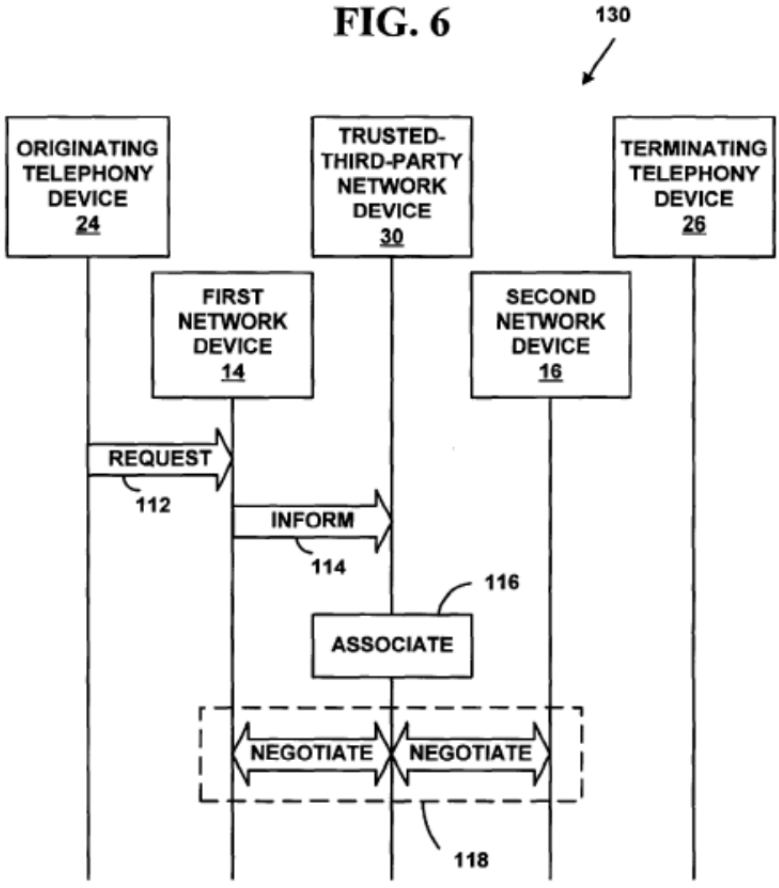
34. *Beser*'s solution involves "initiating a tunnelling association between an originating end [24] and a terminating end [26]" facilitated by an intermediary, trusted-third-party network device 30. (*Id.* at 1:45-67, 7:62-64.) Figure 1 of *Beser* illustrates this solution:



(*Id.* at Fig. 1.)

35. When an originating end device 24 in *Beser* wants to communicate with a terminating end device 26, it sends a tunnel initiation request 112 to first network device 14. (*Id.* at 7:65-67.) This request "includes a unique identifier for the terminating end of the tunnelling association." (*Id.* at 8:1-3.) One of ordinary skill in the art would not understand this request (even containing a "unique identifier") to be a "request to look up an internet protocol (IP) address of the second network device."

FIG. 6



(*Id.* at Fig. 6.)

36. The first network device 14 then sends an inform message 114 with tunnel initiation request 112 to trusted-third-party network device 30 by constructing one or more IP packets 58. (*Id.* at 8:3-4, 11:9-25.) The trusted-third-party network device 30 associates a public IP address of a second network device 16 with the unique identifier of terminating telephony device 26. (*Id.* at 8:4-7, 11:26-32.) The first and second network devices 14 and 16 then "negotiate" private IP addresses through the public network 12. (*Id.* at 8:9-15, 11:58, Fig. 6 (step 118).) This "negotiation" assigns a first private network address to the originating device 24 and a second private network address to the terminating device 26. (*Id.* at 12:2-4.)

37. Once assigned, the private network address of originating device 24 and the public IP address of first network device 14 are communicated to the second network device 14. (*Id.* at 13:33-48.) Similarly, the private network address of the terminating device 26 and the public IP address of the second network device 16 are communicated to the first network device 14. (*Id.* at 14:19-33.)

B. Claims 1 and 14

1. "Send[ing] a Domain Name Service (DNS) Request To Look Up a Network Address of a Second Network Device Based On an Identifier Associated With the Second Network Device"

38. I understand that independent claim 1 recites, *inter alia*, to "send a domain name service (DNS) request to look up a network address of a second network device based on an identifier associated with the second network device." I understand that independent claim 14 similarly recites "sending a domain name service (DNS) request to look up a network address of a second network device based on an identifier associated with the second network device." In addressing these limitations, I understand Petitioner points to *Beser*'s "request to initiate a tunneling association with a terminating end device." (Pet. at 36 (citing Ex. 1007 at 7:64-8:1, 9:64-10:41).) *Beser*'s request, however, is not a "domain name service (DNS) request to look up a network address."

39. In my opinion, *Beser*'s request to initiate a tunneling connection is just that—a request to initiate a tunnel. This understanding is consistent with the purpose of *Beser*'s tunneling method; as explained by Dr. Tamassia, "the general purpose is the one of initiating a tunneling type of communication between two devices." (Ex. 2015 at 110:9-11.) Simply put, a tunneling request is issued and is processed in a pre-established way to initiate a tunnel between two devices.

40. During cross-examination, Dr. Tamassia explained that he understood the "domain name service (DNS) request to look up a network address" recited in claim 1 to be a "request that follows the DNS protocol for such requests." (Ex. 2015 at 102:9-13.) But neither Petitioner nor Dr. Tamassia ever established that *Beser*'s tunneling requests follow the DNS protocol. Indeed, while tunneling requests may be received by a domain name server (*see* Ex. 1007 at 4:9-11), *Beser* is silent as to whether tunneling requests "follow the DNS protocol."

41. The Petition points to incorrect statements about *Beser* in attempting to address these limitations. For example, the Petition alleges that the trusted-third-party network device in *Beser* will "negotiate[] private IP addresses for the originating and terminating end devices." (Pet. at 36.) One of ordinary skill would have understood this to be incorrect. The first and second network devices, not the trusted-third-party network device, "negotiate" private IP addresses, including the private IP address for the originating and terminating device. (Ex. 1007 at 8:9-15, 11:58, Fig. 6 (step 118).) Moreover, one of ordinary skill in the art would have understood that the negotiation does not involve looking up any IP address, but rather involves *assignment* of a first private network address to the originating device and a second private network address to the terminating device. (*Id.* at 12:2-4.)

42. The Petition also alleges that the trusted-third-party network device in *Beser* will "look[] up the public IP address associated with the unique identifier." (Pet. at 36.) But *Beser* simply states that the database entry in the trusted-third-party network device 30 may include a public IP 58 address for the terminating telephony device 26. (Ex. 1007 at 11:50-55.) One of ordinary skill in the art would not have understood *Beser* to suggest that this data structure is looked up when the tunnel request is received by device 30, let alone that the public address of telephony device 26 is specifically looked up. *Beser* only teaches that when a trusted-third-party network device 30 is informed of a request to initiate a tunnel, it associates a public IP address of a second network device 16 with the unique identifier of terminating telephony device 26. (Ex. 1007 at 11:26-32.)

43. In my opinion, none of the processes in *Beser* transform the request to initiate a tunneling connection into a request to look up an IP address. In my opinion one of the novel aspects of the claims is that, while a request to look up an IP address is transmitted, the request is intercepted allowing it *not* to be processed in the conventional manner. (*See, e.g.*, Ex. 1001 at 40:1-29.) Therefore, in my opinion, *Beser* does not teach or suggest to "send a domain name service (DNS) request to look up a network address of a second network device based on an identifier associated with the second network device," as recited in claim 1, or similarly recited in claim 14.

2. "Interception of the DNS Request"

44. I understand that independent claims 1 and 14 recite, *inter alia*, "interception of the DNS request." Petitioner alleges that the tunneling request in *Beser* is "'intercepted' by each of the first network device and the trusted-third-party network device." (Pet. at 38.) Petitioner alleges that this is so because "the request contains a unique identifier associated with the terminating end device." (*Id.*) In other words, under Petitioner's theory, because the tunneling request includes a unique identifier associated with the terminating end device, it "pertains to" the terminating end device, but is received (as intended by *Beser*'s system) by the first network device and the trusted-third-party network device. I have reviewed the cross examination testimony of Dr. Tamassia, and note that he admitted during cross-examination that this understanding of "intercepting" was incorrect, and instead explained that when he referred to the term "pertaining," what he meant was that it could include either a scenario in which a request is "intended for" receipt at a destination other than the destination at which the request is intercepted, or a scenario in which a request is "ordinarily received by another entity, and instead, it is received at the first entity." (Ex. 2015 at 80:3-13.)[1]

[1] I understand that the Board has explained in a related proceeding involving a related patent that "one of ordinary skill in the art would have understood that

In my opinion, neither the first network device nor the trusted-third-party network device in *Beser* performs "intercepting" when analyzed in a manner consistent with how Dr. Tamassia understands the term.

45. In *Beser*, when an originating end device wants to communicate with a terminating end device, it sends a tunnel initiation request to the first network device. (Ex. 1007 at 7:65-67.) One of ordinary skill in the art would have understood that tunneling requests in *Beser* always go to, and are always intended to go to, the first network device. *Beser* does not disclose a single scenario in which a tunneling request is ordinarily received by another entity, but is *instead* received by the first network device. Nor does *Beser* disclose any scenario in which a tunneling request is intended for receipt at another entity, but is *instead* received by the first network device. Therefore, in my opinion, the first network device in *Beser* cannot perform "intercepting" under Dr. Tamassia's understanding of the term, Petitioner's proposed construction, or the Board's construction of the term in related proceedings.

'intercepting' a request would require 'receiving and acting on' a request, the request being 'intended for' receipt at a destination other than the destination at which the request is intercepted." *Apple Inc. v. VirnetX Inc.*, IPR2014-00237, Paper No. 15 at 12 (May 14, 2014).

46. In my opinion, Petitioner's reliance on the trusted-third-party network device is also flawed. For instance, *Beser* explains that when first network device 14 informs trusted-third-party network device 30 of a request, it "constructs an IP 58 packet," where the "header 82 of the IP 58 packet includes the public network 12 address of the trusted-third-party network device 30 in the destination address field 90 and the public network 12 address of the first network device 14 in the source address field 88." (Ex. 1007 at 11:15-20.) Thus, one of skill would have understood that the packet received by trusted-third-party network device 30 is "intended for" and "ordinarily received by" trusted-third-party network device 30 since the destination address of the packet contains the address of the trusted-third-party network device 30. Just as with the first network device, *Beser* does not disclose a single scenario in which a tunneling request is ordinarily received by another entity, but is *instead* received by the trusted-third-party network device. Nor does *Beser* disclose any scenario in which a tunneling request is intended for receipt at another entity, but is *instead* received by the trusted-third-party network device. Therefore, in my opinion, the trusted-third-party network device in *Beser* also cannot perform "intercepting" under any of Dr. Tamassia's understanding of the term, Petitioner's proposed construction, or the Board's construction of the term in a related proceeding. Therefore, in my opinion, *Beser* does not teach or suggest "interception of the DNS request," as recited in claims 1 and 14.

3. *Beser* and RFC 2401 Would Not Have Been Combined as the Petition Suggests

47. Petitioner turns to RFC 2401 for the teaching that data sent between two devices in a tunnel should be encrypted. Relying on a discussion of prior art systems in *Beser*, Petitioner contends that one of skill in the art would have combined *Beser* with RFC 2401 to achieve encrypted IP traffic. (Pet. at 30-34.) I disagree with that contention. In my opinion, Petitioner misconstrues *Beser* and its contentions contradict the express teaching and purpose of *Beser's* method.

48. As *Beser* explains, prior art systems typically addressed Internet security in one of two ways. (Ex. 1007 at 1:54-2:35.) The first involved encrypting information inside IP packets before transmission. (*Id.* at 1:53-56.) The second involved network address translation whereby an IP packet's address information was modified to re-map one address space into another. (*Id.* at 2:18-22.) According to *Beser*, however, each of these prior art systems suffered from certain disadvantages.

49. For example, encryption still allowed a determined hacker to accumulate all packets from a particular source address, ultimately providing the hacker with sufficient information to decrypt the message. (*Id.* at 1:41-48, 1:56-58.) Encryption could also be infeasible for certain data formats where the speed and accuracy of message transmission are important. (*Id.* at 1:58-67.) *Beser* explains that streaming data flows, such as multimedia and Voice-over-Internet-

Protocol ("VoIP") "require a great deal of computing power to encrypt or decrypt the IP packets on the fly." (*Id.* at 1:62-63.) The strain of such computations "may result in jitter, delay, or the loss of some packets." (*Id.* at 1:64-65.)

50. The Institution Decision asserts that *Beser* "recognizes that the use of encryption may cause challenges, [but] also suggests that such problems may be overcome by providing more computer power." (Institution Decision at 12 (citing Ex. 1007 at 1:60-63).) In my opinion, this position reflects a misunderstanding of *Beser*. One of ordinary skill in the art would have understood that if adding computing power to every computational problem was a solution, there would have been no need for Beser's tunneling solution. Indeed, in the passage cited by the Board, *Beser* notes the *problems* with allocating more computing power to encryption, such as "jitter, delay, or the loss of some packets." (Ex. 1007 at 1:60-65.) One of ordinary skill in the art would have understood from *Beser*'s disclosure that *Beser* dismisses the idea of encryption entirely, noting that the "expense of added computer power might also dampen the customer's desire to invest in VoIP equipment" at all. (*Id.* at 1:65-67.)

51. *Beser* further discloses that network address translation was similarly "computationally expensive." (*Id.* at 2:22-23.) And like encryption, this type of security "may be inappropriate for the transmission of multimedia or VoIP packets." (*Id.* at 2:34-35.) "What is more, network address translation interferes

with the end-to-end routing principal of the Internet that recommends that packets flow end-to-end between network devices without changing the contents of any packet along a transmission route." (*Id.* at 2:27-31.)

52. One of skill in the art would have understood that to address the problems of the prior art security methods—in particular, their inability to protect the identity of source and destination users and their disproportionately high use of computing power—*Beser* proposes a method of hiding the addresses of originating and terminating devices. Its method establishes a tunneling association to hide addresses within the payload of tunneled messages. (*See* Ex. 1007 at 2:36-40, 9:49-51.) By hiding the identities of the network devices in this manner, *Beser* touts that its method is able to increase communication security without increasing computational burden. (*Id.* at 2:43-3:14.) Thus, one of ordinary skill in the art would understand that *Beser* is directed to providing a method for securing communications *other than* encryption.

53. Indeed, each of *Beser's* disclosed embodiments is directed at providing increased communication security by hiding the addresses of the originating and terminating devices. (*See generally* Ex. 1007.) And while Petitioner claims that *Beser* "teaches that IP tunnels are and should ordinarily be encrypted," its citations to *Beser* fail to support this point. (Pet. at 31.) Petitioner cites to the statement that "the sender may encrypt the information inside the IP packets before

transmission," but this is found in *Beser's* "Background of the Invention" section and is part of a description of the prior art systems over which *Beser's* method is distinguished. (*Id.* at 26, 28, 30, 31, 47.) Petitioner further claims that because *Beser* refers to the IPSec protocol, one of skill would have combined *Beser's* tunnel with RFC 2401. (*Id.* at 30-31.) But again, the IPSec protocol is mentioned in the "Background of the Invention" and in connection with the problems in the prior art that *Beser* is attempting to overcome. (Ex. 1007 at 1:54-67.)

54. Petitioner next points to *Beser's* teaching that "[t]he first IP 58 packet 232 may require encryption or authentication to ensure that the public IP 58 address of the second network device 16 cannot be read on the public network 12" (*id.* at 18:2-5) to contend that "IP tunnels are and should ordinarily be encrypted." (Pet. at 31; *see also id.* at 26, 28, 33.) In my opinion, Petitioner's statement incorrectly characterizes *Beser*. As Petitioner concedes, this statement in *Beser* describes only the establishment of a tunnel (the alleged encrypted communication link). (*Id.* at 31.) Specifically, *Beser* explains that during the set-up of a tunneling association, encryption may be used to hide the identity of network device 16 (e.g., the router). (*See* Ex. 1007 at 18:2-5.) However, *Beser* also teaches that encryption does not deter a determined hacker from deducing source and identity information, and so, once the tunnel is established, *Beser* eschews encryption in favor of hiding the identities within the tunnel. Moreover, because one of skill would have

understood that the purpose of the encryption is simply to hide address information on the public network prior to *Beser's* tunnel establishment, once the tunnel is created, the originating and terminating device information is hidden and encryption would not only be redundant, it would contravene *Beser's* express objective of increasing security without increasing computational burden. Thus, one of skill would have understood that *Beser* does not use encryption in transmitting data over the established tunnel and, in fact, teaches away from doing so.

55. The Institution Decision points to the fact that *Beser* "characterizes some prior art systems as creating 'security problems by preventing certain types of encryption from being used'" as evidence that *Beser* does not teach away from adding encryption to its system. (Institution Decision at 12 (citing Ex. 1007 at 2:23-24).) In my opinion, one of ordinary skill in the art would understand that the opposite is true. *Beser* acknowledges that in certain systems, certain types of *encryption cannot be used*. *Beser* manages to obtain its desired security without adding encryption to its system.

VII. Conclusion

56. 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 by fine or imprisonment, or both, under Section 1001 or Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the ’009 patent.

Executed this 11th day of December 2015 in Chapel Hill, North Carolina.

/Fabian Monrose/

Fabian Monrose

Appendix A

Fabian N. Monrose

[A] UNIVERSITY OF NORTH CAROLINA, CHAPEL HILL
Computer Science Department
Sitterson Hall, Chapel Hill, NC, 27599

Phone: +919-962-1763
Fax: +919-962-1799
E-mail: fabian@cs.unc.edu

Last update: December 10, 2015

[B] Education

Ph. D., Computer Science, *Courant Institute of Mathematical Sciences*
New York University, New York, USA May, 1999
Advisor: Prof. Zvi Kedem

M. Sc., Computer Science, *Courant Institute of Mathematical Sciences*
New York University, New York, USA May, 1996

B. Sc., Computer Science, *Barry University*
Miami, Florida, USA May, 1993

[C] Professional Experience

DIRECTOR, Computer and Information Security, Renaissance Computing Institute (RENCI, joint appointment), January 2014 — present

PROFESSOR, *University of North Carolina, Chapel Hill*
Computer Science Department, January 2013 — present

ASSOCIATE PROFESSOR, *University of North Carolina, Chapel Hill*
Computer Science Department, July 2008 — December, 2012

ASSOCIATE PROFESSOR, *Johns Hopkins University*
Computer Science Department, July 2007 —June 2008

ASSISTANT PROFESSOR, *Johns Hopkins University*
Computer Science Department, November 2002 — June 2007

RESEARCH SCIENTIST, *Bell Laboratories, Lucent Technologies*
Secure Systems Research, July 1999 — October 2002

RESEARCH INTERN, *AT&T Labs Research*
Secure Systems Research Department, Summer 1998

RESEARCH INTERN, *Bell Communications*
High Availability and Distributed Computing Research Group, Summer 1997

RESEARCH INTERN, *Bell Communications*
Cryptography and Network Security Research Group, Summer 1996

RESEARCH ASSISTANT, *New York University*
Computer Science Department, August 1995 — 1998

RESEARCH ASSISTANT, *New York University*
Distributed Systems Group, Summer 1994

[D] Honors

- Undergraduate Students Teaching Award, *Computer Science Dpt.* May, 2015
- Best Student Paper Award, *IEEE Symposium on Security & Privacy* May, 2013
- Outstanding Research in *Privacy Enhancing Technologies* (PET), July, 2012
- AT&T Best Applied Security Paper Award, *NYU-Poly CSAW*, Nov, 2011
- Best Paper Award, *IEEE Symposium on Security & Privacy*, May, 2011
- Best Paper Award, *Intl. Conf. on Internet Monitoring and Protection*, April, 2011
- Faculty Research Award, *Google* May, 2011
- Faculty Research Award, *Google* March, 2009
- CAREER Award, *National Science Foundation*, February, 2006
- Best Student Paper Award, 8^{th} *USENIX Security Symposium* August, 1999
- Best Overall Paper Award, 8^{th} *USENIX Security Symposium* August, 1999
- USENIX Scholars Research Award Fall 1998
- Bell Communications Research Scholarship Fall 1997

[E]: Funding Awarded Grants & Contracts

[G1] **Co-PI** (with Jan-Michel Frahm (*lead*)), Department of Defense University Research Instrumentation Program (DURIP), UNDERSTANDING PRIVACY RISKS OF UBIQUITOUS PERSONAL AUGMENTED REALITY HEAD-MOUNTED DISPLAYS for $\$95,385.00$, June, 2014 — May 2015.

[G2] **PI** (with A. Stavrou), NSF *Secure and Trustworthy Computing*, TWC: TTP OPTION: SMALL: SCALABLE TECHNIQUES FOR BETTER SITUATIONAL AWARENESS: ALGORITHMIC FRAMEWORKS AND LARGE SCALE EMPIRICAL ANALYSES for $\$667,900.00$, Sept. 2014—August 2017.

[G3] **PI** Department of Homeland Security *Transition to Practice Program*, SUPPLEMENT TO NSF SDCI SEC: NEW SOFTWARE PLATFORMS FOR SUPPORTING NETWORK-WIDE DETECTION OF CODE INJECTION ATTACKS for $\$350,000.00$, Sept. 2014—August 2015.

[G4] **PI**, Department of Defense University Research Instrumentation Program (DURIP), NEXT-GENERATION DEFENSES FOR SECURING VOIP COMMUNICATIONS for $\$114,345.00$,

June, 2013 — May 2014.

[G5] **PI**, NSF *Secure and Trustworthy Computing*, SUPPORT FOR THE 2014 USENIX SECURITY SYMPOSIUM; SAN DEIGO for $\$20,000.00$, July 30, 2014— October 2015.

[G6] **PI** (with Elliott Moreton and Jennifer Smith), NSF *Secure and Trustworthy Computing*, TOWARD PRONOUNCEABLE AUTHENTICATION STRINGS for $\$499,997.00$, Aug. 2013— July 2016.

[G7] **PI**, NSF *Secure and Trustworthy Computing*, SUPPORT FOR THE 2013 USENIX SECURITY SYMPOSIUM; WASHINGTON D.C. for $\$10,000.00$, July 30, 2013— October 2013.

[G8] **PI**, Department of Homeland Security, EFFICIENT TRACKING, LOGGING, AND BLOCKING OF ACCESSES TO DIGITAL OBJECTS (with C. Schmitt and M. Bailey) for $\$1,035,590$. September 2012 — August 2014.

[G9] **Co-PI** (with Jan-Michel Frahm (*lead*)), NSF *Division of Information & Intelligent Systems*, EAGER: AUTOMATIC RECONSTRUCTION OF TYPED INPUT FROM COMPROMISING REFLECTIONS for $\$151,749.00$, August 2011—July 2013.

[G10] **PI**, *Verisign Labs Research Awards Program*, ON EXPLORING APPLICATIONS OF PHONETIC EDIT DISTANCE for $\$65,000.00$, June 2011.

[G11] **PI**, *Google Faculty Research Awards Program*, SHELLOS: AN EFFICIENT RUNTIME PLATFORM FOR DETECTING CODE INJECTION ATTACKS for $\$61,635.00$, May 2011.

[G12] **PI** (with Montek Singh), NSF *Office of Cyberinfrastructure*, SDCI SEC: NEW SOFTWARE PLATFORMS FOR SUPPORTING NETWORK-WIDE DETECTION OF CODE INJECTION ATTACKS for $\$800,000.00$, Aug. 2011—July 2014.

[G13] **PI**, NSF *Trustworthy Computing*, SUPPORT FOR THE 2011 USENIX SECURITY SYMPOSIUM; SAN FRANCISCO for $\$20,000.00$, July 30, 2011— October 2011.

[G14] **PI** (with Kevin Jeffay), NSF *Trustworthy Computing*, TC: SMALL: EXPLORING PRIVACY BREACHES IN ENCRYPTED VOIP COMMUNICATIONS for $\$496,482.00$, Aug. 2010—July 2013.

[G15] **PI**, NSF *Trustworthy Computing*, SUPPORT FOR THE 2010 USENIX SECURITY SYMPOSIUM; WASHINGTON D.C. for $\$20,000.00$, July 30, 2010— October 2010.

[G16] **Co-PI** (with Angelos Stavrou (*lead*)), NSF *Trustworthy Computing*, COLLABORATIVE RESEARCH: SCALABLE MALWARE ANALYSIS USING LIGHTWEIGHT VIRTUALIZATION for $\$259,264.00$, Sept. 2009—August 2011.

[G17] **PI** (with Angelos Stavrou), DETECTING AND MONITORING MALFEASANCE ON THE NET, Google Faculty Research Awards Program for $\$90,000.00$, March 2009–Feb 2010.

[G18] **Co-PI**, NSF *Cyber Trust*: CLEANSE:CROSS-LAYER LARGE-SCALE EFFICIENT ANALYSIS OF NETWORK ACTIVITIES TO SECURE THE INTERNET (with W. Lee (*lead*), N. Feamster, J. Giffin, M.K. Reiter, F. Jahanian, P. Porras, P. Vixie, D. Dagon) for $\$1,839,297.00$, July 2008 — June 2012.

[G19] **PI**, Department of Homeland Security, NEW FRAMEWORKS FOR DETECTING AND MINIMIZING INFORMATION LEAKAGE IN ANONYMIZED NETWORK DATA (with M. K. Reiter and F. Jahanian) for $\$962,609.00$. April 2008—April 2011.

[G20] **Co-PI** (with G. Masson (*lead*)), SECURITY THROUGH VIRTUALIZATION. Information Assurance Scholarship Program for $\$142,948.00$. DoD, ANNEX II, Feb, 2008.

[G21] **Co-PI**, NSF *Cyber Trust*: THINKING AHEAD: A PROACTIVE APPROACH FOR COUNTERING FUTURE INTERNET MALWARE (with A. Terzis (*lead*)) for $\$350,000.00$. September 2006 — August 2009.

[G22] **PI**, NSF *Cyber Trust*: CAREER:TOWARDS EFFECTIVE IDENTIFICATION OF APPLICATION BEHAVIORS IN ENCRYPTED TRAFFIC for $\$400,000.00$. September 2006 — August 2011.

[G23] **PI**, NSF *Cyber Trust*: GENERATIVE MODELS FOR IMPROVING BIOMETRICALLY ENHANCED SYSTEMS (with D. Lopresti and M. K. Reiter) for $\$696,553.00$. December 2004 — October 2007.

[G24] **Co-PI**, NSF *STI*: TOWARDS MORE SECURE INTER-DOMAIN ROUTING (with A. Rubin (*lead*)) for $\$616,923.00$. November 2003 — June 2006.

[F] Bib.

Refereed Conference Publications

[P1] *Detecting Malicious Exploit Kits using Tree-based Similarity Searches*. Teryl Taylor, Xin Hu, Ting Wang, Jiyong Jang, Marc Stoeckin, Fabian Monrose and Reiner Sailer. In Proceedings of the ACM Conference on Data and Application Security and Privacy, March, 2016.

[P2] *Cache, Trigger, Impersonate: Enabling Context-Sensitive Honeyclient Analysis On-the-Wire*. Teryl Taylor, Kevin Snow, Nathan Otterness and Fabian Monrose. In Proceedings of the 23^{nd} ISOC Network and Distributed Systems Security Symposium (NDSS), Feb., 2016. (Acceptance rate=15.4%).

[P3] *Isomeron: Code Randomization Resilient to (Just-in-Time) Return-Oriented Programming*. Luca Davi, Christopher Liebchen, Ahmad-Reza Sadeghi, Kevin Z. Snow, and Fabian Monrose. In Proceedings of the 22^{nd} ISOC Network and Distributed Systems Security Symposium (NDSS), Feb., 2015. (Acceptance rate=21%).

[P4] *Watching the Watchers: Inferring TV Content from Outdoor Light Effusions*. Yi Xu, Jan-Michael Frahm and Fabian Monrose. In Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS), November, 2014. (Acceptance rate=19%).

[P5] *Emergent Faithfulness to Morphological and Semantic Heads in Lexical Blends*. Katherine Shaw, Elliott Moreton, Andrew White and Fabian Monrose. In Proceedings of the Annual Meeting on Phonology, February, 2014.

[P6] *Seeing Double: Reconstructing Obscured Typed Input from Repeated Compromising Reflections*. Yi Xu, Jared Heinly, Andrew M. White, Fabian Monrose and Jan-Michael Frahm. In Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS), November, 2013. (Acceptance rate=20%)

[P7] *Check my profile: Leverage static analysis for fast and accurate detection of ROP gadgets*. Blaine Stancill, Kevin Snow, Nathan Otterness, Fabian Monrose, Lucas Davi, and Ahmad-Reza Sadeghi. In Proceedings of the 16th International Symposium on Research in Attacks, Intrusions, and Defenses, October, 2013.

[P8] *Crossing the Threshold: Detecting Network Malfeasance via Sequential Hypothesis Testing*. Srinivas Krishnan, Teryl Taylor, Fabian Monrose and John McHugh. In Proceedings of the 42^{nd} Annual IEEE/IFIP International Conferences on Dependable Systems and Networks; Performance and Dependability Symposium, June, 2013.

[P9] *Just-In-Time Code Reuse: On the Effectiveness of Fine-Grained Address Space Layout Randomization*. Kevin Snow, Lucas Davi, Alexandra Dmitrienko, Christopher Liebchen, Fabian Monrose and Ahmad-Reza Sadeghi. In Proceedings of 34^{th} IEEE Symposium on Security and Privacy, May, 2013. (**Best Student Paper Award**). (Acceptance rate=12%)

[P10] *Clear and Present Data: Opaque Traffic and its Security Implications for the Future*. Andrew White, Srinivas Krishnan, Michael Bailey, Fabian Monrose and Phil Porras. In Proceedings of the 20^{th} ISOC Network and Distributed Systems Security Symposium, Feb., 2013. (Acceptance rate=18.8%)

[P11] *Security and Usability Challenges of Moving-Object CAPTCHAs: Decoding Codewords in Motion*. Yi Xu, Gerardo Reynaga, Sonia Chiasson, Jan-Michael Frahm, Fabian Monrose and Paul van Oorschot. In Proceedings of the 21^{th} USENIX Security Symposium, August, 2012. (Acceptance rate=19%)

[P12] *Toward Efficient Querying of Compressed Network Payloads*. Teryl Taylor, Scott E. Coull, Fabian Monrose and John McHugh. In USENIX Annual Technical Conference, June, 2012. (Acceptance rate=18%)

[P13] *iSpy: Automatic Reconstruction of Typed Input from Compromising Reflections*. Rahul Raguram, Andrew White, Dibyendusekhar Goswami, Fabian Monrose and Jan-Michael Frahm. In Proceedings of the 18^{th} ACM Conference on Computer and Communications Security (CCS), November, 2011. (Acceptance rate=14%)

[P14] *ShellOS: Enabling Fast Detection and Forensic Analysis of Code Injection Attacks*. Kevin Snow, Srinivas Krishnan, Fabian Monrose and Niels Provos. In Proceedings of the 20^{th} USENIX Security Symposium, August, 2011. (Acceptance rate=17%)

[P15] *An Empirical Study of the Performance, Security and Privacy Implications of Domain Name Prefetching*. Srinivas Krishnan and Fabian Monrose. In Proceedings of the 41^{st} Annual IEEE/IFIP International Conferences on Dependable Systems and Networks; Dependable Computing and Communications Symposium, June, 2011. (Acceptance rate=17.6%)

[P16] *Amplifying Limited Expert Input to Sanitize Large Network Traces*. Xin Huang, Fabian Monrose, and Michael K. Reiter. In Proceedings of the 41^{st} Annual IEEE/IFIP Interna-

tional Conferences on Dependable Systems and Networks; Performance and Dependability Symposium, June, 2011.

[P17] *Phonotactic Reconstruction of Encrypted VoIP Conversations*. Andrew White, Kevin Snow, Austin Matthews and Fabian Monrose. In Proceedings of 32^{nd} IEEE Symposium on Security and Privacy, May, 2011. (**Best Paper Award**). (Acceptance rate=11.1%)

[P18] *Towards Optimized Probe Scheduling for Active Measurement Studies*. Daniel Kumar, Fabian Monrose and Michael K. Reiter. In Proceedings of the 6^{th} International Conference on Internet Monitoring and Protection (ICIMP), March, 2011 (**Best Paper Award**).

[P19] *On Measuring the Similarity of Network Hosts: Pitfalls, New Metrics, and Empirical Analyses*. Scott Coull, Micheal Bailey and Fabian Monrose. In Proceedings of the 18^{th} Annual Network and Distributed Systems Security Symposium, February, 2011. (Acceptance rate=20%)

[P20] *Trail of Bytes: Efficient Support for Forensic Analysis*. Srinivas Krishnan, Kevin Snow, and Fabian Monrose. In Proceedings of the 17^{th} ACM Conference on Computer and Communications Security (CCS), November, 2010. (Acceptance rate=17.2%)

[P21] *The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis*. Yinqian Zhang, Fabian Monrose, and Michael K. Reiter. In Proceedings of the 17^{th} ACM Conference on Computer and Communications Security (CCS), November, 2010. (Acceptance rate=17.2%)

[P22] *Traffic Classification using Visual Motifs: An Empirical Evaluation*. Wilson Lian, Fabian Monrose and John McHugh. In Proceedings of the 7^{th} International Symposium on Visualization for Cyber Security (VizSec), September, 2010.

[P23] *Understanding Domain Registration Abuses*. Scott Coull, Andrew White, Ting-Fang Yen, Fabian Monrose and Michael K. Reiter. In Proceedings of the International Information Security Conference, September, 2010.

[P24] *English Shellcode*. Josh Mason, Sam Small, Greg McManus and Fabian Monrose. In Proceedings of the 16^{th} ACM Conference on Computer and Communications Security (CCS), pages 524-533, November, 2009. (Acceptance rate=18.4%)

[P25] *Browser Fingerprinting from Coarse Traffic Summaries: Techniques and Implications*. Ting-Fang Yen, Xin Huang, Fabian Monrose and Michael K. Reiter. In Proceedings of 6^{th} Conference on Detection of Intrusions and Malware and Vulnerability Assessment, pages 157-175, July, 2009.

[P26] *Toward Resisting Forgery Attacks via Pseudo-Signatures*. Jin Chen, Dan Lopresti and Fabian Monrose. In Proceedings of 10^{th} International Conference on Document Anaalysis and Recognition (ICDAR), July, 2009.

[P27] *The Challenges of Effectively Anonymizing Network Data*. Scott Coull, Fabian Monrose, Michael K. Reiter and Michael Bailey. In Proceedings of the DHS Cybersecurity Applications and Technology Conference for Homeland Security (CATCH), pages 230-236, 2009.

[P28] *Efficient Defenses Against Statistical Traffic Analysis*. Charles Wright, Scott Coull and Fabian Monrose. In Proceedings of Network and Distributed Systems Security, pages 237-250 Feb, 2009. (Acceptance rate=11.7%).

[P29] *Towards Practical Biometric Key Generation with Randomized Biometric Templates*. Lucas Ballard, Seny Kamara, Fabian Monrose, and Michael K. Reiter. In Proceedings of the 15^{th} ACM Conference on Computer and Communications Security, pages 235-244. Oct, 2008. (Acceptance rate=18.2%).

[P30] *All Your iFrames point to us: Characterizing the new malware frontier*. Niels Provos, Panayiotis Mavrommatis, Moheeb Rajab, and Fabian Monrose. In Proceedings of the 17^{th} USENIX Security Symposium, pages 1-15, July, 2008. (Acceptance rate=15.9%).

[P31] *To Catch a Predator: A Natural Language Approach for Eliciting Protocol Interaction*. Sam Small, Josh Mason, Fabian Monrose, Niels Provos and Adam Stubblefield. In Proceedings of the 17^{th} USENIX Security Symposium, pages 171-183, July, 2008. (Acceptance rate=15.9%).

[P32] *Peeking Through the Cloud: DNS-based client estimation techniques and its applications*. Moheeb Rajab, Niels Provos, Fabian Monrose and Andreas Terzis. In Proceedings of the 6^{th} Applied Cryptography and Network Security conference (ACNS), pages 21-38, June, 2008.

[P33] *Spot Me If You Can: recovering spoken phrases in encrypted VOIP conversations*. Charles Wright, Lucas Ballard, Scout Coull and Fabian Monrose. In Proceedings of 29^{th} IEEE Symposium on Security and Privacy, May, 2008 (17 pages).(Acceptance rate=11.2%).

[P34] *Taming the Devil: Techniques for Evaluating Anonymized Network Data*. Scott Coull, Charles Wright, Angelos Keromytis, Fabian Monrose, and Michael Reiter. In Proceedings of the 15^{th} Annual Network and Distributed Systems Security Symposium, pages 125-146, Feb., 2008 (Acceptance rate=18%).

[P35] *On Web Browsing Privacy in Anonymized NetFlows*. Scott Coull, Michael Collins, Charles Wright, Fabian Monrose, and Michael Reiter. In Proceedings of the 16^{th} USENIX Security Symposium, pages 339-352, August, 2007. (Acceptance rate=12.29%).

[P36] *Language Identification of Encrypted VoIP Traffic: Alejandra y Roberto or Alice and Bob?* Charles Wright, Lucas Ballard, Fabian Monrose and Gerald Masson. In Proceedings of the 16^{th} USENIX Security Symposium, pages 43-54, August, 2007. (Acceptance rate=12.29%).

[P37] *Towards Valley-free Inter-domain Routing*. Sophie Qiu, Patrick McDaniel and Fabian Monrose. In Proceedings of the IEEE International Conference on Communications, June, 2007. (8 pages)

[P38] *Playing Devil's Advocate: Inferring Sensitive Information from Anonymized Traces*. Scott Coull, Charles Wright, Fabian Monrose, Michael Collins and Michael Reiter. In Proceedings of the 14^{th} Annual Network and Distributed Systems Security Symposium (NDSS), pages 35-47, February 2007. (Acceptance rate=15%).

[P39] *A Multifaceted Approach to Understanding the Botnet Phenomenon*. Jay Zarfoss, Moheeb Rajab, Fabian Monrose, and Andreas Terzis. In Proceedings of the ACM SIGCOMM/-USENIX Internet Measurement Conference (IMC), pages 41-52, October, 2006. (Acceptance rate=15.25%).

[P40] *Fast and Evasive Attacks: Highlighting the Challenges Ahead*. Moheeb Rajab, Fabian Monrose, and Andreas Terzis. In Proceedings of the 9^{th} International Symposium on Recent Advances in Intrusion Detection (RAID), pages 206-225, September, 2006 (Acceptance rate=17.2%).

[P41] *Biometric Authentication Revisited: Understanding the Impact of Wolves in Sheep's Clothing*. Lucas Ballard, Fabian Monrose, and Daniel Lopresti. In Proceedings of the USENIX Security Symposium, pages 29-41, August 2006 (Acceptance rate=12.3%).

[P42] *On Origin Stability in Inter-Domain Routing*. Sophie Qui, Patrick McDaniel, Fabian Monrose and Aviel D. Rubin. In Proceedings of IEEE International Symposium on Computers and Communications (ISCC), pages 489-496, July, 2006.

[P43] *Memory Bound Puzzles: A Heuristic Approach*. Sujata Doshi, Fabian Monrose and Aviel D. Rubin. In Proceedings of the International Conference on Applied Cryptography and Network Security (ACNS), pages 98-113, June 2006 (Acceptance rate=15.13%).

[P44] *Achieving Efficient Conjunctive Searches on Encrypted Data*. Lucas Ballard, Seny Kamara and Fabian Monrose. In Proceedings of 7^{th} International Conference on Information and Communications Security (ICICS), pages 414-426, December, 2005. (Acceptance rate=18%)

[P45] *On the Effectiveness of Distributed Worm Monitoring*. Moheeb Rajab, Fabian Monrose and Andreas Terzis. In Proceedings of 14^{th} USENIX Security Symposium, pages 225-237, August, 2005. (Acceptance rate=14.8%)

[P46] *Scalable VPNs for the Global Information Grid*. Bharat Doshi, Antonio De Simone, Fabian Monrose, Samuel Small, and Andreas Terzis. In Proceedings of IEEE MILCOM, May, 2005. (7 pages)

[P47] *An Extensible Platform for Evaluating Security Protocols*. Seny Kamara, Darren Davis, Ryan Caudy and Fabian Monrose. In Proceedings of the 38^{th} Annual IEEE Simulation Symposium (ANSS), pages 204-213, April, 2005.

[P48] *Efficient Time Scoped Searches on Encrypted Audit Logs*. Darren Davis, Fabian Monrose, and Michael Reiter. In Proceedings of the 5^{th} International Conference on Information and Communications Security (ICICS), pages 532-545, October, 2004. (Acceptance rate=17%)

[P49] *On User-Choice in Graphical Password Systems*. Darren Davis, Fabian Monrose, and Michael Reiter. In Proceedings of the 13^{th} USENIX Security Symposium, pages 151-164, August, 2004. (Acceptance rate=12%)

[P50] *Toward Speech-Generated Cryptographic Keys on Resource Constrained Devices*. Fabian Monrose, Micheal Reiter, Daniel Lopresti, Chilin Shih, and Peter Li. In Proceedings of the 11^{th} USENIX Security Symposium, pages 283–296, August, 2002. (Acceptance rate=16%)

[P51] *Using Voice to Generate Cryptographic Keys: A Position Paper*. Fabian Monrose, Michael Reiter, Peter Li and Susanne Wetzel. In Proceedings of the 2001: A Speaker Odyssey workshop, pages 237-242, 2001.

[P52] *Cryptographic Key Generation from Voice*. Fabian Monrose, Michael Reiter, Peter Li and Susanne Wetzel. In Proceedings of the 21^{st} Annual IEEE Symposium on Security & Privacy, pages 202-212, May 2001. (Acceptance rate=17.75%)

[P53] *Privacy-Preserving Global Customization*. Bob Arlein, Ben Jai, Markus Jakobsson, Fabian Monrose, and Michael Reiter. In Proceedings of the 2^{nd} ACM Conference on Electronic Commerce, pages 176-184. April 2000. (Acceptance rate=18%)

[P54] *Password Hardening using Keystroke Dynamics*. Fabian Monrose, Michael K. Reiter and Susanne Wetzel. In Proceedings of the 6^{th} ACM Conference on Computer and Communications Security, pages 73-82, November 1999. (Acceptance rate=19.3%)

[P55] *The Design and Analysis of Graphical Passwords*. Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter and Aviel D. Rubin. In Proceedings for the 8^{th} USENIX Security Symposium, pages 1-14, August 1999. (**Best Paper Award**). (Acceptance rate=26%)

[P56] *Distributed Execution with Remote Audit*. Fabian Monrose, Peter Wyckoff and Aviel D. Rubin. In Proceedings of the ISOC Network and Distributed Systems Security Symposium (NDSS), pages 103-113, February 1999. (Acceptance rate=24%)

[P57] *Third Party Validation for Java Applications*. Ian Jermyn, Fabian Monrose, and Peter Wyckoff. In Proceedings of the International Conference on Computers and their Applications, March 1998.

[P58] *Authentication via Keystroke Dynamics*. Fabian Monrose and Aviel D. Rubin. In Proceedings of the 4^{th} ACM Conference on Computer and Communications Security, pages 48-56, April 1997. (Acceptance rate=26.6%)

Refereed
Journal
Publications

[P59] *Security and Usability Challenges of Moving-Object CAPTCHAs: Decoding Codewords in Motion*. Yi Xu, Gerardo Reynaga, Sonia Chiasson, Jan-Michael Frahm and Fabian Monrose. IEEE Transactions on Dependable and Secure Computing, February, 2014.

[P60] *On the Privacy Risks of Virtual Keyboards: Automatic Reconstruction of Typed Input from Compromising Reflections*. Rahul Raguram, Andrew White, Yi Xu, Jan-Michel Frahm, Pierre Georgel, and Fabian Monrose. IEEE Transactions on Dependable and Secure Computing, Volume 10, Issue 3, pages 154-167, May-June, 2013.

[P61] *Trail of Bytes: New Techniques for Supporting Data Provenance and Limiting Privacy Breaches*. Srinivas Krishnan, Kevin Snow, and Fabian Monrose. IEEE Transactions on Information Forensics and Security, pages 1876-1889, Issue 6, Volume 7, 2012.

[P62] *Understanding Domain Registration Abuses (Invited Paper)*. Scott Coull, Andrew White, Ting-Fang Yen, Fabian Monrose and Michael K. Reiter. Special Issue of Computers & Security (COSE), pages 806-815, Volume 31, Number 7, October, 2012.

[P63] *Uncovering Spoken Phrases in Encrypted Conversations*. Charles Wright, Lucas Ballard, Scott Coull, Fabian Monrose, and Gerald Masson. ACM Transactions on Information and Systems Security (TISSEC), Volume 13, Number 4, pages 1 - 30, December, 2010.

[P64] *Peeking Through the Cloud: Client Density Estimation via DNS Cache Probing*. Moheeb Abu Rajab, Fabian Monrose and Niels Provos. ACM Transactions on Internet Technologies (TOIT), Volume 10, Number 3, October, 2010.

[P65] *Forgery Quality for Behavioral Biometric Security*. Lucas Ballard, Daniel Lopresti and Fabian Monrose. IEEE Transactions on System, Man and Cybernetics, (Special Issue on Biometric Security), pages 1107-1118, December, 2006. (Acceptance rate=18.75%).

[P66] *On Inferring Application Protocol Behaviors in Encrypted Network Traffic*. Charles Wright, Fabian Monrose, and Gerald Masson. Journal of Machine Learning Research (Special Issue on Machine Learning for Computer Security), Volume 7, pages 2745-2769, December, 2006. (Acceptance rate=20%)

[P67] *Password Hardening using Keystroke Dynamics*. Fabian Monrose, Micheal Reiter, and Susanne Wetzel. In Journal of Information Security (IJCS), Volume 1, Number 2, pages 69-83, February 2002.

[P68] *Keystroke Dynamics as a Biometric for Authentication*. Fabian Monrose and Aviel D. Rubin. Future Generation Computing Systems Journal: Security on the Web (Special Issue), pages 351-359, volume 16, March 2000.

Refereed
Workshop
Publications

[P69] *Isn't that Fantabulous: Security, Linguistic and Usability Challenges of Pronounceable Tokens*. Andrew White, Katherine Shaw, Fabian Monrose and Elliott Moreton. In Proceedings of the New Security Paradigms Workshop (NSPW), September, 2014. (Acceptance rate=32%).

[P70] *Automatic Hooking for Forensic Analysis of Document-based Code Injection Attacks: Techniques and Empirical Analyses*. Kevin Snow and Fabian Monrose. In Proceedings of the European Workshop on System Security (EuroSec), April, 2012. (6 pages).

[P71] *DNS Prefetching and Its Privacy Implications*. Srinivas Krishnan and Fabian Monrose. In Proceedings of the 3rd USENIX Workshop on Large-Scale Exploits and Emergent Threats, April, 2010. (9 pages)

[P72] *Secure Recording of Accesses to a Protected Datastore*. Srinivas Krishnan and Fabian Monrose. In Proceedings of the 2nd ACM Workshop on Virtual Machine Security (VMSec), pages 23-32, November, 2009.

[P73] *My Botnet is Bigger than Yours (Maybe, Better than Yours): Why size estimates remain challenging.* Moheeb Rajab, Jay Zarfoss, Fabian Monrose and Andreas Terzis. In Proceedings of USENIX Workshop on Hot Topics in Understanding Botnets, April, 2007 (Acceptance rate=32.4%) (8 pages).

[P74] *Using Visual Motifs to Classify Encrypted Traffic*. Charles Wright, Fabian Monrose and Gerald Masson. In Proceedings of the ACM Workshop of Visualization for Computer Security (VizSEC), November, 2006 (Acceptance rate=34%) (8 pages).

[P75] *On the Impact of Dynamic Addressing on Malware Propagation*. Moheeb Rajab, Fabian Monrose, and Andreas Terzis. In Proceedings of the 4^{th} ACM Workshop of Recurring Malcode (WORM), November, 2006 (Acceptance rate=29%) (8 pages)

[P76] *Efficient Techniques for Detecting False Origin Advertisements in Inter-domain Routing*. Sophie Qui, Patrick McDaniel, Fabian Monrose, and Andreas Terzis. In Proceedings of the 2^{nd} Workshop on Secure Network Protocols, pages 12-19, November 2006. (Acceptance rate=40%).

[P77] *Evaluating the Security of Handwriting Biometrics*. Lucas Ballard, Daniel Lopresti and Fabian Monrose. In Proceedings of the 10^{th} International Workshop on Frontiers in Handwriting Recognition, pages 461-466, October, 2006 (Acceptance rate=28.5%).

[P78] *Worm Evolution Tracking via Timing Analysis*. Moheeb Rajab, Fabian Monrose and Andreas Terzis. In Proceedings of the 3^{rd} ACM Workshop on Recurring Malware (WORM), pages 52-59, November, 2005 (Acceptance rate=25%).

[P79] *HMM Profiles for Network Traffic Classification (extended Abstract)*. Charles Wright, Fabian Monrose and Gerald Masson. In Proceedings of ACM Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC), pages 9-15, October, 2004.

Book Chapters

[B1] *Graphical Passwords (revisited)*. Fabian Monrose and Micheal Reiter. *Security and Usability: Designing Security Systems That People Can Use*. Editors: Lorrie Cranor and Simson Garfinkel. OReilly & Associates, 2005.

Manuscripts in Progress

[U80] Mining the Forest for the Subtrees: A Large-scale Comparative Study of Subtree Mining Algorithms. T. Taylor, M. Stoecklin, X. Hu, J. Jang, T. Wang, and F. Monrose. Submitted to International Journal on Data Mining and Knowledge Discovery, March 2015.

[U81] Robust and Efficient Detection of Transformed Video Content. Y. Xu, J-M. Frahm, and Fabian Monrose. In submission to ACM Conference on Computer and Commmunication Security, 2015.

[U82] Finding the Rotten Sapling in the Forest: Detecting Exploit Kits through Tree-based Similarity Searches. T. Taylor, M. Stoecklin, X. Hu, T. Wang, and F. Monrose. In submission to ACM Conference on Computer and Communication Security, 2015.

[U83] Tackling the Fear of the Unknown in Network Security: New methods and large-scale empirical analyses. C. Lever, Y. Nadji, F. Monrose, D. Dagon and M. Antonakakis. In preparation for submission to ACM Internet Measurement Conference, May, 2015.

[U84] Toward Scalable Real-time Identification of Web Pages in Encrypted Traffic. A. White, M. Stoecklin, X. Hu, T. Wang, D.L. Scales, R. Sailer, M. Christodorescu and F. Monrose. In preparation for submission to IEEE EuroS&P, 2015.

Other Manuscripts

[M2] *Towards Stronger User Authentication*, Ph.D. Thesis. Fabian Monrose. Courant Institute of Mathematical Sciences, New York University, May 1999.

[M3] *Correlation Resistant Storage*. Lucas Ballard, Mathew Green, Breno *de* Medeiros and Fabian Monrose. Cryptology ePrint Archive Report 2005/417.

[M4] *Evaluating Biometric Security (Invited Paper)*. Daniel Lopresti, Lucas Ballard and Fabian Monrose. In Proceedings of the 1^{st} Korea-Japan Workshop on Pattern Recognition, November 2006. (6 pages)

[M5] *Biometric Key Generation using Pseudo-Signatures* (Poster Presentation). Lucas Ballard, Jin Chen, Daniel Lopresti and Fabian Monrose. In International Conference on Frontiers of Handwriting Recognition, Feb. 2008 (8 pages).

[M6] *Masquerade: Simulating a Thousand Victims* Sam Small, Josh Mason, Ryan MacArthur. In ;login: The USENIX Magazine, December 2008.

[M7] *Amplifying Limited Expert Input to Sanitize Large Network Traces: Framework and Privacy Analysis*. Xin Huang, Fabian Monrose, and Michael K. Reiter. Submitted to International Journal of Information Security, Sept, 2011. *Under review*.

[G]: Teaching Activities

- *Introduction to Computer Security*, Spring 2013, 40 students.
- *Network Security*, Fall 2008, 21 students.
- *Special Topics in Computer Science*, Spring 2009, 7 students.
- *Network Security*, Fall 2009, 16 students.
- *Introduction to Computer Security*, Spring 2010, 17 students.
- *Network Security*, Fall 2010, 11 students.
- *Introduction to Computer Security*, Spring 2012, 46 students.

Past & Current Students

- Sophie Qui (Co-Advisee), Ph.D., Spring 2007, (*Cisco Systems*)
- Charles Wright, Spring 2008, Ph.D., (*Portland State University*)

- Seny Kamara, Spring 2008, Ph.D., (*Microsoft Research*)
- Moheeb Abu Rajab (Co-Advisee), Ph.D., Spring 2008, (*Google Inc.*)
- Lucas Ballard, Spring 2008, Ph.D., (*Google Inc.*)
- Scott Coull, Fall 2009, Ph.D., (*RedJack*)
- Josh Mason, Fall 2009, Ph.D., (*Independent Consultant*)
- Andrew White (current), Ph.D. candidate, *UNC Chapel Hill*
- Kevin Snow (current), Ph.D. candidate, *UNC Chapel Hill*
- Teryl Taylor (current), Ph.D. candidate, *UNC Chapel Hill*
- Srinivas Krishnan (co-advised with K. Jeffay; current), Ph.D. candidate, *UNC Chapel Hill*
- Yi Xu (co-advised with Jan-Michael Frahm; current), *UNC Chapel Hill*

Doctoral Committees

- (**Reader**) Breno de Medeiros, *New Cryptographic Primitives and Applications*, Ph.D., Johns Hopkins University, May 2004
- (**Reader**) Kendall Giles, *Knowledge Discovery in Computer Network Data: A Security Perspective*, Ph.D., Johns Hopkins University, October, 2006
- (**Advisor**) Sophie Qui, *Towards Stable, Reliable and Policy-Compliant Inter-domain Routing*, Ph.D., Johns Hopkins University, May, 2007
- (**Reader, external examiner**) Julie Thorpe, *On the Predictability and Security of User Choice in Passwords*, Ph.D., Carleton University, Fall, 2007
- (**Reader**) Sujata Doshi, *New Techniques to Defend Against Computer Security Attacks*, Ph.D., Johns Hopkins University, October, 2008
- (**Advisor**) Charles Wright, *On Information Leakage Attacks in Encrypted Network Traffic*, Ph.D., Johns Hopkins University, 2008
- (**Advisor**) Seny Kamara, *Improved Definitions and Efficient Constructions for Secure Obfuscation*, Ph.D., Johns Hopkins University, 2008
- (**Advisor**) Lucas Ballard, *Robust Techniques for Evaluating Biometric Cryptographic Key Generators*, Ph.D., Johns Hopkins University, 2008
- (**Co-Advisor**) Moheeb Abu Rajab, *Towards a Better Understanding of Internet-Scale Threats*, Ph.D., Johns Hopkins University, 2008
- (**Advsior**) Joshua Mason, *Towards Stronger Adversarial Threat Models in Systems Security*, Ph.D., Johns Hopkins University, June, 2009

- (**Advisor**) Scott Coull, *Methods for Evaluating the Privacy of Anonymized Network Data*, Ph.D., Johns Hopkins University, 2009
- (**Reader, external examiner**) Lu Liming, *Traffic Monitoring and Analysis for Source Identification*, Ph.D., Singapore University, Spring, 2011
- (**Reader, external examiner**) M. Antonakakis, *Improving Internet Security via Large-Scale Passive and Active DNS Monitoring*, Ph.D., Georgia Institute of Technology, Spring, 2012
- (**Reader**) Y. Song, *A Behavior-based Approach Towards Statistics-Preserving Network Trace Anonymization*, Ph.D., Columbia University, Spring, 2012
- (**Reader**) V. Pappas, *Defending Against Return-Oriented Programming*, Ph.D., Columbia University, Spring, 2014
- (**Advisor**) Kevin Z. Snow, *Identifying Code Injection and Code Reuse Payloads in Memory Error Exploits*, Ph.D., University of North Carolina at Chapel Hill, Fall, 2014.
- (**Advisor**) Andrew M. White, *Practical Analysis of Encrypted Network Traffic*, Ph.D., University of North Carolina at Chapel Hill, Fall, 2015.

Undergraduate Advisees

- Rob Dallara, *On the (In)effectiveness of Execute-no-Read (XNR) as a Defense against Just-in-Time Code Reuse Attacks.* University of North Carolina at Chapel Hill, Comprehensive paper, 2015.
- Chris Allen, *WarFlying: Creating Aerial WiFi-maps using Custom Drones*, University of North Carolina at Chapel Hill, Honors Thesis, 2013.
- Wilson Lian, *Traffic Classification using Visual Motifs*, University of North Carolina at Chapel Hill, Honors Thesis, 2010.
- Austin Matthews, *Phonetic Edit Distance: New Techniques and Empirical Analyses*, University of North Carolina at Chapel Hill, Honors Thesis, 2011.

[H]: Professional Service

- 18^{th} Symposium on Research in Attacks and Defenses, (**Chair**), 2016
- IEEE APWG Symposium on Electronic Crime Research (eCrime), 2016
- ACM Workshop on Information Sharing and Collaborative Security, 2015
- 17^{th} Symposium on Research in Attacks and Defenses, (**Co-Chair**), 2015
- DARPA Information Science and Technology (ISAT) advisory group 2014
- 9^{th} USENIX Workshop on Hot Topics in Security (**Co-Chair**) 2014

- 16^{th} Symposium on Research in Attacks and Defenses, 2014
- 15^{th} Symposium on Research in Attacks and Defenses, (**General Chair**), 2013
- 22^{nd} USENIX Security Symposium, 2013
- 20^{th} ACM Conference on Computer and Communications Security, 2013
- 11^{th} International Conference on Cryptography and Network Security 2012
- NSF Secure and Trustworthy Cyberspace Panelist, 2012
- 15^{th} International Symposium on Recent Advances in Intrusion Detection 2012
- 12^{th} Annual Digital Forensics Research Conference 2012
- 16^{th} Financial Cryptography and Data Security 2012
- 6^{th} USENIX Workshop on Hot Topics in Security 2011
- NSF Cyber Trust panelist, 2006—2009, 2011
- 11^{th} Annual Digital Forensics Research Conference 2011
- 18^{th} ACM Conference on Computer and Communications Security 2011
- 17^{th} ACM Conference on Computer and Communications Security 2010
- 14^{th} Financial Cryptography and Data Security 2010
- 30^{th} International Conference on Distributed Computing Systems 2010
- 16^{th} ACM Conference on Computer and Communications Security 2009
- 18^{th} USENIX Security Symposium, (**Program Chair**) 2009
- 16^{th} Annual Network and Distributed Systems Security Symposium 2009
- 29^{th} International Conference on Distributed Computing Systems 2008
- 17^{th} USENIX Security Symposium 2008
- 29^{th} Annual IEEE Symposium on Security and Privacy 2008
- 15^{th} Annual Network and Distributed Systems Security Symposium 2008
- 1^{st} USENIX Workshop on Large-scale Exploits & Emergent Threats, (**Program Chair**) 2008
- 6^{th} IEEE Biometrics Symposium 2008
- 14^{th} Annual Network and Distributed Systems Security Symposium 2007
- 2^{nd} USENIX Workshop on Hot Topics in Security 2007
- 10^{th} Information Security Conference 2007
- 1^{st} USENIX Workshop on Hot Topics in Understanding Botnets 2007

- 16^{th} USENIX Security Symposium 2007
- 28^{th} Annual IEEE Symposium on Security and Privacy 2007
- NSF Exploratory Research panelist, 2006–2007
- 15^{th} USENIX Security Symposium 2006
- 4^{th} ACM Workshop of Recurring Malware 2006
- 13^{th} Annual Network and Distributed Systems Security Symposium 2006

Editorial Boards

- ACM Transactions of Information and System Security 2006 — *2009*

Organizing & Steering Committees

- *General and Local Chair*, Research in Attacks, Intrusions and Defenses (RAID) 2013
- *Local Arrangements Chair*, Financial Cryptography and Data Security 2011
- *Steering Committee*, USENIX Security Symposium 2012-*present*
- *Steering Committee*, Network & Distributed Systems Security Symposium 2007-10
- *Steering Committee*, USENIX Wksh. on Large-scale Exploits & Emergent Threats 2009-*present*
- *Publicity Chair*, ACM Workshop on Rapid Malcode, Arlington 2006
- *Co-organizer,* DIMACS Workshop on Security and Usability, Rutgers 2004

Invited Talks

[T1] Keynote — *The Joys, and Challenges, of Cross-Disciplinary Computer Security Research*. XIII Symposium on Information Security and Computer Systems, Brazil, November, 2013.

[T2] *The Joys, and Challenges, of Cross-Disciplinary Research*. NSERC ISSNet Summit, Victoria, CA, April, 2013.

[T3] Keynote — *Hookt on fon-iks: Learning to Read Encrypted VoIP Conversations*. European Workshop on System Security, Switzerland, April, 2012.

[T4] *Hookt on fon-iks: Learning to Read Encrypted VoIP Conversations*. Columbia University, December, 2012. Host: Angelos Keromytis.

[T5] *Hookt on fon-iks: Learning to Read Encrypted VoIP Conversations*. National Science Foundation WATCH Series, Dec., 2011. Host: Keith Marzullo.

[T6] *Exploring Information Leakage in Encrypted VoIP Communications*. Center for Applied Cybersecurity Research, Indiana University, April 2010. Host: Minaxi Gupta.

[T7] *Privacy Leaks In Encrypted Network Traffic*. Security and Privacy Day, Stonybrook University, May 2008. Host: R. Sekar.

[T8] *Traffic Analysis of Encrypted VoIP Communications*. École Polytechnique, Montreal, March, 2008. Host: José M. Fernandez.

[T9] *Covertly Tracking Malfeasance on the Net: Challenges, Pitfalls and some Opportunities*. University of North Carolina, Chapel Hill, Computer Science Department, December, 2007. Host: Mike Reiter.

[T10] *Playing Devil's Advocate: Inferring Sensitive Information from Anonymized logs*. Georgia Institute of Technology, February, 2007. Host: Wenke Lee.

[T11] *Covertly Tracking a Large Collection of Botnets: Challenges, Pitfalls, and Lots of Questions*. Security Seminar Series, Columbia University, December, 2006. Host: Angelos Keromytis.

[T12] *Traffic Classification in the Dark*. Toronto Networking Seminar Series, University of Toronto, Canada, November, 2006. Host: Stefan Saroiu.

[T13] *Unveiling the Dark Corners of the Internet: or, do you know who's using your computer?* Black Faculty and Staff Lecture Series, Johns Hopkins University, November, 2006

[T14] *Covertly Tracking a Large Collection of Botnets*. Security Group, Google Inc., Mountain View, September, 2006. Host: Niels Provos.

[T15] *Biometric Authentication Revisited: Understanding the Impact of Wolves in Sheep's Clothing*, Digital Security Group, Carleton University, Ottawa, April, 2006. Host: Paul van Oorchot.

Patents / Provisional Filings

[F1] S. Krishnan, K. Snow, and F. Monrose. *Methods, Systems, and Computer Readable Media for Efficient Computer Forensic Analysis and Data Access Control*. U.S. Patent Application 2014/0157407-A1, June 5, 2014.

[F2] K. Snow, F. Monrose and S. Krishnan. *Methods, Systems, and Computer Readable Media for Detecting Injected Machine Code*. U.S. Patent Application 2014/0181976-A1, June 26, 2014.

[F3] S. Krishnan, T. Taylor, F. Monrose and J. McHugh. *Methods, Systems, and Computer Readable Media for Detecting Compromised Computing Hosts*. Provisional Patent Application No.421/391 Prov Filed Feb, 2013.

[F4] A. White, S. Krishnan, M. Bailey, P. Porras and F. Monrose. *Rapid Filtering of Opaque Traffic*. Provisional Patent Application No.421/296 Prov Filed April, 2012.

[F5] Robert Arlein, Ben Jai, Markus Jakobsson, Fabian Monrose and Michael Reiter. *Method & Apparatus for Providing Privacy-preserving Global Customization*. U.S. Patent No. 7,107,269, September, 2006.

[F6] Phil L. Bohannon, Markus Jakobsson, Fabian Monrose, Michael K. Reiter and Susanne Wetzel. *Generation of Repeatable Cryptographic Keys Based on Varying Parameters.* U.S. Patent No. 6,901,145, May 31, 2005.

[F7] Markus Jakobbson and Fabian Monrose. *System & Apparatus for Incorporating Advertising into Printed Images*. U.S. Patent No. 6,873,424, March, 2005.