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 IPR2014-00237
Patent 8,504,697

Declaration of Fabian Monrose, Ph.D.

VIRNETX EXHIBIT 2009
Apple v. VirnetX
Trial IPR2015-00812

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. 8,504,697 ("the '697 patent"). I understand the '697 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 '697 patent has a continuation relationship through several applications to 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 '697 patent, including claims 1-30. I have also reviewed the Petition for *Inter Partes* Review (Paper No. 1, the "Petition") filed with the U.S. Patent and Trademark Office ("Office") by Apple Inc. on December 6, 2013. I have also reviewed the Patent Trial and Appeal Board's ("Board")

decision to institute *inter partes* review (Paper No. 15, the "Decision") of May 14, 2014. I understand that in this proceeding the Board instituted review of the '697 patent on two grounds: (1) anticipation of claims 1-11, 14-25, and 28-30 by *Beser*; and (2) obviousness of claims 1-11, 14-25, and 28-30 over *Beser* in view of RFC 2401. I have reviewed the exhibits and other documentation supporting the Petition that are relevant to the Decision and the instituted grounds.

III. Background and Qualifications

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. I am the sole inventor or a co-inventor on five issued US patents and two 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.

9. 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 Co-Chair for the UNENIX 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).

10. 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.

11. 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

12. I am familiar with the level of ordinary skill in the art with respect to the inventions of the '697 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 Apple's expert, Michael Fratto, 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 '697 patent.[1] My findings are set forth below.

[1] As noted, I was asked to opine only with respect to certain issues that are discussed in this declaration. By doing so, however, I do not necessarily agree with other positions taken by Apple or Mr. Fratto that I do not address here.

V. Claim Terms

A. "Secure Communication Link" (Claims 1-3, 11-13, 16-17, and 24-27)

13. I understand that the Decision preliminarily construed "secure communication link" to mean "a transmission path 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." (Decision at 10.) I disagree with this interpretation.

14. The ordinary meaning of "secure communication link" and the broadest reasonable interpretation in light of the teachings of the '697 patent, which I understand is the standard used by the Board in this proceeding, require encryption. (*See* Paper No. 12 at 17-23.) The patent specification teaches that "data security is usually tackled using some form of data encryption," and it repeatedly discusses using encryption in various embodiments. (Ex. 1001 at 1:57-58; *see also id.* at 10:26-27, 11:42-49, 34:38-39.)

15. Additionally, the Decision's construction is technically incorrect. Of the "obfuscation" methods in the construction—authentication, encryption, and address hopping—only encryption restricts access to "data, addresses, or other information on the path." The other techniques alone do not provide the claimed security.

16. 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 '697 patent incorporates by reference. (*See* Ex. 2004 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. 1001 at 52:7-12.)

17. Address hopping alone also does not provide security, as there is nothing inherent in moving from address to address that precludes an eavesdropper from reading the details of a communication. This is why the '697 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. 1001 at 3:36-50, stating in part that "[e]ach TARP packet's true destination is concealed behind a layer of encryption generated using

a link key.") The Decision states that address hopping alone is sufficient because the '697 patent states that "[a]ddress hopping provides security and privacy." (Decision at 9, citing Ex. 1001 at 25:54-56, 40:66-68.) But the address hopping embodiments in the '697 patent also use encryption, and it is the encryption that provides security while moving from address to address. (*See, e.g.*, *id.* at 3:16-4:40.)

18. The Decision cites dictionary definitions, but these definitions are for peripheral terms and do not support the Decision's definition of "secure communication link." (Decision at 9-10; Ex. 3002, 3003.) For example, the Decision refers to an IEEE dictionary definition of "security service." As defined, however, "security service" broadly pertains to securing "system resources" in addition to data. (Ex. 3003.) System resources can be secured through physical means that include access controls or authentication, such as where the computing system is in a locked room and the person attempting to gain access to it must present a guard with credentials to physically access the machine. Securing data that travels over a public network of switches and routers controlled by third parties, where there is no opportunity for physically guarding access, cannot rely solely on techniques like authentication.

19. Additionally, the Decision's dictionary definitions support my understanding that a "secure communication link" requires encryption. For

example, a few lines above the general definition of "security" that the Decision relies on, the dictionary states that "secure visual communications" is defined as "[t]he transmission of an encrypted digital signal consisting of animated visual and audio information; the distance may vary from a few hundred feet to thousands of miles." (Ex. 3002 at 3, emphasis added.) For signals traveling the distances contemplated by the '697 patent, and particularly where those distances include third-party controlled network hardware, encryption is the only viable mechanism for security over those physically unsecured portions of the networks.

20. Thus, while authentication and address hopping may be used in conjunction with encryption to achieve data security, neither is sufficient by itself to make a link a secure communication link.

B. "Virtual Private Network (VPN) Communication Link" (Claims 3 and 17)

21. Neither party nor the Decision construed "virtual private network communication link" ("VPN communication link"), appearing in dependent claims 3 and 17. To the extent the Board finds it helpful, in my opinion, a VPN communication link refers to a communication path between computers in a VPN. The '697 patent supports my view. For example, the specification describes the ultimate VPN communication link as a path between the claimed first network device and the second network device in a VPN. (*See, e.g.*, Ex. 1001 at 51:60-66.) The specification also describes an optional "administrative" VPN communication

link between the first network device and a secure name service (and/or between the secure name service and a gatekeeper computer that provisions the ultimate VPN) that facilitates establishing the ultimate VPN. (*See, e.g.*, *id.* at 41:14-20 51:17.) The administrative VPN communication link is similarly described as a path between these devices in an administrative VPN. (*See, e.g.*, *id.* at. 40:44-48, 41:14-20, 43-56, 47:11-14.)

C. "Intercept[ing] . . . a request to look up an internet protocol (IP) address" (Claims 1 and 16)

22. I understand that the Decision preliminarily construed the "intercepting" phrase in independent claims 1 and 16 to mean "receiving a request pertaining to a first entity at another entity." (Decision at 12-13.) In my opinion, the meaning of this phrase would be apparent to one of ordinary skill in the art without further interpretation. The Decision's construction is inconsistent with that understanding, in part, because it rewrites the language to focus on an aspect that the claimed embodiments may have in common with conventional systems identified in the '697 patent, rather than on aspects that make the claimed embodiments different from those conventional systems.

23. As explained in the '697 patent, in conventional DNS, a DNS request requesting an address of a target web site 2503 (a first entity) is received at a DNS server 2502 (a second entity), which returns the address. (Ex. 1001, FIG. 25, reproduced below; *id.* at 9:38-39, 39:39-48.)

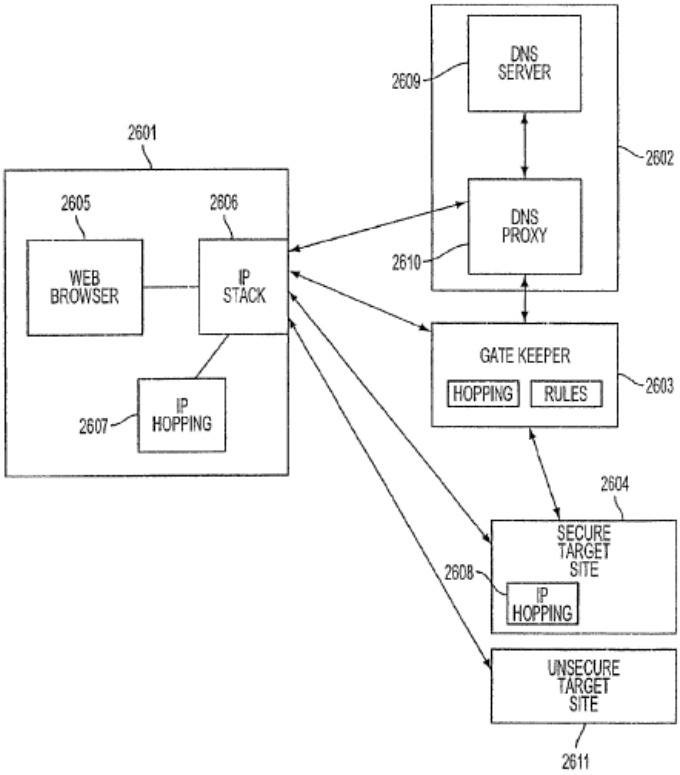


FIG. 26

The same is true of the ’697 patent’s embodiment in which a DNS request to look up a network address of a secure target site 2604 or unsecure target site 2611 (a first entity) is received at a DNS server 2602 (a second entity). (*Id.*, FIG. 26, reproduced below; *see also id.* at 40:31-40.)

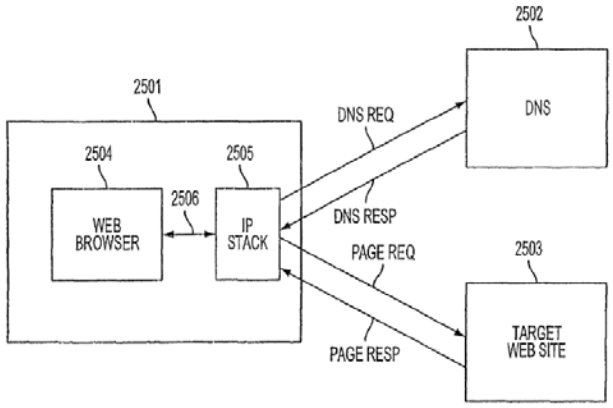


FIG. 25
(PRIOR ART)

24. However, the ’697 patent goes on to explain that the claimed embodiments differ from conventional DNS, in part, because they apply an additional layer of functionality to a request to look up a network address beyond merely resolving it and returning the network address. For example, the DNS proxy 2610 may intercept the request and “determine[ ] whether access to a secure site has been requested,” “determine[ ] whether the user has sufficient security privileges to access the site,” and/or “transmit[ ] a message to gatekeeper 2603 requesting that a virtual private network be created between 40 user computer 2601 and secure target site 2604.” (*Id.* at 40:31-40.) Additionally, the DNS resolves an address and returns it to the first network device. (*Id.* at 44-48.)

25. The Decision’s construction addresses a common aspect of a conventional DNS and the disclosed embodiments, namely that a request to look up an address of one entity may be received at another entity. However, the construction overlooks the aspects distinguishing the “intercepting” phrase from conventional DNS.

26. Thus, in my opinion, the “intercepting” phrase refers to the notion of performing an additional evaluation on a request to look up an IP address related to establishing a secure communication link, beyond conventionally resolving it and returning the address. The independent claims also support this view, for example, by reciting that a determination is made whether the second network device is

available for a secure communications service "in response to the request [to look up an IP address]." (Ex. 1001, claims 1 and 16.) Additionally, dependent claims 10 and 29 expressly specify the evaluation, reciting that "intercepting" involves "receiving the request to determine whether the second network device is available for the secure communications service."

D. "Determining, in response to the request, whether the second network device is available for a secure communications service" (Claims 1 and 16)

27. Independent claims 1 and 16 recite "determining, in response to the request, whether the second network device is available for a secure communications service." I understand that the Decision preliminarily interprets this phrase to mean "determining, one or more of 1) whether the device is listed with a public internet address, and if so, allocating a private address for the second network device, or 2) some indication of the relative permission level or security privileges of the requester." (Decision at 14-15.) I disagree with this interpretation.

28. Determining a public internet address or allocating a private address has no relationship to whether a device is available for a secure communications service. For example, a device listed with a public internet address may or may not be available for a secure communications service. Similarly, a private address may be allocated for a device even if no determination is made that the device is

available for a secure communications service. These features have nothing to do with the claimed determination.

29. The ’697 patent does not limit the determination of whether a network device is available for a secure communications service to require a determination of a public address and an allocation of a private address. Passages of the ’697 patent cited in the Decision disclose an example in which a determination is made that a target computer is available for a secure communications service without “determining . . . whether the device is listed with a public internet address, and if so, allocating a private address for the second network device.” (*See* Ex. 1001 at 41:6-64; *see also* Decision at 15.)

30. The Decision also states that the “determining” phrase can mean “determining . . . some indication of the relative permission level or security privileges of the requester.” I disagree that the claimed “determination” requires “some indication of the relative permission level or security privileges of the requester.” The specification provides examples of determinations focusing on the second network device to which access is requested, as well as examples of separate determinations focusing on the first network device desiring the access. (*Compare*, for example, *id.* at 40:32-33, “determin[ing] whether access to a secure site has been requested” *with id.* at 40:36-37, “determines whether the user has sufficient security privileges to access the site.”) The claimed determination,

however, expressly focuses on the second network device (Ex. 1001, claims 1 and 16, "whether the second network device is available for a secure communications service," emphasis added), so I disagree that the "determining" phrase must be limited to the Decision's determining "permission level or security privileges of the requester."

VI. *Beser*

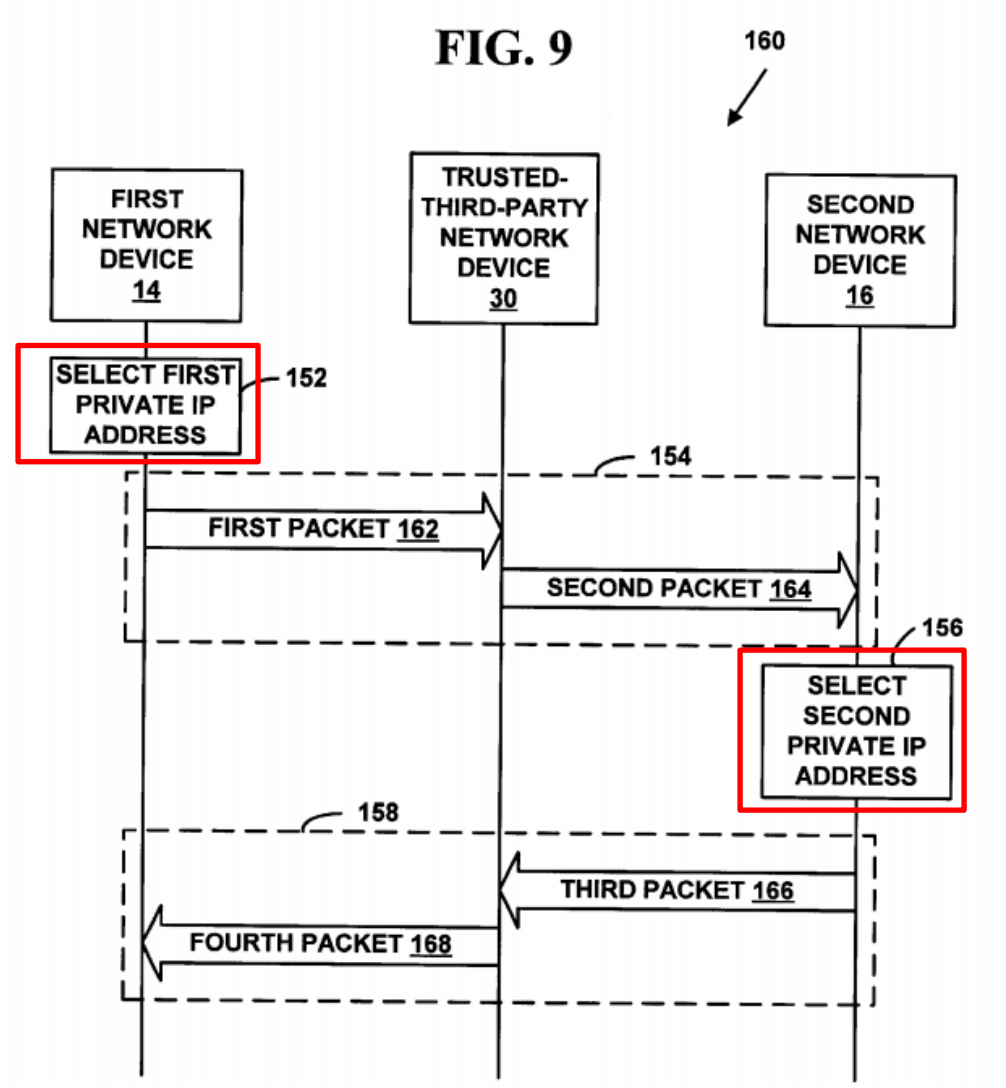
A. *Beser*'s Disclosure

31. *Beser* discloses a method "for initiating a tunnelling association between an originating end and a terminating end of the tunnelling association." (Ex. 1009 at 7:62-64.) A first network device may receive a "request to initiate the tunnelling connection" from an originating end. (*Id.* at 7:65-67.) "The request includes a unique identifier for the terminating end of the tunnelling association." (*Id.* at 8:1-3.) The request may also include a "distinctive sequence of bits [that] indicates to [a] tunnelling application that it should examine the request message for its content and not ignore the datagram." (*Id.* at 8:35-43.)

32. A "trusted-third-party network device is informed of the request." (*Id.* at 8:48-49.) The "informing message includes an indicator that . . . may be a distinctive sequence of bits" that "indicates to the tunnelling application that it should examine the informing message for its content and not ignore the datagram." (*Id.* at 8:60 – 9:1.) A "public network address for a second network

device is associated with the unique identifier." (*Id.* at 9:6-8.) "This association of the public IP 58 address for the second network device [ ] with the unique identifier is made on the trusted-third-party network device." (*Id.* at 11:30-32.) "The second network device is accessible on the public network 12 by transmitting an IP 58 packet with the public IP 58 address for the second network device in the destination address field 90." (*Id.* at 9:16-19.)

33. "[A] first private network address and a second private network address are negotiated on the first network device and the second network device." (*Id.* at 9:26-28.) "In one exemplary preferred embodiment, the negotiation is carried out through the trusted-third party network device." (*Id.* at 9:29-34.) However, as depicted, for example, in Figure 9 of *Beser*, it is the first network device and second network device that select the private network addresses:



34. *Beser* discloses that "the first private network address [is selected] from a first pool of private addresses on the first network device." (*Id.* at 12:40-45.) "[T]he first private network address is communicated from the first network device to the second network device through the public network." (*Id.* at 12:45-48.) "The second private network address is selected from a second pool of private addresses on the second network device" and "communicated from the second network device to the first network device through the public network." (*Id.* at

12:48-54.) "A tunnelling application in the application layer recognizes the private network addresses as being associated with the ends of the tunnelling association. The private network addresses may be included as the payload in data packets and are passed up to the application layer from the transport layer." (*Id.* at 9:46-51.)

35. In one embodiment, *Beser* discloses a method "for initiating a VoIP association between an originating telephony device 24 and a terminating telephony device 26." (*Id.* at 9:64-66.) "First network device 14" may receive "a request to initiate the VoIP association from" the originating telephony device 24. (*Id.* at 10:2-7.) "[T]he request includes a unique identifier for the terminating telephony device 26," which may be "any of a dial-up number, an electronic mail address, or a domain name." (*Id.* at 10:5-6, 10:39-41.) "[T]he unique identifier may be included in the payload of an IP 58 or MAC 54 packet." (*Id.* at 11:3-5.)

36. In my opinion, portions of the Decision's preliminary analysis are based on an inaccurate description of *Beser*'s teachings. For example, the Decision states that "[t]o begin the process for a secure transaction, at step 102, requesting device 24 sends to network device 16, as part of its request, an indicator." (Decision at 17-18.) I disagree. *Beser* explains that "network device 14," not "network device 16," receives a request from "originating telephony device 24." (Ex. 1009 at 10:2-7.) This can also be seen in *Beser*'s Figure 6, which

depicts a request 112 being sent from originating telephony device 24 to network device 14 (not to network device 16).

37. The Decision also states that *Beser* supports Apple's position that "[t]he first network device [14] receives the request, evaluates it, and then sends it to [ ] trusted-third-party network device [30], if appropriate." (Decision at 19-20.) This suggests that *Beser* discloses what to do if it is not "appropriate" to send a request to the trusted-third-party network device, which *Beser* does not do.

B. Claims 1 and 16

1. Intercepting a Request to Look Up an IP Address of the Second Network Device

38. In my opinion, *Beser* does not disclose "intercepting, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device," as recited in claim 1, and the similar "intercept" phrase recited in claim 16. The request that Apple and the Decision identify in *Beser* is a request to initiate an IP tunnel (Decision at 20), not the claimed "request to look up an internet protocol (IP) address of the second network device."

39. The Decision states that the claimed "intercepting" corresponds to operations performed by *Beser*'s "device 14." (*Id.*) The Decision relies on Mr. Fratto's statements that device 14 corresponds to a "router," and "a router evaluates all traffic flowing through it, and if a packet contains a request for

initiating an IP tunnel, it will send the request to trusted-third-party network device." (Decision at 20-21.)

40. The Decision correctly acknowledges that the "request" in *Beser* is a "request for initiating an IP tunnel." (Decision at 20; Ex. 1009 at 7:65-67, stating that the request received by device 14 is a "request to initiate the tunnelling connection.") A request to initiate a tunneling connection, even if it happens to include a domain name in some embodiments, does not convert the tunneling request into the claimed "request to look up an internet protocol (IP) address of the second network device." Whether the request includes a domain name or some other type of identifier does not change the function of the request and is irrelevant to *Beser*'s operation. *Beser* operates the same way regardless of the type of identifier.

41. The trusted-third-party network device 30 does not perform any translation into an IP address of the domain name of the terminating device 26 and or otherwise treat the request to initiate the VoIP tunnel as a request to look up an IP address. After being informed of the request, trusted-third-party network device 30 associates an identifier (e.g., a domain name) of terminating device 26 with a public IP address of a second network device 16. (*Id.* at 11:26-32.) The first and second network devices 14 and 16 then "negotiate" private IP addresses themselves through the public network 12 without the trusted-third-party network

device 30 performing any translation into an IP address of the domain name of the terminating device 26. (*Id*. at 11:58-64; FIG. 6, step 118 "negotiate.") In another embodiment, *Beser* discloses that a private address of the terminating device 26 is selected and transmitted by network device 16 to trusted-third-party network device 30, which then transmits the private address of the terminating device 26 to network device 14. (*Id*. at 13:66-14:27.) Here as well, the trusted-third-party network device 30, acting in a pass-through role, never performs any translation into an IP address of the domain name of the terminating device 26. Thus, the request in *Beser* is not a "request to look up an internet protocol (IP) address," as claimed.

42. I understand Apple and Mr. Fratto had alternatively argued that the "intercepting" of claim 1 is disclosed by the receipt of a request by trusted-third-party network device 30, and that the Decision adopted this reasoning as well. (Decision at 21, citing Pet. at 18-19.) However, the same deficiencies I note above regarding network device 14 apply to trusted-third-party network device 30. Specifically, the request received by trusted-third-party network device 30 is merely a request informing it of the request to initiate a tunneling connection. (*See* Ex. 1009 at 11:9-10; FIG. 6, 114 "INFORM.") So it is no different in purpose than the request to initiate the tunnel received by network device 14, and is not a request "to look up an internet protocol (IP) address of [a] second network device." And,

as I discuss above, the trusted-third-party network device 30 does not perform any translation into an IP address of the domain name of the terminating device 26 or otherwise treat the request as a request to look up an IP address.

2. Determining, in Response to the Request, Whether the Second Network Device Is Available for a Secure Communications Service

43. In my opinion, *Beser* also fails to disclose "determining, in response to the request, whether the second network device is available for a secure communications service," as recited in claim 1, and "determine, in response to the request, whether the second network device is available for a secure communications service," as recited in claim 16. I understand that Apple and/or the Board propose several alternative theories for how *Beser* discloses these features. I address each one below.

44. First, Apple contends that "when methods shown in *Beser* are performed, they will necessarily determine if a second network device is available for secure communications." (Petition at 21.) According to Apple, the determination will "necessarily" happen because, "in the *Beser* system, if a domain name in a request is recognized by the trusted-third-party network device but does not map to a device requiring negotiation of an IP tunnel, the trusted-third-party network device will simply return the IP address associated with the (non-secure)

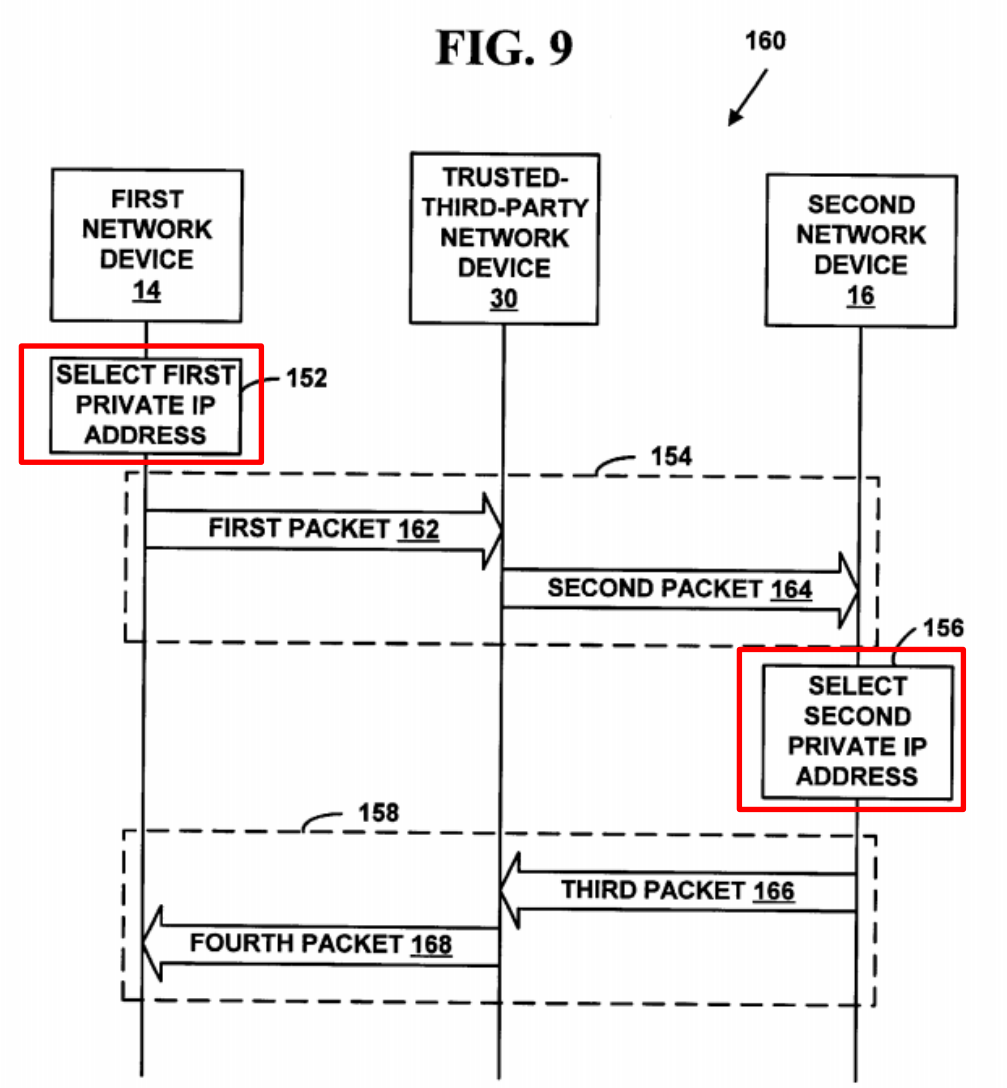
domain, as this is the inherent function of a DNS server on a public network." (Petition at 20-21.) I disagree.

45. *Beser* does not disclose what would happen in Apple's undisclosed hypothetical system in which "a domain name in a request is recognized by the trusted-third-party network device but does not map to a device requiring negotiation of an IP tunnel." The DNS server in *Beser* could operate in a number of ways contrary to the way Apple suggests. For example, the DNS server in *Beser* could return an error message, could discard the request, could do nothing, or could wait until the domain name does map to a device requiring negotiation of an IP tunnel. Even if Apple's proposed manner of operating the DNS server in *Beser* could actually be implemented, it would be one of several possibilities and is not necessarily present in *Beser*'s system.

46. In the next rationale, the Decision states that the claimed "determining" is disclosed by "determining that [device 24 or device 26] has a private internet address assigned to it," as allegedly taught by *Beser*. (Decision at 22-23.) I disagree—no component in *Beser*'s system ever determines that device 24 or device 26 has a private internet address assigned to it in response to a request to look up an IP address of a device based on a domain name.

47. In *Beser*, "a first private network address and a second private network address are negotiated on the first network device and the second network device."

(Ex. 1009 at 9:26-28.) *Beser* notes that "[i]n one exemplary preferred embodiment, the negotiation is carried out through the trusted-third party network device," but discloses that devices 14 and 16 pick the private IP addresses. (*Id.* at 9:29-34.) For example, *Beser*'s Figure 9 (reproduced below in annotated form) depicts a first network device 14 and second network device 16 selecting the private network addresses. The trusted-third-party network device, even when involved in the negotiation of the private IP addresses, only acts as a pass-through intermediary, forwarding the private IP address information between the first network device 14 and the second network device 16. (*Id.* at 13:30-48, Figure 9.)



While private network addresses associated with device 24 and device 26 may be selected by device 14 and device 16 in *Beser*, no determination in *Beser* is ever made in response to a request to look up an IP address of a device based on a domain name—at device 14, device 16, or trusted-third-party network device 30—as to *whether* device 24 or device 26 has a private network address assigned to it.

48. The Decision relies on what Mr. Fratto calls "known DNS operations" to support the notion that private network addresses will not be returned "without a currently valid domain name." (Decision at 22-23.) But *Beser* does not disclose what would happen if a valid domain name (or some other valid unique identifier) were not present in a tunnel initiation request. Mr. Fratto's assumption about how this fictional system would operate is speculative and not supported by *Beser*.

49. Mr. Fratto intermingles two separate and unrelated systems and processes as if they were the same: (1) *Beser*'s tunnel-establishment system and process, and (2) DNS. *Beser* mentions that the trusted-third-party network device might be embodied in a domain name server. (*See* Ex. 1009 at 4:9-10.) This is the extent of *Beser*'s discussion of DNS. DNS and Mr. Fratto's "known DNS operations" are outside the scope of *Beser—Beser* does not discuss them, much less integrate them with the tunnel-establishment process.

50. *Beser*'s tunnel-establishment process occurs in response to *Beser*'s request to initiate a tunnel, but that request is not a "DNS" request that might result in a domain name server performing Mr. Fratto's "known DNS operations." *Beser* provides no teaching on this issue. Also, a "DNS" request has no role in *Beser*'s tunnel-establishment process, so *Beser*'s system would not perform the tunnel-establishment process in response to a "DNS" request. Similarly, if *Beser*'s trusted-third-party network device included a conventional domain name server,

the domain name server would only be capable of performing "known DNS operations" in response to a "DNS" request. It would be unable to recognize or process *Beser*'s request to initiate a tunnel, much less be capable of carrying out *Beser*'s tunnel-establishment process. Thus, in an embodiment where *Beser*'s trusted-third-party network device is part of a domain name server, any DNS functionality and *Beser*'s disclosed tunnel-establishment functionality would be compartmentalized and separate, contrary to Mr. Fratto's characterization intermingling them.

51. The Decision also states that the claimed "determining" is disclosed by *Beser* purportedly determining that "the originating device, device 24, has authorization to communicate." (Decision at 22-23.) The Decision identifies a "unique bit sequence" sent by "*Beser*'s first network device 24" that supposedly indicates that "the first device has authorization to begin a secure network communication with another device." (Decision at 22-23.) I disagree.

52. *Beser* discloses two items sent from first network device 24, but neither pertains to authorization. The first is a unique identifier of device 26 (i.e., the identifier indicating the end device with which the requesting device wishes to communicate), but the unique identifier simply identifies device 26 and provides no indication of the authorization of device 24. (*See, e.g.*, Ex. 1009 at 10:4-6.) The second is a bit sequence from device 24 that merely "indicates to the

tunnelling application that it should examine the informing message for its content and not ignore the datagram." (*Id.* at 8:35-9:1.) It also says nothing about device 24's authorization. Thus, *Beser*'s unique identifier or the bit sequence is not used to make any determination that "the originating device, device 24, has authorization to communicate."

3. Secure Communication Link

53. Claims 1 and 16 also recite a "secure communication link." *Beser*'s alleged "secure communication link," the VoIP tunnel, does not meet the Decision's definition of secure communication link or my understanding of a secure communication link requiring encryption.

54. Under the Decision's definition, a "secure communication link" is "a transmission path 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 hoping." (Decision at 10.) However, *Beser* never discloses that the packets being sent using the allocated private network addresses (over *Beser*'s tunnel) use "authentication," "encryption," or "address hopping." (*See, e.g.*, Ex. 1009 at 25:15-34.) *Beser* discloses using "encryption or authentication to ensure that the unique identifier cannot be read on the public network 12" (*Id.* at 11:22-25), but

this encryption or authentication is used while setting up the tunnel, not after the tunnel is established.

55. The primary purpose of *Beser*'s system is to avoid the computational burden of encrypting data sent through its tunnels. *Beser* explains this burden at length, stating:

> Of course, the sender may encrypt the information inside the IP packets before transmission, e.g. with IP Security ("IPSec"). However, accumulating all the packets from one source address may provide the hacker with sufficient information to decrypt the message. Moreover, encryption at the source and decryption at the destination may be infeasible for certain data formats. For example, streaming data flows, such as multimedia or Voice-over-Internet-Protocol ("VoIP"), may require a great deal of computing power to encrypt or decrypt the IP packets on the fly. The increased strain on computer power may result in jitter, delay, or the loss of some packets. The expense of added computer power might also dampen the customer's desire to invest in VoIP equipment.

(*Id.* at 1:54-67.) *Beser* then explains that, "due to computer power limitations," encrypted VPNs "may be inappropriate for the transmission of multimedia or VoIP packets." (*Id.* at 2:1-17.)

56. *Beser* claims to overcome these computationally intensive, encryption-related issues by stating in its "Summary of the Invention" that its

system hides the ends of its tunneling associations "without an increased computational burden." (*Id.* at 3:1-9.) One of ordinary skill in the art reading this passage would have understood it to mean that encryption is not used, as *Beser* elsewhere explains that encryption is computationally burdensome. *Beser*'s abstract repeats the desire to avoid imposing a computational burden. (*Id.* at Abstract, "The method increases the security of communication on the data network without imposing a computational burden on the devices in the data network.") Given *Beser*'s extensive teaching away from encryption and its associated computational burdens, *Beser* never discloses using encryption or other similarly burdensome techniques for transmitting data through its tunnels.

C. Dependent Claims

1. Dependent Claims 2 and 24—Encryption of Video or Audio Data

57. I understand that claims 2 and 24 recite that "at least one of the video data and the audio data is encrypted over the secure communication link." As I explain above, *Beser*'s tunnel (the alleged secure communication link) does not use encryption, so no video data or audio data are encrypted over *Beser*'s tunnel.

58. The Decision states that *Beser* "specifically employs encryption of at least some of the packets in one embodiment." (Decision at 24.) In the two passages the Decision cites, however, *Beser* does not disclose that any data sent through its tunnel is encrypted, much less video data or audio data. In the first

cited passage, *Beser* discloses that some packets "may require encryption or authentication to ensure that the unique identifier cannot be read on the public network." (Ex. 1009 at 11:22-25.) These packets, however, are not communicated between device 24 and device 26 (i.e., over the tunnel). Rather, the surrounding passages make clear that these packets are transmitted from the network device 14 to the trusted-third-party network device 30 during *Beser*'s "inform" step as part of setting up the tunnel—not over the tunnel after it is established. (*See id*. at 11:9-25; FIG. 6, 114 "INFORM.") *Beser* also does not state that these packets contain any video or audio data, and they do not.

59. Similarly, the second cited passage states that "[t]he first IP 58 packet 272 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 20:11-14.) However, the surrounding passages make clear that this (single) IP packet is transmitted in the context of negotiating private IP addresses while setting up the tunnel, not transmitted on the tunnel after it is established. (*See id.* at 19:38-20:14.) *Beser* also does not state that this packet contains any video or audio data because it does not.

2. Dependent Claims 3 and 17—Virtual Private Network Communication Link

60. I understand that claims 3 and 17 recite that "the secure communication link is a virtual private network communication link." However,

Beser expressly differentiates *Beser*'s tunnel constructed between devices 24 and 26 from a VPN and any related VPN communication link. In the background, *Beser* states that "[o]ne method of thwarting [a] hacker is to establish a Virtual Private Network ('VPN') by initiating a tunneling connection between edge routers on the public network." (Ex. 1009 at 2:6-8.) *Beser* goes on to criticize a VPN as "[a] form of tunneling [that] may be inappropriate for the transmission of multimedia or VoIP packets" (*id.* at 2:6-17), immediately before introducing *Beser*'s tunnel as a solution to the problems posed by VPNs for VoIP (*id.* at 2:43-66). So *Beser* is not just silent on whether its tunnel is VPN communication link, *Beser* expressly teaches that its tunnel is not a VPN communication link.

VII. *Beser* in View of RFC 2401

61. I understand that the Decision cites RFC 2401 for its teaching that the IPsec protocol allows for the creation of an encrypted tunnel. (Decision at 30-31.) RFC 2401, however, is the Network Working Group document outlining the standards for the IPsec protocol, which is the very feature *Beser* suggests not to use. *Beser* acknowledges the existence of the IPsec protocol, but then recognizes its problems for video or audio data. Thus, in my opinion, *Beser* would lead one of ordinary skill in the art away from RFC 2401 and the proposed combination of *Beser* and RFC 2401.

62. *Beser* provides a few reasons why IPsec's particular encryption and encryption generally are undesirable for "streaming data flows" like *Beser*'s VoIP tunnels. (Ex. 1009 at 1:60-62.) One relates to security. The IPsec protocol requires buffering a certain number of packets at a given node before they are sent to the next node or destination. IPsec's buffering would aid *Beser*'s hackers, because "accumulating all the packets from one source address may provide the hacker with sufficient information to decrypt the message." (*Id.* at 1:54-58.)

63. Another reason *Beser* is against encryption relates to computing resources. It explains that encryption/decryption is "infeasible" for VoIP because it would "require a great deal of computing power to encrypt or decrypt the IP packets on the fly," which "may result in jitter, delay, or the loss of some packets" and/or require "[t]he expense of added computer power." (*Id.* at 1:58-66.) These side effects would be unacceptable in *Beser*'s VoIP tunnels. Accordingly, *Beser* teaches away from using RFC 2401's IPsec and encryption generally on its VoIP tunnels. One of ordinary skill in the art would not have combined *Beser* and RFC 2401 as proposed by the Board and Apple, and the combination does not disclose or suggest employing encryption to audio and video packets to enhance security.

VIII. Conclusion

64. 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 ’697 patent.

Executed this 28th day of August 2014 in New York City, NY.

/Fabian Monrose/

Fabian Monrose

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: July 28, 2014

[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

- 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 Defense University Research Instrumentation Program (DURIP), NEXT-GENERATION DEFENSES FOR SECURING VOIP COMMUNICATIONS for $\$114,345.00$, June, 2013 — May 2014.

[G4] **PI**, NSF *Secure and Trustworthy Computing*, SUPPORT FOR THE 2014 USENIX SECURITY SYMPOSIUM; SAN DEIGO for $\$20,000.00$, July 30, 2014— October 2015.

[G5] **PI** (with Elliott Moreton and Jennifer Smith), NSF *Secure and Trustworthy Computing*, TOWARD PRONOUNCEABLE AUTHENTICATION STRINGS for $\$499,997.00$, Aug. 2013— July 2016.

[G6] **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.

[G7] **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.

[G8] **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.

[G9] **PI**, *Verisign Labs Research Awards Program*, ON EXPLORING APPLICATIONS OF PHONETIC EDIT DISTANCE for $\$65,000.00$, June 2011.

[G10] **PI**, *Google Faculty Research Awards Program*, SHELLOS: AN EFFICIENT RUNTIME PLATFORM FOR DETECTING CODE INJECTION ATTACKS for $\$61,635.00$, May 2011.

[G11] **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.

[G12] **PI**, NSF *Trustworthy Computing*, SUPPORT FOR THE 2011 USENIX SECURITY SYMPOSIUM; SAN FRANCISCO for $\$20,000.00$, July 30, 2011— October 2011.

[G13] **PI** (with Kevin Jeffay), NSF *Trustworthy Computing*, TC: SMALL: EXPLORING PRIVACY BREACHES IN ENCRYPTED VOIP COMMUNICATIONS for $\$496,482.00$, Aug. 2010—July 2013.

[G14] **PI**, NSF *Trustworthy Computing*, SUPPORT FOR THE 2010 USENIX SECURITY SYMPOSIUM; WASHINGTON D.C. for $\$20,000.00$, July 30, 2010— October 2010.

[G15] **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.

[G16] **PI** (with Angelos Stavrou), DETECTING AND MONITORING MALFEASANCE ON THE NET, Google Faculty Research Awards Program for $\$90,000.00$, March 2009–Feb 2010.

[G17] **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.

[G18] **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.

[G19] **Co-PI** (with G. Masson (*lead*)), SECURITY THROUGH VIRTUALIZATION. Information Assurance Scholarship Program for $\$142,948.00$. DoD, ANNEX II, Feb, 2008.

[G20] **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.

[G21] **PI**, NSF *Cyber Trust*: CAREER:TOWARDS EFFECTIVE IDENTIFICATION OF APPLICATION BEHAVIORS IN ENCRYPTED TRAFFIC for $\$400,000.00$. September 2006 — August 2011.

[G22] **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.

[G23] **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] *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%).

[P2] *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.

[P3] *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.

[P4] *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%)

[P5] *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.

[P6] *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.

[P7] *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%)

[P8] *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%)

[P9] *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%)

[P10] *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%)

[P11] *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%)

[P12] *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%)

[P13] *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%)

[P14] *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 International Conferences on Dependable Systems and Networks; Performance and Dependability Symposium, June, 2011.

[P15] *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%)

[P16] *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**).

[P17] *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%)

[P18] *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%)

[P19] *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%)

[P20] *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.

[P21] *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.

[P22] *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%)

[P23] *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.

[P24] *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.

[P25] *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.

[P26] *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%).

[P27] *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%).

[P28] *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%).

[P29] *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%).

[P30] *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.

[P31] *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%).

[P32] *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%).

[P33] *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%).

[P34] *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%).

[P35] *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)

[P36] *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%).

[P37] *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%).

[P38] *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%).

[P39] *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%).

[P40] *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.

[P41] *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%).

[P42] *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%)

[P43] *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%)

[P44] *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)

[P45] *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.

[P46] *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%)

[P47] *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%)

[P48] *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%)

[P49] *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.

[P50] *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%)

[P51] *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%)

[P52] *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%)

[P53] *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%)

[P54] *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%)

[P55] *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.

[P56] *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

[P57] *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.

[P58] *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.

[P59] *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.

[P60] *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.

[P61] *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.

[P62] *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.

[P63] *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%).

[P64] *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%)

[P65] *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.

[P66] *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

[P67] *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).

[P68] *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)

[P69] *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.

[P70] *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).

[P71] *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).

[P72] *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)

[P73] *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%).

[P74] *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%).

[P75] *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%).

[P76] *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.

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

Undergraduate Theses

- (**Advisor**) Chris Allen, *WarFlying: Creating Aerial WiFi-maps using Custom Drones*, University of North Carolina at Chapel Hill, 2013 (expected).
- (**Advisor**) Wilson Lian, *Traffic Classification using Visual Motifs*, University of North Carolina at Chapel Hill, 2010.
- (**Advisor**) Austin Matthews, *Phonetic Edit Distance: New Techniques and Empirical Analyses*, University of North Carolina at Chapel Hill, 2011.

[H]: Professional Service

- 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 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 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] K.Snow, S. Krishnan, and F. Monrose. *Efficient Digital Forensics Support using a Virtualized Environment*. Provisional Patent Application No.421/282 filed May, 2011.

[F6] 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.

[F7] 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.

[F8] Markus Jakobbson and Fabian Monrose. *System & Apparatus for Incorporating Advertising into Printed Images*. U.S. Patent No. 6,873,424, March, 2005.