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 IPR2014-00481
Patent 7,188,180

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. 7,188,180 ("the '180 patent"). I understand the '180 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 '180 patent is a divisional of U.S. application no. 09/558,209 filed April 26, 2000 ("the '209 application," abandoned). And I understand the '209 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 '180 patent, including claims 1-41. 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 7, 2014 (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. 11, the "Decision") of September 3, 2014.

3. I understand that in this proceeding the Board instituted review of the '180 patent on two grounds: (1) anticipation of claims 1, 10, 12–15, 17, 26, 28–31, and 37 by *Provino*; and (2) obviousness of claims 4, 6, 20, 22, 35, and 37 over *Provino* in view of *Guillen*. 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

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 '180 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. Roch Guerin, 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 '180 patent. My findings are set forth below.

V. Claim Terms

A. "VPN Communication Link" (Claims 1, 17, and 33)

14. I understand that the parties and the Board have put forth the following constructions:

VirnetX's Proposed Construction	Petitioner's Proposed Construction	Board's Construction
A communication path between computers in a virtual private network	Any communication link between two end points 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

1. A VPN Communication Link is a Link in a VPN

15. I understand that the Decision states that a "VPN communication link" may be satisfied by "a link that merely connects to a virtual private network." (Decision at 6.) I disagree with this interpretation. The '180 patent discloses that a VPN communication link does not exist outside of a virtual private network. Dependent claims 4-10, 20-26, and 35-40 recite characteristics of "the virtual private network" underlying the independent claims' "virtual private network communication link." This is consistent with my understanding that a VPN communication link requires 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. 1001 at 52:27-29.) Then, "VPN gatekeeper 3314 provisions computer 3301 and secure web server computer 3320 . . . thereby creating the VPN" between the devices. (Ex. 1001 at 52:30-33, emphasis added.) Notably, the secure server 3320 "can only be accessed through a VPN communication link." (Ex. 1001 at 52:29-30.)

16. The VPN communication link is initiated to send an access request message between the querying computer 3301 and secure server 3320. (*See* Ex. 1001 at 52:55-57.) "Further communication between computers 3301 and 3320 occurs via the VPN" through the VPN communication link. (Ex. 1001 at 52:60-62.)

17. One of ordinary skill in the art would understand that the VPN communication link and the virtual private network arise contemporaneously and exist between the same devices. Figure 33, depicted below, reflects this. As shown, VPN communication link 3321 traverses the unsecured public network, Internet 3302 to connect computer 3301 with secure server 3320. Thus, in my opinion, the VPN communication link is more than a simple connection to a VPN.

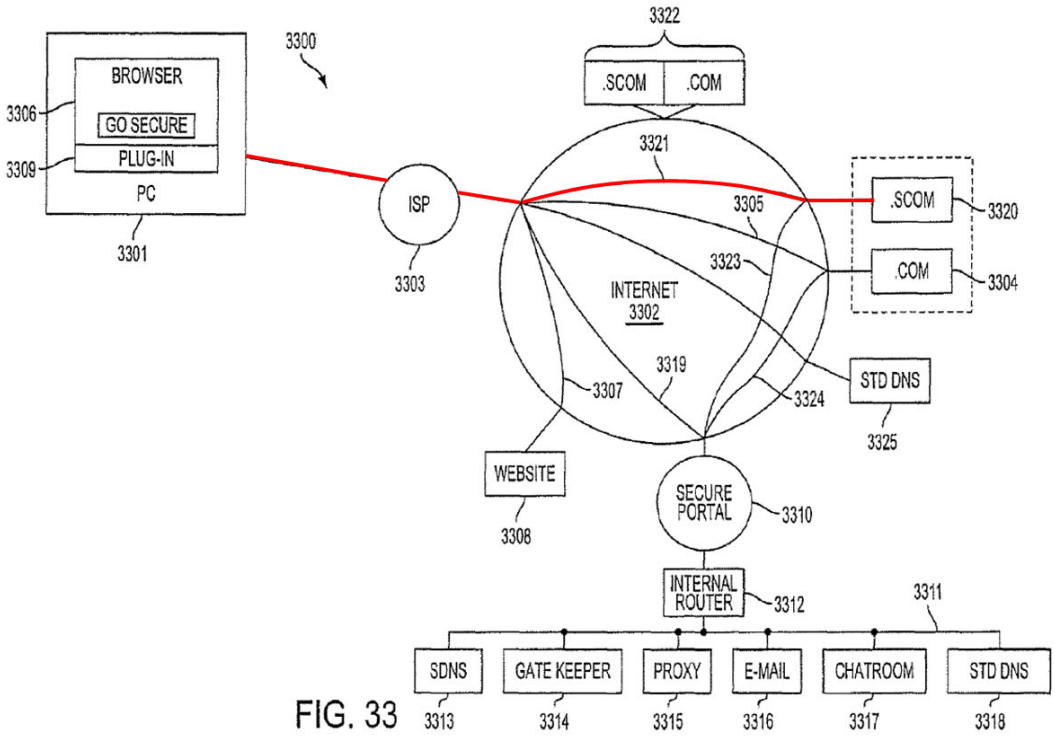

FIG. 33

2. A VPN Requires a Network of Computers

18. I understand that the Decision concludes that a virtual private network communication link may be satisfied by a "path between two devices." (Decision at 7.) In my opinion, the Decision's construction eliminates the "network" from a virtual private network and a virtual private network communication link.

19. 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. In describing a VPN, the '180 patent refers to the "FreeS/WAN" project, which has a glossary of terms. (Ex. 1001 at 40:14 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. 2009 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."

20. The specification further describes a VPN as including multiple "nodes." (*See, e.g.*, Ex. 1001 at 17:14-18, referring to "each node in the network" and "vastly increasing the number of distinctly addressable nodes," 21:61, "nodes on the network"; *see also id.* 19:44-46, 24:48.) More specifically, the network allows "each node . . . to communicate with other nodes in the network." (Ex. 1001 at 17:18-20.) 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. 1001 at 52:41-43, 47-49.)

B. "Secure Computer Network Address" (Claims 1, 12, 17, 28, and 33)

21. I understand that the parties and the Board have put forth the following constructions:

VirnetX's Proposed Construction	Petitioner's Proposed Construction	Board's Construction
A network address that requires authorization for access and is associated with a computer capable of virtual private network communications	A network address that requires authorization for access and is associated with a computer configured to be accessed through a virtual private network	An address that requires authorization for access

22. In my opinion, the parties' proposed constructions requiring a relationship between the associated computer and the virtual private network is supported by the claim language, which recites "sending an access request message to the secure computer network address using a virtual private network communication link." For the sending to occur as claimed, the computer must be capable of virtual private network communications. The '180 patent specification further supports this, describing that "secure server 3320 . . . can only be accessed through a VPN communication link." (Ex. 1001 at 52:27-30.) Thus, in my opinion, the computer must be capable of virtual private network communications.

C. "Client Computer" (Claims 13, 15, 29, and 31)

23. I understand that the parties and the Board have put forth the following constructions:

VirnetX's Proposed Construction	Petitioner's Proposed Construction	Board's Construction
User's computer	No construction proposed	No construction

24. In the context of the ’180 patent, the client computer is repeatedly and consistently discussed in connection with the user. The specification explains that the VPN communication link is initiated between the user’s computer 2601 and the target:

> If [the DNS request from the user’s computer 2601 is requesting access to a secure site and the user is authorized], DNS proxy 2610 transmits a message to gatekeeper 2603 requesting that a virtual private network be created between user computer 2601 and secure target site 2604.

(*See, e.g.*, Ex. 1001 at 40:53-56.) The specification further explains that a software module 3309 for accessing the secure computer network address using the VPN is installed on a computer 3301, (*See* Ex. 1001 at 50:60-64, 52:55-57), and elsewhere describes that the computer 3301 is manned by a user and equipped with a web browser 3306 and user input devices such as a keyboard, display, and/or mouse, (*see id.* at 49:66-50:13, 50:34-48, 50:64-51:14; FIG. 34.) In another embodiment, the specification explains that a “user’s computer 2501” includes this “client application.” (*See id.* at 39:53-55, 40:36-38.) Thus, in my opinion, one of ordinary skill in the art would understand that the ’180 patent equates the user’s computer 2601 with the “client computer” in the claims.

D. Other Terms

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

"Access Request Message" (Claims 1, 12, 13, 17, 28, 29, and 33)		
VirnetX's Proposed Construction	Petitioner's Proposed Construction	Board's Construction
No construction necessary	No construction proposed	A signal in a packet or other message format that signifies that the first network device seeks communication, information, or services, with or from another device associated with the secure network address
"Secure Domain Name" (Claims 1, 17, and 33)		
VirnetX's Proposed Construction	Petitioner's Proposed Construction	Board's Construction
A non-standard domain name that corresponds to a secure computer network address and cannot be resolved by a conventional domain name service (DNS)	A non-standard domain name that corresponds to a secure computer network address and cannot be resolved by a conventional domain name service (DNS)	A name that corresponds to a secure computer network address
"Secure Domain Name (Service)" (Claims 1, 17, and 30)		
VirnetX's Proposed Construction	Petitioner's Proposed Construction	Board's Construction
A lookup service that recognizes that a query message is requesting a secure computer address, and returns a secure computer network address for a requested secure	A service that can resolve secure computer network addresses for a secure domain name for which a conventional domain name service cannot resolve addresses	A service that provides a secure computer network address for a requested secure domain name

domain name		

VI. *Provino*

A. *Provino*'s Disclosure

26. *Provino* describes a system for connecting an external device to a device on a virtual private network. (Ex. 1003, Abstract.) Referring to Figure 1 of *Provino*, reproduced below, when an operator at device 12(m) wishes to connect to device 13 on the Internet, the operator inputs a human-readable address of device 13, causing device 12(m) to send a message to nameserver 17 requesting the corresponding Internet address of the device 13. (Ex. 1003 at 8:14-40, 11:5-11.) If the nameserver 17 has or can obtain the Internet address of device 13, it will provide that address to device 12(m). (Ex. 1003 at 8:48-51.) If nameserver 17 is unable to obtain an Internet address of device 13, it will return a message to device 12(m) stating this fact. (Ex. 1003 at 11:11-14.)

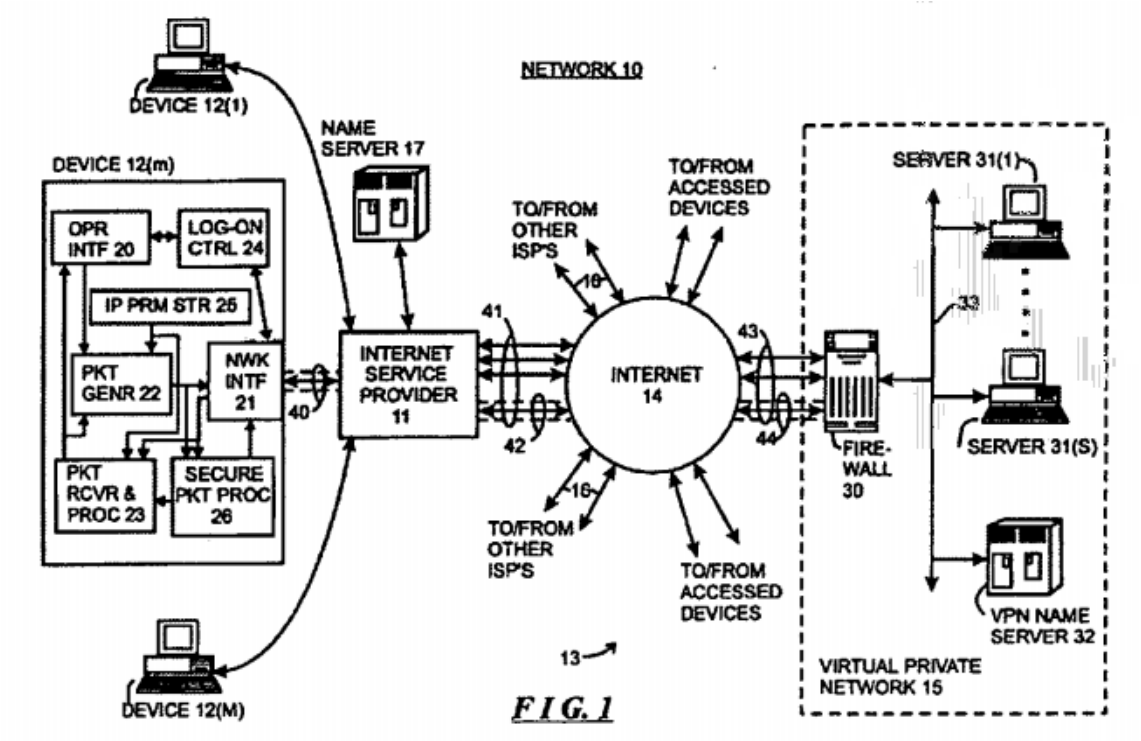

FIG. 1

27. When nameserver 17 receives a request for the address of server 31(s) on virtual private network 15, however, it may return the address of firewall 30 on virtual private network 15 because it does not have the address of server 31(s). (Ex. 1003 at 9:52-56, 10:45-55.) Therefore, to connect to server 31(s) on virtual private network 15, device 12(m) initiates establishment of a secure tunnel with firewall 30. (Ex. 1003 at 10:45-58, 12:1-4, 12:16-35.) After the secure tunnel is established, firewall 30 provides device 12(m) with the identification of second nameserver 32 inside virtual private network 15. (Ex. 1003 at 12:37-40.)

28. The device 12(m) uses the secure tunnel to send nameserver 32 through firewall 30 a request for the Internet address of server 31(s) corresponding to the human-readable address of the server 31(s). (Ex. 1003 at 11:14-17, 13:54-

14:33.) "[I]f the nameserver 32 does not have an association between the human-readable Internet address and an integer Internet address [for server 31(s)], the nameserver 32 can provide a response message packet so indicating." (Ex. 1003 at 11:50-53.) If device 12(m) receives the Internet address of server 31(s), "the device can use that address in generating message packets for transmission to server 31(s) . . . ." (Ex. 1003 at 11:16-25.)

B. Claims 1, 17, and 33

1. "Receiving a Secure Domain Name"

29. I understand that independent claims 1, 17, and 33 recite "receiving a secure domain name." The Decision suggests that *Provino* discloses receiving a domain name by an operator or program providing a human-readable Internet address to device 12(m), and that it is a "secure" domain name because "nameserver 32 verifies the domain name as secure . . . ." (Decision at 14, citing Ex. 1003 at 11:5-23, 13:31-40.) The Petition, on the other hand, contends that *Provino*'s human-readable Internet address is a "secure" domain name not because nameserver 32 verifies it, but because it is supposedly "a non-standard domain name . . . and cannot be resolved by conventional DNS," nameserver 17. (Pet. at 19.) I disagree with the Decision and with Apple.

30. *Provino*'s nameserver 32 does not "verify" that the human-readable Internet address is a secure domain name. As explained by the *Provino* passages

cited in the Decision, nameserver 32's only function is the conventional DNS function of resolving a name into an address, if possible. Specifically, nameserver 32 "determines whether it has an integer Internet address associated with the human-readable Internet address provided in the request message packet," and, if so, "generates a response message packet including the integer Internet address." (Ex. 1003, 14:39-46.) If not, nameserver 32 "provides a response message packet so indicating." (Ex. 1003, 11:50-53.) *Provino* does not disclose that nameserver 32 additionally "verifies the domain name as secure," as suggested by the Decision.

31. In my opinion, even under VirnetX's and Petitioner's construction of "secure domain name," *Provino* does not teach "receiving a secure domain name" because the human-readable Internet address of *Provino* is not a "non-standard" domain name. By "human-readable Internet address," *Provino* simply refers to how conventional DNS "relieve[s] a user of the necessity of remembering and entering specific integer Internet addresses, . . . [by] provid[ing a] second addressing mechanism which is more easily utilized by human operators of the respective devices." (Ex. 1003 at 1:49-52.) *Provino* is not concerned with "standard" versus "non-standard" domain names in its system—*Provino* is silent on this topic entirely. By contrast, the '180 patent discuses exemplary "standard" domain names ending in ".com" and exemplary "non-standard" domain names

ending in ".scom." (Ex. 1001 at 51:16-27.) *Provino* gives no indication that its human-readable names are anything other than standard ones.

32. I understand Apple asserts that *Provino*'s human-readable integer Internet address is "non-standard" because *Provino* teaches that "the human-readable network addresses may be 'any form of secondary or informal network address arrangements.'" (Pet. at 19, citing Ex. 1003 at 16:12-17.) In my opinion, Apple takes the quoted *Provino* statement out of context. It is part of a brief discussion at the end of the patent mentioning that *Provino*'s system can be used in other types of networks even though *Provino* only describes it in the context of the Internet. (Ex. 1003 at 16:8-16.) But *Provino* does not actually describe any such embodiments, much less teach that they use non-standard domain names in any way. Nor does *Provino* describe the role non-standard domain names might play within *Provino*'s overall framework.

2. "Sending a Query Message From to a Secure Domain Name Service, the Query Message Requesting From the Secure Domain Name Service a Secure Computer Network Address Corresponding to a Secure Domain Name"

33. In my opinion, *Provino* does not disclose "sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the domain name," as recited in claim 1. I understand that claims 17 and 33 recite similar features. I understand that the Board has said that *Provino* discloses the

query message "sending" feature because "Provino's secure nameserver 32" receives a "query from first network device 12(m)." (Decision at 15; *see also* Pet. at 26-27.) However, in my opinion, *Provino*'s "nameserver 32" is not the claimed "secure domain name service" in light of the '180 patent's disclosure and Petitioner's claim construction.

a) The '180 Patent Specification

34. In my opinion, one of ordinary skill in the art would understand that the specification of the '180 patent limits the claimed "secure domain name service" to DNSs that perform more than conventional functions. In contrast, *Provino*'s nameserver 32 performs only conventional functions. The '180 patent specification begins disclaiming conventional DNS functions (such as merely returning a requested address or a public key) by describing these actions as "conventional" in the prior art:

> Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host.
>
> . . .
>
> One conventional scheme that provides secure virtual private networks over the Internet provides the DNS server with the public keys of the machines that the DNS server has the addresses for. This allows hosts to retrieve automatically the public keys of a host that the host is to

> communicate with . . . . One implementation of this standard is presently being developed as part of the FreeS/WAN project (RFC 2535).

(Ex. 1001, 39:53-40:14, emphasis added.) The specification explains that DNSs that perform no more than these conventional functions have many shortcomings, and further explains novel DNS-system embodiments that go beyond these conventional functions by supporting establishing secure communications. (Ex. 1001 at 40:15-17, 52:12-29.)

35. Time and again, the '180 patent specification disparages systems with functions limited to conventional IP-address and public-key features. For example, the '180 patent specification explains:

> In the conventional architecture . . . , nefarious listeners on the Internet could intercept the DNS REQ and DNS RESP packets . . . . This would hamper anonymous communications on the Internet. . . .
>
> The conventional scheme suffers from certain drawbacks. . . .
>
> According to certain aspects of the invention, . . . the server does not return [a] true IP address of the target node, but instead automatically sets up a virtual private network . . . .

(Ex. 1001 at 39:63-40:24, emphasis added.)

36. The ’180 patent specification does not stop at disparaging conventional DNS systems. Rather, the ’180 patent specification goes on to describe several embodiments of the novel DNS system, wherein each of the disclosed embodiments performs much more than the conventional DNS functions and supports establishing a secure communication link. For example, in one embodiment, the DNS system does not return an IP address, “but instead automatically sets up a virtual private network between the target node and the user.” (Ex. 1001 at 40:15-24.) In addition, the secure domain service may be able to differentiate between domain names of different security levels. (Ex. 1001 at 52:12-15.) Alternatively, the secure domain service may recognize that a query message is requesting a secure computer address based on the sender. (Ex. 1001 at 52:22-26.)

37. In another embodiment, “DNS proxy 2610 transmits a message to gatekeeper 2603 requesting that a virtual private network be created between user computer 2601 and secure target site 2604,” with an IP address only being returned after the secure communication link is set up. (Ex. 1001 at 40:53-65.) In still another embodiment, “a secure VPN is established between the user’s computer and the secure target,” without any return of DNS records. (Ex. 1001 at 41:44-56.) In still another, “[t]he gatekeeper would establish a VPN between the client and the requested target” before any IP address is returned. (Ex. 1001 at 41:65-42:7.)

Likewise, in another embodiment, the SDNS only returns a secure URL after it has already coordinated with the VPN gatekeeper to establish a VPN. (Ex. 1001 at 52:27-40.)

38. In my opinion, *Provino's* nameserver 32 operates in precisely the same way as the conventional domain name service described and disparaged in the '180 patent. When nameserver 32 receives a human-readable address, it simply checks "whether it has an integer Internet address associated with the human-readable Internet address provided in the request message packet," and, if so, "generate[s] a response message packet including the integer Internet address for transmission to the firewall." (Ex. 1003, 14:39-46.) That nameserver 32 is located within what *Provino* refers to as virtual private network 15 is immaterial to whether it is a secure domain service. The mere fact of its location cannot transform nameserver 32 from a conventional domain service to a secure domain service. Thus, nameserver 32 is a conventional domain service—not the claimed "secure domain service."

b) <u>"Secure Domain Name Service" Under Apple's Construction</u>

39. I understand Apple argues that a "secure domain name service" is "a service that can resolve secure computer network addresses for a secure domain name for which a conventional domain name service cannot resolve addresses." In my opinion, nameserver 32 fails to satisfy this construction. I also understand that

Dr. Guerin argues that nameserver 32 is a secure domain service because it can "resolve the human-readable domain names of the servers 31(s) internal to the VPN 15" whereas "conventional nameserver 17 cannot resolve the human-readable domain names of the servers 31(s) internal to the VPN 15." (*See* Ex. 1011 at 18.) However, the mere fact that a DNS can resolve domain names that another DNS cannot resolve does not make it a secure domain name service.

40. Nameserver 32 behaves just like nameserver 17. When nameserver 17 receives a human-readable address, it simply checks whether it "has an integer Internet address associated with the human-readable Internet address [and, if so,] provide[s] the integer Internet address." (Ex. 1003, 13:43-46.) Likewise, when nameserver 32 receives a human-readable address, it simply checks "whether it has an integer Internet address associated with the human-readable Internet address provided in the request message packet," and, if so, "generate[s] a response message packet including the integer Internet address for transmission to the firewall." (Ex. 1003, 14:39-46.)

41. Nameserver 17 and nameserver 32 also operate in the same manner when they do not have an integer Internet address associated with a human-readable Internet address provided in a request. If "nameserver 17 does not have a integer Internet address associated with the human-readable Internet address, it (that is, the nameserver 17) will provide a response message packet so indicating to

device 12(m)." (Ex. 1003, 13:54-58.) Likewise, "if the nameserver 32 does not have an integer Internet address associated with the human-readable Internet address provided by the device 12(m) in the request message packet, it (that is, nameserver 32) can so indicate in the response message packet generated thereby." (Ex. 1003, 15:31-35.)

42. Therefore, in my opinion *Provino* does not disclose "sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the domain name," as recited in claims 1, 17, and 33.

3. "Sending an Access Request Message to the Secure Computer Network Address Using a Virtual Private Network Communication Link"

43. I understand that claim 1 recites "sending an access request message to the secure computer network address using a virtual private network communication link," and that claims 17, and 33 recite similar features. I understand that, to address this feature, the Board relies on *Provino*'s alleged disclosure of "message packets that . . . request[] the set-up for an encrypted secure tunnel to server/computer 31(s)" for the "access request message" feature. (Decision at 16.) However, what *Provino* discloses is that "device 12(m) . . . generates a message packet for transfer through the ISP 11 and Internet 14 to the firewall 30 requesting establishment of a secure tunnel between the device 12(m)

and firewall 30." (Ex. 1003 at 9:46-52, emphasis added.) Thus, while *Provino* discloses a message packet that requests a tunnel setup, this message packet is sent to firewall 30—not server 31(s), as the Decision alleges.

44. Claim 1 specifies that the "access request message" is sent "to the secure network address" which, based on my review of the Decision, the Board identifies as the address of server 31(s) returned by nameserver 32. (Decision at 14-15, "Provino's secure nameserver 32 sends a secure network integer Internet address for second network (server) device 31 through VPN 15 firewall 30 to client computer 12(m).") Accordingly, firewall 30 does not correspond to the claimed "secure computer network address," and *Provino*'s message packet to firewall 30 requesting setup of the tunnel cannot disclose the claimed "access request message" because it is not sent "to the secure computer network address." In *Provino*, the network address of server 31(s) is not even requested or determined until after the secure tunnel between device 12(m) and firewall 30 is already established. Therefore, *Provino* cannot and does not disclose the sending of any message packets that "request[] the set-up for an encrypted secure tunnel to server/computer 31(s)," as alleged in the Decision. (Decision at 16, emphasis added.)

C. Dependent Claims

1. Dependent Claims 10 and 26 – The VPN Includes the Internet

45. I understand dependent claims 10 and 26 recite that "the virtual private network includes the Internet," which the Decision and Apple both identify as the Internet 14 illustrated in *Provino*'s Fig. 1. (Decision at 16; Pet. at 29.) In my opinion, *Provino*'s embodiment using the Internet 14 is a different embodiment than the one the Petition and the Decision rely on for the independent claims. As I explained above, for the independent claims, the Petition and the Decision rely on an embodiment of *Provino* that uses "any network" other than the Internet 14 for its alleged use of non-standard domain names. (*See* Pet. at 19, citing the non-Internet embodiment discussed in Ex. 1003 at 16:12-17.)

2. Dependent Claims 12 and 28 – The Access Request Message Contains a Request for Information Stored at the Secure Computer Network Address

46. I understand that dependent claims 12 and 18 recite that "the access request message contains a request for information stored at the secure computer network address." As I understand the claims, "the access request message" in these dependent claims refers to the same access request message introduced in the independent claims. For the independent claims, the Decision identifies two potential access request messages in *Provino*: "Provino's message packets that either request[] the set-up for an encrypted secure tunnel" or "request encrypted

information or processes from server/computer 31(s)." (Decision at 16.) In my opinion, neither one satisfies the language of claims 12 and 28.

47. The Decision asserts that the address of the server 31(s) returned by *Provino*'s nameserver 32 is the claimed "secure computer network address." (*See* Decision at 15.) However, the first potential "access request message," the request to establish *Provino*'s tunnel, is sent to the firewall 30 and does not request anything stored at the address of the server 31(s). (*See, e.g.*, Ex. 1003 at 9:46-52.) Rather, when the firewall 30 receives this request, "[it] may provide the device 12(m) with the identification of a decryption algorithm and associated decryption key which the device 12(m) is to use in decrypting the encrypted portions of message packets" received from the tunnel, and "may also provide the device 12(m) with the identification of an encryption algorithm and associated encryption key which the device 12(m) is to use in encrypting the portions of message packets" sent over the tunnel. (Ex. 1003 at 9:61-10:3.) Thus, at best, the first potential "access request message" in *Provino* requests information stored at the firewall 30, not at the alleged secure computer network address of the server 31(s).

48. Moreover, as I explained above, *Provino* provides little information about the second potential "access request message," *Provino*'s message packets sent from device 12(m) to server 31(s) after the tunnel is established. These packets do not necessarily "contain[] a request for information stored at the secure

computer network address," as recited in claims 12 and 28. Indeed, they might serve a different purpose entirely, such as to request that information be stored on server 31(s). Device 12(m) might send an e-mail message to server 31(s), might send a Short Message Service (SMS) message to server 31(s), or might send the content of its internal storage device to server 31(s) for backup storage. In none of these examples would *Provino*'s message packets "contain[] a request for information stored at the secure computer network address," as recited in claims 12 and 28.

VII. *Provino* in View of *Guillen*

49. I understand that claims 4, 20, and 35 recite "the response message contains provisioning information for the virtual private network." I understand claims 6, 22, and 37 depend respectively from claims 4, 20, and 35, and incorporate these same features. (Ex. 1001, claims 4, 20, and 35.) As I understand the claims, "the response message" refers to the response message received from the secure domain name service in the independent claims. (*Id.*)

50. I understand the Petition cites *Guillen* for the notion of including Quality of Service (QoS) information for a VPN in the message received from the secure domain name service, which the Petition contends discloses the claimed "provisioning information." (Pet. at 35-40.) According to the Petition, "a person of ordinary skill in the art would have modified the VPN name server 32 of

Provino to store, in part, topology dependent QoS parameters, as described by Guillen," and "[s]uch a modified VPN name server 32 would . . . respond to requests by device 12(m) to resolve the human-readable network addresses of servers 31(S) with both the integer Internet address of the servers 31(S) and the QoS parameters for the servers 31(S)." (Pet. at 38, Ex. 1011 ¶ 43, citing Ex. 1005 § 2.3, p. 82.) I disagree with the Petition's analysis.

51. *Guillen* discloses "[a] network . . . [that] provide[s] pre-computed and on-demand routes using a variation of the Distance Vector algorithm." (Ex. 1005, p. 1.) *Guillen* calls these routes "Virtual Circuits" over the network. (Ex. 1005, p. 1.) Through a negotiation process, "a set of [Quality of Service] QoS values are associated with each link interconnecting two Systems which give an indication of the quality of this link." (Ex. 1005, p. 2.) *Guillen* teaches an embodiment where "an application should consult some kind of directory services (DNS, X.500, ...) for application address resolution" that "store[s] [QoS] information which is relatively static. (Ex. 1005, p. 3.) According to *Guillen*, by providing QoS information in a directory service, "the user will have an indication of what is feasible." (Ex. 1005, p. 3.)

52. Assuming for sake of argument that one of ordinary skill in the art were to combine *Guillen* with *Provino*, in my opinion, he or she would not have placed *Guillen*'s QoS information in *Provino*'s nameserver 32. As explained by

Guillen, the purpose of providing QoS information in a directory service like DNS is so "the user will have an indication of what is feasible" before establishing the Virtual Circuit. (Ex. 1005, p. 3.) *Guillen* would use the QoS information in the "first part" of his solution to "calculate routes in advance." (Ex. 1005 at 7, § 4, emphasis added; *see also* Ex. 1005 at 7, § 3.9, explaining how QoS information is used to "explore" potential Virtual Circuits.) *Guillen* never discusses providing QoS parameters once a Virtual Circuit has been established. Rather, Guillen explains that "the QoS is negotiated during the VC set-up phase" and "not re-negotiated." (Ex. 1005 at 2, § 2.1 "[W]hen the QoS provided for a given VC no longer matches the values negotiated during the set-up, the network may clear the VC.")

53. In contrast, by the time *Provino*'s device 12(m) accesses nameserver 32, device 12(m) and firewall 30 have already cooperated to establish the tunnel, so *Guillen*'s QoS information would be moot. (*See, e.g.*, Ex. 1003 at 11:66-12:16.) Thus, I do not believe that one of ordinary skill in the art would not have combined *Guillen* with *Provino* as proposed by the Petition.

54. Petitioner has not asserted that one of ordinary skill in the art would have looked to incorporate *Guillen*'s DNS-stored QoS information into *Provino*'s outside nameserver 17 so that the QoS information might be applied to select a

Virtual Circuit when establishing the tunnel. But even if it had, in my opinion, this combination would not meet the claim language.

55. As I understand them, claims 4, 20, and 35 require that the "provisioning information" is contained in the same "response message," from the same "secure domain name service," that contains the same "secure computer network address" in the independent claims. According to the Petition's and the Decision's mapping of *Provino* to the claims, the "response message" is the message from nameserver 32 containing the address of device 31(s), the "secure computer network address" is the address of device 31(s), and the "secure domain name service" is nameserver 32. (Decision at 14-15; Pet. at 26-27.) A response from nameserver 17 containing *Guillen*'s alleged "provisioning information"—the QoS information—would be different response, from a different nameserver, lacking the alleged secure computer network address. Thus, in my opinion, it would not meet the claim language.

VIII. 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 ’180 patent.

Executed this 5th day of January 2015 in Castries, Saint Lucia.

/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: November 1, 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 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] *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.

[P2] *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%).

[P3] *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.

[P4] *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.

[P5] *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%)

[P6] *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.

[P7] *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.

[P8] *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%)

[P9] *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%)

[P10] *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%)

[P11] *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%)

[P12] *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%)

[P13] *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%)

[P14] *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%)

[P15] *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.

[P16] *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%)

[P17] *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**).

[P18] *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%)

[P19] *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%)

[P20] *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%)

[P21] *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.

[P22] *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.

[P23] *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%)

[P24] *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.

[P25] *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.

[P26] *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.

[P27] *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%).

[P28] *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%).

[P29] *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%).

[P30] *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%).

[P31] *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.

[P32] *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%).

[P33] *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%).

[P34] *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%).

[P35] *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%).

[P36] *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)

[P37] *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%).

[P38] *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%).

[P39] *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%).

[P40] *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%).

[P41] *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.

[P42] *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%).

[P43] *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%)

[P44] *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%)

[P45] *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)

[P46] *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.

[P47] *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%)

[P48] *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%)

[P49] *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%)

[P50] *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.

[P51] *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%)

[P52] *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%)

[P53] *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%)

[P54] *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%)

[P55] *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%)

[P56] *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.

[P57] *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

[P58] *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.

[P59] *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.

[P60] *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.

[P61] *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.

[P62] *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.

[P63] *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.

[P64] *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%).

[P65] *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%)

[P66] *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.

[P67] *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

[P68] *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).

[P69] *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)

[P70] *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.

[P71] *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).

[P72] *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).

[P73] *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)

[P74] *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%).

[P75] *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%).

[P76] *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%).

[P77] *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

- 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.