IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)	
	)	
Victor Larson et al.	)	Control No.: 95/001,788
	)	
U.S. Patent No. 7,418,504	)	Group Art Unit: 3992
	)	
Issued: August 26, 2008	)	Examiner: Roland Foster
	)	
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	)	Confirmation No.: 5823

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Declaration of Angelos D. Keromytis, Ph.D.

I declare that the following statements are true to the best of my knowledge, information, and belief, formed after reasonable inquiry under the circumstances.

I, ANGELOS D. KEROMYTIS, declare as follows:

1. I have been retained by VirnetX Inc. ("VirnetX") for the above-referenced reexamination proceeding. I understand that this reexamination involves U.S. Patent No. 7,418,504 ("the '504 patent"). I further understand that the '504 patent is assigned to VirnetX and that it is part of a family of patents ("Munger patent family") 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 '504 patent is a continuation of U.S. application no. 09/558,210 ("the '210 application"), filed April 26, 2000 (now abandoned), which is a continuation-in-part of U.S. application no. 09/504,783 (now U.S. Patent No. 6,502,135, "the '135 patent"). I also understand 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), which claims priority to the '261 and '704 applications.

I. RESOURCES I HAVE CONSULTED

2. I have reviewed the '504 patent, including claims 1-60. I have also reviewed a Request for *Inter Partes* Reexamination of the '504 patent filed by Apple Inc. with the U.S. Patent and Trademark Office on October 18, 2011 ("Request" or "Req."), as well as its accompanying exhibits.[1] Additionally, I have reviewed an Order Granting Request for *Inter Partes* Reexamination of the '504 patent ("the Order") and an Office Action ("the Office Action"), both mailed on December 29, 2011.[2]

3. I have also studied the following documents cited in and included with the Request and/or Office Action: E. Solana et al., "Flexible Internet Secure Transactions Based on Collaborative Domains," Lecture Notes in Computer Science, vol. 1361, at 37-51 (1997) ("*Solana*"); U.S. Patent No. 6,557,037 to Provino ("*Provino*"); U.S. Patent No. 6,496,867 to Beser et al. ("*Beser*"); R. Atkinson, IETF RFC 2230, "Key Exchange Delegation Record for the DNS," November 1997 ("RFC 2230"); D. Eastlake et al., IETF RFC 2538, "Storing Certificates in the Domain Name System (DNS)," March 1999 ("RFC 2538"); S. Kent et al., IETF RFC 2401, "Security Architecture for the Internet Protocol," November 1998 ("RFC 2401"); D. Eastlake et al., IETF RFC 2065, "Domain Name System Security Extensions," January 1997 ("RFC 2065"); J. Postel et al., IETF RFC 920, "Domain Requirements," October 1984 ("RFC 920"); E. Guttman et al., IETF RFC 2504, "Users' Security Handbook," February 1999 ("RFC 2504"); M. Reed et al., "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA (December 9-13) ("*Reed*"); Goldschlag et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK, May 1996 ("Goldschlag"); P. Mockapetris, IETF RFC 1035, "Domain Names – Implementation and Specification," November 1987 ("RFC 1035"); R. Braden, IETF RFC 1123, "Requirements for Internet Hosts – Applications and Support," October 1989 ("RFC 1123"); R. Atkinson, IETF RFC 1825, "Security Architecture for the Internet Protocol," August 1995 ("RFC 1825"); R. Housley et al., IETF RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and

---

[1] I refer to the Request for *Inter Partes* Reexamination as "the Request" and, correspondingly, I will refer to Apple Inc. as "the Requester."

[2] The Office Action incorporates nearly all of the Request by reference. For that reason, when I sometimes refer to "the Request," I am also referring to the Office Action.

CRL Profile," January 1999 ("RFC 2459"); and P. Mockapetris, IETF RFC 1034, "Domain Names – Concepts and Facilities," November 1987 ("RFC 1034").[3]

4. I am familiar with the level of ordinary skill in the art with respect to the inventions of the '504 patent as of February 15, 2000, when the application for the parent '135 patent was filed. 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.

5. I have been asked to consider how one of ordinary skill in the art would have understood the references mentioned above. My findings are set forth below.

II. QUALIFICATIONS

6. I have a great deal of experience and familiarity with computer and network security, and have been working in this field since 1993.

7. I am currently an Associate Professor of Computer Science at Columbia University, as well as Director of the University's Network Security Laboratory. I joined Columbia in 2001 as an Assistant Professor, after receiving my M.Sc. and Ph.D. degrees in Computer Science, both from the University of Pennsylvania. My Ph.D. dissertation work was on the topic of secure access control for distributed systems and, in particular, on the management of trust in distributed computer networks.

8. I received my B.Sc. in Computer Science from the University of Crete, in Greece, in 1996. During my undergraduate studies, I worked as system administrator in the Computing Center at the University of Crete. Following that, I worked as network engineer at the first commercial Internet Service Provider ("ISP") in Greece, FORTHnet SA, where I was exposed to many network security issues.

9. I have actively participated in the Internet Engineering Task Force ("IETF"), a standards-setting body for the Internet, since 1995. In the late 1990s and early 2000s, my work with the IETF was primarily within the Internet Protocol Security ("IPsec") Working Group. In addition

[3] Although I listed dates in these citations, I am not testifying to whether any of these references were actually publicly distributed on the date listed.

to contributing to the specification of the IPsec standards, I wrote the first implementation of the Photuris key management protocol (now RFC 2522). I also contributed to the first open-source implementation of the IKSAMP/IKE key management protocol for the open-source BSD operating system (now RFC 2409), and developed the first such implementation for the Linux operating system. My Linux implementation, named Pluto, was adopted by the National Institute of Standards and Technology ("NIST") in 1999. In addition, my implementation of IPsec for the open-source BSD operating system is currently used by many companies and governments around the world, and serves as the basis for several commercial products that employ cryptographic communications. In 1999, I architected and implemented the first open-source framework for supporting hardware cryptographic accelerators. This framework is used in the open-source OpenBSD, NetBSD, FreeBSD, and Linux operating systems. My work in implementing firewalls and other cryptographic and network protocols has resulted in commercial systems and publications in refereed technical conferences and academic journals. I served as Working Group Secretary for the IETF IPsec Working Group (2003-2005) and as Security Area Advisor to the IETF at large (2003-2008).

10. In my current position at Columbia University, I work with a large group of graduate and postgraduate students in the area of cybersecurity. My past students now work in this field as university professors, as technical researchers for research laboratories, or as engineers for telecommunications companies. I have received federal, state, and corporate sponsorship to conduct cybersecurity research from the Department of Defense, the National Security Agency, the Defense Advanced Research Projects Agency ("DARPA"), the National Science Foundation, the Department of Homeland Security, the Air Force, the Office for Naval Research, the Army Research Office, the Department of the Interior, the National Reconnaissance Office, New York State, Google, Intel, Cisco, and others. In my ten years as a professor, I have received over 36 million dollars to support my research in cybersecurity. I also regularly teach courses on cybersecurity, in addition to more general courses in computer science.

11. I have published over 200 technical papers in refereed journals, conferences, and workshops, all of which are directed to various areas of cybersecurity. I have also authored a book, coauthored another book, and contributed chapters for many other books that relate to cybersecurity. Between 1999 and 2010, I have drafted or codrafted eight standards documents that were published as Request for Comments ("RFCs"). Several of these RFCs are directly related to IP security. For example, RFC 6042 relates to transport layer security; RFC 5708, RFC 2792, and RFC 2704 relate to key signature and encoding for trust management; and RFC 3586 relates to IP security policy

requirements. Additionally, I am a coinventor on twelve issued U.S. patents, and have several other applications pending. Most of these patents and pending applications are related to network and systems security.

12. I have chaired several international technical conferences and workshops in cybersecurity, including, for example, the International Conference on Financial Cryptography and Data Security (FC), ACM Computer and Communication Security (CCS), and the New Security Paradigms Workshop (NSPW). I have also served in over eighty technical program committees for such events. From 2004-2010, I served as Associate Editor for the premier technical journal on cybersecurity—the ACM Transactions on Information and Systems Security (TISSEC). Additionally, I have served on several advisory workshops to the United States Government on cybersecurity, including, among others, the Office of the Director of National Intelligence (ODNI)/National Security Agency (NSA) Invitational Workshop on Computational Cybersecurity in Compromised Environments (C3E) (2011), the Office of Naval Research (ONR) Workshop on Host Computer Security (2010), the Intelligence Community Technical Exchange on Moving Target (2010), Lockheed Martin Future Security Threats Workshop (2009), and the ARO/FSTC Workshop on Insider Attack and Cyber Security.

13. In addition to this work, I have cofounded two companies in cybersecurity. One company, StackSafe Inc. (formerly Revive Systems Inc.), was a provider of a virtualized preproduction staging environment that includes automated testing, analysis, and reporting for IT operations teams. I was with this company from its founding in 2005 until 2009. The second company, Allure Security Technologies (founded in 2010), develops deception-based solutions for detecting and mitigating the malicious cyber-insider threat, commercializing technology developed at Columbia through DHS and DARPA grants and a DARPA SBIR contract.

14. My curriculum vitae, which is appended to this declaration, details my background and technical qualifications. Although I am being compensated at my standard rate of $500/hour for my work on this declaration, the compensation in no way affects the statements in this declaration.

III. BACKGROUND OF THE '504 PATENT

15. Before turning to a discussion of the references relied on in the Request and the Office Action, I summarize my understanding of certain embodiments disclosed in the '504 patent. Generally speaking, the '504 patent discloses, among other things, systems and methods for providing a domain name service ("DNS") for establishing a secure communication link.

16. The '504 patent discloses several embodiments of a domain name service system for establishing a secure communication link, such as a virtual private network ("VPN") communication link. In one such embodiment, a novel, specialized DNS server receives a traditional DNS request, and the DNS server automatically facilitates the establishment of a secure communication link, such as a VPN link, between a target node and a user. ('504 patent 39:46-51.) This specialized DNS server is different from a conventional DNS server known at the time of invention for at least the reason that the specialized DNS server supports the establishment of a secure communication link beyond merely returning a requested IP address or public key.

17. For example, in the exemplars of FIGS. 26 and 27 of the '504 patent, reproduced below, a DNS server 2602 including a DNS proxy 2610 supports establishing a VPN link between a computer 2601 and a secure target site 2604. (*Id.* at 39:67-41:59.)

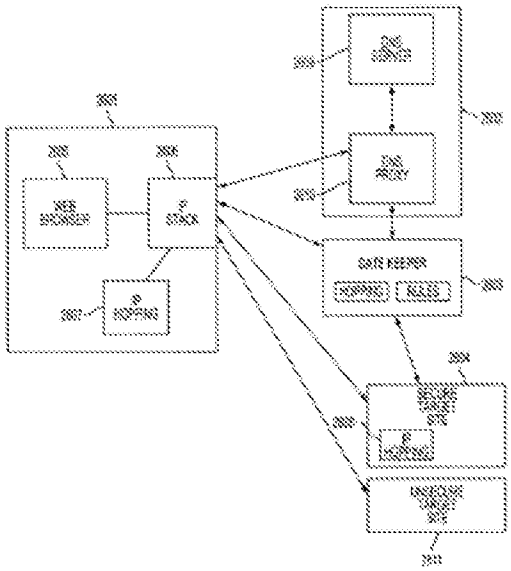


FIG. 26

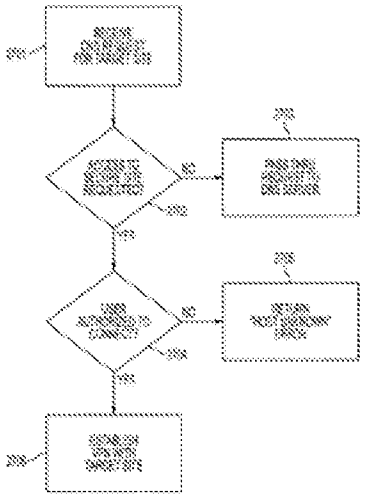


FIG. 27

18. In one embodiment, the DNS server 2602 receives a DNS request for a target site from computer 2601. (*Id.* at 40:49-52.) The DNS proxy 2610 determines whether the target site is a secure site. (*Id.* at 40:6-8, 40:49-56.) If access to a secure site has been requested, the DNS proxy 2610 determines whether the computer 2601 is authorized to access the site. (*Id.* at 40:57-59.) If so, the DNS proxy 2610 transmits a message to gatekeeper 2603 to facilitate the creation of a VPN link between computer 2601 and secure target site 2604. (*Id.* at 40:18-24.) DNS proxy 2610 then responds to the computer's 2601 DNS request with an address received from the gatekeeper 2604. (*Id.* at 40:19-22.) A secure VPN link is then established between the computer 2601 and the secure

target site 2604. (*Id.* at 41:5-8.) As shown in this example, the specialized DNS server supports creating a secure communication link, or, in other words, does more than a conventional DNS server at the time of invention.

19. In fact, the '504 patent highlights this distinction between the specialized DNS server disclosed in its specification and a conventional DNS scheme, which merely returns a requested IP address or public key:

> Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host. For example, when a computer user types in the web name "Yahoo.com," the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser . . . .
>
> . . .
>
> 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 so that the host can set up a VPN without having the user enter the public key of the destination host. One implementation of this standard is presently being developed as part of the FreeS/WAN project (RFC 2535).
>
> The conventional scheme suffers from certain drawbacks. For example, any user can perform a DNS request. Moreover, DNS requests resolve to the same value for all users.
>
> According to certain aspects of the invention, a specialized DNS server traps DNS requests and, if the request is from a special type of user (e.g., one for which secure communication services are defined), the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user.

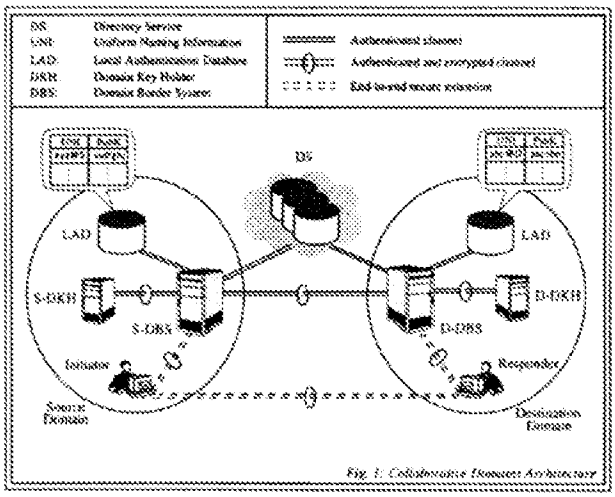
(*Id.* at 39:7-51.) Compared with a conventional DNS known at the time of the filing of the '504 patent, the specialized DNS disclosed in the '504 patent supports establishing a secure communication link. The claims of the '504 patent are also directed to a domain name service for establishing a secure communication link. (*See, e.g.*, '504 patent 55:49-56, 57:48-58, 60:3-14).

IV. REFERENCES CITED AGAINST CLAIMS 1, 36, AND 60

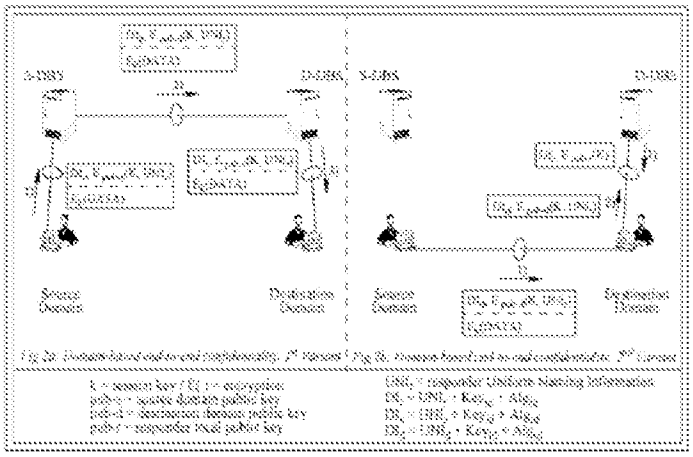
A. *Solana*

20. Generally, *Solana* discloses a domain-based security architecture for Internet transactions. (*Solana* Abstract, Fig. 1.) Regarding Fig. 1, reproduced below, *Solana* discloses that the architecture includes a directory service ("DS") that binds domains to their public keys and a

local authentication database ("LAD") that includes the public keys for each principal within a domain. (*Id.* at 43.) *Solana* discloses that each security domain includes a domain key holder ("DKH") that stores the key ring of domain public/private key pairs and a domain border system ("DBS") that performs various tasks related to inter-domain collaboration. (*Id.* at 43-44.) *Solana* also discloses uniform naming information ("UNI") that is used to designate both domains and principals within domains. (*Id.* at 43.) The UNI may be "a common name, an E-mail address, or a network address." (*Id.*)



21. *Solana* discloses two alternatives for communicating between an initiator in a source domain and a responder in a destination domain. (*Id.* at Figs. 2a and 2b, below.) In the configuration relating to Fig. 2a, the initiator sends a communication 1) to a source DBS ("S-DBS"). (*Id.* at 45.) The communication includes a header that contains a session key and uniform naming information ("UNI") for the responder, and is encrypted with a public key of the source domain. (*Id.*) The S-DBS receives the communication, decrypts the header using its private key, re-encrypts the same header using the public key of the destination domain, and sends the transaction to the destination DBS ("D-DBS"). (*Id.* at 45-46.) The D-DBS likewise extracts the header, finds the local public key of the responder in the LAD, re-encrypts the same header with the responder local public key, and forwards the transaction to the responder. (*Id.* at 46.)



22. In the configuration relating to Fig. 2b, the initiator sends a similar communication directly to the responder that includes the same header as in the configuration of Fig. 2a, except that the header is encrypted with the destination domain public key. (*Id.* at 45-46.) The responder forwards the header to the D-DBS, and the D-DBS sends the header back, this time encrypted with the responder local public key. (*Id.*)

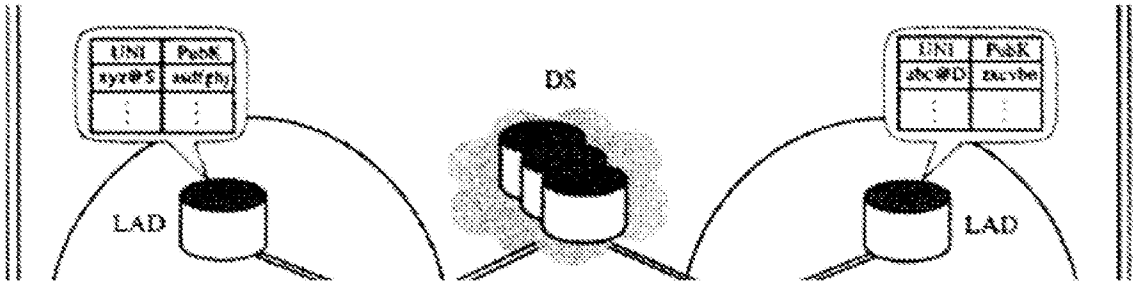
1. *Solana* does not disclose a domain name service system configured to store a plurality of domain names and corresponding network addresses.

23. It is my opinion that *Solana* does not disclose a domain name service system configured to store a plurality of domain names and corresponding network addresses, as recited in various claims of the '504 patent. The Office Action, by incorporating page 42 of the Request, asserts that Solana's Uniform Naming Information ("UNI"), which may be published in a directory service ("DS"), includes both domain names and corresponding network addresses. I disagree for the following reasons.

24. First, *Solana* does not disclose that the DS stores a plurality of domain names and corresponding network addresses. Instead, *Solana* merely discloses that the DS stores "naming information and . . . certificates that securely bind domains to their public keys." (*Solana* 43.) Thus, if anything, *Solana*'s DS stores naming information for domains and *corresponding public keys* for the domains. But *Solana* does not disclose that the DS stores a plurality of domain names and *corresponding network addresses*.

25. Second, the "naming information" stored in *Solana*'s DS also does not include both domain names *and corresponding network addresses*. *Solana* explains that the "naming information" is stored in the DS in the form of UNIs, which may include "a common name, an E-mail address, *or* a network address." (*See id.* ,emphasis added.) Thus, the UNI disclosed by *Solana* does not include *both* a domain name and a corresponding network address.

26. Further, in Fig. 1, reproduced in part below, *Solana* discloses in greater detail how UNIs and corresponding keys may also be stored together in the LAD, another database separate from the DS. But the LAD also does not store domain names and corresponding network addresses:



(*Id.*) The UNI/PubK tables in Fig. 1 show how the LAD associates a UNI of a particular principal with its public key. (*Id.* at 43-44.) As shown, the UNI "xyz@S" for a principal in the source domain corresponds to public key "asdfghj," and the UNI "abc@D" for a principal in the destination domain corresponds to public key "zxcvbn." (*Id.* at Fig. 1.) But again, the UNI itself does not include both a domain name and a corresponding network address. (*Id.* at 43.) Moreover, the UNI stored in the LAD is associated with a public key, and not with a network address. (*Id.* at Fig. 1.)

27. Third, one of ordinary skill in the art would not have understood *Solana*'s DS to be a domain name service system. As discussed, *Solana*'s DS stores naming information (UNIs) for domains and certificates that bind those domains to public keys. But *Solana* does not disclose that the DS resolves domain names—resolving domain names into IP addresses is outside the scope of *Solana*.

2. *Solana* does not disclose a domain name service system configured to receive a query for a network address.

28. It is also my opinion that *Solana* does not disclose a domain name service system configured to receive a query for a network address. The Office Action adopted pages 42-44 of the Request, which asserts that this claim feature is disclosed in three different figures of *Solana*. For the following reasons, I disagree with this assertion.

29. First, contrary to the Request's assertions, Figure 1 does not disclose a domain name service system configured to receive a query for a network address. The Request asserts that *Solana* "explains that its secure DNS systems are designed to handle the 'generic Internet transaction' which . . . is generated by requests initiated by the two principals–the 'initiator' and the 'responder.'" (Req. at 43.) The Request continues: "[I]n Figure 1, the initiator and the responder entities are shown as making requests that are acted upon by the DNS system to establish an authenticated and encrypted channel of communications." (*Id.*) I disagree.

30. Nothing in *Solana* suggests that the identified requests in *Solana* include a query for a network address. To the contrary, the "requests" sent from the initiator and responder, discussed in greater detail below with respect to Figs. 2a and 2b, are queries for *keys* stored in the DS or the LAD. (*See generally id.* at 45-46 ("The initiator . . . issues a DS query *to obtain the destination domain public key*," emphasis added.) Indeed, Fig. 1 of *Solana* discloses an architecture that distributes public keys used to establish authenticated and/or encrypted channels—not an architecture that receives queries for network addresses.

31. Second, contrary to the Request's assertions, Figure 2a in *Solana* does not disclose a domain name service system configured to receive a query for a network address. With respect to Fig. 2a, the Request asserts that "the DNS system acts on requests to determine network addresses of the initiator and responder principals." (*Id.* at 44.) The Request also points to the three communications shown in Fig. 2a and explained on pages 45-46 of *Solana* as allegedly disclosing these "requests to determine network addresses of the initiator and responder principals." (*Id.* at 43-44.) Again, I disagree.

32. *Solana* discloses that the first communication in Fig. 2a is sent from the source domain to the S-DBS and includes "a header containing the session key and the UNI of the responder" and a payload containing encrypted data (depicted in Fig. 2a as "E_k(DATA)"). (*Solana* 45.) Nothing in *Solana* describes or suggests that the communication includes a request for a network address. Moreover, the remaining two communications shown in Fig. 2a merely involve forwarding the communication from the S-DBS to the D-DBS and then from the D-DBS to the responder. (*Id.* at 45-46.) Each of these communications includes the same header containing the same session key and UNI of the responder—the only difference being that the header is encrypted with the public key of the recipient during each communication (i.e., the public key of the destination domain during communication 2 and the public key of the responder during communication 3). (*Id.*)

33. Further, Figure 2a does not disclose "a domain name service system configured to receive a query for a network address" because what the Request alleges is the claimed domain name service system (*Solana*'s DS) does not receive the alleged query for a network address. *Solana* discloses that the configuration of Fig. 2a "is particularly convenient for principals lacking access to a global DS." (*Id.* at 46.) In other words, the DS—the alleged domain name service system—is not involved in the method disclosed in Fig. 2a.

34. Third, contrary to the Request's assertions, Figure 2b does not disclose a domain name service system configured to receive a query for a network address. For example, *Solana*

explains that the first communication in Fig. 2b includes the initiator generating the same header as in the first communication in Fig. 2a. (*Id.*) Then, the initiator issues a "DS query *to obtain the destination domain public key for header encryption.*" (*Id.*, emphasis added.) Thus, the only query issued by the initiator is a query for a public key, and not a query for a network address. (*Id.*)

3. *Solana* does not disclose "a domain name service system configured . . . to comprise an indication that the domain name service system supports establishing a secure communication link."

35. It is also my opinion that *Solana* also fails to teach or suggest "a domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," as required by, for example, claim 1 of the '504 patent. The Request asserts that *Solana* teaches this limitation because: (1) *Solana* teaches that its system includes "a Domain Key Holder (DKH) and a Domain Border System (DBS) that manage and use keys/certificates to handle authentication and encryption functions"; and (2) "the patent owner has asserted that the use of certificates in connection with establishment of secure communication links comprises an 'indication' that a DNS system can support secure communications." (Req. at 45.) I disagree with these assertions.

36. The Request suggests that the keys and certificates in *Solana* are indications that the DS, DKH, and DBS of *Solana* support establishing the alleged secure communication link. But no combination of *Solana*'s DS, DKH, or DBS can be the recited domain name service system because none of these components are configured to (1) store a plurality of domain names and corresponding network addresses or (2) receive a query for a network address as required by some of the claims of the '504 patent. Moreover, one of ordinary skill in the art at the time of the application for the '504 patent would not have understood the DS, DKH, or DBS to be a domain name service system. As I discussed above, the DS described by *Solana* does not store a plurality of domain names and corresponding network addresses or receive a query for a network address. Indeed, the Request and the Office Action do not show how the DKH and DBS disclosed by *Solana* include these features. Nor could they, in the eyes of one of ordinary skill in the art, be considered a domain name service system.

37. In addition, it is irrelevant whether—as the Request and Office Action assert—"the patent owner has asserted that the use of certificates in connection with establishment of secure communication links comprises an 'indication' that a DNS system can support secure communications." (*Id.*) The certificates and keys disclosed by *Solana* and relied upon by the Office Action are distributed by systems that are not domain name service systems.

B. *Solana* in View of RFC 2504

38. It is my opinion that combining RFC 2504 with *Solana* still does not remedy the deficiencies I identified above with respect to *Solana*. The Request relies on RFC 2504 as disclosing an indication that the domain name service system supports establishing a secure communication link. I disagree.

39. RFC 2504 is a document that "provides guidance to the end-users of computer systems and networks about what they can do to keep their data and communication private." (RFC 2504 at 2.) As such, RFC 2504's focus is with end-user functionality and steps that end-users can take to protect their network communications. (*See id.*) RFC 2504 does not discuss DNS functionality. Moreover, RFC 2504 does not disclose storing domain names and corresponding network addresses or receiving a query for a network address. Because RFC 2504 does not disclose a domain name service system, it does not disclose an indication that *the domain name service system* supports establishing a secure communication link.

40. The Request and the Office Action also assert that RFC 2504's "use of visible indications, such as a 'lock' or 'key' icon through a web browser," discloses such an indication. (Req. at 91.) But whatever the lock or key icons of RFC 2504 indicate, they do not indicate that *the domain name service system* supports establishing a secure communication link, because no such domain name service system is disclosed in RFC 2504.

C. *Provino*

41. *Provino* discloses a system for connecting an external device to a device on a virtual private network via a secure tunnel between the external device and a firewall associated with the virtual private network. (*Provino* Abstract.) Referring to FIG. 1 of *Provino*, reproduced below, when an operator at a device 12(m) wishes to connect to a device 13 on the Internet, the operator inputs a human-readable address of the device 13, causing the device 12(m) to send a message to a name server 17 requesting the corresponding Internet address of the device 12(m). (*Id.* at 8:14-40, 11:5-11.) The name server 17 does not have the addresses of the devices 31 on the virtual private network 15, except for the address of the firewall 30 of the virtual private network 15. In response to a request for the Internet address of a device 31 on the virtual private network 15, the name server returns the Internet address of the firewall 30. (*Id.* at 10:45-55, 11:11-16.)

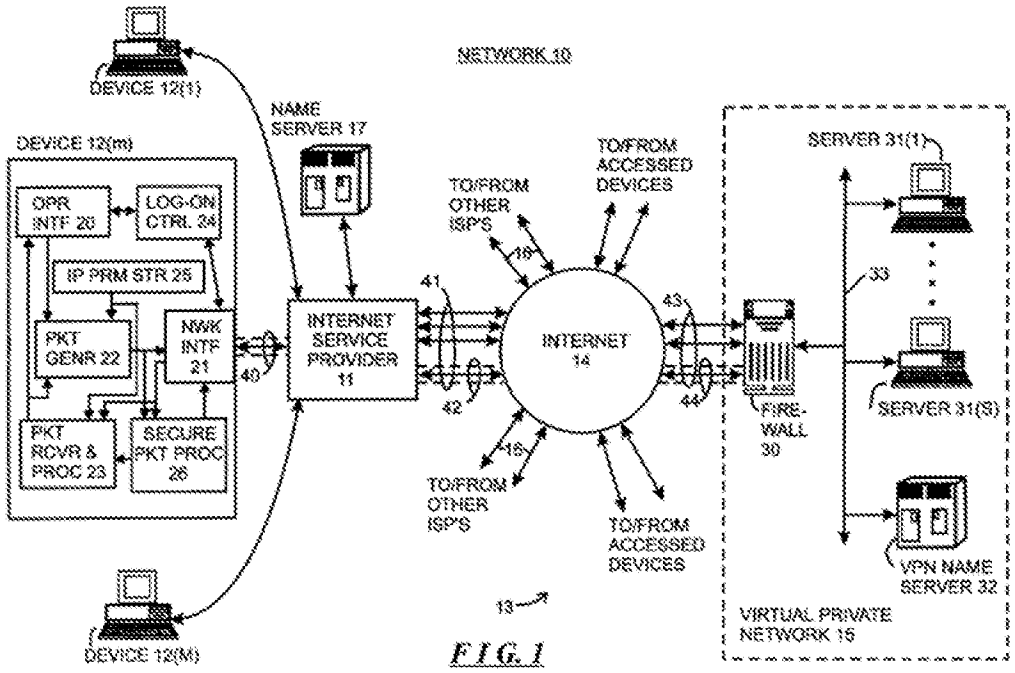


FIG. 1

42. The device 12(m) initiates establishment of a secure tunnel with the firewall 30. (*Id.* at 9:32-56, 10:56-58, 11:13-16.) Further, the firewall 30 provides the device 12(m) with the identification of a second name server 32 inside the virtual private network 15. (*Id.* at 10:62-63.) The device 12(m) sends, over the secure tunnel, a message to the second name server 32 requesting the Internet address of the device 31 on the virtual private network 31 corresponding to the human-readable address of the device 31. (*Id.* at 10:62-67, 11:17-26.) Thereafter, the device 12(m) is able to communicate with the device 31 on the virtual private network 15 via the secure tunnel.

43. The Request asserts that "the identification of Firewall 30 by name server 17 comprises an indication that the name server 17 supports establishing a secure communication link." (Req. at 122.) I disagree.

44. As described in the summary above, *Provino*'s name server 17—which the Request and the Office Action allege discloses the claimed domain name service system—just resolves the Internet address of the firewall 30 in response to a request to resolve the human-readable address of the firewall 30. This is not an indication that the name server 17 (the alleged domain name service system) supports establishing a secure communication link, because the name server 17 resolves the requested Internet address of any device 13 on the Internet, firewall 30 or otherwise, provided that is able to do so. *Provino*'s name server 17 (the alleged domain name service system) operates just like a conventional domain name service system and does not have any additional functionality that could be considered to comprise an indication that the name server 17 supports establishing a secure

communication link. Indeed, since the only disclosed capability of the name server 17 is to indiscriminately return a requested Internet address of a device, *Provino* does not even suggest that the name server 17 has the capability to support establishing a secure communication link. *Provino*'s name server 17 returning a requested Internet address cannot comprise an indication that the name server 17 supports establishing a secure communication link, since *Provino* does not even disclose that is has that capability to begin with.

45. Supporting my conclusion, *Provino*'s alleged domain name service system (the name server 17) is consistent with a conventional domain name service system that the '504 patent distinguishes from a "domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," as recited in claim 1. (*See, e.g.*, '504 patent 39:7-42.) For example, the '504 patent indicates that a conventional domain name service system merely returns an IP address that was requested of it. In one embodiment, the '504 patent explains that "[c]onventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a *requested* computer or host. For example, when a computer user types in the web name 'Yahoo.com,' the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser . . . ." (*Id.* at 39:7-13, emphasis added; *see also id.* at 39:14-42.) In another example, the '504 patent identifies a conventional domain name service system that stores public keys of different machines so that hosts can request and receive those public keys from the domain name service system. (*Id.* at 39:34-42.) Similar to the conventional domain name systems described by the '504 patent, the name server 17 of *Provino* merely returns a requested Internet address of a device corresponding to the human-readable address of that device, such as the requested IP address corresponding to a domain name like "Yahoo.com." (*Compare Provino* 8:48-51 *with* '504 patent 39:7-13.)

46. The '504 patent recognizes that such conventional domain name systems suffer from certain drawbacks and thus discloses embodiments that address them, including a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link. (*See, e.g.*, '504 patent 39:43-41:61.)

47. The Request also alleges that "*Provino* shows the authorization and engagement of device 12(m) through the firewall comprises an indication [sic] of a secure communication link discernible to a user [sic]." (Req. at 122.) Apparently as part of this assertion, it further alleges that "*Provino* also teaches the engagement of device 12(m) to include provision of the decryption

algorithm and associated decryption key from the firewall 30 to use in decrypting message packets from the VPN." (*Id.*) I disagree.

48. Provino does not disclose "an indication that *the domain name service system* supports establishing a secure communication link" (emphasis added). As discussed, *Provino* does not teach that the alleged domain name service system (the name server 17) even has the capability to support establishing a secure communication link and, thus, the reference cannot disclose any indication that the domain name service system supports establishing a secure communication link.

49. In addition, based on the excerpts of *Provino* cited in the Request and the Office Action, it appears that the alleged "authorization and engagement" refers to the process in which the device 12(m) and the firewall 30 engage to establish the secure tunnel (i.e., the alleged secure communication link). (*See Provino* 9:46-47:12.) This process, however, does not involve the alleged domain name service system in *Provino* (the name server 17), and thus cannot disclose or suggest a *domain name service system* configured to comprise an indication that the *domain name service system* supports establishing a secure communication. That the device 12(m) and the firewall 30 establish a secure tunnel does not mean that the alleged *domain name service system* is configured to comprise an indication that the *domain name service system* supports establishing a secure communication link.

D. *Provino* in View of RFC 2230

50. It is my opinion that combining RFC 2230 with *Provino* still does not remedy the deficiencies I identified above with respect to *Provino*. The Request relies on RFC 2230 as disclosing an indication that the domain name service system supports establishing a secure communication link. I disagree.

51. RFC 2230 also does not disclose a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link for at least the reasons I discuss in the paragraphs below addressing RFC 2230.

E. *Provino* in View of RFC 2504

52. It is my opinion that combining RFC 2504 with *Provino* still does not remedy the deficiencies I identified above with respect to *Provino*.

53. The Request and the Office Action rely on RFC 2504 solely to allegedly show an indication that the domain name service system supports establishing a secure communication link. (Req. at 198-99.) As I discussed above with respect to the combination of RFC 2504 with *Solana*, RFC 2504 does not disclose an indication that the domain name service system supports

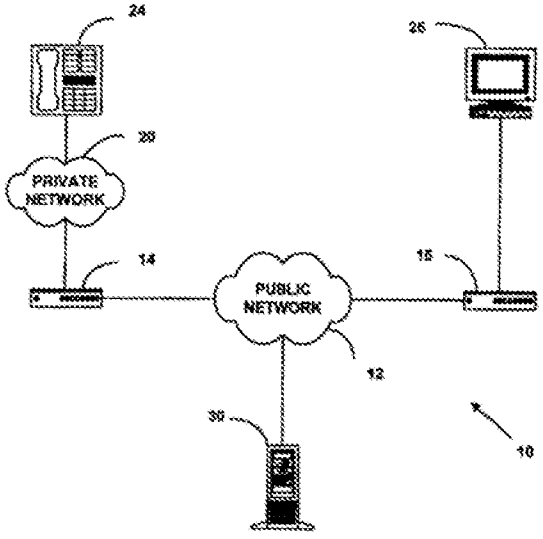
establishing a secure communication link. Instead, RFC 2504 is a document that "provides guidance to the end-users of computer systems and networks about what they can do to keep their data and communication private." (RFC 2504 at 2.) As such, RFC 2504 is primarily concerned with end-user functionality and steps that end-users can take to protect their network communications. (*See* RFC 2504.) RFC 2504 does not discuss DNS functionality. Moreover, RFC 2504 does not disclose storing domain names and corresponding network addresses or receiving a query for a network address. Because RFC 2504 does not disclose a domain name service system, RFC 2504 cannot disclose an indication that the domain name service system_supports establishing a secure communication link.

54. Further, the Request and the Office Action assert that "the use of visible indications, such as a 'lock' or 'key' icon through a web browser," disclose such an indication. (Req. at 198-99.) But whatever the lock or key icons of RFC 2504 indicate, they do not indicate that *the domain name service system* supports establishing a secure communication link, because no such domain name service system is disclosed in RFC 2504.

F. *Beser*

Beser discloses a system for initiating a tunneling connection that hides the identity of the originating and terminating ends of the tunneling association from other users. (*Beser* Abstract.) With reference to Fig. 1, reproduced below, *Beser* discloses that a first network device 14 informs a trusted-third-party network device 30 of a request to initiate a tunneling connection received from an originating telephony device 24. (*Beser* 7:62-8:4, 10:2-6, 11:9-10.)

FIG. 1



55. The request to initiate a tunneling connection includes a unique identifier for a terminating telephony device 26. (*Id.* at 10:4-6.) After being informed of the request, trusted-third-party network device 30 associates an identifier of terminating telephony device 26 with a public IP address of a second network device 16. (*Id.* at 11:26-32.) Then, private IP addresses for each of the originating telephony device 24 and the terminating telephony device 26 are negotiated and distributed to the second network device 16 and the first network device 14, respectively. (*See, e.g.*, *id.* at 11:59-12:54.) This way, the tunneling connection "hides the identity of the originating and terminating ends of the tunneling association from the other users of the public network." (*Id.* at 2:36-39.)

56. For at least the following two reasons, it is my opinion that *Beser* does not disclose a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link.

57. First, *Beser* does not disclose a secure communication link and, thus, cannot disclose an indication that the domain name service system supports establishing a secure communication link. The Request and the Office Action assert that *Beser* discloses a secure communication link by negotiating "first and second private IP addresses . . . in a manner to ensure anonymity and hide the identities of the originating and terminating devices . . . ." (Req. at 231.) I disagree.

58. One of ordinary skill in the art would have understood a secure communication link to require encryption. For example, the '504 patent explains that "[d]ata security is usually tackled using *some form of data encryption*." ('504 patent 1:55-56, emphasis added.) *Beser*, however, does not disclose establishing a secure communication link between the originating and terminating devices because *Beser* does not disclose that the communication between these two devices is encrypted. Instead, *Beser* discloses establishing a tunneling association that merely hides the identity of the originating and terminating ends of the tunneling association from the other users of a public network. (*Beser* 2:36-39; *see also* Req. at 231.) But the communication between these two devices is not encrypted and, thus, no secure communication link is established. In fact, *Beser* acknowledges that encryption was known to exist, but teaches that it is undesirable in the configurations disclosed by *Beser* because, according to *Beser*, encryption may provide insufficient protection, may be infeasible to implement, and/or may create service problems due to computer-power limitations. (*Beser* 1:54-67.) Thus, one of ordinary skill in the art, when reading *Beser*, would understand that *Beser*'s tunneling technique does not establish a secure communication link, but instead provides an alternative to establishing one.

59. Second, *Beser* does not disclose that the domain name service system comprises an *indication* that the domain name service system supports establishing a secure communication link. The Request and the Office Action assert that *Beser*'s "negotiation" discloses the claimed indication. (Req. at 231-32.) I disagree.

60. *Beser*'s "negotiation" is merely a distribution of network addresses. For example, the trusted-third-party network device 30 forwards the public and private IP addresses of the first network device to the second network device, and vice versa. (*See Beser*, 13:10-14:33, Fig. 9.) But distributing IP addresses to the first and second network devices is not an indication that the domain name service system supports establishing a secure communication link. At most, *Beser* merely shows that the trusted-third-party network device 30 is configured to distribute IP addresses to entities seeking them.

G. RFC 2230

61. RFC 2230 discloses a mechanism to delegate authorization for one node to act as key exchanger for a second node. (RFC 2230 at 1.) In particular, RFC 2230 "specifies a new kind of DNS Resource Record (RR), known as the Key Exchanger (KX) record." (*Id.* at 2.) "The KX record is useful in providing an authenticatible method of delegating authorisation for one node to provide key exchange services on behalf of one or more, possibly different, nodes." (*Id.* at 1.)

62. Figure 1 of RFC 2230, reproduced below, shows a Subnet-to-Subnet Example of key exchange delegation. (*Id.* at 3.) When an originating node S sends packets to a destination node D, an IPsec router R1 for originating node S decides whether to provide IPsec service for the traffic. (*Id.* at 2-3.) If R1 has decided that traffic from S to D should be protected, it performs a DNS lookup for the records associated with the domain of D. (*Id.* at 3.) If R1 only knows the IP address for D, then it first performs a reverse DNS lookup to determine the domain of D before it performs the DNS lookup for the records associated with the domain of D. (*Id.*)

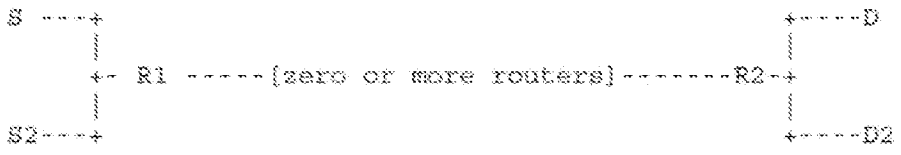


Figure 1: Network Diagram for Subnet-to-Subnet Example

KX record(s) returned from the DNS lookup indicate(s) a set of one or more delegated key exchangers for the domain of D—in this case, R2. (*Id.*) Based on the KX record including the domain name of R2 as the delegated key exchanger for D, R1 selects R2 as a key exchanger and "initiates a key management session with that key exchanger (in this example, R2)." (*Id.*) A KX

record has the following syntax:

```
<domain-name>  IN  KX  <preference> <domain-name>
```

which means that "Internet nodes about to initiate a key exchange with <domain-name 1> should instead contact <domain-name 2> to initiate the key exchange for a security service between the initiator and <domain-name 2>." (*Id.* at 8.)

63. R2 then performs a KX record lookup on S to confirm that R1 is the delegated key exchanger for S. (*Id.* at 3-4.) Then, "[i]f the proposed IPsec Security Association is acceptable to both R1 and R2, each of which might have separate policies, then they create that IPsec Security Association via Key Management." (*Id.* at 4.)

64. The Request and the Office Action propose two alternatives for why RFC 2230 allegedly discloses a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link. (Req. at 280-81.) First, they allege that "[t]he secure DNS systems described in RFC 2230 include indications, via the KX resource record, that the systems support establishing secure communication links." (*Id.* at 280.) Second, the Request and the Office Action allege that "during the establishment of the IPSec Security Association, a further indication is provided that the secure DNS systems support establishing a secure communication link." (*Id.*) I disagree for the following reasons and address each in turn.

65. First, the KX record in RFC 2230 is not an indication that the alleged *domain name service system* supports establishing a secure communication link. Instead, as described above, the KX record includes the domain name of a *delegated key exchanger node* (e.g., R2). Specifically, the KX record includes the domain name(s) of a "*set of nodes* [that] are authorised key exchanger nodes for the destination D." (RFC 2230 at 3, emphasis added.) RFC 2230 specifies that the delegated key exchanger nodes are the "IPsec-capable routers" R1 and R2 or the IPsec-capable router R1 and the destination node D itself, depending upon the configuration (Subnet-to-Subnet, Subnet-to-Host, or Host-to-Subnet). (*Id.* at 2-5.) But based on the description in RFC 2230, one of ordinary skill in the art would have understood that the IPsec-capable routers R1 and R2 and the destination node D are *separate* from the alleged domain name service system to which the DNS lookup was sent and the KX record obtained. Thus, the KX record includes the domain name of a delegated device, *separate* from the alleged domain name service system, which is capable of key management. Accordingly, one of ordinary skill in the art would not have understood the KX record to comprise an indication that the *domain name service system* supports establishing a secure communication link. While

including the domain name of a certain delegated IPsec node capable of key exchange, the KX record includes no indication about the capabilities of the alleged domain name service system itself, and certainly does not include an indication that the domain name service system supports establishing a secure communication link. Indeed, the alleged domain name service system disclosed by RFC 2230 does not support establishing a secure communication link because it merely returns a KX record when one is requested. RFC 2230 does not disclose that the alleged domain name service system does anything else, and does not disclose that it supports establishing a secure communication link. RFC 2230 cannot be viewed as disclosing that a domain name service system comprises an indication that it supports establishing a secure communication link when the reference does not even teach that the alleged domain name service has the capability to support establishing a secure communication link to begin with.

66. Second, according to the Request and the Office Action, "during the establishment of the IPSec Security Association, a further indication is provided that the secure DNS systems support establishing a secure communication link." (Req. at 280.) To support this assertion, the Request and the Office Action block-quote the first four paragraphs of RFC 2230, page 5 (section 2.1.2 Subnet-to-Host Example), and then state, "Thus, D verifies the authorization and permits creation of an IPSec Security Association on behalf of S. This indication supports establishment of the secure communication link between 'S' and 'D.'" (*Id.* at 280-81.) I disagree with this conclusion.

67. The quoted passage of RFC 2230 explains how, in the Subnet-to-Host Example, "D can verify that R1 is authorised to create an IPsec Security Association" before R1 engages in key exchange with the destination D. (RFC 2230 at 5.) The destination D does this by requesting a "forward DNS lookup on S to locate the KX records for S." (*Id.*) The destination D will engage in key management with R1 so long as the returned KX record "indicate[s] that R1 is an authorised key exchanger for S." (*Id.*)

68. As discussed above, however, a KX record does not comprise an indication that the alleged *domain name service system* supports establishing a secure communication link. Based on RFC 2230, one of ordinary skill in the art would have understood a KX record to include the domain name of a device, *separate* from the alleged domain name service system, that supports key management for the source S rather than to indicate whether the alleged domain name service supports establishing a secure communication link. For instance, in the example cited by the Request and the Office Action, the returned KX record must include the domain name of *R1* before the destination D will proceed with key management. (*Id.*, emphasis added.) Accordingly, in the cited

example, one of ordinary skill in the art would have understood the KX record to include the domain name of a *separate IPsec router R1* capable of key exchange on behalf of the source S, not to indicate the alleged *domain name service system* supports establishing a secure communication link. Thus, the destination D's verification that R1 is the authorized key exchanger for the source S in RFC 2230 does not disclose the claimed domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link.

69. In addition, one of ordinary skill in the art would not have understood the creation and use of the IPsec Security Association between D and R1 to disclose an indication that the alleged domain name service system supports establishing a secure communication link. As explained, one of ordinary skill in the art would have understood the destination D and the IPsec router R1 as *separate* from the alleged domain name service system, and thus would not have viewed the establishment and use of an IPsec Security Association between these devices to comprise an indication that the alleged *domain name service* system supports establishing a secure communication link.

70. Confirming the conclusions I have reached above with regard to RFC 2230, the alleged domain name service system in RFC 2230 is consistent with a conventional domain name service system that the '504 patent distinguishes from a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link. (*See, e.g.*, '504 patent 39:7-42.) As discussed, the '504 patent indicates that a conventional domain name service system merely returns an IP address or public key that was requested of it. For instance, the '504 patent explains that "[c]onventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a *requested* computer or host. For example, when a computer user types in the web name 'Yahoo.com,' the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser . . . ." ('504 patent 39:7-13, emphasis added; *see also* '504 patent 39:14-42.) In another example, the '504 patent identifies conventional domain name service systems that store public keys of different machines so that hosts can request and receive those public keys from the domain name service system. (*Id.* at 39:34-42.) Similar to the conventional domain name systems described by the '504 patent, the domain name service system described in RFC 2230 merely returns a KX resource record requested for a particular domain name. (*See, e.g.*, RFC 2230 at 3.)

71. The '504 patent recognizes that such conventional domain name systems suffer from certain drawbacks and thus discloses embodiments that address them, including a domain name

service system configured to comprise an indication that the domain name service system supports establishing a secure communication link. (*See, e.g.*, '504 patent 39:43-41:61.) And since RFC 2230's alleged domain name service system is a mere conventional domain name server of the type distinguished by the '504 patent, one of ordinary skill in the art would not have understood RFC 2230 to disclose or suggest a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link.

H. RFC 2538

72. RFC 2538 discloses a domain name system resource record ("RR"), the CERT RR, for storing certificates in the DNS. (RFC 2538 at 1.) RFC 2538 describes a certificate as "a binding . . . of a public key . . . and identity, authorization, or other information." (*Id.* at 2.) RFC 2538 recommends storing CERT RRs in the DNS under a domain name of the entity that controls the private key corresponding to the public key being certified. (*Id.* at 5.) According to the Request, "[t]his permits the system to provide, in response to a query with respect to the particular domain name, the appropriate public key certificate associated with that domain." (Req. at 324.)

73. The Request and the Office Action assert that the CERT RR of RFC 2538 discloses an "indication that the domain name service system supports establishing a secure communication link." (*Id.* at 324-25.) I disagree.

74. To begin with, the Request suggests that the DNS server that stores the CERT RR is the claimed domain name service system. (*Id.* at 322-24.) But the certificate in a CERT RR merely binds a public key to some "identity, authorization, or other information." (RFC 2538 at 1.) It does not include any indication that the DNS server in which the certificate is stored supports establishing a secure communication link. RFC 2459, relied on by the Request, discloses the basic syntax for one type of certificate mentioned in RFC 2538—the X.509 certificate. But nothing in the basic syntax includes any information that indicates that the DNS server supports establishing a secure communication link. (RFC 2459 at 15-24.) Indeed, the DNS server disclosed by RFC 2538 does not support establishing a secure communication link—it merely returns a certificate when one is requested. RFC 2538 does not disclose that the DNS server does anything else, and does not disclose that it supports establishing a secure communication link. RFC 2538 cannot be viewed as disclosing that a domain name service system comprises an indication that the domain name service system supports establishing a secure communication link when the reference fails to disclose that the domain name service has the capability to support establishing a secure communication link to begin with.

75. In fact, RFC 2538's alleged domain name service system, the DNS, is consistent with a conventional domain name service system that the '504 patent distinguishes from a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link," as recited in claim 1. (*See, e.g.*, '504 patent 39:7-42.) For example, the '504 patent indicates that a conventional domain name service system merely returns an IP address or public key that was requested of it. In one embodiment, the '504 patent explains that "[c]onventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host." (*Id.* at 39:7-13; *see also id. at* 39:14-42.) In another example, the '504 patent identifies a conventional domain name server that stores public keys of different machines so that hosts can request and receive those public keys from the domain name service system. (*Id.* at 39:34-42.) Similar to the conventional domain name servers described by the '504 patent, the DNS of RFC 2538 merely returns a CERT RR with a public key in response to a request for one. (*See, e.g.*, Req. at 324, "This permits the system to provide, in response to a query with respect to the particular domain name, the appropriate public key certificate associated with that domain.")

76. The '504 patent recognizes that such conventional domain name servers suffer from certain drawbacks and thus discloses embodiments that address them, including a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link." (*See, e.g.*, '504 patent 39:43-41:61.) And since RFC 2538's DNS (i.e., the alleged domain name service system) is a mere conventional domain name server of the type distinguished by the '504 patent, one of ordinary skill in the art would not have understood RFC 2538 to disclose or suggest a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link.

V. REFERENCES CITED AGAINST DEPENDENT CLAIMS 5, 23, AND 47

77. I understand that the Office Action and the Request rely on *Provino* as disclosing a domain name service system configured to authenticate the query for the network address or to authenticate the query for the network address using a cryptographic technique. The Request asserts that "Provino teaches systems that receive a query for a network address from the operator (and subsequently) from device 12(m). . . . This occurs during dialog between the initiating and responding entities." (*See, e.g.*, Req. at 123, 168.) To support their assertion, the Request and the Office Action block-quote a passage of *Provino* discussing the dialog between the device 12(m) and

the firewall 30 that sets up the secure tunnel. (Req. at 123, citing *Provino* 9:56-10:12.) I disagree with this interpretation of Provino.

78. The only encryption or decryption described in the cited passage of *Provino* refers to encrypting *message packets* sent between the device 12(m) and the firewall 30 over the secure tunnel. (*Provino* 9:56-10:12.) This encryption of message packets does not occur until the secure tunnel has been set up—*after* the device 12(m) has already sent the alleged query for the network address of the firewall 30 to the alleged domain name service system (name server 17). *Provino* is silent regarding authenticating the alleged query for a network address, that is, the message sent to the name server 17 requesting the Internet address of a device corresponding to a provided human-readable address of that device. It is therefore my opinion that *Provino* does not disclose a domain name service system configured to authenticate the query for the network address using a cryptographic technique or otherwise.

VI. REFERENCES CITED AGAINST DEPENDENT CLAIMS 8 AND 9

79. I understand that the Request and the Office Action assert that the following quotation from *Solana* discloses that a domain name service system is connectable to a virtual private network: "organizations concerned by security issues conceive strong internal security policies and interact with the Internet through very restrictive firewalls or by means of well-protected Virtual Private Networks (VPN)." (Req. at 47, quoting *Solana* 38.) But this quotation only says that organizations may use virtual private networks. It does not disclose or even suggest that the alleged domain name service system (*Solana*'s DS) is connectable to a virtual private network. In fact, the quotation discussed above is the only time *Solana* mentions virtual private networks, and *Solana* is silent regarding the DS being connectable to a virtual private network. It is therefore my opinion that Solana does not disclose a domain name service system is connectable to a virtual private network.

80. I understand that the Office Action and the Request also rely on *Provino* as disclosing a domain name service system that is connectable to a virtual private network, asserting that "Fig.1 of *Provino* discloses secure DNS systems connectable to a virtual private network (15) through the communication network (Internet 14.)" (*Id.* at 124; *see id.* at 168, 199.) I disagree.

81. As I stated above, the Request and the Office Action allege that *Provino*'s name server 17 discloses the claimed domain name service system. But *Provino* does not teach that the name server 17 ever connects to *Provino*'s virtual private network 15 (the alleged virtual private network). In fact, it is the external device 12(m) rather than the name server 17 that connects to

Provino's virtual private network 14 over the secure tunnel with the firewall 30. *Provino* just discloses that the name server 17 performs the conventional domain name service function of returning the Internet address of a device 13 on the Internet (e.g., firewall 30) in response to receiving a request from the external device 12(m) containing the human-readable address of that device. The system diagram in Fig. 1 of *Provino* also does not show that the alleged domain name service system (name server 17) is connectable to the virtual private network 15. Because the alleged domain name service system (*Provino*'s name server 17) is not taught to ever connect to the virtual private network 15, it is my opinion that *Provino* fails to disclose that the domain name service system is connectable to a virtual private network through the communication network.

82. The Request also asserts that *Beser* and RFC 2401 disclose that the domain name service system is connectable to a virtual private network. The Request and the Office Action assert that *Beser* in view of RFC 2401 would have rendered this feature obvious because "RFC 2401 describes . . . a model where edge routers on two different networks are used to establish the encrypted IP tunnel through which the network devices (i.e., the 'first' and 'second' network devices of *Beser*) will communicate." (*Id.* at 270.) However, even if *Beser* and RFC 2401 were combined in the way asserted by the Request and Office Action, this combination would not disclose or suggest the domain name service system connectable to a virtual private network. Instead, the Request and Office Action's combination would result in a virtual private network between the *first and second network devices* of *Beser*. As I mentioned above, the Request and the Office Action assert that the *trusted-third-party network device 30*, and not the *first and second network devices*, is the domain name service system. Thus, even if the combination were made, it would not result in the domain name service system being connectable to a virtual private network.

83. The Request also asserts that RFC 2230 and RFC 2401 disclose that the domain name service system is connectable to a virtual private network. The Request and the Office Action assert that RFC 2230 in view of RFC 2401 would have rendered this feature obvious because "RFC 2401 describes . . . a model where edge routers on two different networks are used to establish the encrypted IP tunnel through which the network devices (*i.e.*, the 'S' and 'D' network devices of RFC 2230) will communicate." (*Id.* at 314.) However, even if RFC 2230 and RFC 2401 were combined in the way asserted by the Request and Office Action, this combination would not disclose or suggest the subject matter of claim 8 and its dependent claim 9. Instead, the Request and Office Action's combination would allegedly result in a virtual private network between *the originating device S and the destination device D* of RFC 2230. As discussed above with respect to independent claim 1, one

of ordinary skill in the art would have understood these devices to be *separate* from the alleged domain name service system (to which the KX record lookup is sent). Thus, even if the combination were made, it would not result in the alleged domain name service system being connectable to a virtual private network.

84. The Request and the Office Action also assert that the combination of RFC 2538 with RFC 2401 would render obvious a domain name service system connectable to a virtual private network. (*Id.* at 354-55.) I disagree. As I discussed above, RFC 2538 merely discloses the use of CERT RRs for storing certificates in the domain name system. RFC 2401 discloses the IPsec protocol. (RFC 2401 at 2.) But neither reference discloses a domain name service system connectable to a virtual private network. Indeed, the Request and the Office Action assert that RFC 2401 discloses establishing a virtual private network between *network devices*. (*See* Req. at 355, "RFC 2401 describes . . . a model where edge routers on two different networks are used to establish the encrypted IP tunnel through which the network devices will communicate." Nothing in RFC 2401 discloses or suggests that these network devices are domain name service systems, let alone the claimed domain name service system. Thus, even if the combination proposed by the Office Action were made, it would not result in a domain name service system being connectable to a virtual private network.

VII. REFERENCES CITED AGAINST DEPENDENT CLAIMS 18 AND 42

85. I understand that the Office Action rejects dependent claims 18 and 42 as anticipated by *Solana*, and as being obvious over *Solana* in view of RFC 2504. The Request and the Office Action assert that *Solana*'s "domain names employing Uniform Naming Information (UNI) of the responder" disclose that at least one of the plurality of domain names is reserved for secure communication links. (Req. at 50-51; *see also id.* at 64, 94, 102.) I disagree. *Solana* discloses that the UNI may be a common name, an e-mail address, or a network address. (*Solana* 43.) But *Solana* does not disclose that this common name, e-mail address, or network address is *reserved* for secure communication links. *Solana* does not disclose that the UNI can only be used for secure communication links, and merely establishing an alleged secure communication link with the responder UNI does not disclose that the responder UNI is *reserved* for secure communication links. As such, *Solana* does not disclose domain names reserved for secure communication links.

86. I understand that the Office Action also rejects dependent claims 18 and 42 as being anticipated by *Beser*. The Request and the Office Action assert that *Beser* discloses domain names reserved for secure communication links because *Beser* discloses associating a unique identifier (which may be a domain name) in a tunneling request with the first and second network devices. (Req. at 236, 251.) But merely associating the unique identifier of terminating telephony device 26 that is included in the request with another network device does not disclose reserving that unique identifier for secure communication links. *Beser* discloses that the unique identifier may include a dial-up number, an E-mail address, a domain name, an employee number, a driver's license number, etc. (*Beser* 10:37-11:8.) But *Beser* does not disclose reserving any of these identifiers for secure communication links. The portions in *Beser* relied upon by the Request and the Office Action as allegedly disclosing this feature merely point to the negotiation process of *Beser* that the Request and the Office Action earlier asserted was an indication that the domain name service system supports establishing a secure communication link. These portions do not disclose reserving domain names for secure communication links.

87. I understand that the Office Action rejects dependent claims 18 and 42 as being anticipated by RFC 2230. The Request and the Office Action allege RFC 2230 discloses that at least one of the plurality of domain names is reserved for secure communication links, citing to RFC 2230's statement that "[o]nce R1 has decided that the packet from S to D should be protected, it performs a secure DNS lookup for the records associated with domain D." (Req. at 284, 296.) RFC 2230 does not support this position.

88. While RFC 2230 discloses that IPsec Security Associations *can* be established between domains, the reference does not disclose that any domain names are *reserved* for secure communication links. As highlighted by the passage cited by the Request and the Office Action, in the Subnet-to-Subnet Example, before R1 even performs a DNS lookup, "R1 [first] makes the *policy decision* to provide the IPsec service for traffic from R1 destined for R2. *Once R1 has decided* that the packet from S to D should be protected, it performs a secure DNS lookup for the records associated with domain D." (RFC 2230 at 3, emphases added.) R1 or D makes a similar policy decision in the other embodiments as well:

> R1 makes the *policy decision* that IP Security is needed for the packet travelling from S to D. Then, R1 performs the secure DNS lookup for D (*id.* at 4, emphasis added); and

> D makes the *policy decision* that IP Security is needed for the packets from D to S. Then D performs the secure DNS lookup for S (*id.* at 6, emphasis added).

Since an external policy decision determines whether to provide security for packets sent between given domains, it is possible to establish a connection to a domain with or without IP Security. Thus, it is my opinion that RFC 2230 does not disclose *reserving* any domain names for secure communication links.

89. I understand that the Office Action rejects dependent claims 18 and 42 as being anticipated by RFC 2538. The Request and Office Action assert RFC 2538 discloses reserving domain names for secure communication links because it discloses that "domain names are associated with certificates used for secure communication links." (Req. at 328, 340.) But merely storing a certificate under a domain name related to its subject, as disclosed in RFC 2538, does not mean that the domain name is reserved for secure communication links. (RFC 2538 at 5.) In fact, nothing in RFC 2538 discloses or suggests that the domain name associated with the certificate may be used only for secure communication. As such, RFC 2538 does not disclose that domain names stored are reserved for secure communication links.

VIII. REFERENCES CITED AGAINST DEPENDENT CLAIMS 24 AND 48

90. The Office Action rejects dependent claims 24 and 48 as anticipated by *Solana*, and as being obvious over *Solana* in view of RFC 920 and/or RFC 2504. The Request and the Office Action assert that because *Solana* discloses domain names that are associated with certificates needed for secure transactions, those domain names are "'secure names' associated with secure communications and thereby comprise indications that its secure DNS systems support establishing a secure communication link." (Req. at 52-53.) I disagree.

91. The mere association of a domain name with a certificate does not disclose anything about what the domain name itself comprises. In particular, just because a domain name is associated with a certificate does not mean that the domain name itself comprises an indication that a domain name system supports establishing a secure communication link.

92. In fact, *Solana* does not disclose that the UNIs (the alleged domain names) include any indication of the capabilities of the DS (the alleged domain name service system), much less an indication that the DS supports establishing a secure communication link. For example, *Solana* discloses two examples of UNIs in Fig. 1: xyz@S and abc@D. (*Solana* 43, Fig. 1.) But *Solana*

does not disclose that these UNIs, or any other UNIs, comprise an indication that the DS supports establishing a secure communication link.

93. RFC 920 and RFC 2504 also do not disclose that a domain name itself comprises an indication that a domain name system supports establishing a secure communication link. The Request relies on RFC 920 as "including general criteria for establishing new domain names." (Req. at 80.) But the "general criteria" in RFC 920 do not disclose a domain name that comprises an indication that the domain name service system supports establishing a secure communication link. I understand that the Request and the Office Action do not assert that it does. (*Id.* at 80, 111-12.) RFC 2504 also does not disclose, and is not relied upon as allegedly disclosing, that a domain name itself comprises an indication that a domain name system supports establishing a secure communication link. (*Id.* at 95-96, 111-12.)

94. I understand that the Office Action rejects dependent claims 24 and 48 as anticipated by *Provino*, and as being obvious over *Provino* in view of RFC 920, RFC 2230, and/or RFC 2504. The Request and the Office Action allege that *Provino* discloses a domain name that comprises or includes an indication that the domain name service system supports establishing a secure communication link because "Provino also discloses use of nameservers to resolve human-readable domain names to provide appropriate Internet address[es], and that domain names (e.g., domain name associated with VPN 15) are associated with secure transactions over the Internet." (*Id.* at 128.) This is incorrect for at least two reasons.

95. First, as discussed above with respect to the independent claims, *Provino*'s alleged domain name service system (name server 17) is not configured to comprise an indication that the domain name service system supports establishing a secure communication link. Rather, *Provino*'s alleged domain name service system is a conventional domain name service system, recognized and distinguished by the '504 patent, that merely responds to a request for the Internet address of a device (firewall 30 or otherwise) corresponding to the human-readable name for that device. Thus, *Provino*'s alleged domain name service system does not even have the capability to support establishing a secure communication link, let alone to comprise an indication that the domain name service system supports establishing a secure communication link. And because *Provino*'s alleged domain name service system does not even have the capability to support establishing a secure communication link, it cannot store a domain name that comprises or includes an indication that the alleged domain name service system supports establishing a secure communication link.

96. In addition, the fact that *Provino*'s alleged domain name service system resolves the Internet address of the firewall 30 (with which the device 12(m) may at some point later establish a secure tunnel) when it is requested does not disclose anything about what the alleged domain name of the firewall 30 itself comprises. Just because a domain name is associated with a firewall does not mean that the domain name itself includes or comprises an indication that a domain name system supports establishing a secure communication link. *Provino* does not provide any specifics about the content of the alleged domain names stored in *Provino*'s name server 17, and certainly does not disclose that they can comprise or include an indication of the capabilities of the alleged domain name service system, much less an indication that it supports establishing a secure communication link. As I explained above, *Provino* does not even disclose that the alleged domain name service system is capable of supporting establishing a secure communication to begin with.

97. I understand that the Office Action also rejects dependent claims 24 and 48 as being anticipated by *Beser*, and as being obvious over *Beser* in view of RFC 920. The Request and the Office Action assert that *Beser* discloses a domain name that comprises an indication that the domain name service system supports establishing a secure communication link because the domain names in *Beser* "are 'secure names' associated with secure communications." (Req. at 239.) I disagree.

98. Merely using a domain name in secure communications, as asserted by the Request and the Office Action, does not disclose anything about what the domain name itself comprises. In particular, just because a domain name is "associated with secure communications" does not mean that the domain name comprises an indication that a domain name system supports establishing a secure communication link. In fact, *Beser* does not disclose that the alleged domain names (i.e., unique identifiers) include any indication of the capabilities of the alleged domain name service system (i.e., trusted-third-party network device 30), let alone an indication that the alleged domain name service system supports establishing a secure communication link.

99. RFC 920 also does not disclose a domain name that comprises an indication that the domain name supports establishing a secure communication link. The Request relies on RFC 920 as "including general criteria for establishing new domain names." (*Id.* at 265-66.) But, as discussed, the "general criteria" in RFC 920 do not disclose a domain name that comprises an indication that the domain name service system supports establishing a secure communication link.

100. I understand that the Office Action further rejects dependent claims 24 and 48 as being anticipated by RFC 2230, and as being obvious over RFC 2230 in view of RFC 920. The Request and the Office Action allege that RFC 2230 discloses a domain name that comprises or

includes an indication that the domain name service system supports establishing a secure communication link because "RFC 2230 discloses secure DNS systems providing for secure communication links between multiple domains ('S' and 'D') that are established via use of systems that incorporate and use the KX resource record." (*Id.* at 286.) This is incorrect for at least two reasons.

101. First, as I describe above, RFC 2230's alleged domain name service system is not configured to comprise an indication that the domain name service system supports establishing a secure communication link. Rather, RFC 2230 discloses a conventional domain name service system, recognized and distinguished by the '504 patent. Thus, RFC 2230's alleged domain name service system does not even have the capability to support establishing a secure communication link, let alone to comprise an indication that the domain name service system supports establishing a secure communication link, as recited by independent claim 1. Because the alleged domain name service system does not even have the capability to support establishing a secure communication link, RFC 2230 cannot disclose or suggest that the alleged domain name service system stores at least one domain name that comprises or includes an indication that the alleged domain name service system supports establishing a secure communication link.

102. In addition, the mere fact that RFC 2230 discloses that IPsec Security Associations can be created between an originating device S and a destination device D does not disclose anything about what the domain names associated with these devices themselves include. Specifically, just because a Security Association is created between two devices does not mean that their domain names include or comprise an indication that the alleged domain name system supports establishing a secure communication link. RFC 2230 does not provide any specifics about the content of the domain names, and certainly does not disclose that they can comprise or include an indication of the capabilities of the alleged domain name service system. Thus, RFC 2230 does not disclose that at least one of the plurality of domain names comprises or includes an indication that the domain name service system supports establishing a secure communication link.

103. I understand that the Office Action rejects dependent claims 24 and 48 as being anticipated by RFC 2538, and as being obvious over RFC 2538 in view of RFC 920. The Request and the Office Action assert that RFC 2538 discloses a domain name that comprises an indication that the domain name service system supports establishing a secure communication link because the domain names in RFC 2538 "are 'secure names' associated with secure communications." (Req. at 330.) I disagree.

104. Merely associating a domain name with secure communications, as asserted by the Request and the Office Action, does not disclose anything about what the domain name itself comprises. In particular, just because a domain name is "associated with secure communications" does not mean that the domain name includes an indication that a domain name system supports establishing a secure communication link. In fact, RFC 2538 does not disclose domain names that include any indication of the capabilities of the alleged domain name service system in RFC 2538, much less an indication that the alleged domain name service system supports establishing a secure communication link. Thus, RFC 2538 does not disclose the features of claims 24 and 48.

105. RFC 920 does not make up for the above-noted deficiencies of RFC 2538. The Request relies on RFC 920 as "including general criteria for establishing new domain names." (*Id.* at 351-52.) But, as discussed, the "general criteria" in RFC 920 do not disclose a domain name that comprises an indication that the domain name service system supports establishing a secure communication link.

IX. REFERENCES CITED AGAINST DEPENDENT CLAIMS 26 AND 50

106. I understand that the Office Action rejects dependent claims 26 and 50 as anticipated by *Solana*, and as being obvious over *Solana* in view of RFC 2504. The Request and the Office Action assert that *Solana* discloses UNIs to designate principals and domains, and that the UNI is used when establishing the alleged secure communication link. (*See, e.g.*, Req. at 53, citing *Solana* 43-46, Figs. 2a-b, 3a-b.) But merely using a UNI when establishing an alleged secure communication link does not mean that the UNI itself enables (or is configured so as to enable) establishment of the secure communication link. As discussed, *Solana* discloses two exemplary UNIs in connection with Fig. 1: xyz@S and abc@D. (*Solana* 43, Fig. 1.) But *Solana* does not disclose that these exemplary UNIs enable establishment of a secure communication link.

107. I understand that the Office Action further rejects dependent claims 26 and 50 as anticipated by *Provino*, and as being obvious over *Provino* in view of RFC 2230 or RFC 2504. The Request and the Office Action allege that *Provino* discloses that at least one of the plurality of domain names enables, or is configured so as to enable, establishment of a secure communication link because "[t]he domain names and Internet addresses maintained in name server 32 are used to establish virtual private networks, which are secure communication links." (*See, e.g.*, Req. at 129.) I disagree.

108. Merely *using* a domain name when establishing an alleged secure communication link does not mean that the domain name itself *enables* establishment of the secure communication link. *Provino* is silent regarding the content of the alleged domain names (human-readable addresses), and certainly does not disclose that they include anything special that enables, or is configured so as to enable, establishment of a secure communication link.

109. I understand that the Office Action also rejects dependent claims 26 and 50 as being anticipated by *Beser*. The Request and the Office Action assert that *Beser* discloses that at least one of the plurality of domain names enables, or is configured so as to enable, establishment of a secure communication link because *Beser* "discloses systems in which a unique identifier, which may be a domain name, *is used to* establish a secure communication link." (*See, e.g.*, *id.* at 239, emphasis added.) But merely *using* a domain name when establishing an alleged secure communication link does not mean that the domain name itself *enables* establishment of the secure communication link. *Beser* does not disclose that the unique identifiers *enable* (or are configured so as to enable) establishment of a secure communication link.

110. I understand that the Office Action further rejects dependent claims 26 and 50 as being anticipated by RFC 2230. The Request and the Office Action allege that RFC 2230 discloses that at least one of the plurality of domain names enables, or is configured so as to enable, establishment of a secure communication link because RFC 2230 discloses secure communication links between R1 and R2 and between R1 and D. (*See, e.g.*, *id.* at 287.) I disagree.

111. Merely *using* a domain name when establishing an alleged secure communication link does not mean that the domain name itself *enables* establishment of the secure communication link. In fact, RFC 2230 does not disclose that the unique identifiers *enable* establishment of a secure communication link, and thus does not anticipate claims 26 and 50. Accordingly, the rejection of these claims should be withdrawn. As with other references discussed above, RFC 2230 is silent regarding the content of the alleged domain names, and certainly does not disclose that they include anything special that enables, or is configured so as to enable, establishment of a secure communication link.

112. In addition, as I explain, before an IPsec node in RFC 2230 even seeks the DNS records of its target domain, it first makes a *policy decision* of whether to provide IPsec services for traffic between given domains. (*See*, *e.g.*, RFC 2230 at 3, 4, 6.) Because an external policy decision determines whether to provide security for packets sent between given domains, it is possible to establish a connection to a domain with or without IP Security. Thus, RFC 2230 does not disclose

that at least one of the plurality of *domain names enables*, or *is configured so as to enable*, establishment of a secure communication link.

113. I understand that the Office Action further rejects dependent claims 26 and 50 as being anticipated by RFC 2538. The Request and the Office Action assert that RFC 2538 discloses domain names that enable, or is configured so as to enable, establishment of a secure communication link because the domain names in RFC 2538 are associated with a CERT RR. (*See, e.g.*, Req. at 330-31.) But merely associating a domain name with a public key contained in a certificate (the CERT RR) does not mean that the domain name itself enables establishment of a secure communication link. That is, merely associating a domain name with a public key has nothing to do with the capabilities of the actual domain name, such as whether the domain name enables establishment of a secure communication link. Thus, RFC 2538 merely discloses domain names associated with public keys and does not disclose that the domain names enable, or are configured so as to enable, establishment of a secure communication link.

Truth and Accuracy of Statements

I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that willful false statements or the like may jeopardize the validity of the '504 patent.

Signed at New York, New York, this 29th day of March, 2012.

s/Angelos D. Keromytis/
Angelos D. Keromytis

Angelos D. Keromytis - *Curriculum Vitae*

Positions Held

- **January 2006 - Present**
  Associate Professor, Department of Computer Science, Columbia University, New York.
- **January 2009 - January 2010**
  Senior Research Engineer, Symantec Research Labs Europe, Sophia Antipolis, France.
- **July 2001 - December 2005**
  Assistant Professor, Department of Computer Science, Columbia University, New York.
- **September 1996 - July 2001**
  Research Assistant, Computer and Information Science Department, University of Pennsylvania, Philadelphia.
- **January 1993 - October 1995**
  Member of the Technical Staff, FORTHnet S.A., Heraclion, Greece.
- **September 1991 - January 1993**
  Member of the Technical Staff, Education Team, Computer Center of the University of Crete, Heraclion, Greece.

Education

- **November 2001**
  Ph.D. (Computer Science), University of Pennsylvania, USA.
- **August 1997**
  M.Sc. (Computer Science), University of Pennsylvania, USA.
- **June 1996**
  B.Sc. (Computer Science), University of Crete, Greece.

Service and Teaching

Editorial Boards and Steering Committees

- Associate Editor, Encyclopedia of Cryptography and Security (2nd Edition), Springer, 2010 - 2011.
- Associate Editor, IET (formerly IEE) Proceedings Information Security, 2005 - 2010.
- Steering Committee, *ISOC Symposium on Network and Distributed System Security (SNDSS)*, 2006 - 2009.
- Steering Committee, *New Security Paradigms Workshop (NSPW)*, 2007 onward.
- Associate Editor, ACM Transactions on Information and System Security (TISSEC), 2004 - 2010.
- Steering Committee, *USENIX Workshop on Hot Topics in Security (HotSec)*, 2006 - 2009.
- Steering Committee, *Computer Security Architecture Workshop (CSAW)*, 2007 - 2009.

Program Chair

- Program Chair, 16th International Conference on Financial Cryptography and Data Security (FC), 2012.
- Program co-Chair, 17th ACM Computer and Communication Security (CCS), 2010.
- Program co-Chair, 16th ACM Computer and Communication Security (CCS), 2009.
- Program co-Chair, New Security Paradigms Workshop (NSPW), 2008.
- Program co-Chair, New Security Paradigms Workshop (NSPW), 2007.
- Chair, 27th International Conference on Distributed Computing Systems (ICDCS), *Security Track,* 2007.
- Chair, 16th World Wide Web (WWW) Conference, *Security, Privacy, Reliability and Ethics Track,* 2007.
- Chair, 15th USENIX Security Symposium, 2006.
- Deputy Chair, 15th World Wide Web (WWW) Conference, *Security, Privacy and Ethics Track,* 2006.
- Chair, 3rd Workshop on Rapid Malcode (WORM), 2005.
- Program co-Chair, 3rd Applied Cryptography and Network Security (ACNS) Conference, 2005.
- Program co-Chair, OpenSig Workshop, 2003.

Program Organization

- General Chair, New Security Paradigms Workshop (NSPW), 2010.
- General Vice Chair, New Security Paradigms Workshop (NSPW), 2009.
- Co-chair, Invited Talks, 17th USENIX Security Symposium, 2008.
- General co-chair, Applied Cryptography and Network Security (ACNS) Conference, 2008.
- Co-chair, Invited Talks, 16th USENIX Security Symposium, 2007.
- Organizing Committee, Columbia/IBM/Stevens Security & Privacy Day (bi-annual event).
    - Organizer, Columbia/IBM/Stevens Security & Privacy Day, December 2010.
    - Organizer, Columbia/IBM/Stevens Security & Privacy Day, June 2007.
- Co-organizer, ARO/FSTC Workshop on Insider Attack and Cyber Security, 2007.
- Publicity co-Chair, ACM Conference on Computer and Communications Security, 2006.
- General co-Chair, OpenSig Workshop, 2003.

Program Committees

- Program Committee, ISOC Symposium on Network and Distributed Systems Security (SNDSS), 2003, 2004, 2006, 2007, 2008, 2012.
- Program Committee, International Workshop on Security (IWSEC), 2006, 2007, 2008, 2009, 2010, 2011.
- Program Committee, ACM Conference on Computer and Communications Security (CCS), 2005, 2007, 2008, 2009, 2010.

- Program Committee, Applied Cryptography and Network Security (ACNS) Conference, 2005, 2006, 2010, 2011, 2012.
- Program Committee, USENIX Security Symposium, 2004, 2005, 2006, 2008.
- Program Committee, International Conference on Distributed Computing Systems (ICDCS), *Security Track*, 2005, 2006, 2007, 2008.
- Program Committee, Workshop on Rapid Malcode (WORM), 2004, 2005, 2006, 2007.
- Program Committee, Information Security Conference (ISC), 2005, 2007, 2009, 2011.
- Program Committee, World Wide Web Conference (WWW), 2005, 2006, 2007.
- Program Committee, USENIX Workshop on Hot Topics in Security (HotSec), 2006, 2007, 2010.
- Program Committee, Financial Cryptography (FC) Conference, 2002, 2010, 2011, 2012.
- Program Committee, European Workshop on Systems Security (EuroSec), 2009, 2010, 2011.
- Program Committee, Annual Computer Security Applications Conference (ACSAC), 2006, 2007, 2011.
- Program Committee, USENIX Technical Conference, *Freely Distributable Software (Freenix) Track*, 1998, 1999, 2003.
- Program Committee, IEEE Security & Privacy Symposium, 2006, 2008.
- Program Committee, ACM SIGCOMM Workshop on Large Scale Attack Defense (LSAD), 2006, 2007.
- Program Committee, New Security Paradigms Workshop (NSPW), 2007, 2008.
- Program Committee, IEEE WETICE Workshop on Enterprise Security, 2002, 2003.
- Program Committee, International Conference on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS), 2007, 2010.
- Program Committee, USENIX Annual Technical Conference (ATC), 2008, 2011.
- Program Committee, European Sumposium on Research in Computer Security (ESORICS), 2011.
- Program Committee, International Workshop on Mobile Security (WMS), 2010.
- Program Committee, 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Dependable Computing and Communication Symposium (DCCS), 2010.
- Program Committee, Computer Forensics in Software Engineering Workshop, 2009.
- Program Committee, USENIX Workshop on Large-scale Exploits and Emergent Threats (LEET), 2008.
- Program Committee, 23rd International Information Security Conference (IFIP SEC), 2008.
- Program Committee, Joint iTrust and PST Conferences on Privacy, Trust Management and Security (IFIPTM), 2008.
- Program Committee, 1st Computer Security Architecture Workshop (CSAW), 2007.
- Program Committee, 8th IEEE Information Assurance Workshop (IAW), 2007.
- Program Committee, Anti-Phishing Working Group (APWG) eCrime Researchers Summit, 2007.
- Program Committee, 4th GI International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA), 2007.
- Program Committee, 2nd ACM Symposium on InformAtion, Computer and Communications Security (AsiaCCS), 2007.

- Program Committee, 6th International Conference on Cryptology and Network Security (CANS), 2007.
- Program Committee, 2nd Workshop on Advances in Trusted Computing (WATC), 2006.
- Program Committee, International Conference on Information and Communications Security (ICICS), 2006.
- Program Committee, 2nd Workshop on Secure Network Protocols (NPSec), 2006.
- Program Committee, 1st Workshop on Hot Topics in System Dependability (HotDep), 2005.
- Program Committee, 20th ACM Symposium on Applied Computing (SAC), Trust, Recommendations, Evidence and other Collaboration Know-how (TRECK) Track, 2005.
- Program Committee, 1st Workshop on Operating System and Architecture Support for the on demand IT Infrastructure (OASIS), 2004.
- Program Committee, Workshop on Information Security Applications (WISA), 2004.
- Program Committee, Workshop on Logical Foundations of an Adaptive Security Infrastructure (WOLFASI), 2004.
- Program Committee, 29th IEEE Conference on Local Computer Networks (LCN), 2004.
- Program Committee, 2nd International Conference on Trust Management, 2004.
- Program Committee, Asia BSD Conference, 2004.
- Program Committee, 2nd Annual New York Metro Area Networking Workshop (NYMAN), 2002.
- Program Committee, Cloud Computing Security Workshop (CCSW), 2009.
- Program Committee, Workshop on Grid and Cloud Security (WGC-Sec), 2011.
- Program Committee, Workshop on Cyber Security Experimentation and Test (CSET), 2011.

Advisory Workshops

- ODNI/NSA Invitational Workshop on Computational Cybersecurity in Compromised Environments (C3E), Keystone, CO, September 2011.
- ONR Workshop on Host Computer Security, Chicago, IL, October 2010.
- Intel Workshop on Trust Evidence and End-to-end Trust in Heterogeneous Environments, Santa Clara, CA, May 2010.
- Intelligence Community Technical Exchange on Moving Target, Washington, DC, April 2010.
- Lockheed Martin Future Security Threats Workshop, New York, NY, November 2009.
- Air Force Office for Scientific Research (AFOSR) Invitational Workshop on Homogeneous Enclave Software *vs* Heterogeneous Enclave Software, Arlington, VA, October 2007.
- NSF Future Internet Network Design Working Meeting, Arlington, VA, June 2007.
- ARO/FSTC Workshop on Insider Attack and Cyber Security, Arlington, VA, June 2007.
- NSF Invitational Workshop on Future Directions for the CyberTrust Program, Pittsburgh, PA, October 2006.
- ARO/HSARPA Invitational Workshop on Malware Detection, Arlington, VA, August 2005.
- Department of Defense Invitational Workshop on the Complex Behavior of Adaptive,

Network-Centric Systems, College Park, MD, July 2005.
- ARDA Next Generation Malware Invitational Workshop, Annapolis Junction, MD, March 2005.
- Co-leader of session on "Securing software environments", joint NSF and Department of Treasury Invitational Workshop on Resilient Financial Information Systems, Washington, DC, March 2005.
- DARPA Application Communities Invitational Workshop, Arlington, VA, October 2004.
- DARPA APNets Invitational Workshop, Philadelphia, PA, December 2003.
- NSF/NIST Invitational Workshop on Cybersecurity Workforce Needs Assessment and Educational Innovation, Arlington, VA, August 2003.
- NSF Invitational Workshop on Large Scale Cyber-Security, Lansdowne, VA, March 2003.
- IP Security Working Group Secretary, Internet Engineering Task Force (IETF), 2003 - 2008.
- Session moderator, Workshop on Intelligence and Research, Florham Park, NJ, October 2001.
- DARPA Composable High Assurance Trusted Systems #2 (CHATS2) Invitational Workshop, Napa, CA, November 2000.

Other Professional Activities

- Co-chair, ACM Computing Classification System Update Committee ("Security and Privacy" top-level node), 2011.
- Member, ACM Computing Classification System Update Committee (top two levels), 2010.
- External Advisory Board member, *"i-code: Real-time Malicious Code Identification"*, EU project, 2010 - 2012.
- Reviewer (grant applications), Greek Ministry of Education, 2010.
- Reviewer (grant applications), Danish National Research Foundation, 2010.
- Member of the Scientific Advisory Board, Centre for Research and Technology, Hellas (CERTH), 2008 - 2011.
- Senior Member of the ACM, 2008 onward.
- Senior Member of the IEEE, 2009 onward.
- Visiting Scientist, Institute for Infocomm Research (I^2R), Singapore, February - May 2007.
- Columbia Representative to the Institute for Information Infrastructure Protection (I3P), 2006 - 2008.
- Technical Advisory Board, *StackSafe Inc. (formerly Revive Systems Inc.),* 2006 - 2009.
- Technical Advisory Board, *Radiuz Inc.*, 2006.
- Reviewer (grant applications), Institute for Security Technology Studies (ISTS), Dartmouth College, 2006.
- Reviewer, Singapore National Science and Technology Awards (NSTA), 2006.
- Board of Directors, *StackSafe Inc.(formerly Revive Systems Inc.),* 2005 - 2009.
- Founder, *StackSafe Inc. (formerly Revive Systems Inc.),* 2005 - 2009.
- Expert witness in criminal and intellectual property litigation cases, 2005, 2006, 2007,

2009, 2010, 2011.
- Science Fair Judge, Middle School for Democracy and Leadership, Brooklyn, NY, 2005, 2006.
- Reviewer (grant applications), Swiss National Science Foundation, 2007.
- Reviewer (grant applications), Netherlands Organisation for Scientific Research, 2005, 2006.
- Reviewer (grant applications), US/Israel Binational Science Foundation, 2003, 2005.
- NSF reviewer & panelist, 2002, 2003, 2006, 2008, 2009, 2011.
- Internet Engineering Task Force (IETF) Security Area Advisor, 2001 - 2008.

Ph.D. Thesis Committee Service

- Michalis Polychronakis, *"Generic Code Injection Attack Detection using Code Emulation"*, Computer Science Department, University of Crete, October 2009.
- Spyros Antonatos, *"Defending against Known and Unknown Attacks using a Network of Affined Honeypots"*, Computer Science Department, University of Crete, October 2009.
- Van-Hau Pham, *"Honeypot Traces Forensics by Means of Attack Event Identification"*, Computer Science Group, Communications and Electronics Department, Ecole Nationale Superieure des Telecommunications, September 2009.
- Gabriela F. Ciocarlie, *"Towards Self-Adaptive Anomaly Detection Sensors"*, Department of Computer Science, Columbia University, September 2009.
- Vanessa Frias-Martinez, *"Behavior-Based Admission and Access Control for Network Security"*, Department of Computer Science, Columbia University, September 2008.
- Wei-Jen Li, *"SPARSE: A Hybrid System for Malcode-Bearing Document Detection"*, Department of Computer Science, Columbia University, June 2008.
- Raj Kumar Rajendran, *"The Method for Strong Detection for Distributed Routing"*, Electrical Engineering Department, Columbia University, March 2008.
- Constantin Serban, *"Advances in Decentralized and Stateful Access Control"*, Computer Science Department, Rutgers University, December 2007.
- Ricardo A. Baratto, *"THINC: A Virtual and Remote Display Architecture for Desktop Computing"*, Computer Science Department, Columbia University, October 2007.
- Zhenkai Liang, *"Techniques in Automated Cyber-Attack Response and Recovery"*, Computer Science Department, Stony Brook University, November 2006.
- Ke Wang, *"Network Payload-based Anomaly Detection and Content-based Alert Correlation"*, Computer Science Department, Columbia University, August 2006.
- Seoung-Bum Lee, *"Adaptive Quality of Service for Wireless Ad hoc Networks"*, Electrical Engineering Department, Columbia University, June 2006.
- Shlomo Hershkop, *"Behavior-based Email Analysis with Application to Spam Detection"*, Computer Science Department, Columbia University, August 2005.
- Gaurav S. Kc, *"Defending Software Against Process-subversion Attacks"*, Computer Science Department, Columbia University, April 2005.
- Gong Su, *"MOVE: A New Virtualization Approach to Mobile Communication"*, Computer Science Department, Columbia University, May 2004.
- Jonathan M. Lennox, *"Services for Internet Telephony"*, Computer Science Department, Columbia University, December 2003.

- Michael E. Kounavis, *"Programming Network Architectures"*, Electrical Engineering Department, Columbia University, June 2003.
- Wenyu Jiang, *"QoS Measurement and Management for Internet Real-time Multimedia Services"*, Computer Science Department, Columbia University, April 2003.

Post-doctoral Students

- Hyung Chan Kim (October 2007 - October 2008)
- Stelios Sidiroglou (October 2008 - December 2008)
- Georgios Portokalidis (March 2010 - present)
- Michalis Polychronakis (May 2010 - present)
- Dimitris Geneiatakis (June 2010 - present)

Current Ph.D. Students

- Georgios Kontaxis (September 2011)
- Vasilis Pappas (September 2009 - present)
- Vasileios Kemerlis (September 2008 - present)
- Kangkook Jee (January 2008 - present)
- Sambuddho Chakravarty (January 2007 - present)
- Angelika Zavou (September 2006 - present)

Graduated Ph.D. Students

- Debra Cook (January 2002 - June 2006)
  - Thesis title: *"Elastic Block Ciphers"*
  - Post-graduation: Member of the Technical Staff, Bell Labs
  - Currently: Research Staff Member, Telcordia Research
- Angelos Stavrou (January 2003 - August 2007)
  - Thesis title: *"An Overlay Architecture for End-to-End Service Availability"* (awarded with distinction)
  - Post-graduation: Assistant Professor, Computer Science Department, George Mason University (GMU)
  - Currently: Assistant Professor, Computer Science Department, George Mason University (GMU)
- Michael E. Locasto (September 2002 - December 2007)
  - Thesis title: *"Integrity Postures for Software Self-Defense"* (awarded with distinction)
  - Post-graduation: ISTS Research Fellow, Dartmouth College
  - Currently: Assistant Professor, Department of Computer Science, University of Calgary
- Stelios Sidiroglou (June 2003 - May 2008)
  - Thesis title: *"Software Self-healing Using Error Virtualization"*
  - Post-graduation: Research Scientist, Columbia University

    - Currently: Research Scientist, MIT CSAIL
- Mansoor Alicherry (September 2006 - October 2010)
    - Thesis title: *"A Distributed Policy Enforcement Architecture for Mobile Ad Hoc Networks"*
    - Post-graduation: Member of the Technical Staff, Alcatel-Lucent Bell Labs
    - Currently: Member of the Technical Staff, Alcatel-Lucent Bell Labs
- Brian Bowen (September 2007 - December 2010; co-advised with Salvatore J. Stolfo)
    - Thesis title: *"Design and Analysis of Decoy Systems for Computer Security"*
    - Post-graduation: Member of the Technical Staff, Sandia National Laboratories
    - Currently: Member of the Technical Staff, Sandia National Laboratories

Service at Columbia

- Computer Science Department Ph.D. Committee, 2010 - 2011
- Computer Science Department Facilities committee, 2001 - 2008, 2010 - current
    - Chair, Facilities committee, 2003 - 2005, 2011 - current
- M.Sc. Admissions committee, 2007 - current.
- M.Sc. Committee, 2008 - current.
- Computer Science Department Faculty Recruiting committee, 2002, 2008
- Columbia committee on Research Conflict of Interest Policy, 2007 - 2008
- Co-organizer, Computer Science Faculty Retreat, Fall 2007
- Advisor for the School of Engineering Computer Science Majors, Freshmen & Sophomores, 2004 - 2005
- Computer Science Department Undergraduate Admissions Representative, 2003 - 2008
- Advisor for the School of Engineering Computer Science Majors, Seniors, 2003 - 2004, 2006 - 2007
- Computer Science Department Space Allocation Policy committee, 2002 - 2010
- Computer Science Department Events Representative, 2002 - 2008
- Advisor for the School of Engineering Computer Science Majors, Juniors, 2002 - 2003, 2005 - 2006
- Computer Science Department CRF Director Hiring committee, 2003
- Advisor for the School of Engineering Computer Science Majors, Sophomores, 2001 - 2002
- Computer Science Department Faculty Recruiting committee, 2001 - 2002
- Executive Vice Provost committee on Columbia's response to the 9/11 events, Fall 2001

Teaching

(Scores indicate mean course quality rating from student survey; survey not conducted for summer sessions)

- Instructor, COMS E6183-1 - Advanced Topics in Network Security, Columbia University
    - Fall 2006: 17 on-campus students *(4.58/5)*
- Instructor, COMS W6998.1 - Advanced Topics in Network Security, Columbia

University
    - Fall 2004: 17 on-campus students *(4.62/5)*
    - Spring 2003: 18 on-campus students *(N/A)*
- Instructor, COMS W4180 - Network Security, Columbia University
    - Spring 2011: 4 CVN students *(N/A)*
    - Fall 2010: 2 CVN students *(N/A)*
    - Spring 2010: 25 on-campus and 5 CVN students *(4.48/5)*
    - Summer 2006: 7 CVN students *(N/A)*
    - Spring 2006: 63 on-campus and 9 CVN students *(4.14/5)*
    - Summer 2005: 4 CVN students *(N/A)*
    - Spring 2005: 41 on-campus and 5 CVN students *(4.25/5)*
    - Summer 2004: 6 CVN students *(N/A)*
    - Fall 2003: 45 on-campus and 12 CVN students *(3.74/5)*
    - Summer 2003: 5 CVN students *(N/A)*
    - Fall 2002: 43 on-campus and 9 CVN students *(3.21/5)*
    - Fall 2001: 23 on-campus students *(3.6/5)*
- Instructor, COMS W4118 - Operating Systems, Columbia University
    - Summer 2007: 8 CVN students *(N/A)*
    - Fall 2006: 59 on-campus and 7 CVN students *(3.73/5)*
    - Summer 2006: 15 CVN students *(N/A)*
    - Fall 2005: 52 on-campus and 9 CVN students *(3.86/5)*
    - Spring 2004: 32 on-campus and 4 CVN students *(3.39/5)*
    - Spring 2002: 37 on-campus students *(3.13/5)*
- Instructor, COMS W3157 - Advanced Programming, Columbia University
    - Fall 2010: 37 on-campus students *(3.25/5)*
    - Fall 2007: 30 on-campus students *(4.16/5)*
- Instructor, CIS700/002 - Building Secure Systems, University of Pennsylvania, Spring 1998

Support for Research and Teaching (Gifts and Grants)

1. PI (co-PIs: Roxana Geambasu, Junfeng Yang, Simha Sethumadhavan, Sal Stolfo), *"MEERKATS: Maintaining EnterprisE Resiliency via Kaleidoscopic Adaptation & Transformation of Software Services"*, DARPA MRC, **$6,619,270** (09/2011 - 09/2015; leading team that includes George Mason University and Symantec Corp.)
2. PI, *"NSF Support for the 2011 New Security Paradigms Workshop Financial Aid (Supplement)"*, NSF Trustworthy Computing, **$10,000** (06/2011 - 07/2012)
3. PI, *"Leveraging the Cloud to Audit Use of Sensitive Infomation"*, Google (research gift), **$60,200** (05/2011)
4. co-PI (with Sal Stolfo), *"ADAMS Advanced Behavioral Sensors (ABS)"*, DARPA ADAMS, **$780,996** (05/2011 - 04/2013)
5. PI, *"Tracking Sensitive Information Flows in Modern Enterprises"*, Intel, **$84,951** (12/2010 - 12/2011)

6. co-PI (with Simha Sethumadhavan, Sal Stolfo, Junfeng Yang, and David August @ Princeton), *"SPARCHS: Symbiotic, Polymorphic, Autotomic, Resilient, Clean-slate, Host Security"*, DARPA CRASH, **$6,424,180** (10/2010 - 09/2014)
7. PI, *"NSF Support for the 2010 New Security Paradigms Workshop Financial Aid"*, NSF Trustworthy Computing, **$10,000** (09/2010 - 08/2011)
8. PI (co-PIs: Junfeng Yang, Sal Stolfo), *"MINESTRONE"*, IARPA, **$7,530,113** (08/2010 - 07/2014; leading team that includes Stanford University, George Mason University, and Symantec Corp.)
9. co-PI (with Junfeng Yang and Dawson Engler @ Stanford), *"Seed: CSR: Large: Collaborative Research: SemGrep: Improving Software Reliability Through Semantic Similarity Bug Search"*, NSF CSR, CNS-10-12107, **$325,000** (07/2010 - 06/2011)
10. PI, *"Tracking Sensitive Information Flows in Modern Enterprises"*, Intel, **$82,286** (08/2009 - 07/2010)
11. PI, *"Supplement for International Research Collaborations"*, NSF Trustworthy Computing, $41,769 (09/2009 - 08/2011)
12. PI, *"NSF Support for the 2009 New Security Paradigms Workshop Financial Aid"*, NSF Trustworthy Computing, **$10,000** (09/2009 - 08/2010)
13. PI, *"Measuring the Health of Internet Routing: A Longitudinal Study"*, Google (research gift), **$60,000** (07/2009)
14. PI, *"CSR: Small: An Information Accountability Architecture for Distributed Enterprise Systems"*, NSF Trustworthy Computing, CNS-09-14312, **$450,000** (07/2009 - 06/2012)
15. co-PI (with Jason Nieh), *"TC: Small: Exploiting Software Elasticity for Automatic Software Self-Healing"*, NSF Trustworthy Computing, CNS-09-14845, **$450,000** (07/2009 - 06/2012)
16. co-PI (with Steve Bellovin and Sal Stolfo), *"Pro-actively Removing the Botnet Threat"*, Office of Naval Research (ONR), **$294,625** (04/2009 - 09/2010)
17. co-PI (with Simha Sethumadhavan and Sal Stolfo), *"SCOPS: Secure Cyber Operations and Parallelization Studies Cluster"*, Air Force Office for Scientific Research (AFOSR), **$650,000** (04/15/2009 - 04/14/2010)
18. PI (co-PIs: Sal Stolfo), *"Program Whitelisting, Vulnerability Analytics and Risk Assessment"*, Symantec (research gift), **$65,000** (12/2008)
19. co-PI (with Sal Stolfo), *"Automated Creation of Network and Content Traffic For the National Cyber Range"*, DARPA/STO, **$85,000** (01/01/2009 - 06/30/2011; part of a larger project)
20. co-PI (with Steve Bellovin, Tal Malkin, and Sal Stolfo), *"Secure Encrypted Search"*, IARPA, $648,787 (09/2008 - 02/2010)
21. PI, *"Tracking Sensitive Information Flows in Modern Enterprises"*, Intel (research gift), $64,000 (05/2008)
22. PI, *"Privacy and Search: Having it Both Ways in Web Services"*, Google (research gift), $50,000 (03/2008)
23. PI (co-PI: Sal Stolfo), *"Continuation: Safe Browsing Through Web-based Application Communities"*, Google (research gift), **$50,000** (03/2008)
24. co-PI (with Steve Bellovin, Vishal Misra, Henning Schulzrinne, Dan Rubenstein, Nick Maxemchuck), *"Zero Outage Dynamic Intrinsically Assurable Communities (ZODIAC)"*, DARPA/STO, **$835,357** (11/2007 - 05/2009; part of a larger project with Telcordia, Sparta, GMU, and the University of Pennsylvania)

25. PI, *"Travel Supplement under the US/Japan Critical Infrastructure Protection Cooperation Program"*, NSF CyberTrust, **$38,640** (09/2007 - 08/2009)
26. PI, *"PacketSpread: Practical Network Capabilities"*, NSF CyberTrust, CNS-07-14277, **$280,000** (09/2007 - 08/2010)
27. PI, *"Integrated Enterprise Security Management"*, NSF CyberTrust, CNS-07-14647, **$286,486** (08/2007 - 07/2009)
28. PI, *"Safe Browsing Through Web-based Application Communities"*, NY State/Polytechnic CAT, **$25,000** (06/2007 - 06/2009)
29. PI, *"MURI: Foundational and Systems Support for Quantitative Trust Management"*, Office of Naval Research (ONR), **$750,000** (05/2007 - 04/2012; part of a larger project with the University of Pennsylvania and Georgia Institute of Technology)
30. PI (co-PIs: Jason Nieh, Sal Stolfo), *"MURI: Autonomic Recovery of Enterprise-Wide Systems After Attack or Failure with Forward Correction"*, Air Force Office of Scientific Research (AFOSR), **$1,368,000** (05/2007 - 04/2012; part of a larger project with GMU and Penn State University)
31. co-PI (with Sal Stolfo), *"Human Behavior, Insider Threat, and Awareness"*, DHS/I3P, **$616,442** (04/2007 - 03/2009)
32. PI (co-PI: Sal Stolfo), *"Safe Browsing Through Web-based Application Communities"*, Google (research gift), **$50,000** (01/2007)
33. PI (co-PI: Sal Stolfo), *"Supplement to Behavior-based Access Control and Communication in MANETs grant"*, DARPA/IPTO and NRO, **$96,627** (09/2006 - 07/2007)
34. PI, *"Secure Overlay Services"*, NY State/Polytechnic CAT, **$10,000** (09/2006 - 06/2007)
35. PI (co-PIs: Gail Kaiser, Sal Stolfo), *"Enabling Collaborative Self-healing Software Systems"*, NSF CyberTrust, CNS-06-27473, $800,000 (09/2006 - 08/2010)
36. PI (co-PI: Sal Stolfo), *"Behavior-based Access Control and Communication in MANETs"*, DARPA/IPTO, **$100,000** (07/2006 - 06/2007)
37. co-PI (with Steve Bellovin and Sal Stolfo), *"Large-Scale System Defense"*, DTO, **$535,555** (07/2006 - 12/2007)
38. PI, *"Active Decoys for Spyware"*, NY State/Polytechnic CAT, **$25,000** (06/2006 - 12/2007)
39. PI, *"Retrofitting A Flow-oriented Paradigm in Commodity Operating Systems for High-Performance Computing"*, NSF CPA, CCF-05-41093, **$378,091** (01/2006 - 12/2008)
40. co-PI (with Jason Nieh, Gail Kaiser), *"Broadening Participation in Research"*, NSF BPC, **$133,565** (09/2005 - 08/2006)
41. PI, *"Secure Overlay Services"*, NY State/Polytechnic CAT, **$12,500** (09/2005 - 06/2006)
42. co-PI (with Dan Rubenstein, Vishal Misra), *"Secure Overlay Services"*, Intel Corp. (research gift), **$75,000** (08/2005)
43. PI, *"Snakeyes"*, New York State Center for Advanced Technology, **$14,999** (07/2005 - 06/2006)
44. PI, *"Self-protecting Software"*, Columbia Science and Technology Ventures (research gift), $65,000 (06/2005 - 09/2005)
45. co-PI (with Gail Kaiser), *"Trustworthy Computing Curriculum Development"*, Microsoft Research (research gift), **$50,000** (12/2004 - 12/2005)
46. co-PI (with Jason Nieh, Gail Kaiser), *"Secure Remote Computing Services"*, NSF ITR, CNS-04-26623, $1,200,000 (09/2004 - 08/2009)

47. PI, *"Secure Overlay Services"*, NY State/Polytechnic CAT, **$12,500** (09/2004 - 06/2005)
48. co-PI (with Dan Rubenstein, Vishal Misra), *"Secure Overlay Services"*, Intel Corp. (research gift), **$90,000** (06/2004)
49. co-PI (with Dan Rubenstein, Vishal Misra), *"Secure Overlay Services"*, Intel Corp. (research gift), **$120,000** (08/2003)
50. PI (co-PIs: Dan Rubenstein, Vishal Misra), *"Secure Overlay Services"*, Cisco Corp. (research gift), **$76,000** (07/2003)
51. co-PI (with Sal Stolfo, Tal Malkin, Vishal Misra), *"Distributed Intrusion Detection Feasibility Study"*, Department of Defense, **$300,000** (03/2003 - 03/2004)
52. PI, *"STRONGMAN"*, DARPA/ATO, **$23,782** (09/2002 - 08/2003; part of a larger project with the University of Pennsylvania)
53. PI, *"POSSE"*, DARPA/ATO, $16,341 (09/2002 - 08/2003; part of a larger project with the University of Pennsylvania)
54. PI, *"GRIDLOCK"*, NSF Trusted Computing, CCR-TC-02-08972, **$207,000** (07/2002 - 06/2005; part of a larger project with the University of Pennsylvania and Yale University)
55. PI (co-PIs: Dan Rubenstein, Vishal Misra), *"Secure Overlay Services"*, Cisco Corp. (research gift), **$70,000** (07/2002)
56. PI (co-PIs: Dan Rubenstein, Vishal Misra), *"Secure Overlay Services"*, DARPA/ATO, **$695,000** (06/2002 - 05/2004)
57. PI, *"Code Security Analysis Kit (CoSAK)"*, DARPA/ATO, **$37,000** (07/2001 - 06/2003; part of a larger project with Drexel University)

- **Total:** $34,240,062
- **Total as PI:** $20,625,555

Select Invited Talks

- *"Collaborative, Adaptive Software Defense"*, invited talk, ONR Workshop on Host Computer Security, Chicago, IL, October 2010.
- *"Using Decoys to Identify Malicious Insiders"*, invited talk, Computer Science Department, National University of Singapore, Singapore, August 2010.
- *"Behavior-based Access Control in Wired and Wireless Networks"*, invited talk, 5th Ph.D. School on Security in Wireless Networking (SWING), Bertinoro, Italy, June/July 2010.
- *"MANET Security: Background and Distributed Defense"*, invited talk, 5th Ph.D. School on Security in Wireless Networking (SWING), Bertinoro, Italy, June/July 2010.
- *"Detecting Insider Attackers"*, invited talk, 5th Ph.D. School on Security in Wireless Networking (SWING), Bertinoro, Italy, June/July 2010.
- *"Self-healing and Collaborative Software Defenses"*, invited talk, 5th Ph.D. School on Security in Wireless Networking (SWING), Bertinoro, Italy, June/July 2010.
- *"Voice over IP: Risks, Threats, and Vulnerabilities"*, invited talk, 5th Ph.D. School on Security in Wireless Networking (SWING), Bertinoro, Italy, June/July 2010.
- *"Determining Device Trustworthiness in Heterogeneous Environments"*, invited talk, Intel Workshop on Trust Evidence and End-to-end Trust in Heterogeneous Environments, Santa Clara, CA, May 2010.

- *"Moving Code: Instruction Set Randomization"*, invited talk, IC Technical Exchange on Moving Target, Washington, DC, April 2010.
- *"Voice over IP: Risks, Threats and Vulnerabilities"*, invited talk, AT&T Labs Research, Florham Park, NJ, April 2010.
- *"Voice over IP: Risks, Threats and Vulnerabilities"*, keynote talk, 5th International Conference on Information Systems Security (ICISS), Kolkata, India, December 2009.
- *"Voice over IP: Risks, Threats and Vulnerabilities"*, Cyber Infrastructure Protection (CIP) Conference, New York, June 2009.
- *"Voice over IP: Risks, Threats and Vulnerabilities"*, keynote talk, Applied Cryptography and Network Security (ACNS) Conference, Paris, France, June 2009.
- *"Automatic Software Self-Healing: Present and Future"*, keynote talk, European Workshop on Systems Security (EuroSec), Nuremberg, Germany, March 2009.
- *"VAMPIRE Project Overview"*, Symantec Research Labs, Culver City, CA, March 2009.
- *"Survey of IMS/VoIP Security Work"*, Agence Nationale de Reserche (ANR), Paris, France, February 2009.
- *"Simulating a Global Passive Adversary for Attacking Tor-like Anonymity Systems"*, National Institute for Advanced Industrial Science and Technology (AIST), Japan, November 2008.
- *"Denial of Service Attacks and Resilient Overlay Networks"*, ENISA-FORTH Summer School on Network & Information Security, Heraklion, Greece, September 2008.
- *"von Neumann and the Current Computer Security Landscape"*, Onassis Foundation Lectures in Science, Heraklion, Greece, July 2008.
- *"Simulating a Global Passive Adversary for Attacking Tor-like Anonymity Systems"*, Institute of Computer Science/FORTH, Heraklion, Greece, July 2008.
- *"Race to the bottom: Malicious Hardware"*, 1st FORWARD Invitational Workshop for Identifying Emerging Threats in Information and Communication Technology Infrastructures, Goteborg, Sweden, April 2008.

Publications

(Student co-authors are underlined.)

Patents

1. *"Microbilling using a trust management system"*
   Matthew A. Blaze, John Ioannidis, and Angelos D. Keromytis. U.S. Patent Number 7,996,325. Issued on August 9th 2011.
2. *"Methods, systems and media for software self-healing"*
   Michael E. Locasto, Angelos D. Keromytis, Salvatore J. Stolfo, Angelos Stavrou, Gabriela Cretu, Stylianos Sidiroglou, Jason Nieh, and Oren Laadan. U.S. Patent Number 7,962,798. Issued on June 14th, 2011.
3. *"Systems and methods for detecting and inhibiting attacks using honeypots"*
   Stylianos Sidiroglou, Angelos D. Keromytis, and Kostas G. Anagnostakis. U.S. Patent Number 7,904,959. Issued on March 8th, 2011.
4. *"Systems and methods for correlating and distributing intrusion alert information among collaborating computer systems"*

Salvatore J. Stolfo, Angelos D. Keromytis, Vishal Misra, Michael Locasto, and Janak Parekh. U.S. Patent Number 7,784,097. Issued on August 24th, 2010.

5. *"Systems and methods for correlating and distributing intrusion alert information among collaborating computer systems"*
   Salvatore J. Stolfo, Tal Malkin, Angelos D. Keromytis, Vishal Misra, Michael Locasto, and Janak Parekh. U.S. Patent Number 7,779,463. Issued on August 17th, 2010.
6. *"Systems and methods for computing data transmission characteristics of a network path based on single-ended measurements"*
   Angelos D. Keromytis, Sambuddho Chakravarty, and Angelos Stavrou. U.S. Patent Number 7,660,261. Issued on February 9th, 2010.
7. *"Microbilling using a trust management system"*
   Matthew A. Blaze, John Ioannidis, and Angelos D. Keromytis. U.S. Patent Number 7,650,313. Issued on January 19th 2010.
8. *"Methods and systems for repairing applications"*
   Angelos D. Keromytis, Michael E. Locasto, and Stylianos Sidiroglou. U.S. Patent Number 7,490,268. Issued on February 10th 2009.
9. *"System and method for microbilling using a trust management system"*
   Matthew A. Blaze, John Ioannidis, and Angelos D. Keromytis. U.S. Patent Number 6,789,068. Issued on September 7th 2004.
10. *"Secure and reliable bootstrap architecture"*
    William A. Arbaugh, David J. Farber, Angelos D. Keromytis, and Jonathan M. Smith. U.S. Patent Number 6,185,678. Issued on February 6th 2001.

Journal Publications

1. *"A Comprehensive Survey of Voice over IP Security Research"*
   Angelos D. Keromytis. To appear in the *IEEE Communications Surveys and Tutorials.*
2. *"A System for Generating and Injecting Indistinguishable Network Decoys"*
   Brian M. Bowen, Vasileios P. Kemerlis, Pratap Prabhu, Angelos D. Keromytis, and Salvatore J. Stolfo. To appear in the *Journal of Computer Security (JCS).*
3. *"The Efficient Dual Receiver Cryptosystem and Its Applications"*
   Ted Diament, Homin K. Lee, Angelos D. Keromytis, and Moti Yung. In *International Journal of Network Security (IJNS),* vol 13, no. 3, pp. 135 - 151, November 2011.
4. *"On the Infeasibility of Modeling Polymorphic Shellcode: Re-thinking the Role of Learning in Intrusion Detection Systems"*
   Yingbo Song, Michael E. Locasto, Angelos Stavrou, Angelos D. Keromytis, and Salvatore J. Stolfo. In *Machine Learning Journal (MLJ),* vol. 81, no. 2, pp. 179 - 205, November 2010.
5. *"On The General Applicability of Instruction-Set Randomization"*
   Stephen W. Boyd, Gaurav S. Kc, Michael E. Locasto, Angelos D. Keromytis, and Vassilis Prevelakis. In *IEEE Transactions on Dependable and Secure Computing (TDSC),* vol. 7, no. 3, pp. 255 - 270, July - September 2010.
6. *"Shadow Honeypots"*
   Michalis Polychronakis, Periklis Akritidis, Stelios Sidiroglou, Kostas G. Anagnostakis, Angelos D. Keromytis, and Evangelos Markatos. In *International Journal of Computer and Network Security (IJCNS),* vol. 2, no. 9, pp. 1 - 15, September 2010.
7. *"Ethics in Security Vulnerability Research"*

Andrea M. Matwyshyn, Ang Cui, Salvatore J. Stolfo, and Angelos D. Keromytis. In *IEEE Security & Privacy Magazine,* vol. 8, no. 2, pp. 67 - 72, March/April 2010.

8. *"Voice over IP Security: Research and Practice"*
   Angelos D. Keromytis. In *IEEE Security & Privacy Magazine,* vol. 8, no. 2, pp. 76 - 78, March/April 2010.
9. *"A Market-based Bandwidth Charging Framework"*
   David Michael Turner, Vassilis Prevelakis, and Angelos D. Keromytis. In *ACM Transactions on Internet Technology (ToIT),* vol. 10, no. 1, pp. 1 - 30, February 2010.
10. *"A Look at VoIP Vulnerabilities"*
    Angelos D. Keromytis. In *USENIX ;login: Magazine,* vol. 35, no. 1, pp. 41 - 50, February 2010.
11. *"Designing Host and Network Sensors to Mitigate the Insider Threat"*
    Brian M. Bowen, Malek Ben Salem, Shlomo Hershkop, Angelos D. Keromytis, and Salvatore J. Stolfo. In *IEEE Security & Privacy Magazine,* vol. 7, no. 6, pp. 22 - 29, November/December 2009.
12. *"Elastic Block Ciphers: Method, Security and Instantiations"*
    Debra L. Cook, Moti Yung, and Angelos D. Keromytis. In *Springer International Journal of Information Security (IJIS),* vol 8, no. 3, pp. 211 - 231, June 2009.
13. *"On the Deployment of Dynamic Taint Analysis for Application Communities"*
    Hyung Chan Kim and Angelos D. Keromytis. In *IEICE Transactions,* vol. E92-D, no. 3, pp. 548 - 551, March 2009.
14. *"Dynamic Trust Management"*
    Matt Blaze, Sampath Kannan, Insup Lee, Oleg Sokolsky, Jonathan M. Smith, Angelos D. Keromytis, and Wenke Lee. In *IEEE Computer Magazine,* vol. 42, no. 2, pp. 44 - 52, February 2009.
15. *"Randomized Instruction Sets and Runtime Environments: Past Research and Future Directions"*
    Angelos D. Keromytis. In *IEEE Security & Privacy Magazine,* vol. 7, no. 1, pp. 18 - 25, January/February 2009.
16. *"Anonymity in Wireless Broadcast Networks"*
    Matt Blaze, John Ioannidis, Angelos D. Keromytis, Tal Malkin, and Avi Rubin. In *International Journal of Network Security (IJNS),* vol. 8, no. 1, pp. 37 - 51, January 2009.
17. *"Decentralized Access Control in Networked File Systems"*
    Stefan Miltchev, Jonathan M. Smith, Vassilis Prevelakis, Angelos D. Keromytis, and Sotiris Ioannidis. In *ACM Computing Surveys,* vol. 40, no. 3, pp. 10:1 - 10:30, August 2008.
18. *"Robust Reactions to Potential Day-Zero Worms through Cooperation and Validation"*
    Kostas G. Anagnostakis, Michael Greenwald, Sotiris Ioannidis, and Angelos D. Keromytis. In *Springer International Journal of Information Security (IJIS), ISC 2006 Special Issue,* vol.6, no. 6, pp. 361 - 378, October 2007. (Extended version of the ISC 2006 paper.)
19. *"Requirements for Scalable Access Control and Security Management Architectures"*
    Angelos D. Keromytis and Jonathan M. Smith. In *ACM Transactions on Internet Technology (ToIT),* vol. 7, no. 2, pp. 1 - 22, May 2007.
20. *"Virtual Private Services: Coordinated Policy Enforcement for Distributed Applications"*
    Sotiris Ioannidis, Steven M. Bellovin, John Ioannidis, Angelos D. Keromytis, Kostas G.

Anagnostakis, and Jonathan M. Smith. In *International Journal of Network Security (IJNS)*, vol. 4, no. 1, pp. 69 - 80, January 2007.

21. *"Countering DDoS Attacks with Multi-path Overlay Networks"*
Angelos Stavrou and Angelos D. Keromytis. In *Information Assurance Technology Analysis Center (IATAC) Information Assurance Newsletter (IAnewsletter)*, vol. 9, no. 3, pp. 26 - 30, Winter 2006. *(Invited paper, based on the CCS 2005 paper.)*
22. *"Conversion Functions for Symmetric Key Ciphers"*
Debra L. Cook and Angelos D. Keromytis. In *Journal of Information Assurance and Security (JIAS)*, vol. 1, no. 2, pp. 119 - 128, June 2006. *(Extended version of the IAS 2005 paper.)*
23. *"Execution Transactions for Defending Against Software Failures: Use and Evaluation"*
Stelios Sidiroglou and Angelos D. Keromytis. In *Springer International Journal of Information Security (IJIS)*, vol. 5, no. 2, pp. 77 - 91, April 2006. *(Extended version of the ISC 2005 paper.)*
24. *"Worm Propagation Strategies in an IPv6 Internet"*
Steven M. Bellovin, Bill Cheswick, and Angelos D. Keromytis. In *USENIX ;login*, vol. 31, no. 1, pp. 70 - 76, February 2006.
25. *"Cryptography As An Operating System Service: A Case Study"*
Angelos D. Keromytis, Theo de Raadt, Jason Wright, and Matthew Burnside. In *ACM Transactions on Computer Systems (ToCS)*, vol. 24, no. 1, pp. 1 - 38, February 2006. *(Extended version of USENIX Technical 2003 paper.)*
26. *"Countering Network Worms Through Automatic Patch Generation"*
Stelios Sidiroglou and Angelos D. Keromytis. In *IEEE Security & Privacy*, vol. 3, no. 6, pp. 41 - 49, November/December 2005.
27. *"WebSOS: An Overlay-based System For Protecting Web Servers From Denial of Service Attacks"*
Angelos Stavrou, Debra L. Cook, William G. Morein, Angelos D. Keromytis, Vishal Misra, and Dan Rubenstein. In *Elsevier Journal of Computer Networks, special issue on Web and Network Security*, vol. 48, no. 5, pp. 781 - 807, August 2005. *(Extended version of the CCS 2003 paper.)*
28. *"Hardware Support For Self-Healing Software Services"*
Stelios Sidiroglou, Michael E. Locasto, and Angelos D. Keromytis. In *ACM SIGARCH Computer Architecture News, Special Issue on Workshop on Architectural Support for Security and Anti-Virus (WASSA)*, vol. 33, no. 1, pp. 42 - 47, March 2005. Also appeared in the Proceedings of the *Workshop on Architectural Support for Security and Anti-Virus (WASSA)*, held in conjunction with the *11th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS-XI)*, pp. 37 - 43. October 2004, Boston, MA.
29. *"The Case For Crypto Protocol Awareness Inside The OS Kernel"*
Matthew Burnside and Angelos D. Keromytis. In *ACM SIGARCH Computer Architecture News, Special Issue on Workshop on Architectural Support for Security and Anti-Virus (WASSA)*, vol. 33, no. 1, pp. 58 - 64, March 2005. Also appeared in the Proceedings of the *Workshop on Architectural Support for Security and Anti-Virus (WASSA)*, held in conjunction with the *11th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS-XI)*, pp. 54 - 60. October 2004, Boston, MA.

30. *"Patch-on-Demand Saves Even More Time?"*
Angelos D. Keromytis. In *IEEE Computer*, vol. 37, no. 8, pp. 94 - 96, August 2004.
31. *"Just Fast Keying: Key Agreement In A Hostile Internet"*
William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, and Omer Reingold. In *ACM Transactions on Information and System Security (TISSEC)*, vol. 7, no. 2, pp. 1 - 32, May 2004. *(Extended version of the CCS 2002 paper.)*
32. *"SOS: An Architecture for Mitigating DDoS Attacks"*
Angelos D. Keromytis, Vishal Misra, and Dan Rubenstein. In *IEEE Journal on Selected Areas in Communications (JSAC), special issue on Recent Advances in Service Overlay Networks*, vol. 22, no. 1, pp. 176 - 188, January 2004. *(Extended version of the SIGCOMM 2002 paper.)*
33. *"A Secure PLAN"*
Michael Hicks, Angelos D. Keromytis, and Jonathan M. Smith. In *IEEE Transactions on Systems, Man, and Cybernetics (T-SMC) Part C: Applications and Reviews, Special issue on technologies promoting computational intelligence, openness and programmability in networks and Internet services: Part I*, vol. 33, no. 3, pp. 413 - 426, August 2003. *(Extended version of the DANCE 2002 paper.)*
34. *"Drop-in Security for Distributed and Portable Computing Elements"*
Vassilis Prevelakis and Angelos D. Keromytis. In MCB Press *Emerald Journal of Internet Research: Electronic Networking, Applications and Policy*, vol. 13, no. 2, pp. 107 - 115, 2003. *(Extended version of the INC 2002 paper.)*
35. *"Trust Management for IPsec"*
Matt Blaze, John Ioannidis, and Angelos D. Keromytis. In *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 2, pp. 1 - 24, May 2002. *(Extended version of the NDSS 2001 paper.)*
36. *"The Price of Safety in an Active Network"*
D. Scott Alexander, Paul B. Menage, Angelos D. Keromytis, William A. Arbaugh, Kostas G. Anagnostakis, and Jonathan M. Smith. In *Journal of Communications and Networks (JCN), special issue on programmable switches and routers*, vol. 3, no. 1, pp. 4 - 18, March 2001. Older versions are available as *University of Pennsylvania Technical Report MS-CIS-99-04* and *University of Pennsylvania Technical Report MS-CIS-98-02.*
37. *"Secure Quality of Service Handling (SQoSH)"*
D. Scott Alexander, William A. Arbaugh, Angelos D. Keromytis, Steve Muir, and Jonathan M. Smith. In *IEEE Communications Magazine*, vol. 38, no. 4, pp. 106 - 112, April 2000. An older version is available as *University of Pennsylvania Technical Report MS-CIS-99-05.*
38. *"Safety and Security of Programmable Network Infrastructures"*
D. Scott Alexander, William A. Arbaugh, Angelos D. Keromytis, and Jonathan M. Smith. In *IEEE Communications Magazine, issue on Programmable Networks*, vol. 36, no. 10, pp. 84 - 92, October 1998.
39. *"A Secure Active Network Environment Architecture"*
D. Scott Alexander, William A. Arbaugh, Angelos D. Keromytis, and Jonathan M. Smith. In *IEEE Network Magazine, special issue on Active and Controllable Networks*, vol. 12, no. 3, pp. 37 - 45, May/June 1998.
40. *"The SwitchWare Active Network Architecture"*

D. Scott Alexander, William A. Arbaugh, Michael Hicks, Pankaj Kakkar, Angelos D. Keromytis, Jonathan T. Moore, Carl A. Gunter, Scott M. Nettles, and Jonathan M. Smith. In *IEEE Network Magazine, special issue on Active and Programmable Networks,* vol. 12, no. 3, pp. 29 - 36, May/June 1998.

Peer-Reviewed Conference Proceedings

1. *"A Multilayer Overlay Network Architecture for Enhancing IP Services Availability Against DoS"*
   Dimitris Geneiatakis, Georgios Portokalidis, and Angelos D. Keromytis. To appear in the Proceedings of the *7th International Conference on Information Systems Security (ICISS).* December 2011, Kolkata, India. *(Acceptance rate: 22.8%)*
2. *"ROP Payload Detection Using Speculative Code Execution"*
   Michalis Polychronakis and Angelos D. Keromytis. To appear in the Proceedings of the *6th International Conference on Malicious and Unwanted Software (MALWARE).* October 2011, Fajardo, PR.
3. *"Detecting Traffic Snooping in Tor Using Decoys"*
   Sambuddho Chakravarty, Georgios Portokalidis, Michalis Polychronakis, and Angelos D. Keromytis. To appear in Proceedings of the *14th International Symposium on Recent Advances in Intrusion Detection (RAID).* September 2011, Menlo Park, CA. *(Acceptance rate: 23%)*
4. *"Measuring the Deployment Hiccups of DNSSEC"*
   Vasilis Pappas and Angelos D. Keromytis. In Proceedings of the *International Conference on Advances in Computing and Communications (ACC), Part III,* pp. 44 - 54. July 2011, Kochi, India. *(Acceptance rate: 39%)*
5. *"Misuse Detection in Consent-based Networks"*
   Mansoor Alicherry and Angelos D. Keromytis. In Proceedings of the *9th International Conference on Applied Cryptography and Network Security (ACNS),* pp. 38 - 56. June 2011, Malaga, Spain. *(Acceptance rate: 18%)*
6. *"Retrofitting Security in COTS Software with Binary Rewriting"*
   Padraig O'Sullivan, Kapil Anand, Aparna Kothan, Matthew Smithson, Rajeev Barua, and Angelos D. Keromytis. In Proceedings of the *26th IFIP International Information Security Conference (SEC),* pp. 154 - 172. June 2011, Lucerne, Switzerland. *(Acceptance rate: 24%)*
7. *"Fast and Practical Instruction-Set Randomization for Commodity Systems"*
   Georgios Portokalidis and Angelos D. Keromytis. In Proceedings of the *26th Annual Computer Security Applications Conference (ACSAC),* pp. 41 - 48. December 2010, Austin, TX. *(Acceptance rate: 17%)*
8. *"An Adversarial Evaluation of Network Signaling and Control Mechanisms"*
   Kangkook Jee, Stelios Sidiroglou-Douskos, Angelos Stavrou, and Angelos D. Keromytis. In Proceedings of the *13th International Conference on Information Security and Cryptology (ICISC).* December 2010, Seoul, Korea.
9. *"Evaluation of a Spyware Detection System using Thin Client Computing"*
   Vasilis Pappas, Brian M. Bowen, and Angelos D. Keromytis. In Proceedings of the *13th International Conference on Information Security and Cryptology (ICISC),* pp. 222 - 232. December 2010, Seoul, Korea.
10. *"Crimeware Swindling without Virtual Machines"*

Vasilis Pappas, Brian M. Bowen, and Angelos D. Keromytis. In Proceedings of the *13th Information Security Conference (ISC)*, pp. 196 - 202. October 2010, Boca Raton, FL. *(Acceptance rate: 27.6%)*

11. *"iLeak: A Lightweight System for Detecting Inadvertent Information Leaks"*
Vasileios P. Kemerlis, Vasilis Pappas, Georgios Portokalidis, and Angelos D. Keromytis. In Proceedings of the *6th European Conference on Computer Network Defense (EC2ND)*, pp. 21 - 28. October 2010, Berlin, Germany.
12. *"Traffic Analysis Against Low-Latency Anonymity Networks Using Available Bandwidth Estimation"*
Sambuddho Chakravarty, Angelos Stavrou, and Angelos D. Keromytis. In Proceedings of the *15th European Symposium on Research in Computer Security (ESORICS)*, pp. 249 - 267. September 2010, Athens, Greece. *(Acceptance rate: 20%)*
13. *"BotSwindler: Tamper Resistant Injection of Believable Decoys in VM-Based Hosts for Crimeware Detection"*
Brian M. Bowen, Pratap Prabhu, Vasileios P. Kemerlis, Stelios Sidiroglou, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *13th International Symposium on Recent Advances in Intrusion Detection (RAID)*, pp. 118 - 137. September 2010, Ottawa, Canada. *(Acceptance rate: 23.5%)*
14. *"An Analysis of Rogue AV Campaigns"*
Marco Cova, Corrado Leita, Olivier Thonnard, Angelos D. Keromytis, and Marc Dacier. In Proceedings of the *13th International Symposium on Recent Advances in Intrusion Detection (RAID)*, pp. 442 - 463. September 2010, Ottawa, Canada. *(Acceptance rate: 23.5%)*
15. *"DIPLOMA: Distributed Policy Enforcement Architecture for MANETs"*
Mansoor Alicherry and Angelos D. Keromytis. In Proceedings of the *4th International Conference on Network and System Security (NSS)*, pp. 89 - 98. September 2010, Melbourne, Australia. *(Acceptance rate: 26%)*
16. *"Automating the Injection of Believable Decoys to Detect Snooping" (Short Paper)*
Brian M. Bowen, Vasileios Kemerlis, Pratap Prabhu, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *3rd ACM Conference on Wireless Network Security (WiSec)*, pp. 81 - 86. March 2010, Hoboken, NJ. *(Acceptance rate: 21%)*
17. *"BARTER: Behavior Profile Exchange for Behavior-Based Admission and Access Control in MANETs"*
Vanessa Frias-Martinez, Salvatore J. Stolfo, and Angelos D. Keromytis. In Proceedings of the *5th International Conference on Information Systems Security (ICISS)*, pp. 193 - 207. December 2009, Kolkata, India. *(Acceptance rate: 19.8%)*
18. *"A Survey of Voice Over IP Security Research"*
Angelos D. Keromytis. In Proceedings of the *5th International Conference on Information Systems Security (ICISS)*, pp. 1 - 17. December 2009, Kolkata, India. *(Invited paper)*
19. *"A Network Access Control Mechanism Based on Behavior Profiles"*
Vanessa Frias-Martinez, Joseph Sherrick, Salvatore J. Stolfo, and Angelos D. Keromytis. In Proceedings of the *25th Annual Computer Security Applications Conference (ACSAC)*, pp. 3 - 12. December 2009, Honolulu, HI. *(Acceptance rate: 20%)*
20. *"Gone Rogue: An Analysis of Rogue Security Software Campaigns"*
Marco Cova, Corrado Leita, Olivier Thonnard, Angelos D. Keromytis, and Marc Dacier. In Proceedings of the *5th European Conference on Computer Network Defense (EC2ND)*,

pp. 1 - 3. November 2009, Milan, Italy. *(Invited paper)*

21. *"Baiting Inside Attackers Using Decoy Documents"*
Brian M. Bowen, Shlomo Hershkop, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *5th International ICST Conference on Security and Privacy in Communication Networks (SecureComm)*, pp. 51 - 70. September 2009, Athens, Greece. *(Acceptance rate: 25.3%)*
22. *"Deny-by-Default Distributed Security Policy Enforcement in Mobile Ad Hoc Networks (Short Paper)"*
Mansoor Alicherry, Angelos D. Keromytis, and Angelos Stavrou. In Proceedings of the *5th International ICST Conference on Security and Privacy in Communication Networks (SecureComm)*, pp. 41 - 50. September 2009, Athens, Greece. *(Acceptance rate: 34.7%)*
23. *"Adding Trust to P2P Distribution of Paid Content"*
Alex Sherman, Angelos Stavrou, Jason Nieh, Angelos D. Keromytis, and Clifford Stein. In Proceedings of the *12th Information Security Conference (ISC)*, pp. 459 - 474. September 2009, Pisa, Italy. *(Acceptance rate: 27.6%)*
24. *"A2M: Access-Assured Mobile Desktop Computing"*
Angelos Stavrou, Ricardo A. Baratto, Angelos D. Keromytis, and Jason Nieh. In Proceedings of the *12th Information Security Conference (ISC)*, pp. 186 - 201. September 2009, Pisa, Italy. *(Acceptance rate: 27.6%)*
25. *"F3ildCrypt: End-to-End Protection of Sensitive Information in Web Services"*
Matthew Burnside and Angelos D. Keromytis. In Proceedings of the *12th Information Security Conference (ISC)*, pp. 491 - 506. September 2009, Pisa, Italy. *(Acceptance rate: 27.6%)*
26. *"DoubleCheck: Multi-path Verification Against Man-in-the-Middle Attacks"*
Mansoor Alicherry and Angelos D. Keromytis. In Proceedings of the *IEEE Symposium on Computers and Communications (ISCC)*, pp. 557 - 563. July 2009, Sousse, Tunisia. *(Acceptance rate: 36%)*
27. *"Voice over IP: Risks, Threats and Vulnerabilities"*
Angelos D. Keromytis. In Proceedings (electronic) of the *Cyber Infrastructure Protection (CIP) Conference*. June 2009, New York, NY. *(Invited paper)*
28. *"Capturing Information Flow with Concatenated Dynamic Taint Analysis"*
Hyung Chan Kim, Angelos D. Keromytis, Michael Covington, and Ravi Sahita. In Proceedings of the *4th International Conference on Availability, Reliability and Security (ARES)*, pp. 355 - 362. March 2009, Fukuoka, Japan. *(Acceptance rate: 25%)*
29. *"ASSURE: Automatic Software Self-healing Using REscue points"*
Stelios Sidiroglou, Oren Laadan, Nico Viennot, Carlos-René Pérez, Angelos D. Keromytis, and Jason Nieh. In Proceedings of the *14th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, pp. 37 - 48. March 2009, Washington, DC. *(Acceptance rate: 25.6%)*
30. *"Spectrogram: A Mixture-of-Markov-Chains Model for Anomaly Detection in Web Traffic"*
Yingbo Song, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *16th Internet Society (ISOC) Symposium on Network and Distributed Systems Security (SNDSS)*, pp. 121 - 135. February 2009, San Diego, CA. *(Acceptance rate: 11.7%)*
31. *"Constructing Variable-Length PRPs and SPRPs from Fixed-Length PRPs"*
Debra L. Cook, Moti Yung, and Angelos D. Keromytis. In Proceedings of the *4th*

International Conference on Information Security and Cryptology (Inscrypt), pp. 157 - 180. December 2008, Beijing, China. *(Acceptance rate: 17.5%)*

32. *"Behavior-Profile Clustering for False Alert Reduction in Anomaly Detection Sensors"* Vanessa Frias-Martinez, Salvatore J. Stolfo, and Angelos D. Keromytis. In Proceedings of the *24th Annual Computer Security Applications Conference (ACSAC)*, pp. 367 - 376. December 2008, Anaheim, CA. *(Acceptance rate: 24.2%)*
33. *"Authentication on Untrusted Remote Hosts with Public-key Sudo"* Matthew Burnside, Mack Lu, and Angelos D. Keromytis. In Proceedings of the *22nd USENIX Large Installation Systems Administration (LISA) Conference*, pp. 103 - 107. November 2008, San Diego, CA.
34. *"Behavior-Based Network Access Control: A Proof-of-Concept"* Vanessa Frias-Martinez, Salvatore J. Stolfo, and Angelos D. Keromytis. In Proceedings of the *11th Information Security Conference (ISC)*, pp. 175 - 190. Taipei, Taiwan, September 2008. *(Acceptance rate: 23.9%)*
35. *"Path-based Access Control for Enterprise Networks"* Matthew Burnside and Angelos D. Keromytis. In Proceedings of the *11th Information Security Conference (ISC)*, pp. 191 - 203. Taipei, Taiwan, September 2008. *(Acceptance rate: 23.9%)*
36. *"Methods for Linear and Differential Cryptanalysis of Elastic Block Ciphers"* Debra L. Cook, Moti Yung, and Angelos D. Keromytis. In Proceedings of the *13th Australasian Conference on Information Security and Privacy (ACISP)*, pp. 187 - 202. July 2008, Wollongong, Australia.*(Acceptance rate: 29.7%)*
37. *"Pushback for Overlay Networks: Protecting against Malicious Insiders"* Angelos Stavrou, Michael E. Locasto, and Angelos D. Keromytis. In Proceedings of the *6th International Conference on Applied Cryptography and Network Security (ACNS)*, pp 39 - 54. June 2008, New York, NY. *(Acceptance rate: 22.9%)*
38. *"Casting out Demons: Sanitizing Training Data for Anomaly Sensors"* Gabriela F. Cretu, Angelos Stavrou, Michael E. Locasto, Salvatore J. Stolfo, and Angelos D. Keromytis. In Proceedings of the *IEEE Symposium on Security & Privacy*, pp. 81 - 95. May 2008, Oakland, CA. *(Acceptance rate: 11.2%)*
39. *"Taming the Devil: Techniques for Evaluating Anonymized Network Data"* Scott E. Coull, Charles V. Wright, Angelos D. Keromytis, Fabian Monrose, and Michael K. Reiter. In Proceedings of the *15th Internet Society (ISOC) Symposium on Network and Distributed Systems Security (SNDSS)*, pp. 125 - 135. February 2008, San Diego, CA. *(Acceptance rate: 17.8%)*
40. *"SSARES: Secure Searchable Automated Remote Email Storage"* Adam J. Aviv, Michael E. Locasto, Shaya Potter, and Angelos D. Keromytis. In Proceedings of the *23rd Annual Computer Security Applications Conference (ACSAC)*, pp. 129 - 138. December 2007, Miami Beach, FL. *(Acceptance rate: 22%)*
41. *"On the Infeasibility of Modeling Polymorphic Shellcode"* Yingbo Song, Michael E. Locasto, Angelos Stavrou, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *13th ACM Conference on Computer and Communications Security (CCS)*, pp. 541 - 551. October/November 2007, Alexandria, VA. *(Acceptance rate: 18.1%)*
42. *"Defending Against Next Generation Attacks Through Network/Endpoint Collaboration and Interaction"*

Spiros Antonatos, Michael E. Locasto, Stelios Sidiroglou, Angelos D. Keromytis, and Evangelos Markatos. In Proceedings of the *3rd European Conference on Computer Network Defense (EC2ND).* October 2007, Heraclion, Greece. *(Invited paper)*

43. *"Elastic Block Ciphers in Practice: Constructions and Modes of Encryption"* Debra L. Cook, Moti Yung, and Angelos D. Keromytis. In Proceedings of the *3rd European Conference on Computer Network Defense (EC2ND).* October 2007, Heraclion, Greece.
44. *"The Security of Elastic Block Ciphers Against Key-Recovery Attacks"* Debra L. Cook, Moti Yung, and Angelos D. Keromytis. In Proceedings of the *10th Information Security Conference (ISC),* pp. 89 - 103. Valparaiso, Chile, October 2007. *(Acceptance rate: 25%)*
45. *"Characterizing Self-healing Software Systems"* Angelos D. Keromytis. In Proceedings of the *4th International Conference on Mathematical Methods, Models and Architectures for Computer Networks Security (MMM-ACNS),* pp. 22 - 33. September 2007, St. Petersburg, Russia. *(Invited paper)*
46. *"A Study of Malcode-Bearing Documents"* Wei-Jen Li, Salvatore J. Stolfo, Angelos Stavrou, Elli Androulaki, and Angelos D. Keromytis. In Proceedings of the *4th GI International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA),* pp. 231 - 250. July 2007, Lucerne, Switzerland. *(Acceptance rate: 21%)*
47. *"From STEM to SEAD: Speculative Execution for Automated Defense"* Michael E. Locasto, Angelos Stavrou, Gabriela F. Cretu, and Angelos D. Keromytis. In Proceedings of the *USENIX Annual Technical Conference,* pp. 219 - 232. June 2007, Santa Clara, CA. *(Acceptance rate: 18.75%)*
48. *"Using Rescue Points to Navigate Software Recovery (Short Paper)"* Stelios Sidiroglou, Oren Laadan, Angelos D. Keromytis, and Jason Nieh. In Proceedings of the *IEEE Symposium on Security & Privacy,* pp. 273 - 278. May 2007, Oakland, CA. *(Acceptance rate: 8.3%)*
49. *"Mediated Overlay Services (MOSES): Network Security as a Composable Service"* Stelios Sidiroglou, Angelos Stavrou, and Angelos D. Keromytis. In Proceedings of the *IEEE Sarnoff Symposium.* May 2007, Princeton, NJ. *(Invited paper)*
50. *"Elastic Block Ciphers: The Basic Design"* Debra L. Cook, Moti Yung, and Angelos D. Keromytis. In Proceedings of the *2nd ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS),* pp. 350 - 355. March 2007, Singapore.
51. *"Robust Reactions to Potential Day-Zero Worms through Cooperation and Validation"* Kostas G. Anagnostakis, Michael B. Greenwald, Sotiris Ioannidis, and Angelos D. Keromytis. In Proceedings of the *9th Information Security Conference (ISC),* pp. 427 - 442. August/September 2006, Samos, Greece. *(Acceptance rate: 20.2%)*
52. *"Low Latency Anonymity with Mix Rings"* Matthew Burnside and Angelos D. Keromytis. In Proceedings of the *9th Information Security Conference (ISC),* pp. 32 - 45. August/September 2006, Samos, Greece. *(Acceptance rate: 20.2%)*
53. *"W3Bcrypt: Encryption as a Stylesheet"* Angelos Stavrou, Michael E. Locasto, and Angelos D. Keromytis. In Proceedings of the *4th International Conference on Applied Cryptography and Network Security (ACNS),* pp.

349 - 364. June 2006, Singapore.

54. *"Software Self-Healing Using Collaborative Application Communities"*
Michael E. Locasto, Stelios Sidiroglou, and Angelos D. Keromytis. In Proceedings of the *13th Internet Society (ISOC) Symposium on Network and Distributed Systems Security (SNDSS)*, pp. 95 - 106. February 2006, San Diego, CA. *(Acceptance rate: 13.6%)*

55. *"Remotely Keyed Cryptographics: Secure Remote Display Access Using (Mostly) Untrusted Hardware"*
Debra L. Cook, Ricardo A. Baratto, and Angelos D. Keromytis. In Proceedings of the *7th International Conference on Information and Communications Security (ICICS)*, pp. 363 - 375. December 2005, Beijing, China. *(Acceptance rate: 17.4%)*

56. *"e-NeXSh: Achieving an Effectively Non-Executable Stack and Heap via System-Call Policing"*
Gaurav S. Kc and Angelos D. Keromytis. In Proceedings of the *21st Annual Computer Security Applications Conference (ACSAC)*, pp. 259 - 273. December 2005, Tucson, AZ. *(Acceptance rate: 19.6%)*

57. *"Action Amplification: A New Approach To Scalable Administration"*
Kostas G. Anagnostakis and Angelos D. Keromytis. In Proceedings of the *13th IEEE International Conference on Networks (ICON)*, vol. 2, pp. 862 - 867. November 2005, Kuala Lumpur, Malaysia.

58. *"A Repeater Encryption Unit for IPv4 and IPv6"*
Norimitsu Nagashima and Angelos D. Keromytis. In Proceedings of the *13th IEEE International Conference on Networks (ICON)*, vol. 1, pp. 335 - 340. November 2005, Kuala Lumpur, Malaysia.

59. *"Countering DoS Attacks With Stateless Multipath Overlays"*
Angelos Stavrou and Angelos D. Keromytis. In Proceedings of the *12th ACM Conference on Computer and Communications Security (CCS)*, pp. 249 - 259. November 2005, Alexandria, VA. *(Acceptance rate: 15.2%)*

60. *"A Dynamic Mechanism for Recovering from Buffer Overflow Attacks"*
Stelios Sidiroglou, Giannis Giovanidis, and Angelos D. Keromytis. In Proceedings of the *8th Information Security Conference (ISC)*, pp. 1 - 15. September 2005, Singapore. *(Acceptance rate: 14%)*

61. *"gore: Routing-Assisted Defense Against DDoS Attacks"*
Stephen T. Chou, Angelos Stavrou, John Ioannidis, and Angelos D. Keromytis. In Proceedings of the *8th Information Security Conference (ISC)*, pp. 179 - 193. September 2005, Singapore. *(Acceptance rate: 14%)*

62. *"FLIPS: Hybrid Adaptive Intrusion Prevention"*
Michael E. Locasto, Ke Wang, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *8th International Symposium on Recent Advances in Intrusion Detection (RAID)*, pp. 82 - 101. September 2005, Seattle, WA. *(Acceptance rate: 20.4%)*

63. *"Detecting Targeted Attacks Using Shadow Honeypots"*
Kostas G. Anagnostakis, Stelios Sidiroglou, Periklis Akritidis, Konstantinos Xinidis, Evangelos Markatos, and Angelos D. Keromytis. In Proceedings of the *14th USENIX Security Symposium*, pp. 129 - 144. August 2005, Baltimore, MD. *(Acceptance rate: 14%)*

64. *"The Bandwidth Exchange Architecture"*
David Michael Turner, Vassilis Prevelakis, and Angelos D. Keromytis. In Proceedings of

the *10th IEEE Symposium on Computers and Communications (ISCC)*, pp. 939 - 944. June 2005, Cartagena, Spain.

65. *"An Email Worm Vaccine Architecture"*
Stelios Sidiroglou, John Ioannidis, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *1st Information Security Practice and Experience Conference (ISPEC)*, pp. 97 - 108. April 2005, Singapore.

66. *"Building a Reactive Immune System for Software Services"*
Stelios Sidiroglou, Michael E. Locasto, Stephen W. Boyd, and Angelos D. Keromytis. In Proceedings of the *USENIX Annual Technical Conference*, pp. 149 - 161. April 2005, Anaheim, CA. *(Acceptance rate: 20.3%)*

67. *"Conversion and Proxy Functions for Symmetric Key Ciphers"*
Debra L. Cook and Angelos D. Keromytis. In Proceedings of the *IEEE International Conference on Information Technology: Coding and Computing (ITCC), Information and Security (IAS) Track*, pp. 662 - 667. April 2005, Las Vegas, NV.

68. *"The Effect of DNS Delays on Worm Propagation in an IPv6 Internet"*
Abhinav Kamra, Hanhua Feng, Vishal Misra, and Angelos D. Keromytis. In Proceedings of *IEEE INFOCOM*, vol. 4, pp. 2405 - 2414. March 2005, Miami, FL. *(Acceptance rate: 17%)*

69. *"MOVE: An End-to-End Solution To Network Denial of Service"*
Angelos Stavrou, Angelos D. Keromytis, Jason Nieh, Vishal Misra, and Dan Rubenstein. In Proceedings of the *12th Internet Society (ISOC) Symposium on Network and Distributed Systems Security (SNDSS)*, pp. 81 - 96. February 2005, San Diego, CA. *(Acceptance rate: 12.9%)*

70. *"CryptoGraphics: Secret Key Cryptography Using Graphics Cards"*
Debra L. Cook, John Ioannidis, Angelos D. Keromytis, and Jake Luck. In Proceedings of the *RSA Conference, Cryptographer's Track (CT-RSA)*, pp. 334 - 350. February 2005, San Francisco, CA.

71. *"The Dual Receiver Cryptogram and Its Applications"*
Ted Diament, Homin K. Lee, Angelos D. Keromytis, and Moti Yung. In Proceedings of the *11th ACM Conference on Computer and Communications Security (CCS)*, pp. 330 - 343. October 2004, Washington, DC. *(Acceptance rate: 13.9%)*

72. *"Hydan: Hiding Information in Program Binaries"*
Rakan El-Khalil and Angelos D. Keromytis. In Proceedings of the *6th International Conference on Information and Communications Security (ICICS)*, pp. 187 - 199. October 2004, Malaga, Spain. *(Acceptance rate: 16.9%)*

73. *"Recursive Sandboxes: Extending Systrace To Empower Applications"*
Aleksey Kurchuk and Angelos D. Keromytis. In Proceedings of the *19th IFIP International Information Security Conference (SEC)*, pp. 473 - 487. August 2004, Toulouse, France. *(Acceptance rate: 22%)*

74. *"SQLrand: Preventing SQL Injection Attacks"*
Stephen W. Boyd and Angelos D. Keromytis. In Proceedings of the *2nd International Conference on Applied Cryptography and Network Security (ACNS)*, pp. 292 - 302. June 2004, Yellow Mountain, China. *(Acceptance rate: 12.1%)*

75. *"CamouflageFS: Increasing the Effective Key Length in Cryptographic Filesystems on the Cheap"*
Michael E. Locasto and Angelos D. Keromytis. In Proceedings of the *2nd International*

Conference on Applied Cryptography and Network Security (ACNS), pp. 1 - 15. June 2004, Yellow Mountain, China. *(Acceptance rate: 12.1%)*

76. *"A Pay-per-Use DoS Protection Mechanism For The Web"*
Angelos Stavrou, John Ioannidis, Angelos D. Keromytis, Vishal Misra, and Dan Rubenstein. In Proceedings of the *2nd International Conference on Applied Cryptography and Network Security (ACNS)*, pp. 120 - 134. June 2004, Yellow Mountain, China. *(Acceptance rate: 12.1%)*

77. *"Dealing with System Monocultures"*
Angelos D. Keromytis and Vassilis Prevelakis. In Proceedings (electronic) of the *NATO Information Systems Technology (IST) Panel Symposium on Adaptive Defense in Unclassified Networks*. April 2004, Toulouse, France.

78. *"Managing Access Control in Large Scale Heterogeneous Networks"*
Angelos D. Keromytis, Kostas G. Anagnostakis, Sotiris Ioannidis, Michael Greenwald, and Jonathan M. Smith. In Proceedings (electronic) of the *NATO NC3A Symposium on Interoperable Networks for Secure Communications (INSC)*. November 2003, The Hague, Netherlands.

79. *"Countering Code-Injection Attacks With Instruction-Set Randomization"*
Gaurav S. Kc, Angelos D. Keromytis, and Vassilis Prevelakis. In Proceedings of the *10th ACM International Conference on Computer and Communications Security (CCS)*, pp. 272 - 280. October 2003, Washington, DC. *(Acceptance rate: 13.8%)*

80. *"Using Graphic Turing Tests to Counter Automated DDoS Attacks Against Web Servers"*
William G. Morein, Angelos Stavrou, Debra L. Cook, Angelos D. Keromytis, Vishal Misra, and Dan Rubenstein. In Proceedings of the *10th ACM International Conference on Computer and Communications Security (CCS)*, pp. 8 - 19. October 2003, Washington, DC. *(Acceptance rate: 13.8%)*

81. *"EasyVPN: IPsec Remote Access Made Easy"*
Mark C. Benvenuto and Angelos D. Keromytis. In Proceedings of the *17th USENIX Large Installation Systems Administration (LISA) Conference*, pp. 87 - 93. October 2003, San Diego, CA. *(Acceptance rate: 25%)*

82. *"A Cooperative Immunization System for an Untrusting Internet"*
Kostas G. Anagnostakis, Michael B. Greenwald, Sotiris Ioannidis, Angelos D. Keromytis, and Dekai Li. In Proceedings of the *11th IEEE International Conference on Networks (ICON)*, pp. 403 - 408. September/October 2003, Sydney, Australia.

83. *"Accelerating Application-Level Security Protocols"*
Matthew Burnside and Angelos D. Keromytis. In Proceedings of the *11th IEEE International Conference on Networks (ICON)*, pp. 313 - 318. September/October 2003, Sydney, Australia.

84. *"WebSOS: Protecting Web Servers From DDoS Attacks"*
Debra L. Cook, William G. Morein, Angelos D. Keromytis, Vishal Misra, and Dan Rubenstein. In Proceedings of the *11th IEEE International Conference on Networks (ICON)*, pp. 455 - 460. September/October 2003, Sydney, Australia.

85. *"TAPI: Transactions for Accessing Public Infrastructure"*
Matt Blaze, John Ioannidis, Sotiris Ioannidis, Angelos D. Keromytis, Pekka Nikander, and Vassilis Prevelakis. In Proceedings of the *8th IFIP Personal Wireless Communications (PWC) Conference*, pp. 90 - 100. September 2003, Venice, Italy.

86. *"Tagging Data In The Network Stack: mbuf_tags"*

Angelos D. Keromytis. In Proceedings of the *USENIX BSD Conference (BSDCon)*, pp. 125 - 131. September 2003, San Mateo, CA.

87. *"The Design of the OpenBSD Cryptographic Framework"*
Angelos D. Keromytis, Jason L. Wright, and Theo de Raadt. In Proceedings of the *USENIX Annual Technical Conference*, pp. 181 - 196. June 2003, San Antonio, TX. *(Acceptance rate: 23%)*

88. *"Secure and Flexible Global File Sharing"*
Stefan Miltchev, Vassilis Prevelakis, Sotiris Ioannidis, John Ioannidis, Angelos D. Keromytis, and Jonathan M. Smith. In Proceedings of the *USENIX Annual Technical Conference, Freenix Track*, pp. 165 - 178. June 2003, San Antonio, TX.

89. *"Experience with the KeyNote Trust Management System: Applications and Future Directions"*
Matt Blaze, John Ioannidis, and Angelos D. Keromytis. In Proceedings of the *1st International Conference on Trust Management*, pp. 284 - 300. May 2003, Heraclion, Greece.

90. *"The STRONGMAN Architecture"*
Angelos D. Keromytis, Sotiris Ioannidis, Michael B. Greenwald, and Jonathan M. Smith. In Proceedings of the *3rd DARPA Information Survivability Conference and Exposition (DISCEX III)*, volume 1, pp. 178 - 188. April 2003, Washington, DC.

91. *"Efficient, DoS-Resistant, Secure Key Exchange for Internet Protocols"*
William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, and Omer Reingold. In Proceedings of the *9th ACM International Conference on Computer and Communications Security (CCS)*, pp. 48 - 58. November 2002, Washington, DC. *(Acceptance rate: 17.6%)*

92. *"Secure Overlay Services"*
Angelos D. Keromytis, Vishal Misra, and Dan Rubenstein. In Proceedings of the *ACM SIGCOMM Conference*, pp. 61 - 72. August 2002, Pittsburgh, PA. Also available through the *ACM Computer Communications Review (SIGCOMM Proceedings)*, vol. 32, no. 4, October 2002. *(Acceptance rate: 8.3%)*

93. *"Using Overlays to Improve Network Security"*
Angelos D. Keromytis, Vishal Misra, and Dan Rubenstein. In Proceedings of the *ITCom Conference*, special track on *Scalability and Traffic Control in IP Networks*, pp. 245 - 254. July/August 2002, Boston, MA. *(Invited paper)*

94. *"Designing an Embedded Firewall/VPN Gatweway"*
Vassilis Prevelakis and Angelos D. Keromytis. In Proceedings of the *International Network Conference (INC)*, pp. 313 - 322. July 2002, Plymouth, England. **(Best Paper Award)**

95. *"A Study of the Relative Costs of Network Security Protocols"*
Stefan Miltchev, Sotiris Ioannidis, and Angelos D. Keromytis. In Proceedings of the *USENIX Annual Technical Conference, Freenix Track*, pp. 41 - 48. June 2002, Monterey, CA.

96. *"A Secure Plan (Extended Version)"*
Michael W. Hicks, Angelos D. Keromytis, and Jonathan M. Smith. In Proceedings of the *DARPA Active Networks Conference and Exposition (DANCE)*, pp. 224 - 237. May 2002, San Francisco, CA. *(Extended version of the paper IWAN 1999 paper.)*

97. *"Fileteller: Paying and Getting Paid for File Storage"*

John Ioannidis, Sotiris Ioannidis, Angelos D. Keromytis, and Vassilis Prevelakis. In Proceedings of the 6th *Financial Cryptography (FC) Conference*, pp. 282 - 299. March 2002, Bermuda. *(Acceptance rate: 25.6%)*

98. *"Offline Micropayments without Trusted Hardware"*
Matt Blaze, John Ioannidis, and Angelos D. Keromytis. In Proceedings of the 5th *Financial Cryptography (FC) Conference*, pp. 21 - 40. February 2001, Cayman Islands.

99. *"Trust Management for IPsec"*
Matt Blaze, John Ioannidis, and Angelos D. Keromytis. In Proceedings of the 8th *Internet Society (ISOC) Symposium on Network and Distributed Systems Security (SNDSS)* , pp. 139 - 151. February 2001, San Diego, CA. *(Acceptance rate: 24%)*

100. *"Implementing a Distributed Firewall"*
Sotiris Ioannidis, Angelos D. Keromytis, Steven M. Bellovin, and Jonathan M. Smith. In Proceedings of the 7th *ACM International Conference on Computer and Communications Security (CCS)*, pp. 190 - 199. November 2000, Athens, Greece. *(Acceptance rate: 21.4%)*

101. *"Implementing Internet Key Exchange (IKE)"*
Niklas Hallqvist and Angelos D. Keromytis. In Proceedings of the *USENIX Annual Technical Conference, Freenix Track*, pp. 201 - 214. June 2000, San Diego, CA.

102. *"Transparent Network Security Policy Enforcement"*
Angelos D. Keromytis and Jason Wright. In Proceedings of the *USENIX Annual Technical Conference, Freenix Track*, pp. 215 - 226. June 2000, San Diego, CA.

103. *"Cryptography in OpenBSD: An Overview"*
Theo de Raadt, Niklas Hallqvist, Artur Grabowski, Angelos D. Keromytis, and Niels Provos. In Proceedings of the *USENIX Annual Technical Conference, Freenix Track*, pp. 93 - 101. June 1999, Monterey, CA.

104. *"DHCP++: Applying an efficient implementation method for fail-stop cryptographic protocols"*
William A. Arbaugh, Angelos D. Keromytis, and Jonathan M. Smith. In Proceedings of the *IEEE Global Internet (GlobeCom)*, pp. 59 - 65. November 1998, Sydney, Australia.

105. *"Automated Recovery in a Secure Bootstrap Process"*
William A. Arbaugh, Angelos D. Keromytis, David J. Farber, and Jonathan M. Smith. In Proceedings of the 5th *Internet Society (ISOC) Symposium on Network and Distributed System Security (SNDSS)*, pp. 155 - 167. March 1998, San Diego, CA. An older version is available as *University of Pennsylvania Technical Report MS-CIS-97-13.*

106. *"Implementing IPsec"*
Angelos D. Keromytis, John Ioannidis, and Jonathan M. Smith. In Proceedings of the *IEEE Global Internet (GlobeCom)*, pp. 1948 - 1952. November 1997, Phoenix, AZ.

Books/Book Chapters

1. *"Voice over IP Security: A Comprehensive Survey of Vulnerabilities and Academic Research"*
Angelos D. Keromytis. Springer Briefs, ISBN 978-1-4419-9865-1, April 2011.
2. *"Buffer Overflow Attacks"*
Angelos D. Keromytis. In *Encyclopedia of Cryptography and Security, 2nd Edition.* Springer, 2011.
3. *"Network Bandwidth Denial of Service (DoS)"*

Angelos D. Keromytis. In *Encyclopedia of Cryptography and Security, 2nd Edition*. Springer, 2011.

4. *"Monitoring Technologies for Mitigating Insider Threats"*
   Brian M. Bowen, Malek Ben Salem, Angelos D. Keromytis, and Salvatore J. Stolfo. In *Insider Threats in Cyber Security and Beyond*, Matt Bishop, Dieter Gollman, Jeffrey Hunker, and Christian Probst (editors), pp. 197 - 218. Springer, 2010.
5. *"Voice over IP: Risks, Threats, and Vulnerabilities"*
   Angelos D. Keromytis. In *Cyber Infrastructure Security*, Tarek Saadawi and Louis Jordan (editors). Strategic Study Institute (SSI), 2010.
6. *Proceedings of the 2008 New Security Paradigms Workshop (NSPW)*
   Angelos D. Keromytis, Anil Somayaji, and M. Hossain Heydari (editors).
7. *Proceedings of the 6th International Conference on Applied Cryptography and Network Security (ACNS)*
   Steven M. Bellovin, Rosario Gennaro, Angelos D. Keromytis, and Moti Yung (editors). Lecture Notes in Computer Science (LNCS). Springer, 2008.
8. *"Insider Attack and Cyber Security: Beyond the Hacker"*
   Salvatore J. Stolfo, Steven M. Bellovin, Angelos D. Keromytis, Sara Sinclair, and Sean W. Smith (editors). Advances in Information Security Series, ISBN 978-0387773216. Springer, 2008.
9. *Proceedings of the 2007 New Security Paradigms Workshop (NSPW)*
   Kostantin Beznosov (Editor), Angelos D. Keromytis (editor), and M. Hossain Heydari (Editor).
10. *"The Case for Self-Healing Software"*
    Angelos D. Keromytis. In *Aspects of Network and Information Security: Proceedings NATO Advanced Studies Institute (ASI) on Network Security and Intrusion Detection, held in Nork, Yerevan, Armenia, October 2006*, E. Haroutunian, E. Kranakis, and E. Shahbazian (editors). IOS Press, 2007. *(By invitation, as part of the NATO ASI on Network Security, October 2005.)*
11. *"Designing Firewalls: A Survey"*
    Angelos D. Keromytis and Vassilis Prevelakis. In *Network Security: Current Status and Future Directions*, Christos Douligeris and Dimitrios N. Serpanos (editors), pp. 33 - 49. Wiley - IEEE Press, April 2007.
12. *"Composite Hybrid Techniques for Defending against Targeted Attacks"*
    Stelios Sidiroglou and Angelos D. Keromytis. In *Malware Detection*, vol. 27 of Advances in Information Security Series, Mihai Christodorescu, Somesh Jha, Douglas Maughan, Dawn Song, and Cliff Wang (editors). Springer, October 2006. *(By invitation, as part of the ARO/DHS 2005 Workshop on Malware Detection.)*
13. *"Trusted computing platforms and secure Operating Systems"*
    Angelos D. Keromytis. In *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*, Markus Jakobsson and Steven Myers (editors), pp. 387 - 405. Wiley, 2006.
14. *"CryptoGraphics: Exploiting Graphics Cards for Security"*
    Debra Cook and Angelos D. Keromytis. Advances in Information Security Series, ISBN 0-387-29015-X. Springer, 2006.
15. *Proceedings of the 3rd Workshop on Rapid Malcode (WORM)*
    Angelos D. Keromytis (editor). ACM Press, 2005.

16. *Proceedings of the 3rd International Conference on Applied Cryptography and Network Security (ACNS)*
    John Ioannidis, Angelos D. Keromytis, and Moti Yung (editors). Lecture Notes in Computer Science (LNCS) 3531. Springer, 2005.
17. *"Distributed Trust"*
    John Ioannidis and Angelos D. Keromytis. In *Practical Handbook of Internet Computing*, Munindar Singh (editor), pp. 47/1 - 47/16. CRC Press, 2004.
18. *"Experiences Enhancing Open Source Security in the POSSE Project"*
    Jonathan M. Smith, Michael B. Greenwald, Sotiris Ioannidis, Angelos D. Keromytis, Ben Laurie, Douglas Maughan, Dale Rahn, and Jason L. Wright. In *Free/Open Source Software Development*, Stefan Koch (editor), pp. 242 - 257. Idea Group Publishing, 2004. Also re-published in *Global Information Technologies: Concepts, Methodologies, Tools, and Applications*, Felix B. Tan (editor), pp. 1587 - 1598. Idea Group Publishing, 2007.
19. *"STRONGMAN: A Scalable Solution to Trust Management in Networks"*
    Angelos D. Keromytis. Ph.D. Thesis, University of Pennsylvania, November 2001.
20. *"The Role of Trust Management in Distributed Systems Security"*
    Matt Blaze, Joan Feigenbaum, John Ioannidis, and Angelos D. Keromytis. In *Secure Internet Programming: Issues in Distributed and Mobile Object Systems*, Jan Vitek and Christian Jensen (editors), pp. 185 - 210. Springer-Verlag Lecture Notes in Computer Science *State-of-the-Art* series, 1999.
21. *"Security in Active Networks"*
    D. Scott Alexander, William A. Arbaugh, Angelos D. Keromytis, and Jonathan M. Smith. In *Secure Internet Programming: Issues in Distributed and Mobile Object Systems*, Jan Vitek and Christian Jensen (editors), pp. 433 - 451. Springer-Verlag Lecture Notes in Computer Science *State-of-the-Art* series, 1999.

Workshops

1. *"REASSURE: A Self-contained Mechanism for Healing Software Using Rescue Points"*
   Georgios Portokalidis and Angelos D. Keromytis. To appear in the Proceedings of the *6th International Workshop on Security (IWSEC)*. November 2011, Tokyo, Japan.
2. *"Taint-Exchange: a Generic System for Cross-process and Cross-host Taint Tracking"*
   Angeliki Zavou, Georgios Portokalidis, and Angelos D. Keromytis. To appear in the Proceedings of the *6th International Workshop on Security (IWSEC)*. November 2011, Tokyo, Japan.
3. *"The MINESTRONE Architecture: Combining Static and Dynamic Analysis Techniques for Software Security"*
   Angelos D. Keromytis, Salvatore J. Stolfo, Junfeng Yang, Angelos Stavrou, Anup Ghosh, Dawson Engler, Marc Dacier, Matthew Elder, and Darrell Kienzle. In Proceedings of the *1st Workshop on Systems Security (SysSec)*. July 2011, Amsterdam, Netherlands.
4. *"The SPARCHS Project: Hardware Support for Software Security"*
   Simha Sethumadhavan, Salvatore J. Stolfo, David August, Angelos D. Keromytis, and Junfeng Yang. In Proceedings of the *1st Workshop on Systems Security (SysSec)*. July 2011, Amsterdam, Netherlands.
5. *"Towards a Forensic Analysis for Multimedia Communication Services"*
   Dimitris Geneiatakis and Angelos D. Keromytis. In Proceedings of the *7th International Symposium on Frontiers in Networking with Applications (FINA)*, pp. 424 - 429. March

2011, Biopolis, Singapore.

6. *"Security Research with Human Subjects: Informed Consent, Risk, and Benefits"* Maritza Johnson, Steven M. Bellovin, and Angelos D. Keromytis. In Proceedings of the *2nd Workshop on Ethics in Computer Security Research (WECSR)*. March 2011, Saint Lucia.
7. *"Global ISR: Toward a Comprehensive Defense Against Unauthorized Code Execution"* Georgios Portokalidis and Angelos D. Keromytis. In Proceedings of the *ARO Workshop on Moving Target Defense*. October 2010, Fairfax, VA.
8. *"Securing MANET Multicast Using DIPLOMA"* Mansoor Alicherry and Angelos D. Keromytis. In Proceedings of the *5th International Workshop on Security (IWSEC)*, pp. 232 - 250. November 2010, Kobe, Japan. *(Acceptance rate: 29%)*
9. *"Evaluating a Collaborative Defense Architecture for MANETs"* Mansoor Alicherry, Angelos Stavrou, and Angelos D. Keromytis. In Proceedings (electronic) of the *IEEE Workshop on Collaborative Security Technologies (CoSec)*, pp. 37 - 42. December 2009, Bangalore, India. *(Acceptance rate: 17.2%)*
10. *"Identifying Proxy Nodes in a Tor Anonymization Circuit"* Sambuddho Chakravarty, Angelos Stavrou, and Angelos D. Keromytis. In Proceedings of the *2nd Workshop on Security and Privacy in Telecommunications and Information Systems (SePTIS)*, pp. 633 - 639. December 2008, Bali, Indonesia. *(Acceptance rate: 37.5%)*
11. *"Online Network Forensics for Automatic Repair Validation"* Michael E. Locasto, Matthew Burnside, and Angelos D. Keromytis. In Proceedings of the *3rd International Workshop on Security (IWSEC)*, pp. 136 - 151. November 2008, Kagawa, Japan. *(Acceptance rate: 19.1%)*
12. *"Return Value Predictability for Self-Healing"* Michael E. Locasto, Angelos Stavrou, Gabriela F. Cretu, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *3rd International Workshop on Security (IWSEC)*, pp. 152 - 166. November 2008, Kagawa, Japan. *(Acceptance rate: 19.1%)*
13. *"Asynchronous Policy Evaluation and Enforcement"* Matthew Burnside and Angelos D. Keromytis. In Proceedings of the *2nd Computer Security Architecture Workshop (CSAW)*, pp. 45 - 50. October 2008, Fairfax, VA.
14. *"Race to the bottom: Malicious Hardware"* Angelos D. Keromytis, Simha Sethumadhavan, and Ken Shepard. In Proceedings of the *1st FORWARD Invitational Workshop for Identifying Emerging Threats in Information and Communication Technology Infrastructures*. April 2008, Goteborg, Sweden. *(Invited paper)*
15. *"Arachne: Integrated Enterprise Security Management"* Matthew Burnside and Angelos D. Keromytis. In Proceedings of the *8th Annual IEEE SMC Information Assurance Workshop (IAW)*, pp. 214 - 220. June 2007, West Point, NY.
16. *"Poster Paper: Band-aid Patching"* Stelios Sidiroglou, Sotiris Ioannidis, and Angelos D. Keromytis. In Proceedings of the *3rd Workshop on Hot Topics in System Dependability (HotDep)*, pp. 102 - 106. June 2007, Edinburgh, UK.
17. *"Data Sanitization: Improving the Forensic Utility of Anomaly Detection Systems"* Gabriela F. Cretu, Angelos Stavrou, Salvatore J. Stolfo, and Angelos D. Keromytis. In

Proceedings of the *3rd Workshop on Hot Topics in System Dependability (HotDep)*, pp. 64 - 70. June 2007, Edinburgh, UK.

18. *"Bridging the Network Reservation Gap Using Overlays"*
Angelos Stavrou, David Michael Turner, Angelos D. Keromytis, and Vassilis Prevelakis. In Proceedings of the *1st Workshop on Information Assurance for Middleware Communications (IAMCOM)*, pp. 1 - 6. January 2007, Bangalore, India.
19. *"Next Generation Attacks on the Internet"*
Evangelos Markatos and Angelos D. Keromytis. In Proceedings (electronic) of the *EU-US Summit Series on Cyber Trust: Workshop on System Dependability & Security*, pp. 67 - 73. November 2006, Dublin, Ireland. *(Invited paper)*
20. *"Dark Application Communities"*
Michael E. Locasto, Angelos Stavrou, and Angelos D. Keromytis. In Proceedings of the *New Security Paradigms Workshop (NSPW)*, pp. 11 - 18. September 2006, Schloss Dagstuhl, Germany.
21. *"Privacy as an Operating System Service"*
Sotiris Ioannidis, Stelios Sidiroglou, and Angelos D. Keromytis. In Proceedings (electronic) of the *1st Workshop on Hot Topics in Security (HotSec)*. July 2006, Vancouver, Canada.
22. *"PalProtect: A Collaborative Security Approach to Comment Spam"*
Benny Wong, Michael E. Locasto, and Angelos D. Keromytis. In Proceedings of the *7th Annual IEEE SMC Information Assurance Workshop (IAW)*, pp. 170 - 175. June 2006, West Point, NY.
23. *"Adding a Flow-Oriented Paradigm to Commodity Operating Systems"*
Christian Soviani, Stephen A. Edwards, and Angelos D. Keromytis. In Proceedings of the *Workshop on Interaction between Operating System and Computer Architecture (IOSCA)*, held in conjunction with the IEEE International Symposium on Workload Characterization, pp. 1 - 6. October 2005, Austin, TX.
24. *"Speculative Virtual Verification: Policy-Constrained Speculative Execution"*
Michael E. Locasto, Stelios Sidiroglou, and Angelos D. Keromytis. In Proceedings of the *New Security Paradigms Workshop (NSPW)*, pp. 119 - 124. September 2005, Lake Arrowhead, CA.
25. *"Application Communities: Using Monoculture for Dependability"*
Michael E. Locasto, Stelios Sidiroglou, and Angelos D. Keromytis. In Proceedings of the *1st Workshop on Hot Topics in System Dependability (HotDep)*, held in conjunction with the International Conference on Dependable Systems and Networks (DSN), pp. 288 - 292. June 2005, Yokohama, Japan.
26. *"Towards Collaborative Security and P2P Intrusion Detection"*
Michael E. Locasto, Janak Parekh, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *6th Annual IEEE SMC Information Assurance Workshop (IAW)*, pp. 333 - 339. June 2005, West Point, NY.
27. *"FlowPuter: A Cluster Architecture Unifying Switch, Server and Storage Processing"*
Alfred V. Aho, Angelos D. Keromytis, Vishal Misra, Jason Nieh, Kenneth A. Ross, and Yechiam Yemini. In Proceedings of the *1st International Workshop on Data Processing and Storage Networking: towards Grid Computing (DPSN)*, pp. 2/1 - 2/7. May 2004, Athens, Greece.
28. *"One Class Support Vector Machines for Detecting Anomalous Windows Registry*

Accesses"
Katherine Heller, Krysta Svore, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *ICDM Workshop on Data Mining for Computer Security,* held in conjunction with the *3rd International IEEE Conference on Data Mining,* pp. 2 - 9. November 2003, Melbourn, FL.

29. *"A Holistic Approach to Service Survivability"*
Angelos D. Keromytis, Janak Parekh, Philip N. Gross, Gail Kaiser, Vishal Misra, Jason Nieh, Dan Rubenstein, and Salvatore J. Stolfo. In Proceedings of the *1st ACM Workshop on Survivable and Self-Regenerative Systems (SSRS),* held in conjunction with the *10th ACM International Conference on Computer and Communications Security (CCS),* pp. 11 - 22. October 2003, Fairfax, VA.
30. *"High-Speed I/O: The Operating System As A Signalling Mechanism"*
Matthew Burnside and Angelos D. Keromytis. In Proceedings of the *ACM SIGCOMM Workshop on Network-I/O Convergence: Experience, Lessons, Implications (NICELI),* held in conjunction with the *ACM SIGCOMM Conference,* pp. 220 - 227. August 2003, Karlsruhe, Germany.
31. *"A Network Worm Vaccine Architecture"*
Stelios Sidiroglou and Angelos D. Keromytis. In Proceedings of the *12th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Workshop on Enterprise Security,* pp. 220 - 225. June 2003, Linz, Austria.
32. *"Design and Implementation of Virtual Private Services"*
Sotiris Ioannidis, Steven M. Bellovin, John Ioannidis, Angelos D. Keromytis, and Jonathan M. Smith. In Proceedings of the *12th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Workshop on Enterprise Security, Special Session on Trust Management in Collaborative Global Computing,* pp. 269 - 274. June 2003, Linz, Austria.
33. *"WebDAVA: An Administrator-Free Approach To Web File-Sharing"*
Alexander Levine, Vassilis Prevelakis, John Ioannidis, Sotiris Ioannidis, and Angelos D. Keromytis. In Proceedings of the *12th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Workshop on Distributed and Mobile Collaboration,* pp. 59 - 64. June 2003, Linz, Austria.
34. *"Protocols for Anonymity in Wireless Networks"*
Matt Blaze, John Ioannidis, Angelos D. Keromytis, Tal Malkin, and Avi Rubin. In Proceedings of the *11th International Workshop on Security Protocols.* April 2003, Cambridge, England.
35. *"xPF: Packet Filtering for Low-Cost Network Monitoring"*
Sotiris Ioannidis, Kostas G. Anagnostakis, John Ioannidis, and Angelos D. Keromytis. In Proceedings of the *Workshop on High Performance Switching and Routing (HPSR),* pp. 121 - 126. May 2002, Kobe, Japan.
36. *"Toward Understanding the Limits of DDoS Defenses"*
Matt Blaze, John Ioannidis, and Angelos D. Keromytis. In Proceedings of the *10th International Workshop on Security Protocols,* Springer-Verlag Lecture Notes in Computer Science, vol. 2467. April 2002, Cambridge, England.
37. *"Toward A Unified View of Intrusion Detection and Security Policy"*
Matt Blaze, Angelos D. Keromytis, and Salvatore J. Stolfo. In Proceedings of the *10th*

International Workshop on Security Protocols, Springer-Verlag Lecture Notes in Computer Science, vol. 2467. April 2002, Cambridge, England.

38. *"Efficient, DoS-resistant, Secure Key Exchange for Internet Protocols"*
William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, and Omer Reingold. In Proceedings of the *9th International Workshop on Security Protocols*, Springer-Verlag Lecture Notes in Computer Science, vol. 2133, pp. 40 - 48. April 2001, Cambridge, England.
39. *"Scalable Resource Control in Active Networks"*
Kostas G. Anagnostakis, Michael W. Hicks, Sotiris Ioannidis, Angelos D. Keromytis, and Jonathan M. Smith. In Proceedings of the *2nd International Workshop for Active Networks (IWAN)*, pp. 343 - 357. October 2000, Tokyo, Japan.
40. *"A Secure Plan"*
Michael W. Hicks and Angelos D. Keromytis. In Proceedings of the *1st International Workshop for Active Networks (IWAN)*, pp. 307 - 314. June - July 1999, Berlin, Germany. An extended version is available as *University of Pennsylvania Technical Report MS-CIS-99-14*, and was also published in the Proceedings of the *DARPA Active Networks Conference and Exposition (DANCE)*, May 2002.
41. *"Trust Management and Network Layer Security Protocols"*
Matt Blaze, John Ioannidis, and Angelos D. Keromytis. In Proceedings of the *7th International Workshop on Security Protocols*, Springer-Verlag Lecture Notes in Computer Science, vol. 1796, pp. 103 - 108. April 1999, Cambridge, England.
42. *"The SwitchWare Active Network Implementation"*
D. Scott Alexander, Michael W. Hicks, Pankaj Kakkar, Angelos D. Keromytis, Marianne Shaw, Jonathan T. Moore, Carl A. Gunter, Trevor Jim, Scott M. Nettles, and Jonathan M. Smith. In Proceedings of the *ACM SIGPLAN Workshop on ML*, held in conjunction with the *International Conference on Functional Programming (ICFP)*, pp. 67 - 76. September 1998, Baltimore, MD.
43. *"KeyNote: Trust Management for Public-Key Infrastructures"*
Matt Blaze, Joan Feigenbaum, and Angelos D. Keromytis. In Proceedings of the *6th International Workshop on Security Protocols*, Springer-Verlag Lecture Notes in Computer Science, vol. 1550, pp. 59 - 63. April 1998, Cambridge, England. Also available as *AT&T Technical Report 98.11.1*.

Additional Publications

1. *"Transport Layer Security (TLS) Authorization Using KeyNote"*
Angelos D. Keromytis. *Request For Comments (RFC) 6042*, October 2010.
2. *"X.509 Key and Signature Encoding for the KeyNote Trust Management System"*
Angelos D. Keromytis. *Request For Comments (RFC) 5708*, January 2010.
3. *"SSARES: Secure Searchable Automated Remote Email Storage"*
Adam J. Aviv, Michael E. Locasto, Shaya Potter, and Angelos D. Keromytis. In the Columbia Computer Science Student Research Symposium, Fall 2006.
4. *"IP Security Policy Requirements"*
Matt Blaze, Angelos D. Keromytis, Michael Richardson, and Luis Sanchez. *Request For Comments (RFC) 3586*, August 2003.
5. *"On the Use of Stream Control Transmission Protocol (SCTP) with IPsec"*
Steven M. Bellovin, John Ioannidis, Angelos D. Keromytis, and Randal R. Stewart.

Request For Comments (RFC) 3554, June 2003.

6. *"The Use of HMAC-RIPEMD-160-96 within ESP and AH"*
   Angelos D. Keromytis and Niels Provos. *Request For Comments (RFC) 2857*, June 2000.
7. *"DSA and RSA Key and Signature Encoding for the KeyNote Trust Management System"*
   Matt Blaze, John Ioannidis, and Angelos D. Keromytis. *Request For Comments (RFC) 2792*, March 2000.
8. *"The KeyNote Trust-Management System, Version 2"*
   Matt Blaze, Joan Feigenbaum, John Ioannidis, and Angelos D. Keromytis. *Request For Comments (RFC) 2704*, September 1999.

Technical Reports/Works in Progress

1. *"Symantec Report on Rogue Security Software, July 2008 - June 2009"*
   Marc Fossi, Dean Turner, Eric Johnson, Trevor Mack, Teo Adams, Joseph Blackbird, Mo King Low, David McKinney, Marc Dacier, Angelos D. Keromytis, Corrado Leita, Marco Cova, Jon Orbeton, and Olivier Thonnard. Symantec Technical Report, October 2009.
2. *"LinkWidth: A Method to Measure Link Capacity and Available Bandwidth using Single-End Probes"*
   Sambuddho Chakravarty, Angelos Stavrou, and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-002-08*, January 2008.
3. *"Can P2P Replace Direct Download for Content Distribution?"*
   Alex Sherman, Angelos Stavrou, Jason Nieh, Cliff Stein, and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-020-07*, March 2007.
4. *"A Model for Automatically Repairing Execution Integrity"*
   Michael E. Locasto, Gabriela F. Cretu, Angelos Stavrou, and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-005-07*, January 2007.
5. *"Speculative Execution as an Operating System Service"*
   Michael E. Locasto and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-024-06*, May 2006.
6. *"Quantifying Application Behavior Space for Detection and Self-Healing"*
   Michael E. Locasto, Angelos Stavrou, Gabriela F. Cretu, Angelos D. Keromytis, and Salvatore J. Stolfo. *Columbia University Computer Science Department Technical Report CUCS-017-06*, April 2006.
7. *"Bloodhound: Searching Out Malicious Input in Network Flows for Automatic Repair Validation"*
   Michael E. Locasto, Matthew Burnside, and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-016-06*, April 2006.
8. *"Binary-level Function Profiling for Intrusion Detection and Smart Error Virtualization"*
   Michael E. Locasto and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-002-06*, January 2006.
9. *"A General Analysis of the Security of Elastic Block Ciphers"*
   Debra Cook, Moti Yung, and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-038-05*, September 2005.
10. *"The Pseudorandomness of Elastic Block Ciphers"*

Debra Cook, Moti Yung, and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-037-05*, September 2005.

11. *"PachyRand: SQL Randomization for the PostgreSQL JDBC Driver"*
Michael E. Locasto and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-033-05*, August 2005.
12. *"Elastic Block Ciphers: The Feistel Cipher Case"*
Debra L. Cook, Moti Yung, and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-021-04*, May 2004.
13. *"Collaborative Distributed Intrusion Detection"*
Michael E. Locasto, Janak J. Parekh, Salvatore J. Stolfo, Angelos D. Keromytis, Tal Malkin, and Vishal Misra. *Columbia University Computer Science Department Technical Report CUCS-012-04*, March 2004.
14. *"Elastic Block Ciphers"*
Debra L. Cook, Moti Yung, and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-010-04*, February 2004.
15. *"Just Fast Keying (JFK)"*
William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, and Omer Reingold. *IETF IPsec Working Group*, April 2002,.
16. *"CASPER: Compiler-Assisted Securing of Programs at Runtime"*
Gaurav S. Kc, Stephen A. Edwards, Gail E. Kaiser, and Angelos D. Keromytis. *Columbia University Computer Science Department Technical Report CUCS-025-02*, 2002.
17. *"The 'suggested ID' extension for IKE"*
Angelos D. Keromytis and William Sommerfeld. *IETF IPsec Working Group*, November 2001.
18. *"SPKI: ShrinkWrap"*
Angelos D. Keromytis and William A. Simpson. *IETF SPKI Working Group*, September 1997.
19. *"Active Network Encapsulation Protocol (ANEP)"*
D. Scott Alexander, Bob Braden, Carl A. Gunter, Alden W. Jackson, Angelos D. Keromytis, Gary J. Minden, and David Wetherall. *Active Networks Group, DARPA Active Networks Project*, August 1997.
20. *"Creating Efficient Fail-Stop Cryptographic Protocols"*
Angelos D. Keromytis and Jonathan M. Smith. *University of Pennsylvania Technical Report MS-CIS-96-32*, December 1996.