

Angelos D. Keromytis - *Curriculum Vitae*

Professional Distinctions

- DARPA Superior Public Service Medal, December 2018.
- DARPA Results Matter award, October 2018.
- IEEE Fellow, 2018 onward.
- ACM Fellow, 2017 onward.
- ACM Distinguished Scientist, 2012 onward.

Positions Held

- **August 2019 - Present**
President
Voreas Laboratories Incorporated, Atlanta, GA

Co-founder, Chairman of the Board, and President of technology startup in the Atlanta area, commercializing technologies around network analytics and cyber attribution.
- **August 2018 - Present**
John H. Weinauer, Jr. Endowed Chair Professor and Georgia Research Alliance Eminent Scholar
School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA

Co-founder and co-director of the [Center for Cyber Operations Enquiry and Unconventional Sensing \(COEUS\)](#). Co-founded two technology startup companies. Raised over \$11.5M for research. Awarded an additional 14 issued US patents.
- **July 2014 - December 2018**
Program Manager
Information Innovation Office (I2O), Defense Advanced Research Projects Agency (DARPA), Arlington, VA

Conceived, launched, and managed 5 new major research programs ([Transparent Computing \(TC\)](#), [Leveraging the Analog Domain for Security \(LADS\)](#), [Enhanced Attribution \(EA\)](#), [Warfighter Analytics using Smartphones for Health \(WASH\)](#), and [Harnessing Autonomy for Countering Cyberadversary Systems \(HACCS\)](#)) and managed an additional 4 programs ([Active Authentication \(AA\)](#), [Active Cyber Defense \(ACD\)](#), [Anomaly Detection at Multiple Scales \(ADAMS\)](#), and [Computer Science Study Group \(CSSG\)](#)), with a total budget of almost \$500M. Responsible for technical and programmatic direction for each of these efforts, and interfaced with the rest of the Department of Defense, US Government, and private industry and academia. Successfully transitioned technologies that contributed to the DARPA and DoD mission. For these efforts, I was awarded the DARPA Superior Public Service Metal and a DARPA Results Matter award.
- **July 2013 - July 2014**
Program Director
Division of Computer and Network Systems (CNS), Directorate for Computer & Information Science & Engineering (CISE)
National Science Foundation (NSF), Arlington, VA

Helped manage the \$80M/year [Secure and Trustworthy Cyberspace \(SaTC\)](#) program, which is the primary NSF source of funding for academic research in cybersecurity across the nation. With colleagues from the [SBE](#) and [ENG](#) Directorates, I helped create the [Resilient Interdependent Infrastructure Processes and Systems \(RIPS\)](#) program, which seeks to enhance the understanding and design of interdependent critical infrastructure systems (ICIs) and processes that provide essential goods and services despite disruptions and failures from any cause, natural, technological, or malicious. I also led the creation of the [NSF/Intel Partnership on Cyber-Physical Systems Security and Privacy \(CPS-Security\)](#) program, which seeks to foster a research community committed to advancing research and education at the confluence of cybersecurity, privacy, and cyber-physical systems, and to transitioning its findings into engineering practice. I was also involved in the [Secure, Trustworthy, Assured and Resilient Semiconductors and Systems \(SaTC: STARSS\)](#) track, which represented a joint partnership between NSF and the [Semiconductor Research Corporation \(SRC\)](#) that supports research on new strategies for architecture, specification and verification, especially at the stages of design in which formal methods are currently weak or absent, with the aim of decreasing the likelihood of unintended behavior or access, increasing resistance and resilience to tampering, and improving the ability to provide authentication throughout the supply chain and in the field.
- **January 2009 - January 2010**
Senior Research Engineer
Symantec Research Labs Europe, Sophia Antipolis, France

Sabbatical leave with Symantec Research Labs Europe, where I worked primarily on security for voice over IP (VoIP) and on [rogue security software](#).
- **January 2006 - July 2017**
Associate Professor
Department of Computer Science, Columbia University, New York, NY

After receiving tenure, continued expanding the research scope of the Network Security Lab, including work on [clean-slate hardware-assisted system design for security](#), [cloud security](#), [security for open source / third-party software](#), [deception-based security](#), [security applications of information flow](#), [scalable private databases](#), [operating system kernel security](#), [security for mobile ad hoc networks \(MANETs\)](#), [anomaly detection](#), [voice over IP \(VoIP\) security](#), [anonymity](#), and [privacy](#). Demonstrated vulnerabilities against [digital broadcast TV](#), [CAPTCHAs](#), [location proximity services](#), [photo-based social authentication](#), the [Tor anonymity network](#), and others. Co-founded two technology startup companies. Raised an additional \$30M for research, with major sponsors including DARPA, IARPA, and NSF. Published an additional 23 journal, 76 conference, and 20 workshop papers, and was awarded an additional 46 issued US patents. Taught courses on security, operating systems, and software engineering.
- **July 2001 - December 2005**
Assistant Professor
Department of Computer Science, Columbia University, New York, NY

Established and directed the Network Security Laboratory, supervising several postdoc, Ph.D., and M.Sc. students conducting research on a variety of projects. Major research efforts include the [Secure Overlay Services \(SOS\)](#) anti-DDoS architecture (which anticipated current CDN-based commercial services available today), the [GRIDLOCK](#) architecture for managing access control policies for distributed networked resources, [autonomic software patching](#) and the [ASSURE](#) self-healing software framework, the concept of [Instruction Set Randomization](#) (which was awarded the 2013 ACM CCS Test of Time Award), the concept of [Application Communities](#) for improving security of software monocultures, the design and analysis of [Elastic Block Ciphers](#), and others. Raised almost \$9.5M in 12 major projects and numerous smaller gifts and awards, was awarded 2 issued US patents, and published 27 journal, 71 conference, and 30 workshop papers. Taught courses on security, operating systems, and software engineering.
- **September 1996 - July 2001**
Research Assistant
Computer and Information Science Department, University of Pennsylvania, Philadelphia, PA

Conducted research on [cryptographic protocols](#), [security for active networks](#), the [IP security protocol \(IPsec\)](#) suite, and [access control](#) (including the concept of [distributed firewalls](#)). Contributed the [IPsec stack](#) and the [framework for hardware-based cryptographic acceleration](#) to the OpenBSD kernel. Co-designed and developed the [KeyNote trust management system](#), and demonstrated its applications to a number of domains such as [offline micropayments](#) and [network authorization](#).
- **January 1993 - October 1995**
Member of the Technical Staff
FORTHnet S.A., Heraclion, Greece

Employee #3 at the first commercial Internet Service Provider in Greece. Responsible for network reliability and security. Developed the first usage-based network accounting system, which was used for several years thereafter. Established and operated the Freenet IRC node for Greece and maintained an FTP mirror site.
- **September 1991 - January 1993**
Member of the Technical Staff
Education Team, Computer Center of the University of Crete, Heraclion, Greece

Served as system administrator for a cluster of IBM AIX systems supporting the educational mission of the University.

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 co-Chair, 8th International ICST Conference on Security and Privacy in Communication Networks (SecureComm), 2012.
- 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

1. Program Committee, Information Security Conference (ISC), 2005, 2007, 2009, 2011, 2012, 2014, 2020, 2021, 2022, 2023.
2. Program Committee, International Workshop on Security (IWSEC), 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014.
3. Program Committee, ACM Conference on Computer and Communications Security (CCS), 2005, 2007, 2008, 2009, 2010, 2012, 2013, 2014.
4. Program Committee, ISOC Symposium on Network and Distributed Systems Security (SNDSS), 2003, 2004, 2006, 2007, 2008, 2012.
5. Program Committee, Applied Cryptography and Network Security (ACNS) Conference, 2005, 2006, 2010, 2011, 2012, 2013.
6. Program Committee, Financial Cryptography (FC) Conference, 2002, 2010, 2011, 2012, 2013.
7. Program Committee, European Workshop on Systems Security (EuroSec), 2009, 2010, 2011, 2012, 2013.
8. Program Committee, USENIX Security Symposium, 2004, 2005, 2006, 2008.
9. Program Committee, International Conference on Distributed Computing Systems (ICDCS), *Security Track*, 2005, 2006, 2007, 2008.
10. Program Committee, Workshop on Rapid Malcode (WORM), 2004, 2005, 2006, 2007.
11. Program Committee, World Wide Web Conference (WWW), 2005, 2006, 2007.
12. Program Committee, USENIX Workshop on Hot Topics in Security (HotSec), 2006, 2007, 2010.
13. Program Committee, Annual Computer Security Applications Conference (ACSAC), 2006, 2007, 2011.
14. Program Committee, USENIX Technical Conference, *Freely Distributable Software (Freenix) Track*, 1998, 1999, 2003.
15. Program Committee, International Conference on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS), 2007, 2010, 2012.
16. Program Committee, IEEE Security & Privacy Symposium, 2006, 2008.
17. Program Committee, ACM SIGCOMM Workshop on Large Scale Attack Defense (LSAD), 2006, 2007.
18. Program Committee, New Security Paradigms Workshop (NSPW), 2007, 2008.
19. Program Committee, IEEE WETICE Workshop on Enterprise Security, 2002, 2003.
20. Program Committee, USENIX Annual Technical Conference (ATC), 2008, 2011.
21. Program Committee, 6th International Conference on Cryptology and Network Security (CANS), 2007, 2012.
22. Program Committee, Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Dependable Computing and Communication Symposium (DCCS), 2010, 2013.
23. Program Committee, Australasian Conference on Information Security and Privacy (ACISP), 2022, 2023.
24. Program Committee, ACM Workshop on Moving Target Defense (MTD), 2014, 2015.
25. Program Committee, 1st International Conference on Human Aspects of Information Security, Privacy and Trust (HAS), 2013.
26. Program Committee, Workshop on Information Security Theory and Practice (WISTP), 2012.
27. Program Committee, European Symposium on Research in Computer Security (ESORICS), 2011.
28. Program Committee, International Workshop on Mobile Security (WMS), 2010.
29. Program Committee, Computer Forensics in Software Engineering Workshop, 2009.
30. Program Committee, USENIX Workshop on Large-scale Exploits and Emergent Threats (LEET), 2008.
31. Program Committee, 23rd International Information Security Conference (IFIP SEC), 2008.
32. Program Committee, Joint iTrust and PST Conferences on Privacy, Trust Management and Security (IFIPTM), 2008.
33. Program Committee, 1st Computer Security Architecture Workshop (CSAW), 2007.
34. Program Committee, 8th IEEE Information Assurance Workshop (IAW), 2007.
35. Program Committee, Anti-Phishing Working Group (APWG) eCrime Researchers Summit, 2007.
36. Program Committee, 4th GI International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA), 2007.
37. Program Committee, 2nd ACM Symposium on InformAtion, Computer and Communications Security (AsiaCCS), 2007.
38. Program Committee, 2nd Workshop on Advances in Trusted Computing (WATC), 2006.
39. Program Committee, International Conference on Information and Communications Security (ICICS), 2006.
40. Program Committee, 2nd Workshop on Secure Network Protocols (NPSec), 2006.
41. Program Committee, 1st Workshop on Hot Topics in System Dependability (HotDep), 2005.
42. Program Committee, 20th ACM Symposium on Applied Computing (SAC), Trust, Recommendations, Evidence and other Collaboration Know-how (TRECK) Track, 2005.
43. Program Committee, 1st Workshop on Operating System and Architecture Support for the on demand IT Infrastructure (OASIS), 2004.
44. Program Committee, Workshop on Information Security Applications (WISA), 2004.
45. Program Committee, Workshop on Logical Foundations of an Adaptive Security Infrastructure (WOLFASI), 2004.
46. Program Committee, 29th IEEE Conference on Local Computer Networks (LCN), 2004.
47. Program Committee, 2nd International Conference on Trust Management, 2004.
48. Program Committee, Asia BSD Conference, 2004.
49. Program Committee, 2nd Annual New York Metro Area Networking Workshop (NYMAN), 2002.
50. Program Committee, Cloud Computing Security Workshop (CCSW), 2009.
51. Program Committee, Workshop on Grid and Cloud Security (WGC-Sec), 2011.
52. Program Committee, Workshop on Cyber Security Experimentation and Test (CSET), 2011.
53. Program Committee, OWASP AppSec EU, 2012.

54. Program Committee, 1st International Workshop on Cyber Crime (IWCC), 2012.
55. Program Committee, 8th China International Conference on Information Security and Cryptology (INSCRYPT), 2012.
56. Program Committee, NDSS Workshop on Security of Emerging Networking Technologies (SENT), 2014.

Advisory Workshops (Not During Federal Government Service)

- NSF Workshop on Secure and Trustworthy Cyberspace (SaTC) 2.0, Dallas, TX, March 2023.
- DARPA ISAT Workshop, Pittsburgh, PA, February/March 2023.
- ARO Workshop on AI for Security and Security for AI, Arlington, VA, January 2023.
- Steering Committee Chair, US Open-Source Security Initiative Workshop, August 2022.
- ODNI/NSA Invitational Workshop on Computational Cybersecurity in Compromised Environments (C3E), Menlo Park, September 2019.
- NITRD/SCORE Invitational Workshop on Artificial Intelligence and Cybersecurity, College Park, MD, June 2019.
- DARPA ISAT Summer Meeting, Arlington, VA, August 2013.
- NITRD/SCORE Invitational Workshop on Designing-in Security: Current Practices and Research Needs, Arlington, VA, July 2013.
- MITRE/NSA Invitational Annual Secure and Resilient Cyber Architectures Workshop, McLean, VA, June 2013.
- ONR Workshop on Automated Software Complexity Reduction for Retaining Software Execution Efficiency and Increasing Security, McLean, VA, June 2013.
- ARO Cloud Security Workshop, Fairfax, VA, March 2013.
- ODNI/NSA Invitational Workshop on Computational Cybersecurity in Compromised Environments (C3E), West Point, NY, September 2012.
- Cyber Security Research Institute (CSRI) Invitational Workshop, Arlington, VA, April 2012.
- 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

- Member, Georgia Secretary of State Bipartisan Task Force for Safe, Secure, and Accessible Elections, 2020.
- Member, ACM SIGSAC CCS Test of Time Award Committee, 2020.
- Vice Chair, IEEE Computer Society Fellows Evaluation Committee, 2020.
- Founder and President, [Voreas Laboratories Incorporated](#), 2019 - present.
- Reviewer, IEEE Computer Society Fellows Evaluation Committee, 2018.
- Member, IEEE Security & Magazine Editor-in-Chief Search Committee, 2017.
- Advisory Board, Aponix Financial Technologists, 2014 - 2015.
- Member, Executive Committee for the [Institute for Data Sciences and Engineering \(IDSE\)](#), Columbia University, 2012 - 2013.
- Co-chair, ACM Computing Classification System Update Committee ("Security and Privacy" top-level node), 2011.
- Founder, [Allure Security Technology Inc.](#), 2010 - present.
- 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 (I²R), 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, 2012, 2013.
- 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, 2012, 2013, 2015, 2017.
- Internet Engineering Task Force (IETF) Security Area Advisor, 2001 - 2008.

Ph.D. Thesis Committee Service

1. Amos Imbati Alubala, "[Towards A Secure Account Recovery: Machine Learning Based User Modeling for Protection of Account Recovery](#)", Department of Computer Science, Columbia University, November 2022.
2. Panagiotis Kintis, "[Characterizing Network Infrastructure Using the Domain Name System](#)", School of Computer Science, Georgia Institute of Technology, October 2020.
3. Nader Sehatbakhsh, "[Leveraging Side-Channel Signals for Security and Trust](#)", School of Computer Science, Georgia Institute of Technology, May 2020.
4. Baki Berkay Yilmaz, "[Covert/Side Channel Analysis, Modeling and Capacity Estimation](#)", School of Electrical and Computer Engineering, Georgia Institute of Technology, March 2020.
5. Luong N. Nguyen, "[New Side-Channel and Techniques for Hardware Trojan Detection](#)", School of Electrical and Computer Engineering, Georgia Institute of Technology, March 2020.
6. Mohammad Hamad, "[A Multilayer Secure Framework for Vehicular Systems](#)", Institute of Computer and Network Engineering, Technical University of Braunschweig, Germany, February 2020.
7. Ruian Duan, "[Toward Solving The Security Risks Of Open Source Software Use](#)", School of Computer Science, Georgia Institute of Technology, October 2019.
8. Monjur Alam, "[Making Crypto Libraries Robust Against Physical Side-Channel Attacks](#)", School of Computer Science, Georgia Institute of Technology, September 2019.
9. Yang Ji, "[Efficient and Refinable Attack Investigation](#)", School of Computer Science, Georgia Institute of Technology, August 2019.
10. Nathaniel Boggs, "[Empirical Measurement of Defense in Depth](#)", Department of Computer Science, Columbia University, March 2015.
11. Ang Cui, "[Embedded System Security: A Software-based Approach](#)", Department of Computer Science, Columbia University, March 2015.
12. Binh Vo, "[Private, Distributed, and Searchable Content Providers](#)", Department of Computer Science, Columbia University, December 2014.
13. Jingyue Wu, "[Sound and Precise Analysis of Multithreaded Programs through Schedule Specialization](#)", Department of Computer Science, Columbia University, May 2014.
14. Dimitris Mitropoulos, "[Secure Software Development Technologies](#)", Department of Management Science and Technology, Athens University of Economics and Business, March 2014.
15. Iasonas Polakis, "[Online Social Networks From A Malicious Perspective: Novel Attack Techniques and Defense Mechanisms](#)", Computer Science Department, University of Crete, February 2014.
16. Kapil Anand, "[Binary Analysis Based on a Compiler-level Intermediate Representation](#)", Electrical and Computer Engineering Department, University of Maryland, July 2013.
17. Theodor Scholte, "[Securing Web Applications by Design](#)", Computer Science Group, Communications and Electronics Department, Ecole Nationale Supérieure des Telecommunications, May 2012.
18. Maritza Johnson, "[Toward Usable Access Control for End-Users: A Case Study of Facebook Privacy Settings](#)", Department of Computer Science, Columbia University, April 2012.
19. Collin R. Mulliner, "[On the Impact of the Cellular Modem on the Security of Mobile Phones](#)", Technische Universität Berlin, December 2011.
20. Malek Ben Salem, "[Towards Effective Masquerade Attack Detection](#)", Department of Computer Science, Columbia University, October 2011.
21. Michalis Polychronakis, "[Generic Code Injection Attack Detection using Code Emulation](#)", Computer Science Department, University of Crete, October 2009.
22. Spyros Antonatos, "[Defending against Known and Unknown Attacks using a Network of Affined Honeypots](#)", Computer Science Department, University of Crete, October 2009.
23. Van-Hau Pham, "[Honeypot Traces Forensics by Means of Attack Event Identification](#)", Computer Science Group, Communications and Electronics Department, Ecole Nationale Supérieure des Telecommunications, September 2009.
24. Gabriela F. Ciocarlie, "[Towards Self-Adaptive Anomaly Detection Sensors](#)", Department of Computer Science, Columbia University, September 2009.
25. Wei-Jen Li, "[SPARSE: A Hybrid System for Malcode-Bearing Document Detection](#)", Department of Computer Science, Columbia University, June 2008.
26. Raj Kumar Rajendran, "[The Method for Strong Detection for Distributed Routing](#)", Electrical Engineering Department, Columbia University, March 2008.
27. Constantin Serban, "[Advances in Decentralized and Stateful Access Control](#)", Computer Science Department, Rutgers University, December 2007.
28. Ricardo A. Baratto, "[THINC: A Virtual and Remote Display Architecture for Desktop Computing](#)", Computer Science Department, Columbia University, October 2006.

29. Zhenkai Liang, "Techniques in Automated Cyber-Attack Response and Recovery", Computer Science Department, Stony Brook University, November 2006.
30. Ke Wang, "Network Payload-based Anomaly Detection and Content-based Alert Correlation", Computer Science Department, Columbia University, August 2006.
31. Seoung-Bum Lee, "Adaptive Quality of Service for Wireless Ad hoc Networks", Electrical Engineering Department, Columbia University, June 2006.
32. Shlomo Hershkop, "Behavior-based Email Analysis with Application to Spam Detection", Computer Science Department, Columbia University, August 2005.
33. Gaurav S. Kc, "Defending Software Against Process-subversion Attacks", Computer Science Department, Columbia University, April 2005.
34. Gong Su, "MOVE: A New Virtualization Approach to Mobile Communication", Computer Science Department, Columbia University, May 2004.
35. Jonathan M. Lennox, "Services for Internet Telephony", Computer Science Department, Columbia University, December 2003.
36. Michael E. Kounavis, "Programming Network Architectures", Electrical Engineering Department, Columbia University, June 2003.
37. Wenyu Jiang, "QoS Measurement and Management for Internet Real-time Multimedia Services", Computer Science Department, Columbia University, April 2003.

Post-doctoral Students / Research Scientists

1. Hyung Chan Kim (October 2007 - October 2008)
2. Stelios Sidiroglou (October 2008 - December 2008)
3. Dimitris Geneiatakis (June 2010 - September 2011)
4. Georgios Portokalidis (March 2010 - December 2012)
5. Elias Athanasopoulos (January 2012 - November 2013)
6. Michalis Polychronakis (May 2010 - December 2014)
7. Yossef Oren (December 2013 - August 2015)
8. Iasonas Polakis (April 2014 - July 2016)
9. Dimitris Mitropoulos (September 2014 - July 2016)

Current Ph.D. Students (including co-advisees)

1. George Kokolakis (Georgia Tech; August 2022 - Present)
2. Matthew Pruett (Georgia Tech; August 2021 - Present)
3. Kevin Sam Tharayil (Georgia Tech; January 2021 - present)
4. Kostantinos Karakatsanis (Georgia Tech; August 2018 - present)
5. Athanasios Moschos (Georgia Tech; January 2020 - present)
6. Athanasios Avgetidis (Georgia Tech; January 2020 - present)

Graduated Ph.D. Students

18. Athanasios Kountouras (Georgia Institute of Technology; September 2018 - February 2023; co-advised with Manos Antonakakis)
 - o Thesis title: *"Improving Access to DNS Datasets Through the Large-scale Collection of Active-DNS Data"*
 - o Post-graduation: Big Data Lead Engineer, SOC, Georgia Institute of Technology
 - o Currently: Big Data Lead Engineer, Security Operations Center, Georgia Institute of Technology
17. Marios Pomonis (Columbia University; September 2012 - August 2019)
 - o Thesis title: *"Preventing Code Reuse Attacks On Modern Operating Systems"*
 - o Post-graduation: Security Software Engineer, Google
 - o Currently: Security Software Engineer, Google
16. Georgios Argyros (Columbia University; September 2012 - October 2018)
 - o Thesis title: *"Symbolic Model Learning: New Algorithms and Applications"*
 - o Post-graduation: Member of the Technical Staff, Amazon Web Services
 - o Currently: Member of the Technical Staff, Amazon Web Services
15. Suphannee Sivakorn (Columbia University; September 2013 - April 2018)
 - o Thesis title: *"Understanding Flaws in the Deployment and Implementation of Web Encryption"*
 - o Post-graduation: Member of the Technical Staff, Bloomberg
 - o Currently: Assistant Professor, Rajamangala University of Technology, Thailand
14. Theofilos Petsios (Columbia University; September 2012 - March 2018)
 - o Thesis title: *"Compiler-assisted Adaptive Software Testing"*
 - o Post-graduation: Research Scientist, Capsule8 Inc.
 - o Currently: Member of the Technical Staff, Amazon Web Services
13. Georgios Kontaxis (Columbia University; September 2011 - May 2017)
 - o Thesis title: *"Reducing Third Parties in the Network through Client-side Intelligence"*
 - o Post-graduation: Privacy Engineer, Apple Inc.
 - o Currently: Privacy Engineer, Apple Inc.
12. Vasileios Kemerlis (Columbia University; September 2008 - July 2015)
 - o Thesis title: *"Protecting Commodity Operating Systems through Strong Kernel Isolation"*
 - o Post-graduation: Assistant Professor, Department of Computer Science, Brown University
 - o Currently: Assistant Professor, Department of Computer Science, Brown University
11. Kangkook Jee (Columbia University; January 2008 - June 2015)
 - o Thesis title: *"On Efficiency and Accuracy of Data Flow Tracking Systems"*
 - o Post-graduation: Research Scientist, NEC Research Labs
 - o Currently: Assistant Professor, Department of Computer Science, University of Texas at Dallas
10. Vasilis Pappas (Columbia University; September 2009 - May 2014)
 - o Thesis title: *"Defending against Return-Oriented Programming"*
 - o Post-graduation: Senior Research Scientist, Apphorthy Inc.
 - o Currently: Symantec Corp.
9. Angelika Zavou (Columbia University; September 2006 - May 2014)
 - o Thesis title: *"Information Flow Auditing in the Cloud"*
 - o Post-graduation: Assistant Professor, Department of Computer Science, Hofstra University
 - o Currently: Security Automation Lead, Northwestern Mutual
8. Sambuddho Chakravarty (Columbia University; January 2007 - December 2013)
 - o Thesis title: *"Traffic Analysis Attacks and Defense in Low Latency Anonymous Communication"*
 - o Post-graduation: Assistant Professor, Department of Computer Science, IIT Delhi, India
 - o Currently: Associate Professor, Department of Computer Science, IIT Delhi, India
7. Brian Bowen (Columbia University; September 2007 - December 2010; co-advised with Salvatore J. Stolfo)
 - o Thesis title: *"Design and Analysis of Decoy Systems for Computer Security"*
 - o Post-graduation: Member of the Technical Staff, Sandia National Laboratories
 - o Currently: Dragos Inc.
6. Mansoor Alicherry (Columbia University; September 2006 - October 2010)
 - o Thesis title: *"A Distributed Policy Enforcement Architecture for Mobile Ad Hoc Networks"*
 - o Post-graduation: Member of the Technical Staff, Alcatel-Lucent Bell Labs
 - o Currently: VP of Engineering, Vizuri Interactive
5. Vanessa Frias-Martinez (Columbia University; September 2003 - October 2008; co-advised with Salvatore J. Stolfo)
 - o Thesis title: *"Behavior-Based Admission and Access Control for Network Security"*
 - o Post-graduation: Researcher, Telefonica Research
 - o Currently: Assistant Professor, University of Maryland
4. Stelios Sidiroglou (Columbia University; June 2003 - May 2008)
 - o Thesis title: *"Software Self-healing Using Error Virtualization"*
 - o Post-graduation: Research Scientist, Columbia University
 - o Currently: Research Scientist, MIT CSAIL
3. Michael E. Locasto (Columbia University; September 2002 - December 2007)
 - o Thesis title: *"Integrity Postures for Software Self-Defense"* (awarded with distinction)
 - o Post-graduation: ISTS Research Fellow, Dartmouth College
 - o Currently: SRI International
2. Angelos Stavrou (Columbia University; January 2003 - August 2007)
 - o Thesis title: *"An Overlay Architecture for End-to-End Service Availability"* (awarded with distinction)
 - o Post-graduation: Assistant Professor, Computer Science Department, George Mason University (GMU)
 - o Currently: Professor, Electrical and Computer Engineering Department, Virginia Institute of Technology (VT)
1. Debra Cook (Columbia University; January 2002 - June 2006)
 - o Thesis title: *"Elastic Block Ciphers"*
 - o Post-graduation: Member of the Technical Staff, Bell Labs
 - o Currently: Research Staff Member, Peraton Labs

Service at Georgia Tech

- School of Electrical and Computer Engineering Review, Promotion, and Tenure (RPT) Committee, 2023 - 2024.
- School of Electrical and Computer Engineering Recruiting Committee, 2018 - 2023.

Service at Columbia

- Computer Science Department Ph.D. Committee, 2010 - 2011
- Computer Science Department Computing Research Facilities Committee, 2001 - 2008, 2010 - 2013
 - Chair, 2003 - 2005, 2011 - 2013
- M.Sc. Admissions Committee, 2007 - 2013
- M.Sc. Committee, 2008 - 2013
- Computer Science Department Faculty Recruiting Committee, 2002, 2008, 2012
- 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 University response to the 9/11 events, Fall 2001

Teaching

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

- Instructor, ECE 4115 - Introduction to Computer Security, Georgia Tech
 - Spring 2023: 39 on-campus students
 - Fall 2022: 40 on-campus students
 - Spring 2022: 45 on-campus students
 - Fall 2021: 58 on-campus students
 - Spring 2021: 47 on-campus students
 - Spring 2020: 56 on-campus students
- 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
 - Fall 2012: 19 on-campus and 3 CVN students (4.64/5)
 - Spring 2012: 21 on-campus and 2 CVN students (4.33/5)
 - 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. co-PI (joint effort with Virginia Tech and University of Kentucky), "Collaborative Research: SaTC: CORE: Medium: An Anti-tracking and Robocall-free Architecture for Next-G Mobile Networks", NSF Secure and Trustworthy Computing (SaTC), **\$1,200,000** (Georgia Tech portion: \$299,731, 10/2023 - 09/2027)
2. co-PI (with Manos Antonakakis), "Antikythera: A Novel Framework to Assess, Statistically Model, and Evade Cyber Attack Infrastructure", DARPA SMOKE, **\$22,704,951** (09/2022 - 08/2025)
3. PI, "U.S. Open-Source Software Security Initiative Workshop", NSF, CNS-22-32616, **\$73,444** (07/2022 - 12/2022)
4. co-PI (with Charles Lever, Manos Antonakakis, and Robert Perdisci), "A Behavioral Engine for Detecting Network Abuse", DARPA CHASE, **\$1,767,684** (06/2021 - 05/2023)
5. co-PI (with Brendan Saltaformaggio), "KILLER ORCA", DARPA, **\$1,357,707** (10/2020 - 09/2023; part of a larger project)
6. co-PI (with Manos Antonakakis), "Programmable Infrastructure for CounterIng Pugnacious Adversaries on a Large Scale (PRINCIPALS)", DARPA OPS-5G, **\$7,292,076** (10/2020 - 09/2024)
7. co-PI (with Alenka Zajic and Milos Prvulovic), "Dormant Hardware Trojan Detection Using Back-Scattering Side Channels", ONR, **\$4,401,742** (03/2019 - 02/2022)
8. PI (with Sal Stolfo), "Trust Estimation System for Wireless Networks via Multi-Pronged Detection (TREND)", DARPA Wireless Network Defense (WND), **\$253,700** (10/2013 - 09/2014; part of a larger project)
9. co-PI (with Michalis Polychronakis), "TWC: Small: Virtual Private Social Networks", NSF Secure and Trustworthy Computing (SaTC), CNS-13-18415, **\$498,332** (09/2013 - 08/2016)
10. PI, "Runtime Program Behavior Monitoring Combining Control and Data Flow Tracking", Intel (research gift), **\$92,000** (06/2013)
11. PI, "REU: TWC: Small: Auditing PII in the Cloud with CloudFence", NSF Secure and Trustworthy Computing (SaTC), **\$15,600** (05/2013 - 08/2013)
12. PI, "Runtime Program Behavior Monitoring Combining Control and Data Flow Tracking", Intel (research gift), **\$92,000** (09/2012)
13. PI, "TWC: Small: Auditing PII in the Cloud with CloudFence", NSF Secure and Trustworthy Computing (SaTC), CNS-12-22748, **\$499,998** (09/2012 - 08/2015)
14. PI, "MINESTRONE Task: Automatic Discovery of Rescue Points Using Static and Dynamic Analysis", IARPA, **\$270,400** (09/2012 - 11/2014)
15. PI, "Vulnerability Protections for End Nodes (VPEN)", Air Force Research Labs (AFRL), **\$263,385** (08/2012 - 07/2013)
16. PI, "NSF Support for the 2012 New Security Paradigms Workshop Financial Aid", NSF Trustworthy Computing, **\$10,000** (07/2012 - 08/2013)
17. co-PI (with Junfeng Yang), "Transparently Extending Programs at Compilation to Prevent Bugs", ONR, **\$749,975** (07/2012 - 06/2015)
18. PI (co-PIs: Junfeng Yang, Sal Stolfo), "MINESTRONE, Phase 2 Extension", IARPA, **\$637,624** (08/2010 - 11/2014; leading team that includes Stanford University, George Mason University, and Symantec Corp.)
19. 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.)
20. co-PI (with Tal Malkin, Steve Bellovin, and Vladimir Kolesnikov), "Practical and Secure Database Access Using Encrypted Bloom Filters", IARPA, **\$2,236,144** (09/2011 - 03/2015)
21. PI, "NSF Support for the 2011 New Security Paradigms Workshop Financial Aid (Supplement)", NSF Trustworthy Computing, **\$10,000** (06/2011 - 07/2012)
22. PI, "Leveraging the Cloud to Audit Use of Sensitive Information", Google (research gift), **\$60,200** (05/2011)
23. co-PI (with Sal Stolfo), "ADAMS Advanced Behavioral Sensors (ABS)", DARPA ADAMS, **\$780,996** (05/2011 - 04/2013)
24. PI, "Tracking Sensitive Information Flows in Modern Enterprises", Intel, **\$84,951** (12/2010 - 12/2011)
25. 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)
26. PI, "NSF Support for the 2010 New Security Paradigms Workshop Financial Aid", NSF Trustworthy Computing, **\$10,000** (09/2010 - 08/2011)
27. 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.)
28. 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)
29. PI, "Tracking Sensitive Information Flows in Modern Enterprises", Intel, **\$82,286** (08/2009 - 07/2010)
30. PI, "Supplement for International Research Collaborations", NSF Trustworthy Computing, **\$41,769** (09/2009 - 08/2011)

31. PI, "NSF Support for the 2009 New Security Paradigms Workshop Financial Aid", NSF Trustworthy Computing, **\$10,000** (09/2009 - 08/2010)
32. PI, "Measuring the Health of Internet Routing: A Longitudinal Study", Google (research gift), **\$60,000** (07/2009)
33. PI, "CSR: Small: An Information Accountability Architecture for Distributed Enterprise Systems", NSF Trustworthy Computing, CNS-09-14312, **\$450,000** (07/2009 - 06/2012)
34. 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)
35. 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)
36. 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)
37. PI (co-PIs: Sal Stolfo), "Program Whitelisting, Vulnerability Analytics and Risk Assessment", Symantec (research gift), **\$65,000** (12/2008)
38. 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)
39. co-PI (with Steve Bellovin, Tal Malkin, and Sal Stolfo), "Secure Encrypted Search", IARPA, **\$648,787** (09/2008 - 02/2010)
40. PI, "Tracking Sensitive Information Flows in Modern Enterprises", Intel (research gift), **\$64,000** (05/2008)
41. PI, "Privacy and Search: Having it Both Ways in Web Services", Google (research gift), **\$50,000** (03/2008)
42. PI (co-PI: Sal Stolfo), "Continuation: Safe Browsing Through Web-based Application Communities", Google (research gift), **\$50,000** (03/2008)
43. 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)
44. PI, "Travel Supplement under the US/Japan Critical Infrastructure Protection Cooperation Program", NSF CyberTrust, **\$38,640** (09/2007 - 08/2009)
45. PI, "PacketSpread: Practical Network Capabilities", NSF CyberTrust, CNS-07-14277, **\$280,000** (09/2007 - 08/2010)
46. PI, "Integrated Enterprise Security Management", NSF CyberTrust, CNS-07-14647, **\$286,486** (08/2007 - 07/2009)
47. PI, "Safe Browsing Through Web-based Application Communities", NY State/Polytechnic CAT, **\$25,000** (06/2007 - 06/2009)
48. 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)
49. 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)
50. co-PI (with Sal Stolfo), "Human Behavior, Insider Threat, and Awareness", DHS/I3P, **\$616,442** (04/2007 - 03/2009)
51. PI (co-PI: Sal Stolfo), "Safe Browsing Through Web-based Application Communities", Google (research gift), **\$50,000** (01/2007)
52. 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)
53. PI, "Secure Overlay Services", NY State/Polytechnic CAT, **\$10,000** (09/2006 - 06/2007)
54. PI (co-PIs: Gail Kaiser, Sal Stolfo), "Enabling Collaborative Self-healing Software Systems", NSF CyberTrust, CNS-06-27473, **\$800,000** (09/2006 - 08/2010)
55. PI (co-PI: Sal Stolfo), "Behavior-based Access Control and Communication in MANETs", DARPA/IPTO, **\$100,000** (07/2006 - 06/2007)
56. co-PI (with Steve Bellovin and Sal Stolfo), "Large-Scale System Defense", DTO, **\$535,555** (07/2006 - 12/2007)
57. PI, "Active Decoys for Spyware", NY State/Polytechnic CAT, **\$25,000** (06/2006 - 12/2007)
58. 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)
59. co-PI (with Jason Nieh, Gail Kaiser), "Broadening Participation in Research", NSF BPC, **\$133,565** (09/2005 - 08/2006)
60. PI, "Secure Overlay Services", NY State/Polytechnic CAT, **\$12,500** (09/2005 - 06/2006)
61. co-PI (with Dan Rubenstein, Vishal Misra), "Secure Overlay Services", Intel Corp. (research gift), **\$75,000** (08/2005)
62. PI, "Snakeeyes", New York State Center for Advanced Technology, **\$14,999** (07/2005 - 06/2006)
63. PI, "Self-protecting Software", Columbia Science and Technology Ventures (research gift), **\$65,000** (06/2005 - 09/2005)
64. co-PI (with Gail Kaiser), "Trustworthy Computing Curriculum Development", Microsoft Research (research gift), **\$50,000** (12/2004 - 12/2005)
65. co-PI (with Jason Nieh, Gail Kaiser), "Secure Remote Computing Services", NSF ITR, CNS-04-26623, **\$1,200,000** (09/2004 - 08/2009)
66. PI, "Secure Overlay Services", NY State/Polytechnic CAT, **\$12,500** (09/2004 - 06/2005)
67. co-PI (with Dan Rubenstein, Vishal Misra), "Secure Overlay Services", Intel Corp. (research gift), **\$90,000** (06/2004)
68. co-PI (with Dan Rubenstein, Vishal Misra), "Secure Overlay Services", Intel Corp. (research gift), **\$120,000** (08/2003)
69. PI (co-PIs: Dan Rubenstein, Vishal Misra), "Secure Overlay Services", Cisco Corp. (research gift), **\$76,000** (07/2003)
70. co-PI (with Sal Stolfo, Tal Malkin, Vishal Misra), "Distributed Intrusion Detection Feasibility Study", Department of Defense, **\$300,000** (03/2003 - 03/2004)
71. PI, "STRONGMAN", DARPA/ATO, **\$23,782** (09/2002 - 08/2003; part of a larger project with the University of Pennsylvania)
72. PI, "POSSE", DARPA/ATO, **\$16,341** (09/2002 - 08/2003; part of a larger project with the University of Pennsylvania)
73. 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)
74. PI (co-PIs: Dan Rubenstein, Vishal Misra), "Secure Overlay Services", Cisco Corp. (research gift), **\$70,000** (07/2002)
75. PI (co-PIs: Dan Rubenstein, Vishal Misra), "Secure Overlay Services", DARPA/ATO, **\$695,000** (06/2002 - 05/2004)
76. PI, "Code Security Analysis Kit (CoSAK)", DARPA/ATO, **\$37,000** (07/2001 - 06/2003; part of a larger project with Drexel University)

- **Total:** \$78,656,824
- **Total as Principal Investigator (PI):** \$22,506,562

Publications

(Student co-authors/co-inventors are underlined.)

Patents

1. "Detecting return-oriented programming payloads by evaluating data for a gadget address space address and determining whether operations associated with instructions beginning at the address indicate a return-oriented programming payload"
Michalis Polychronakis and **Angelos D. Keromytis**. U.S. Patent 11,599,628. Issued on March 7, 2023.
2. "Methods, media, and systems for detecting an anomalous sequence of function calls"
Angelos D. Keromytis and Salvatore J. Stolfo. U.S. Patent 11,106,799. Issued on August 31, 2021.
3. "Methods, media, and systems for detecting attack on a digital processing device"
Salvatore J. Stolfo, Wei-Jen Li, **Angelos D. Keromytis**, and Elli Androulaki. U.S. Patent 10,902,111. Issued on January 26, 2021.
4. "Detecting network anomalies by probabilistic modeling of argument strings with markov chains"
Yingbo Song, **Angelos D. Keromytis**, and Salvatore J. Stolfo. U.S. Patent 10,819,726. Issued on October 27, 2020.
5. "Methods, media, and systems for detecting an anomalous sequence of function calls"
Angelos D. Keromytis, and Salvatore J. Stolfo. U.S. Patent 10,423,788. Issued on September 24, 2019.
6. "Methods, systems, and media for authenticating users using multiple services"
Angelos D. Keromytis, Elias Athanasopoulos, Georgios Kontaxis, and Georgios Portokalidis. U.S. Patent 10,367,797. Issued on July 30, 2019.
7. "Systems and methods for inhibiting attacks on applications"
Michael E. Locasto, Salvatore J. Stolfo, **Angelos D. Keromytis**, and Ke Wang. U.S. Patent 10,305,919. Issued on May 28, 2019.
8. "Diversified instruction set processing to enhance security"
Lakshminarasimhan Sethumadhavan, Kanad Sinha, **Angelos D. Keromytis**, Vasileios Pappas, and Vasileios Kemerlis. U.S. Patent 10,237,059. Issued on March 19, 2019.
9. "Detecting return-oriented programming payloads by evaluating data for a gadget address space address and determining whether operations associated with instructions beginning at the address indicate a return-oriented programming payload"
Michalis Polychronakis and **Angelos D. Keromytis**. U.S. Patent 10,192,049. Issued on January 29, 2019.
10. "Methods, media, and systems for detecting attack on a digital processing device"
Salvatore J. Stolfo, Wei-Jen Li, **Angelos D. Keromytis**, and Elli Androulaki. U.S. Patent 10,181,026. Issued on January 15, 2019.
11. "Systems, methods, and media for generating sanitized data, sanitizing anomaly detection models, and/or generating sanitized anomaly detection models"
Gabriela F. Ciocarlie, Angelos Stavrou, Salvatore J. Stolfo and **Angelos D. Keromytis**. U.S. Patent 10,178,113. Issued on January 8, 2019.
12. "Methods, media, and systems for securing communications between a first node and a second node"
Salvatore J. Stolfo, Gabriela F. Ciocarlie, Vanessa Frias-Martinez, Janak Parekh, **Angelos D. Keromytis**, and Joseph Sherrick. U.S. Patent 10,178,104. Issued on January 8, 2019.
13. "Detecting network anomalies by probabilistic modeling of argument strings with markov chains"
Yingbo Song, **Angelos D. Keromytis**, and Salvatore J. Stolfo. U.S. Patent 10,063,576. Issued on August 28, 2018.
14. "Systems and methods for correlating and distributing intrusion alert information among collaborating computer systems"
Salvatore J. Stolfo, Tal Malkin, **Angelos D. Keromytis**, Michael Locasto, and Janak Parekh. U.S. Patent 10,038,704. Issued on July 31, 2018.
15. "Systems and methods for inhibiting attacks with a network"
Angelos Stavrou and **Angelos D. Keromytis**. U.S. Patent 9,992,222. Issued on June 5, 2018.
16. "Methods, systems, and media for detecting covert malware"
Brian M. Bowen, Pratap V. Prabhu, Vasileios P. Kemerlis, Syvlanos Sidiropoulos, Salvatore J. Stolfo, and **Angelos D. Keromytis**. U.S. Patent 9,971,891. Issued on May 15, 2018.

17. "Methods, media, and systems for securing communications between a first node and a second node"
Salvatore J. Stolfo, Gabriela F. Ciocarlie, Vanessa Frias-Martinez, Janak Parekh, **Angelos D. Keromytis**, and Joseph Sherrick. U.S. Patent 9,654,478. Issued on May 16, 2017.
18. "Systems, methods, and media for testing software patches"
Angelos D. Keromytis and Sylianios Sidiroglou. U.S. Patent 9,606,906. Issued on March 28, 2017.
19. "Methods, media, and systems for detecting attack on a digital processing device"
Salvatore J. Stolfo, Wei-Jen Li, **Angelos D. Keromytis**, and Elli Androulaki. U.S. Patent 9,576,127. Issued on February 21, 2017.
20. "Systems, methods, and media protecting a digital data processing device from attack"
Sylianios Sidiroglou, **Angelos D. Keromytis**, and Salvatore J. Stolfo. U.S. Patent 9,544,322. Issued on January 10, 2017.
21. "Methods, systems, and media for baiting inside attackers"
Salvatore J. Stolfo, **Angelos D. Keromytis**, Brian M. Bowen, Shloma HersHKop, Vasileios P. Kemerlis, Pratap V. Prabhu, and Malek Ben Salem. U.S. Patent 9,501,639. Issued on November 22, 2016.
22. "Detecting return-oriented programming payloads by evaluating data for a gadget address space address and determining whether operations associated with instructions beginning at the address indicate a return-oriented programming payload"
Michalis Polychronakis and **Angelos D. Keromytis**. U.S. Patent 9,495,541. Issued on November 15, 2016.
23. "Methods, media, and systems for detecting an anomalous sequence of function calls"
Angelos D. Keromytis and Salvatore J. Stolfo. U.S. Patent 9,450,979. Issued on September 20, 2016.
24. "Methods, media, and systems for securing communications between a first node and a second node"
Salvatore J. Stolfo, Gabriela F. Ciocarlie, Vanessa Frias-Martinez, Janak Parekh, **Angelos D. Keromytis**, and Joseph Sherrick. U.S. Patent 9,419,981. Issued on August 16, 2016.
25. "Systems, methods, and media for generating bait information for trap-based defenses"
Angelos D. Keromytis and Salvatore J. Stolfo. U.S. Patent 9,356,957. Issued on May 31, 2016.
26. "Systems and methods for inhibiting attacks with a network"
Angelos Stavrou and **Angelos D. Keromytis**. U.S. Patent 9,344,418. Issued on May 17, 2016.
27. "Systems and methods for inhibiting attacks on applications"
Michael E. Locasto, Salvatore J. Stolfo, **Angelos D. Keromytis**, and Ke Wang. U.S. Patent 9,338,174. Issued on May 10, 2016.
28. "Detecting network anomalies by probabilistic modeling of argument strings with markov chains"
Yingbo Song, **Angelos D. Keromytis**, and Salvatore J. Stolfo. U.S. Patent 9,253,201. Issued on February 2, 2016.
29. "Systems, methods, and media for recovering an application from a fault or attack"
Michael E. Locasto, **Angelos D. Keromytis**, Angelos Stavrou, and Gabriela F. Ciocarlie. U.S. Patent 9,218,254. Issued on December 22, 2015.
30. "Systems, methods, and media protecting a digital data processing device from attack"
Sylianios Sidiroglou, **Angelos D. Keromytis**, and Salvatore J. Stolfo. U.S. Patent 9,143,518. Issued on September 22, 2015.
31. "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 9,135,438. Issued on September 15, 2015.
32. "Systems, methods, and media for generating sanitized data, sanitizing anomaly detection models, and/or generating sanitized anomaly detection models"
Gabriela F. Ciocarlie, Angelos Stavrou, Salvatore J. Stolfo and **Angelos D. Keromytis**. U.S. Patent 9,088,596. Issued on July 21, 2015.
33. "Methods, systems, and media for baiting inside attackers"
Salvatore J. Stolfo, **Angelos D. Keromytis**, Brian M. Bowen, Shloma HersHKop, Vasileios P. Kemerlis, Pratap V. Prabhu, and Malek Ben Salem. U.S. Patent 9,009,829. Issued on April 14, 2015.
34. "Systems, methods, and media for recovering an application from a fault or attack"
Michael E. Locasto, **Angelos D. Keromytis**, Angelos Stavrou, and Gabriela F. Ciocarlie. U.S. Patent 8,924,782. Issued on December 30, 2014.
35. "Systems, methods, and media for detecting network anomalies using a trained probabilistic model"
Yingbo Song, **Angelos D. Keromytis**, and Salvatore J. Stolfo. U.S. Patent 8,844,033. Issued on September 23, 2014.
36. "Systems, methods, and media for generating bait information for trap-based defenses"
Angelos D. Keromytis and Salvatore J. Stolfo. U.S. Patent 8,819,825. Issued on August 26, 2014.
37. "Systems and methods for inhibiting attacks on applications"
Michael E. Locasto, Salvatore J. Stolfo, **Angelos D. Keromytis**, and Ke Wang. U.S. Patent Number 8,763,103. Issued on June 24, 2014.
38. "Methods, media, and systems for detecting an anomalous sequence of function calls"
Angelos D. Keromytis and Salvatore J. Stolfo. U.S. Patent 8,694,833. Issued on April 8, 2014.
39. "Systems, methods, and media for testing software patches"
Angelos D. Keromytis and Sylianios Sidiroglou. U.S. Patent Number 8,683,450. Issued on March 25, 2014.
40. "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 8,667,588. Issued on March 4, 2014.
41. "Systems and methods for inhibiting attacks with a network"
Angelos Stavrou and **Angelos D. Keromytis**. U.S. Patent 8,631,484. Issued on January 14, 2014.
42. "Methods, media and systems for detecting anomalous program executions"
Salvatore J. Stolfo, **Angelos D. Keromytis**, and Sylianios Sidiroglou. U.S. Patent 8,601,322. Issued on December 3, 2013.
43. "Methods, media and systems for responding to a denial of service attack"
Angelos Stavrou, **Angelos D. Keromytis**, Jason Nieh, Vishal Misra, and Daniel Rubenstein. U.S. Patent 8,549,646. Issued on October 1, 2013.
44. "Methods, systems, and media for detecting covert malware"
Brian M. Bowen, Pratap V. Prabhu, Vasileios P. Kemerlis, Sylianios Sidiroglou, Salvatore J. Stolfo, and **Angelos D. Keromytis**. U.S. Patent 8,528,091. Issued on September 3, 2013.
45. "Systems, methods, and media for enforcing a security policy in a network including a plurality of components"
Matthew Burnside and **Angelos D. Keromytis**. U.S. Patent 8,516,575. Issued on August 20, 2013.
46. "Methods, media, and systems for detecting an anomalous sequence of function calls"
Angelos D. Keromytis and Salvatore J. Stolfo. U.S. Patent 8,489,931. Issued on July 16, 2013.
47. "Systems, methods, and media protecting a digital data processing device from attack"
Sylianios Sidiroglou, **Angelos D. Keromytis**, and Salvatore J. Stolfo. U.S. Patent 8,407,785. Issued on March 26, 2013.
48. "Systems, methods, and media for generating sanitized data, sanitizing anomaly detection models, and/or generating sanitized anomaly detection models"
Gabriela Cretu, Angelos Stavrou, Salvatore J. Stolfo, **Angelos D. Keromytis**, and Michael E. Locasto. U.S. Patent Number 8,407,160. Issued on March 26, 2013.
49. "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 8,381,295. Issued on February 19, 2013.
50. "Systems and methods for computing data transmission characteristics of a network path based on single-ended measurements"
Angelos D. Keromytis, Sambuddho Chakravarthy, and Angelos Stavrou. U.S. Patent 8,228,815. Issued on July 24, 2012.
51. "Methods, media, and systems for detecting an anomalous sequence of function calls"
Angelos D. Keromytis and Salvatore J. Stolfo. U.S. Patent 8,135,994. Issued on March 13, 2012.
52. "Methods, media and systems for detecting anomalous program executions"
Salvatore J. Stolfo, **Angelos D. Keromytis**, and Stelios Sidiroglou. U.S. Patent 8,074,115. Issued on December 6, 2011.
53. "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 9, 2011.
54. "Methods, systems and media for software self-healing"

- Michael E. Locasto*, **Angelos D. Keromytis**, Salvatore J. Stolfo, *Angelos Stavrou*, *Gabriela Cretu*, *Strylianos Sidiroglou*, Jason Nieh, and *Oren Lauadan*. U.S. Patent Number 7,962,798. Issued on June 14, 2011.
55. "Systems and methods for detecting and inhibiting attacks using honeypots"
Strylianos Sidiroglou, **Angelos D. Keromytis**, and Kostas G. Anagnostakis. U.S. Patent 7,904,959. Issued on March 8, 2011.
 56. "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 24, 2010.
 57. "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 17, 2010.
 58. "Systems and methods for computing data transmission characteristics of a network path based on single-ended measurements"
Angelos D. Keromytis, *Sambuddha Chakravarty*, and *Angelos Stavrou*. U.S. Patent 7,660,261. Issued on February 9, 2010.
 59. "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 19, 2010.
 60. "Methods and systems for repairing applications"
Angelos D. Keromytis, *Michael E. Locasto*, and *Strylianos Sidiroglou*. U.S. Patent 7,490,268. Issued on February 10, 2009.
 61. "System and method for microbilling using a trust management system"
Matthew A. Blaze, John Ioannidis, and **Angelos D. Keromytis**. U.S. Patent 6,789,068. Issued on September 7, 2004.
 62. "Secure and reliable bootstrap architecture"
William A. Arbaugh, David J. Farber, **Angelos D. Keromytis**, and Jonathan M. Smith. U.S. Patent 6,185,678. Issued on February 6, 2001.

Journal Publications

1. "Defending Against Web Application Attacks: Approaches, Challenges and Implications"
Dimitris Mitropoulos, **Angelos D. Keromytis**, Panagiotis Louridas, and Michalis Polychronakis. In *IEEE Transactions on Dependable and Secure Computing (TDSC)*, vol. 5, no. 2, pp. 188 - 203, March/April 2019.
2. "Kernel Protection against Just-In-Time Code Reuse"
Marios Pomonis, *Theofilos Petsios*, **Angelos D. Keromytis**, Michalis Polychronakis, and Vasileios P. Kemerlis. In *ACM Transactions on Privacy and Security (TOPS)*, vol. 22, no. 1, January 2018.
3. "Evaluating the Privacy Guarantees of Location Proximity Services"
George Argyros, *Theofilos Petsios*, *Suphannee Sivakorn*, **Angelos D. Keromytis**, and *Iasonas Polakis*. In *ACM Transactions on Privacy and Security (TOPS)*, vol. 19, no. 4, pp. 12:1 - 12:31, February 2017.
4. "How to Train your Browser: Preventing XSS Attacks Using Contextual Script Fingerprints"
Dimitris Mitropoulos, Konstantinos Stroggiolos, Diomidis Spinellis, and **Angelos D. Keromytis**. In *ACM Transactions on Privacy and Security (TOPS)*, vol. 19, no. 1, pp. 2:1 - 2:31, July 2016.
5. "A Stack Memory Abstraction and Symbolic Analysis Framework for Executables"
Kapil Anand, *Khaled Elwazeer*, *Matthew Smithson*, Rajeev Barua, and **Angelos D. Keromytis**. In *ACM Transactions on Software Engineering and Methodology (TOSEM)*, vol. 25, no. 2, pp. 19:1 - 19:38, May 2016.
6. "An efficient and easily deployable method for dealing with DoS in SIP services"
Zisis Tsiatsikas, Dimitris Geneiatakis, Georgios Kambourakis, and **Angelos D. Keromytis**. In the *Journal of Computer Communications*, vol. 57, pp. 50 - 63, 2015.
7. "Detection and Analysis of Eavesdropping in Anonymous Communication Networks"
Sambuddha Chakravarty, Michalis Polychronakis, Georgios Portokalidis, and **Angelos D. Keromytis**. In the *International Journal of Information Security (IJIS)*, vol. 14, no. 3, pp. 205 - 220, June 2015.
8. "Attacking the Internet using Broadcast Digital Television"
Yusef Oren and **Angelos D. Keromytis**. In the *ACM Transactions on Information and Systems Security (TISSEC)*, vol. 17, no. 4, April 2015.
9. "Privacy Policy-driven Mashups"
Soon Ae Chun, Janice Warner, and **Angelos D. Keromytis**. In the *International Journal of Business Continuity and Risk Management (IJBCRM)*, vol. 4, no. 4, pp. 344 - 370, 2013.
10. "kGuard: Lightweight Kernel Protection"
Vasileios P. Kemerlis, *Georgios Portokalidis*, *Elias Athanasopoulos*, and **Angelos D. Keromytis**. In the *USENIX ;login: Magazine*, vol. 37, no. 6, pp. 7 - 14, December 2012.
11. "A System for Generating and Injecting Indistinguishable Network Decoys"
Brian M. Bowen, *Vasileios P. Kemerlis*, *Pratap Prabhu*, **Angelos D. Keromytis**, and Salvatore J. Stolfo. In the *Journal of Computer Security (JCS)*, vol. 20, no. 2 - 3, pp. 199 - 221, June 2012.
12. "A Comprehensive Survey of Voice over IP Security Research"
Angelos D. Keromytis. In the *IEEE Communications Surveys and Tutorials*, vol. 14, no. 2, pp. 514 - 537, May 2012.
13. "The Efficient Dual Receiver Cryptosystem and Its Applications"
Ted Diamant, *Homin K. Lee*, **Angelos D. Keromytis**, and Moti Yung. In the *International Journal of Network Security (IJNS)*, vol. 13, no. 3, pp. 135 - 151, November 2011.
14. "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 the *Machine Learning Journal (MLJ)*, vol. 81, no. 2, pp. 179 - 205, November 2010.
15. "On The General Applicability of Instruction-Set Randomization"
Stephen W. Boyd, *Gaurav S. Kc*, *Michael E. Locasto*, **Angelos D. Keromytis**, and Vassilis Prevelakis. In the *IEEE Transactions on Dependable and Secure Computing (TDSC)*, vol. 7, no. 3, pp. 255 - 270, July - September 2010.
16. "Shadow Honeypots"
Michalis Polychronakis, *Periklis Akrkitidis*, Stelios Sidiroglou, Kostas G. Anagnostakis, **Angelos D. Keromytis**, and Evangelos P. Markatos. In the *International Journal of Computer and Network Security (IJCNS)*, vol. 2, no. 9, pp. 1 - 15, September 2010.
17. "Ethics in Security Vulnerability Research"
Andrea M. Matwyshyn, *Ang Cui*, Salvatore J. Stolfo, and **Angelos D. Keromytis**. In the *IEEE Security & Privacy Magazine*, vol. 8, no. 2, pp. 67 - 72, March/April 2010.
18. "Voice over IP Security: Research and Practice"
Angelos D. Keromytis. In the *IEEE Security & Privacy Magazine*, vol. 8, no. 2, pp. 76 - 78, March/April 2010.
19. "A Market-based Bandwidth Charging Framework"
David Michael Turner, Vassilis Prevelakis, and **Angelos D. Keromytis**. In the *ACM Transactions on Internet Technology (ToIT)*, vol. 10, no. 1, pp. 1 - 30, February 2010.
20. "A Look at VoIP Vulnerabilities"
Angelos D. Keromytis. In the *USENIX ;login: Magazine*, vol. 35, no. 1, pp. 41 - 50, February 2010.
21. "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 the *IEEE Security & Privacy Magazine*, vol. 7, no. 6, pp. 22 - 29, November/December 2009.
22. "Elastic Block Ciphers: Method, Security and Instantiations"
Debra L. Cook, Moti Yung, and **Angelos D. Keromytis**. In the *Springer International Journal of Information Security (IJIS)*, vol. 8, no. 3, pp. 211 - 231, June 2009.
23. "On the Deployment of Dynamic Taint Analysis for Application Communities"
Hyung Chan Kim and **Angelos D. Keromytis**. In the *IEICE Transactions*, vol. E92-D, no. 3, pp. 548 - 551, March 2009.
24. "Dynamic Trust Management"
Matt Blaze, Sampath Kannan, Insup Lee, Oleg Sokolsky, Jonathan M. Smith, **Angelos D. Keromytis**, and Wenke Lee. In the *IEEE Computer Magazine*, vol. 42, no. 2, pp. 44 - 52, February 2009.
25. "Randomized Instruction Sets and Runtime Environments: Past Research and Future Directions"
Angelos D. Keromytis. In the *IEEE Security & Privacy Magazine*, vol. 7, no. 1, pp. 18 - 25, January/February 2009.
26. "Anonymity in Wireless Broadcast Networks"
Matt Blaze, John Ioannidis, **Angelos D. Keromytis**, Tal Malkin, and Avi Rubin. In the *International Journal of Network Security (IJNS)*, vol. 8, no. 1, pp. 37 - 51, January 2009.
27. "Decentralized Access Control in Networked File Systems"
Stefan Mitchev, Jonathan M. Smith, Vassilis Prevelakis, **Angelos D. Keromytis**, and Sotiris Ioannidis. In the *ACM Computing Surveys*, vol. 40, no. 3, pp. 10:1 - 10:30, August 2008.
28. "Robust Reactions to Potential Day-Zero Worms through Cooperation and Validation"

- Kostas G. Anagnostakis, Michael Greenwald, Sotiris Ioannidis, and **Angelos D. Keromytis**. In the *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.)
29. **"Requirements for Scalable Access Control and Security Management Architectures"**
Angelos D. Keromytis and Jonathan M. Smith. In the *ACM Transactions on Internet Technology (ToIT)*, vol. 7, no. 2, pp. 1 - 22, May 2007.
 30. **"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 the *International Journal of Network Security (IJNS)*, vol. 4, no. 1, pp. 69 - 80, January 2007.
 31. **"Countering DDos Attacks with Multi-path Overlay Networks"**
Angelos Stavrou and **Angelos D. Keromytis**. In the *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.)
 32. **"Conversion Functions for Symmetric Key Ciphers"**
Debra L. Cook and **Angelos D. Keromytis**. In the *Journal of Information Assurance and Security (JIAS)*, vol. 1, no. 2, pp. 119 - 128, June 2006. (Extended version of the IAS 2005 paper.)
 33. **"Execution Transactions for Defending Against Software Failures: Use and Evaluation"**
Stelios Sidiroglou and **Angelos D. Keromytis**. In the *Springer International Journal of Information Security (IJIS)*, vol. 5, no. 2, pp. 77 - 91, April 2006. (Extended version of the ISC 2005 paper.)
 34. **"Worm Propagation Strategies in an IPv6 Internet"**
Steven M. Bellovin, Bill Cheswick, and **Angelos D. Keromytis**. In the *USENIX ;login*, vol. 31, no. 1, pp. 70 - 76, February 2006.
 35. **"Cryptology As An Operating System Service: A Case Study"**
Angelos D. Keromytis, Theo de Raadt, Jason Wright, and Matthew Burnside. In the *ACM Transactions on Computer Systems (ToCS)*, vol. 24, no. 1, pp. 1 - 38, February 2006. (Extended version of USENIX Technical 2003 paper.)
 36. **"Countering Network Worms Through Automatic Patch Generation"**
Stelios Sidiroglou and **Angelos D. Keromytis**. In the *IEEE Security & Privacy Magazine*, vol. 3, no. 6, pp. 41 - 49, November/December 2005.
 37. **"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 the *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.)
 38. **"Hardware Support For Self-Healing Software Services"**
Stelios Sidiroglou, Michael E. Locasto, and **Angelos D. Keromytis**. In the *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.
 39. **"The Case For Crypto Protocol Awareness Inside The OS Kernel"**
Matthew Burnside and **Angelos D. Keromytis**. In the *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.
 40. **"Patch-on-Demand Saves Even More Time?"**
Angelos D. Keromytis. In the *IEEE Computer*, vol. 37, no. 8, pp. 94 - 96, August 2004.
 41. **"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 the *ACM Transactions on Information and System Security (TISSEC)*, vol. 7, no. 2, pp. 1 - 32, May 2004. (Extended version of the CCS 2002 paper.)
 42. **"SOS: An Architecture for Mitigating DDos Attacks"**
Angelos D. Keromytis, Vishal Misra, and Dan Rubenstein. In the *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.)
 43. **"A Secure PLAN"**
Michael Hicks, **Angelos D. Keromytis**, and Jonathan M. Smith. In the *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.)
 44. **"Drop-in Security for Distributed and Portable Computing Elements"**
Vassilis Prevelakis and **Angelos D. Keromytis**. In the *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.)
 45. **"Trust Management for IPsec"**
Matt Blaze, John Ioannidis, and **Angelos D. Keromytis**. In the *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 2, pp. 1 - 24, May 2002. (Extended version of the NDSS 2001 paper.)
 46. **"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 the *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*.
 47. **"Secure Quality of Service Handling (SQoSH)"**
D. Scott Alexander, William A. Arbaugh, **Angelos D. Keromytis**, Steve Muir, and Jonathan M. Smith. In the *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*.
 48. **"Safety and Security of Programmable Network Infrastructures"**
D. Scott Alexander, William A. Arbaugh, **Angelos D. Keromytis**, and Jonathan M. Smith. In the *IEEE Communications Magazine, issue on Programmable Networks*, vol. 36, no. 10, pp. 84 - 92, October 1998.
 49. **"A Secure Active Network Environment Architecture"**
D. Scott Alexander, William A. Arbaugh, **Angelos D. Keromytis**, and Jonathan M. Smith. In the *IEEE Network Magazine, special issue on Active and Controllable Networks*, vol. 12, no. 3, pp. 37 - 45, May/June 1998.
 50. **"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 the *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. **"UCBlocker: Unwanted Call Blocking Using Anonymous Authentication"**
Changlai Du, Hexuan Yu, Y. Thomas Hou, **Angelos D. Keromytis**, and Wenjing Lou. In Proceedings of the **32nd USENIX Security Symposium**. August 2023, Anaheim, CA.
2. **"Beyond The Gates: An Empirical Analysis of HTTP-Managed Password Stealers and Operators"**
Athanasios Avgetidis, Omar Alrawi, Kevin Valakuly, Charles Lever, Paul Burbage, **Angelos D. Keromytis**, Fabian Monrose, and Manos Antonakakis. In Proceedings of the **32nd USENIX Security Symposium**. August 2023, Anaheim, CA.
3. **"View from Above: Exploring the Malware Ecosystem from the Upper DNS Hierarchy"**
Aaron Faulkenberry, Athanasios Avgetidis, Zane Ma, Omar Alrawi, Charles Lever, Panagiotis Kintis, Fabian Monrose, **Angelos D. Keromytis**, and Manos Antonakakis. In Proceedings of the **38th Annual Computer Security Applications Conference (ACSAC)**. December 2022, Austin, TX. (Acceptance rate: 24%)
4. **"On the Feasibility of Remotely Triggered Automotive Hardware Trojans"**
Athanasios Moschos, Kevin Valakuly, and **Angelos D. Keromytis**. In Proceedings of the **2nd International Conference on Electrical, Computer, Communications, and Mechatronics Engineering (ICECCME)**. November 2022, Male, Maldives.
5. **"HammerScope: Observing DRAM Power Consumption Using Rowhammer"**
Yaakov Cohen, Kevin Sam Tharavil, Arie Haenel, Daniel Genkin, **Angelos D. Keromytis**, Yossi Oren, and Yuval Yarom. In Proceedings of the **29th ACM Conference on Computer and Communications Security (CCS)**. November 2022, Los Angeles, CA.
6. **"Privacy in E-Shopping Transactions: Exploring and Addressing the Trade-Offs"**

Jesus Diaz, Seung Geol Choi, David Arroyo, **Angelos D. Keromytis**, Francisco B. Rodriguez, and Moti Yung. In Proceedings of the 2nd International Symposium on Cyber Security Cryptography and Machine Learning (CSCML), pp. 206 - 226. June 2018, Be'er Sheva, Israel.

7. *"SlowFuzz: Automated Domain-Independent Detection of Algorithmic Complexity Vulnerabilities"*
Theofilos Petsios, Jason Zhao, **Angelos D. Keromytis**, and Suman Jana. In Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS), pp. 2155 - 2168. October/November 2017, Dallas, TX. (Acceptance rate: 18%)
8. *"HVLearn: Automated Black-box Analysis of Hostname Verification in SSL/TLS Implementations"*
Suphanee Sivakorn, George Argyros, Kevin Pei, **Angelos D. Keromytis**, and Suman Jana. In Proceedings of the 38th IEEE Symposium on Security and Privacy (S&P), pp. 521 - 538. May 2017, San Jose, CA. (Acceptance rate: 13.3%)
9. *"NEZHA: Efficient Domain-independent Differential Testing"*
Theofilos Petsios, Adrian Tang, Salvatore J. Stolfo, **Angelos D. Keromytis**, and Suman Jana. In Proceedings of the 38th IEEE Symposium on Security and Privacy (S&P), pp. 615 - 632. May 2017, San Jose, CA. (Acceptance rate: 13.3%)
10. *"kRAX: Comprehensive Kernel Protection against Just-In-Time Code Reuse"*
Marios Pomonis, Theofilos Petsios, **Angelos D. Keromytis**, Michalis Polychronakis, and Vasileios P. Kemerlis. In Proceedings of the 12th European Conference on Computer Systems (EuroSys), pp. 420 - 436. April 2017, Belgrade, Serbia.
11. *"Protecting Insecure Communications with Topology-aware Network Tunnels"*
Georgios Kontaxis and **Angelos D. Keromytis**. In Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS), pp. 1280 - 1291. October 2016, Vienna, Austria. (Acceptance rate: 16%)
12. *"SFADiff: Automated Evasion Attacks and Fingerprinting Using Blackbox Differential Automata Learning"*
George Argyros, Ioannis Stais, Suman Jana, **Angelos D. Keromytis**, and Aggelos Kiayias. In Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS), pp. 1690 - 1701. October 2016, Vienna, Austria. (Acceptance rate: 16%)
13. *"Provable Network Activity for Protecting Users against False Accusation"*
Panagiotis Papadopoulos, Elias Athanasopoulos, Eleni Kosta, George Siganos, **Angelos D. Keromytis**, and Evangelos P. Markatos. In Proceedings of the 10th WISTP Conference in Information Security Theory and Practice (WISTP), pp. 254 - 261. September 2016, Heraklion, Crete, Greece.
14. *"NaCIDroid: Native Code Isolation for Android Applications"*
Elias Athanasopoulos, Vasileios P. Kemerlis, Georgios Portokalidis, and **Angelos D. Keromytis**. In Proceedings of the 21st European Symposium on Research in Computer Security (ESORICS), pp. 422 - 439. September 2016, Heraklion, Crete, Greece. (Acceptance rate: 21%)
15. *"The Cracked Cookie Jar: HTTP Cookie Hijacking and the Exposure of Private Information"*
Iasonas Polakis, Suphanee Sivakorn, and **Angelos D. Keromytis**. In Proceedings of the 37th IEEE Symposium on Security and Privacy (S&P), pp. 724 - 742 May 2016, San Jose, CA. (Acceptance rate: 13.75%)
16. *"Back in Black: Towards Formal, Black Box Analysis of Sanitizers and Filters"*
George Argyros, Ioannis Stais, **Angelos D. Keromytis**, and Aggelos Kiayias. In Proceedings of the 37th IEEE Symposium on Security and Privacy (S&P), pp. 91 - 109. May 2016, San Jose, CA. (Acceptance rate: 13.75%)
17. *"I am Robot: (Deep) Learning to Break Semantic Image CAPTCHAs"*
Suphanee Sivakorn, Iasonas Polakis, and **Angelos D. Keromytis**. In Proceedings of the 1st IEEE European Symposium on Security and Privacy (EuroS&P), pp. 388 - 403. March 2016, Saarbrücken, Germany. (Acceptance rate: 17.3%)
18. *"DynaGuard: Armoring Canary-based Protections against Brute-force Attacks"*
Theofilos Petsios, Vasileios P. Kemerlis, Michalis Polychronakis, and **Angelos D. Keromytis**. In Proceedings of the 31st Annual Computer Security Applications Conference (ACSAC), pp. 351 - 360. December 2015, Los Angeles, CA. (Acceptance rate: 24.4%)
19. *"The Spy in the Sandbox: Practical Cache Attacks in Javascript and their Implications"*
Yossef Oren, Vasileios P. Kemerlis, **Angelos D. Keromytis**, and Simha Sethumadhavan. In Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS), pp. 1406 - 1418. October 2015, Denver, CO. (Acceptance rate: 19.8%)
20. *"Where's Wally? Precise User Discovery Attacks in Location Proximity Services"*
Iasonas Polakis, Georgios Argyros, Theofilos Petsios, Suphanee Sivakorn, and **Angelos D. Keromytis**. In Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS), pp. 817 - 828. October 2015, Denver, CO. (Acceptance rate: 19.8%)
21. *"IntFlow: Improving the Accuracy of Arithmetic Error Detection Using Information Flow Tracking"*
Kangkook Lee, Theofilos Petsios, Marios Pomonis, Michalis Polychronakis, and **Angelos D. Keromytis**. In Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC), pp. 416 - 425. December 2014, New Orleans, LA. (Acceptance rate: 19.9%)
22. *"Faces in the Distorting Mirror: Revisiting Photo-based Social Authentication"*
Iasonas Polakis, Panagiotis Ilija, Federico Maggi, Marco Lancini, Georgios Kontaxis, Stefano Zanero, Sotiris Ioannidis, and **Angelos D. Keromytis**. In Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS), pp. 501 - 512. November 2014, Scottsdale, AZ. (Acceptance rate: 19.5%)
23. *"Dynamic Reconstruction of Relocation Information for Stripped Binaries"*
Vasilis Pappas, Michalis Polychronakis, and **Angelos D. Keromytis**. In Proceedings of the 17th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), pp. 68 - 87. September 2014, Gothenburg, Sweden. (Acceptance rate: 19.5%)
24. *"ret2dir: Rethinking Kernel Isolation"*
Vasileios P. Kemerlis, Michalis Polychronakis, and **Angelos D. Keromytis**. In Proceedings of the 23rd USENIX Security Symposium, pp. 957 - 972. August 2014, San Diego, CA. (Acceptance rate: 19%)
25. *"From the Aether to the Ethernet - Attacking the Internet using Broadcast Digital Television"*
Yossef Oren and **Angelos D. Keromytis**. In Proceedings of the 23rd USENIX Security Symposium, pp. 353 - 368. August 2014, San Diego, CA. (Acceptance rate: 19%)
26. *"Blind Seer: A Scalable Private DBMS"*
Vasilis Pappas, Fernando Krell, Binh Vo, Vladimir Kolesnikov, Tal Malkin, Seung Geol Choi, Wesley George, **Angelos D. Keromytis**, and Steven M. Bellovin. In Proceedings of the 35th IEEE Symposium on Security & Privacy (S&P), pp. 359 - 374. May 2014, San Jose, CA. (Acceptance rate: 13.5%)
27. *"On the Effectiveness of Traffic Analysis Against Anonymity Networks Using Flow Records"*
Sambuddho Chakravarty, Marco V. Barbera, Georgios Portokalidis, Michalis Polychronakis, and **Angelos D. Keromytis**. In Proceedings of the 15th Passive and Active Measurement Conference (PAM), pp. 247 - 254. March 2014, Los Angeles, CA. (Acceptance rate: 31.5%)
28. *"SAuth: Protecting User Accounts from Password Database Leaks"*
George Kontaxis, Elias Athanasopoulos, Georgios Portokalidis, and **Angelos D. Keromytis**. In Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS), pp. 187 - 198. November 2013, Berlin, Germany. (Acceptance rate: 19.8%)
29. *"ShadowReplica: Efficient Parallelization of Dynamic Data Flow Tracking"*
Kangkook Lee, Vasileios P. Kemerlis, **Angelos D. Keromytis**, and Georgios Portokalidis. In Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS), pp. 235 - 246. November 2013, Berlin, Germany. (Acceptance rate: 19.8%)
30. *"CloudFence: Data Flow Tracking as a Cloud Service"*
Vasilis Pappas, Vasileios P. Kemerlis, Angeliki Zavou, Michalis Polychronakis, and **Angelos D. Keromytis**. In Proceedings of the 16th International Symposium on Recent Advances in Intrusion Detection (RAID), pp. 411 - 431. October 2013, Saint Lucia. (Acceptance rate: 23%)
31. *"An Accurate Stack Memory Abstraction and Symbolic Analysis Framework for Executables"*
Kapil Anand, Khaled Elwaeer, Aparna Kothe, Matthew Smithson, Rajeev Barua, and **Angelos D. Keromytis**. In Proceedings of the 29th IEEE International Conference on Software Maintenance (ICSM), pp. 90 - 99. September 2013, Eindhoven, Netherlands. (Acceptance rate: 22%)
32. *"CellFlood: Attacking Tor Onion Routers on the Cheap"*
Marco Valerio Barbera, Vasileios P. Kemerlis, Vasilis Pappas, and **Angelos D. Keromytis**. In Proceedings of the 18th European Symposium on Research in Computer Security (ESORICS), pp. 664 - 681. September 2013, Egham, UK. (Acceptance rate: 18%)
33. *"A Privacy-Preserving Entropy-Driven Framework for Tracing DoS Attacks in VoIP"*

- Zisis Tsitsikas, Dimitris Geneiatakis, Georgios Kambourakis, and Angelos D. Keromytis. In Proceedings of the 8th International Conference on Availability, Reliability and Security (ARES), pp. 224 - 229. September 2013, Regensburg, Germany.
34. **"Transparent ROP Exploit Mitigation using Indirect Branch Tracing"**
Vasilis Pappas, Michalis Polychronakis, and **Angelos D. Keromytis**. In Proceedings of the 22nd USENIX Security Symposium, pp. 447 - 462. August 2013, Washington, DC. (Acceptance rate: 16.2%)
 35. **"Cloudopsy: an Autopsy of Data Flows in the Cloud"**
Angeliki Zavou, Vasilis Pappas, Vasileios P. Kemerlis, Michalis Polychronakis, Georgios Portokalidis, and **Angelos D. Keromytis**. In Proceedings of the 15th International Conference on Human-Computer Interaction (HCI), pp. 366 - 375. July 2013, Las Vegas, NV.
 36. **"SecureGov: Secure Government Data Sharing"**
Jong Uk Choi, Soon Ae Chun, Dong Hwa Kim, and **Angelos D. Keromytis**. In Proceedings of the 14th Annual International Conference on Digital Government Research (dg.o), pp. 127 - 135. June 2013, Quebec City, Canada.
 37. **"Bait and Snitch: Defending Computer Systems with Decoys"**
Jonathan Voris, Jill Jermyn, **Angelos D. Keromytis**, and Salvatore J. Stolfo. In Proceedings (electronic) of the Cyber Infrastructure Protection (CIP) Conference. September 2012, New York, NY. (Invited paper)
 38. **"All Your Face Are Belong to Us: Breaking Facebook's Social Authentication"**
Iasonas Polakis, Marco Lancini, George Kontaxis, Federico Maggi, Sotiris Ioannidis, **Angelos D. Keromytis**, and Stefano Zanero. In Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC), pp. 399 - 408. December 2012, Orlando, FL. (Acceptance rate: 19%)
 39. **"Self-healing Multitier Architectures Using Cascading Rescue Points"**
Angelika Zavou, Georgios Portokalidis, and **Angelos D. Keromytis**. In Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC), pp. 379 - 388. December 2012, Orlando, FL. (Acceptance rate: 19%)
 40. **"Adaptive Defenses for Commodity Software Through Virtual Application Partitioning"**
Dimitris Geneiatakis, Georgios Portokalidis, Vasileios P. Kemerlis, and **Angelos D. Keromytis**. In Proceedings of the 19th ACM Conference on Computer and Communications Security (CCS), pp. 133 - 144. October 2012, Raleigh, NC. (Acceptance rate: 18.9%)
 41. **"Privacy-Preserving Social Plugins"**
George Kontaxis, Michalis Polychronakis, **Angelos D. Keromytis**, and Evangelos P. Markatos. In Proceedings of the 21st USENIX Security Symposium, pp. 631 - 646. August 2012, Bellevue, WA. (Acceptance rate: 19.4%)
 42. **"kGuard: Lightweight Kernel Protection against Return-to-user Attacks"**
Vasileios P. Kemerlis, Georgios Portokalidis, and **Angelos D. Keromytis**. In Proceedings of the 21st USENIX Security Symposium, pp. 459 - 474. August 2012, Bellevue, WA. (Acceptance rate: 19.4%)
 43. **"Towards a Universal Data Provenance Framework using Dynamic Instrumentation"**
Eleni Gessiou, Vasilis Pappas, Elias Athanasopoulos, **Angelos D. Keromytis**, and Sotiris Ioannidis. In Proceedings of the 27th IFIP International Information Security and Privacy Conference (SEC), pp. 103 - 114. June 2012, Heraklion, Crete, Greece. (Acceptance rate: 25%)
 44. **"Smashing the Gadgets: Hindering Return-Oriented Programming Using In-Place Code Randomization"**
Vasilis Pappas, Michalis Polychronakis, and **Angelos D. Keromytis**. In Proceedings of the 33rd IEEE Symposium on Security & Privacy (S&P), pp. 601 - 615. May 2012, San Francisco, CA. (Acceptance rate: 13%)
 45. **"libdft: Practical Dynamic Data Flow Tracking for Commodity Systems"**
Vasileios P. Kemerlis, Georgios Portokalidis, Kangkook Lee, and **Angelos D. Keromytis**. In Proceedings of the 8th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments (VEE), pp. 121 - 132. March 2012, London, UK.
 46. **"A General Approach for Efficiently Accelerating Software-based Dynamic Data Flow Tracking on Commodity Hardware"**
Kangkook Lee, Georgios Portokalidis, Vasileios P. Kemerlis, Soumyadeep Ghosh, David I. August, and **Angelos D. Keromytis**. In Proceedings of the 19th Internet Society (ISOC) Symposium on Network and Distributed Systems Security (SNDSS), February 2012, San Diego, CA. (Acceptance rate: 17.8%)
 47. **"A Multilayer Overlay Network Architecture for Enhancing IP Services Availability Against DoS"**
Dimitris Geneiatakis, Georgios Portokalidis, and **Angelos D. Keromytis**. In Proceedings of the 7th International Conference on Information Systems Security (ICISS), pp. 322 - 336. December 2011, Kolkata, India. (Acceptance rate: 22.8%)
 48. **"ROP Payload Detection Using Speculative Code Execution"**
Michalis Polychronakis and **Angelos D. Keromytis**. In Proceedings of the 6th International Conference on Malicious and Unwanted Software (MALWARE), pp. 58 - 65. October 2011, Fajardo, PR. (Best Paper Award)
 49. **"Detecting Traffic Snooping in Tor Using Decoys"**
Samuddha Chakravarty, Georgios Portokalidis, Michalis Polychronakis, and **Angelos D. Keromytis**. In Proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection (RAID), pp. 222 - 241. September 2011, Menlo Park, CA. (Acceptance rate: 23%)
 50. **"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%)
 51. **"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%)
 52. **"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%)
 53. **"Fast and Precise 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%)
 54. **"An Adversarial Evaluation of Network Signaling and Control Mechanisms"**
Kangkook Lee, 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.
 55. **"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.
 56. **"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%)
 57. **"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.
 58. **"Traffic Analysis Against Low-Latency Anonymity Networks Using Available Bandwidth Estimation"**
Samuddha 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%)
 59. **"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%)
 60. **"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%)
 61. **"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%)
62. "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%)
63. "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%)
64. "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)
65. "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%)
66. "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)
67. "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%)
68. "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%)
69. "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%)
70. "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%)
71. "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%)
72. "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%)
73. "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)
74. "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%)
75. "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%)
76. "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%)
77. "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%)
78. "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%)
79. "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.
80. "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%)
81. "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%)
82. "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%)
83. "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%)
84. "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 (S&P), pp. 81 - 95. May 2008, Oakland, CA. (Acceptance rate: 11.2%)
85. "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%)
86. "SSARES: Secure Searchable Automated Remote Email Storage"
Adam J. Aviv, Michael E. Locasto, Shava 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%)
87. "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 14th ACM Conference on Computer and Communications Security (CCS), pp. 541 - 551. October/November 2007, Alexandria, VA. (Acceptance rate: 18.1%)
88. "Defending Against Next Generation Attacks Through Network/Endpoint Collaboration and Interaction"
Spiros Antonatos, Michael E. Locasto, Stelios Sidiroglou, **Angelos D. Keromytis**, and Evangelos P. Markatos. In Proceedings of the 3rd European Conference on Computer Network Defense (EC2ND). October 2007, Heraclion, Greece. (Invited paper)
89. "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.
90. "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. Valparaíso, Chile, October 2007. (Acceptance rate: 25%)
91. "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)
92. "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%)
93. "From STEM to SEAD: Speculative Execution for Automated Defense"
Michael E. Locasto, Angelos Stavrou, Gabriela F. Creteu, and **Angelos D. Keromytis**. In Proceedings of the USENIX Annual Technical Conference, pp. 219 - 232. June 2007, Santa Clara, CA. (Acceptance rate: 18.75%)
94. "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 (S&P), pp. 273 - 278. May 2007, Oakland, CA. (Acceptance rate: 8.3%)
95. "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)
96. "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.
97. "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%)
98. "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%)
99. "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.
100. "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%)
101. "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%)
102. "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%)
103. "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.
104. "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.
105. "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%)
106. "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%)
107. "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%)
108. "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%)
109. "Detecting Targeted Attacks Using Shadow Honey Pots"
Kostas G. Anagnostakis, Stelios Sidiroglou, Periklis Akritidis, Konstantinos Xinidis, Evangelos P. Markatos, and **Angelos D. Keromytis**. In Proceedings of the 14th USENIX Security Symposium, pp. 129 - 144. August 2005, Baltimore, MD. (Acceptance rate: 14%)
110. "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.
111. "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.
112. "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%)
113. "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.
114. "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%)
115. "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%)
116. "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.
117. "The Dual Receiver Cryptogram and Its Applications"
Ted Diamant, 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%)
118. "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%)
119. "Recursive Sandboxes: Extending Sysrace 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%)
120. "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%)

121. [*"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%)
122. [*"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%)
123. [*"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.
124. [*"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.
125. [*"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%) (ACM CCS 2013 Test of Time Award)
126. [*"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%)
127. [*"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%)
128. [*"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.
129. [*"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.
130. [*"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.
131. [*"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.
132. [*"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.
133. [*"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%)
134. [*"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.
135. [*"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.
136. [*"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.
137. [*"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%)
138. [*"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%)
139. [*"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)
140. [*"Designing an Embedded Firewall/VPN Gateway"*](#)
Vassilis Prevelakis and [Angelos D. Keromytis](#). In Proceedings of the International Network Conference (INC), pp. 313 - 322. July 2002, Plymouth, England. (Best Paper Award)
141. [*"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.
142. [*"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.)
143. [*"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%)
144. [*"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.
145. [*"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%)
146. [*"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%)
147. [*"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.
148. [*"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.
149. [*"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.
150. [*"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.
151. [*"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.

152. **"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. **"A Methodology for Retrofitting Privacy and Its Application to e-Shopping Transactions"**
Jesus Diaz, Seung Geol Choi, David Arroyo, **Angelos D. Keromytis**, Francisco B. Rodriguez, and Moti Yung. In *"Advances in Cyber Security: Principles, Techniques, and Applications"*, Kuan-Ching Li, Xiaofeng Chen, Willy Susilo (editors), pp. 143 - 183. Springer, 2019.
2. **"Practical Software Diversification Using In-Place Code Randomization"**
Vasilis Pappas, Michalis Polychronakis, and **Angelos D. Keromytis**. In *"Moving Target Defense II: Application of Game Theory and Adversarial Modeling"*, Sushil Jajodia, Anup K. Ghosh, V. S. Subrahmanian, Vipin Swarup, Cliff Wang, and X. Sean Wang (editors), pp. 169 - 196. Springer, 2012.
3. **Proceedings of the 2012 Financial Cryptography and Data Security (FC) Conference**
Angelos D. Keromytis (editor). Lecture Notes in Computer Science (LNCS) 7397. Springer, 2012.
4. **"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.
5. **"Buffer Overflow Attacks"**
Angelos D. Keromytis. In *Encyclopedia of Cryptography and Security, 2nd Edition*, pp. 174 - 177. Springer, 2011.
6. **"Network Bandwidth Denial of Service (DoS)"**
Angelos D. Keromytis. In *Encyclopedia of Cryptography and Security, 2nd Edition*, pp. 836 - 838. Springer, 2011.
7. **"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.
8. **"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.
9. **Proceedings of the 2008 New Security Paradigms Workshop (NSPW)**
Angelos D. Keromytis, Anil Somayaji, and M. Hossain Heydari (editors).
10. **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.
11. **"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.
12. **Proceedings of the 2007 New Security Paradigms Workshop (NSPW)**
Kostantin Beznosov (Editor), **Angelos D. Keromytis** (editor), and M. Hossain Heydari (Editor).
13. **"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.)
14. **"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.
15. **"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.)
16. **"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.
17. **"CryptoGraphics: Exploiting Graphics Cards for Security"**
Debra Cook and **Angelos D. Keromytis**. Advances in Information Security Series, ISBN 0-387-29015-X. Springer, 2006.
18. **Proceedings of the 3rd Workshop on Rapid Malcode (WORM)**
Angelos D. Keromytis (editor). ACM Press, 2005.
19. **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.
20. **"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.
21. **"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.
22. **"STRONGMAN: A Scalable Solution to Trust Management in Networks"**
Angelos D. Keromytis. Ph.D. Thesis, University of Pennsylvania, November 2001.
23. **"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.
24. **"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. **"That's the Way the Cookie Crumbles: Evaluating HTTPS Enforcing Mechanisms"**
Suphanee Sivakorn, **Angelos D. Keromytis**, and Jason Polakis. In Proceedings of the 15th Workshop on Privacy in the Electronic Society (WPES), pp. 71 - 81. October 2016, Vienna, Austria. (Acceptance rate: 19.4%)
2. **"Privacy Threats in E-Shopping (Position Paper)"**
Jesus Diaz, Seung Geol Choi, David Arroyo, **Angelos D. Keromytis**, Francisco B. Rodriguez, and Moti Yung. In Proceedings of the 10th Data Privacy Management International Workshop (DPM), pp. 217 - 225. September 2015, Vienna, Austria.
3. **"Security and Privacy Measurements on Social Networks: Experiences and Lessons Learned"**
Iasonas Polakis, Federico Maggi, Stefano Zanero, and **Angelos D. Keromytis**. In Proceedings of the 3rd International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS). September 2014, Wroclaw, Poland.
4. **"Computational Decoys for Cloud Security"**
George Kontaxis, Michalis Polychronakis, and **Angelos D. Keromytis**. In Proceedings of the ARO Workshop on Cloud Security, pp. 261 - 270. March 2013, Fairfax, VA.
5. **"Exploiting Split Browsers for Efficiently Protecting User Data"**
Angelika Zavou, Elias Athanasopoulos, Georgios Portokalidis, and **Angelos D. Keromytis**. In Proceedings of the ACM Cloud Computing Security Workshop (CCSW), pp. 37 - 47. October 2012, Raleigh, NC.

6. **"The MEERKATS Cloud Security Architecture"**
Angelos D. Keromytis, Roxana Geambasu, Simha Sethumadhavan, Salvatore J. Stolfo, Junfeng Yang, Azzedine Benameur, Marc Dacier, Matthew Elder, Darrell Kienle, and Angelos Stavrou. In Proceedings of the 3rd International Workshop on Security and Privacy in Cloud Computing (ICDCS-SPCC), pp. 446 - 450. June 2012, Macao, China.
7. **"Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud"**
Salvatore J. Stolfo, Malek Ben Salem, and **Angelos D. Keromytis**. In Proceedings of the Workshop on Research for Insider Threat (WRIT). May 2012, San Francisco, CA.
8. **"REASSURE: A Self-contained Mechanism for Healing Software Using Rescue Points"**
Georgios Portokalidis and **Angelos D. Keromytis**. In Proceedings of the 6th International Workshop on Security (IWSEC), pp. 16 - 32. November 2011, Tokyo, Japan. (Best Paper Award)
9. **"Taint-Exchange: a Generic System for Cross-process and Cross-host Taint Tracking"**
Angeliki Zavou, **Georgios Portokalidis**, and **Angelos D. Keromytis**. In Proceedings of the 6th International Workshop on Security (IWSEC), pp. 113 - 128. November 2011, Tokyo, Japan.
10. **"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 Kienle. In Proceedings of the 1st Workshop on Systems Security (SysSec). July 2011, Amsterdam, Netherlands.
11. **"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.
12. **"Towards a Forensic Analysis for Multimedia Communication Services"**
Dimitris Geciciakis 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.
13. **"Security Research with Human Subjects: Informed Consent, Risk, and Benefits"**
Maritza Johnson, Steven M. Bellvin, and **Angelos D. Keromytis**. In Proceedings of the 2nd Workshop on Ethics in Computer Security Research (WECSR). March 2011, Saint Lucia.
14. **"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, pp. 49 - 76. October 2010, Fairfax, VA.
15. **"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%)
16. **"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%)
17. **"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%)
18. **"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%)
19. **"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%)
20. **"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.
21. **"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)
22. **"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.
23. **"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.
24. **"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.
25. **"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.
26. **"Next Generation Attacks on the Internet"**
Evangelos P. 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)
27. **"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.
28. **"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.
29. **"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.
30. **"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.
31. **"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.
32. **"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.
33. **"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.
34. **"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.
35. **"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, Melbourne, FL.
36. **"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.

37. **"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.
38. **"A Network Worm Vaccine Architecture"**
Stelios Sidiropoulos 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.
39. **"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.
40. **"WebDAV: 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.
41. **"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.
42. **"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.
43. **"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.
44. **"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.
45. **"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.
46. **"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.
47. **"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.
48. **"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.
49. **"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.
50. **"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. **"Backing Visionary Entrepreneurs: Realising the Deep-Tech Entrepreneurial Talent of Europe"**
Cheryl Martin, Jes Broeng, Julien Chiaroni, Arnaud Cottet, Lars Frolund, **Angelos Dennis Keromytis**, Florian Muellerhausen, and Mirjam Storim. Report of the EIC Expert Group on Design of the EIC Marketplace and Tech-to-Market Activities, April 2022.
2. **"Implementing the pro-active management of the EIC for breakthrough technologies & innovations: Lessons from the ARPA model & other international practices"**
Lars Frolund, Jes Broeng, Julien Chiaroni, Carsten Dreher, Franz-Werner Haas, **Angelos Dennis Keromytis**, Cheryl Martin, Fiona Murray, Marie-Elisabeth Rusling, and Spela Stres. Directorate-General for Research and Innovation Enhanced European Innovation Council (EIC) Pilot, November 2020.
3. **"Transport Layer Security (TLS) Authorization Using KeyNote"**
Angelos D. Keromytis. *Request For Comments (RFC) 6042*, October 2010.
4. **"X.509 Key and Signature Encoding for the KeyNote Trust Management System"**
Angelos D. Keromytis. *Request For Comments (RFC) 5708*, January 2010.
5. **"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.
6. **"IP Security Policy Requirements"**
Matt Blaze, **Angelos D. Keromytis**, Michael Richardson, and Luis Sanchez. *Request For Comments (RFC) 3586*, August 2003.
7. **"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.
8. **"The Use of HMAC-RIPEMD-160-96 within ESP and AH"**
Angelos D. Keromytis and Niels Provos. *Request For Comments (RFC) 2857*, June 2000.
9. **"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.
10. **"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.