Michalis Polychronakis

355 Computer Science
Stony Brook University
Stony Brook, NY 11794-2424

mikepo@cs.stonybrook.edu
http://www.cs.stonybrook.edu/~mikepo

Education

Ph.D. in Computer Science — Nov. 2005 – Nov. 2009
University of Crete
Thesis: *Generic Detection of Code Injection Attacks using Network-level Emulation*
Advisor: Prof. Evangelos P. Markatos

M.Sc. in Computer Science — Sep. 2003 – Nov. 2005
University of Crete
Thesis: *A Programming Abstraction for Distributed Passive Network Monitoring*
Advisor: Prof. Evangelos P. Markatos

B.Sc. in Computer Science — Sep. 1999 – Sep. 2003
University of Crete
(ranked first in class)
Thesis: *Implementation of an Application Programming Interface for Network Traffic Monitoring*
Advisor: Prof. Evangelos P. Markatos

Work Experience

Assistant Professor — Jan. 2015 – present
Computer Science Department, Stony Brook University

Associate Research Scientist — July 2013 – Dec. 2014
Network Security Lab, Columbia University

Marie Curie IOF Fellow — June 2010 – June 2013
Columbia University and FORTH-ICS
Supervisors: Prof. Angelos Keromytis, Prof. Evangelos P. markatos
Research on various topics in the areas of malicious code analysis and intrusion detection.

Postdoctoral Researcher — Nov. 2009 – May 2010
Distributed Computing Systems Lab, FORTH-ICS
Supervisor: Prof. Evangelos P. Markatos
Research on intrusion detection and network monitoring.

Research Assistant — Nov. 2003 – Nov. 2010
Distributed Computing Systems Lab, FORTH-ICS
Supervisor: Prof. Evangelos P. Markatos
Participation in the EU-funded projects SCAMPI (scalable passive network monitoring), LOBSTER (distributed passive network monitoring), NoAH (network of affined honeypots), MOMENT (network monitoring and measurement), WOMBAT (malware collection and analysis).

Software Engineering Intern — Nov. 2007 – Jan. 2008
Google Inc.
Supervisor: Niels Provos
Anti-malware team. Work on dynamic malware analysis.

Undergraduate Trainee — June 2002 – Nov. 2003
Distributed Computing Systems Lab, FORTH-ICS
Supervisor: Prof. Evangelos P. Markatos
Research on fast pattern matching for network intrusion detection systems.

Service and Teaching

Teaching

- Instructor, CSE590 - Offensive Security, Stony Brook University. Fall 2016.
- Instructor, CSE508 - Network Security, Stony Brook University. Spring 2015, 2016.
- Instructor, CS345 - Operating Systems, University of Crete. Fall 2012.
- Teaching Assistant, CS345 - Operating Systems, University of Crete. Fall 2003, fall 2004.
- Teaching Assistant, CS459 - Internet Measurement, University of Crete. Fall 2009.
- Teaching Assistant, CS555 - Parallel Systems and Grids, University of Crete. Fall 2005, fall 2006, fall 2007.
- Teaching Assistant, CS558 - Internet Systems and Technologies, University of Crete. Spring 2004, spring 2005, spring 2006, spring 2007, spring 2008.

Editorial Boards

- IET Information Security, 2014–2017.

Program Chair

- Program Chair, 14th International Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), 2017
- Program co-Chair, 9th European Workshop on Systems Security (EuroSec), 2016.
- Program co-Chair, 8th European Workshop on Systems Security (EuroSec), 2015.

Conference Organization

- Publication Chair, 20th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2017.
- General co-Chair, 13th International Conference on Applied Cryptography and Network Security (ACNS), 2015.

Program Committees

- IEEE European Symposium on Security and Privacy (EuroS&P), 2018.
- Network and Distributed System Security Symposium (NDSS), 2018.
- IEEE International Conference on Distributed Computing Systems (ICDCS), 2016, 2018.
- USENIX Security Symposium, 2015–2017.

- ACM Conference on Computer and Communications Security (CCS), 2014, 2016, 2017.
- Annual Computer Security Applications Conference (ACSAC), 2012–2017.
- ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2014, 2015, 2017.
- European Symposium on Research in Computer Security (ESORICS), 2012, 2013, 2016, 2017.
- International Conference on Cryptology And Network Security (CANS), 2017.
- International Conference on Network and System Security (NSS), 2016, 2017.
- Innovations in Mobile Privacy and Security workshop (IMPS), 2017.
- APWG Symposium on Electronic Crime Research (eCrime), 2014, 2017.
- European Workshop on System Security (EuroSec), 2012–2014, 2017.
- International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2013, 2014, 2016.
- IEEE International Conference on Parallel and Distributed Systems (ICPADS), 2014, 2016.
- International Information Security Conference (ISC), 2015, 2016.
- International Workshop on Cyber Crime (IWCC), 2013–2016.
- International Workshop on Security and Trust Management (STM), 2016.
- Australasian Conference on Information Security and Privacy (ACISP), 2016.
- International Conference on Privacy, Security and Trust (PST), 2013–2015.
- Internet Measurement Conference (IMC), 2014.
- International Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), 2013, 2014.
- IEEE International Conference on Embedded and Ubiquitous Computing (EUC), 2014.
- European Conference on Computer Network Defense (EC2ND), 2007–2009.
- USENIX Workshop on Hot Topics in Security (HotSec), 2008.

Other Professional Activities

- NSF panelist, 2014, 2017.

Support for Research

- Multi-layer Software Transformation for Attack Surface Reduction and Shielding. Co-PI (PI: R. Sekar, co-PI: Long Lu), Office of Naval Research, N00014-17-1-2891, $3,496,688 (9/30/2017 – 9/30/2022).
- Detection and Prevention of Advanced ROP Exploits. Qualcomm (research gift), $50,000 (8/2016).
- TWC: Small: Combating Environment-aware Malware. PI (co-PI: Nick Nikiforakis), NSF Secure and Trustworthy Computing (SaTC), CNS-1617902, $498,036 (9/1/2016 – 8/31/2019).
- Software Diversification for Attack Prevention and Forecasting. PI (co-PIs: Long Lu, R. Sekar), Office of Naval Research, N00014-15-1-2378, $821,836 (7/1/2015 – 6/30/2018).
- TWC: Small: Virtual Private Social Networks. PI (co-PI: Angelos Keromytis), NSF Secure and Trustworthy Computing (SaTC), CNS-1318415, $498,332 (8/1/2013 – 7/31/2016).
- MALCODE: Malicious Code Detection using Emulation. FP7-PEOPLE-2009-IOF, Marie Curie Actions—International Outgoing Fellowships (IOF), Project Number 254116, €230,952 (7/1/2010 – 6/31/2013).

Distinctions and Awards

- Most Influential DIMVA Paper 2004-2008 Award, 9th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), 2012.
- Best Paper Award, 6th International Conference on Malicious and Unwanted Software (MALWARE), 2011
- Maria M. Manassaki Bequest Scholarship, University of Crete. Given to the best Ph.D. student of the Computer Science Department, 2009.
- Ericsson Award of Excellence in Telecommunications. My thesis ranked first among the best undergraduate theses in class, 2004.
- Scholarship by the State Scholarships Foundation of Greece for ranking first in average grade during the third year of my undergraduate studies, 2003.

Refereed Publications

Journal

1. Dimitris Mitropoulos, Angelos D. Keromytis, Panagiotis Louridas, and Michalis Polychronakis. Defending against web application attacks: Approaches, challenges and implications. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, to appear.
2. Thanasis Petsas, Antonis Papadogiannakis, Michalis Polychronakis, Evangelos P. Markatos, and Thomas Karagiannis. Measurement, modeling, and analysis of the mobile app ecosystem. *ACM Transactions on Modeling and Performance Evaluation of Computing Systems (TOMPECS)*, 2(2):7:1–7:33, March 2017.
3. Giorgos Vasiliadis, Lazaros Koromilas, Michalis Polychronakis, and Sotiris Ioannidis. Design and implementation of a stateful network packet processing framework for GPUs. *IEEE/ACM Transactions on Networking (ToN)*, 25(1):610–623, February 2017.
4. Amin Hassanzadeh, Zhaoyan Xu, Radu Stoleru, Guofei Gu, and Michalis Polychronakis. PRIDE: A practical intrusion detection system for resource constrained wireless mesh networks. *Computers & Security*, 62:114–132, September 2016.
5. Sambuddho Chakravarty, Georgios Portokalidis, Michalis Polychronakis, and Angelos D. Keromytis. Detection and analysis of eavesdropping in anonymous communication networks. *International Journal of Information Security (IJIS)*, 14(3):205–220, June 2015.
6. Giorgos Vasiliadis, Michalis Polychronakis, and Sotiris Ioannidis. GPU-assisted malware. *International Journal of Information Security (IJIS)*, 14(3):289–297, June 2015.
7. Antonis Papadogiannakis, Michalis Polychronakis, and Evangelos P. Markatos. Stream-oriented network traffic capture and analysis for high-speed networks. *IEEE Journal on Selected Areas in Communications (JSAC)*, 32(10):1849–1863, October 2014.
8. Amin Hassanzadeh, Radu Stoleru, Michalis Polychronakis, and Geoffrey Xie. RAPID: Traffic-agnostic intrusion detection for resource-constrained wireless mesh networks. *Computers & Security*, 46:1–17, July 2014.
9. Georgios Kontaxis, Michalis Polychronakis, and Evangelos P. Markatos. Minimizing information disclosure to third parties in social login platforms. *International Journal of Information Security (IJIS)*, 11(5):321–332, October 2012.
10. Antonis Papadogiannakis, Giorgos Vasiliadis, Demetres Antoniades, Michalis Polychronakis, and Evangelos P. Markatos. Improving the performance of passive network monitoring applications with memory locality enhancements. *Computer Communications*, 35(1):129–140, January 2012.

11. Kostas G. Anagnostakis, Stelios Sidiroglou, Periklis Akritidis, Michalis Polychronakis, Angelos D. Keromytis, and Evangelos P. Markatos. Shadow honeypots. *International Journal of Computer and Network Security (IJCNS)*, 2(9):1–16, September 2010.

12. Michalis Polychronakis, Kostas G. Anagnostakis, and Evangelos P. Markatos. Network-level polymorphic shellcode detection using emulation. *Journal in Computer Virology*, 2(4):257–274, February 2007.

Conference Proceedings

1. Micah Morton, Hyungjoon Koo, Forrest Li, Kevin Z. Snow, Michalis Polychronakis, and Fabian Monrose. Defeating zombie gadgets by re-randomizing code upon disclosure. In *Proceedings of the 9th International Symposium on Engineering Secure Software and Systems (ESSoS)*, July 2017.

2. Najmeh Miramirkhani, Mahathi Priya Appini, Nick Nikiforakis, and Michalis Polychronakis. Spotless sandboxes: Evading malware analysis systems using wear-and-tear artifacts. In *Proceedings of the 38th IEEE Symposium on Security & Privacy (S&P)*, May 2017.

3. Marios Pomonis, Theofilos Petsios, Angelos D. Keromytis, Michalis Polychronakis, and Vasileios P. Kemerlis. kRˆX: Comprehensive kernel protection against just-in-time code reuse. In *Proceedings of the 12th European Conference on Computer Systems (EuroSys)*, April 2017.

4. Roman Rogowski, Micah Morton, Forrest Li, Kevin Z. Snow, Fabian Monrose, and Michalis Polychronakis. Revisiting browser security in the modern era: New data-only attacks and defenses. In *Proceedings of the 2nd IEEE European Symposium on Security & Privacy (Euro S&P)*, April 2017.

5. Kevin Z. Snow, Roman Rogowski, Jan Werner, Hyungjoon Koo, Fabian Monrose, and Michalis Polychronakis. Return to the zombie gadgets: Undermining destructive code reads via code inference attacks. In *Proceedings of the 37th IEEE Symposium on Security & Privacy (S&P)*, pages 954–968, May 2016.

6. Hyungjoon Koo and Michalis Polychronakis. Juggling the gadgets: Binary-level code randomization using instruction displacement. In *Proceedings of the 11th ACM Asia Conference on Computer and Communications Security (ASIACCS)*, pages 23–34, May 2016.

7. Jan Werner, George Baltas, Rob Dallara, Nathan Otternes, Kevin Snow, Fabian Monrose, and Michalis Polychronakis. No-execute-after-read: Preventing code disclosure in commodity software. In *Proceedings of the 11th ACM Asia Conference on Computer and Communications Security (ASIACCS)*, pages 35–46, May 2016.

8. David Tagatac, Michalis Polychronakis, and Salvatore Stolfo. Using diversity to harden multithreaded programs against exploitation. In *Proceedings of the 2nd IEEE International Conference on High Performance and Smart Computing (HPSC)*, April 2016.

9. Theofilos Petsios, Vasileios P. Kemerlis, Michalis Polychronakis, and Angelos D. Keromytis. Dynaguard: Armoring canary-based protections against brute-force attacks. In *Proceedings of the 31st Annual Computer Security Applications Conference (ACSAC)*, pages 351–360, December 2015.

10. Evangelos Ladakis, Giorgos Vasiliadis, Michalis Polychronakis, Sotiris Ioannidis, and Georgios Portokalidis. GPU-disasm: A GPU-based x86 disassembler. In *Proceedings of the 18th Information Security Conference (ISC)*, pages 472–489, September 2015.

11. Michalis Athanasakis, Elias Athanasopoulos, Michalis Polychronakis, Georgios Portokalidis, and Sotiris Ioannidis. The devil is in the constants: Bypassing defenses in browser JIT engines. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, February 2015.

12. Marios Pomonis, Theofilos Petsios, Kangkook Jee, Michalis Polychronakis, and Angelos D. Keromytis. IntFlow: Improving the accuracy of arithmetic error detection using information flow tracking. In *Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC)*, pages 416–425, December 2014.

13. Giorgos Vasiliadis, Elias Athanasopoulos, Michalis Polychronakis, and Sotiris Ioannidis. PixelVault: Using GPUs for securing cryptographic operations. In *Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS)*, pages 1131–1142, November 2014.

14. Vasilis Pappas, Michalis Polychronakis, and Angelos D. Keromytis. Dynamic reconstruction of relocation information for stripped binaries. In *Proceedings of the 17th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, pages 68–87, September 2014.

15. Vasileios P. Kemerlis, Michalis Polychronakis, and Angelos D. Keromytis. ret2dir: Rethinking kernel isolation. In *Proceedings of the 23rd USENIX Security Symposium*, pages 957–972, August 2014.

16. Enes Göktaş, Elias Athanasopoulos, Michalis Polychronakis, Herbert Bos, and Georgios Portokalidis. Size does matter: Why using gadget-chain length to prevent code-reuse attacks is hard. In *Proceedings of the 23rd USENIX Security Symposium*, pages 417–432, August 2014.

17. Giorgos Vasiliadis, Lazaros Koromilas, Michalis Polychronakis, and Sotiris Ioannidis. GASPP: A GPU-accelerated stateful packet processing framework. In *Proceedings of the USENIX Annual Technical Conference (ATC)*, pages 321–332, June 2014.

18. Sambuddho Chakravarty, Marco V. Barbera, Georgios Portokalidis, Michalis Polychronakis, and Angelos D. Keromytis. On the effectiveness of traffic analysis against anonymity networks using flow records. In *Proceedings of the 15th Passive and Active Measurement Conference (PAM)*, pages 247–257, March 2014.

19. Panagiotis Papadopoulos, Antonis Papadogiannakis, Michalis Polychronakis, Apostolis Zarras, Thorsten Holz, and Evangelos P. Markatos. K-subscription: Privacy-preserving microblogging browsing through obfuscation. In *Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC)*, pages 49–58, December 2013.

20. Amin Hassanzadeh, Zhaoyan Xu, Radu Stoleru, Guofei Gu, and Michalis Polychronakis. PRIDE: Practical intrusion detection in resource constrained wireless mesh networks. In *Proceedings of the 9th International Conference on Information, Communications and Signal Processing (ICICS)*, pages 213–228, December 2013.

21. Antonis Papadogiannakis, Michalis Polychronakis, and Evangelos P. Markatos. Scap: Stream-oriented network traffic capture and analysis for high-speed networks. In *Proceedings of the Internet Measurement Conference (IMC)*, pages 441–454, October 2013.

22. Thanasis Petsas, Antonis Papadogiannakis, Michalis Polychronakis, Evangelos P. Markatos, and Thomas Karagiannis. Rise of the planet of the apps: A systematic study of the mobile app ecosystem. In *Proceedings of the Internet Measurement Conference (IMC)*, pages 277–290, October 2013.

23. Jakob Fritz, Corrado Leita, and Michalis Polychronakis. Server-side code injection attacks: A historical perspective. In *Proceedings of the 16th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, pages 41–61, October 2013.

24. Vasilis Pappas, Vasileios P. Kemerlis, Angeliki Zavou, Michalis Polychronakis, and Angelos D. Keromytis. CloudFence: Data flow tracking as a cloud service. In *Proceedings of the 16th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, pages 411–431, October 2013.

25. Vasilis Pappas, Michalis Polychronakis, and Angelos D. Keromytis. Transparent ROP exploit mitigation using indirect branch tracing. In *Proceedings of the 22nd USENIX Security Symposium*, pages 447–462, August 2013.

26. Angeliki Zavou, Vasilis Pappas, Vasileios P. Kemerlis, Michalis Polychronakis, Georgios Portokalidis, and Angelos D. Keromytis. Cloudopsy: an autopsy of data flows in the cloud. In *Proceedings of the 15th International Conference on Human-Computer Interaction (HCI)*, pages 366–375, July 2013.

27. Georgios Kontaxis, Michalis Polychronakis, Angelos D. Keromytis, and Evangelos P. Markatos. Privacy-preserving social plugins. In *Proceedings of the 21st USENIX Security Symposium*, pages 631–646, August 2012.

28. Elias Athanasopoulos, Vasileios P. Kemerlis, Michalis Polychronakis, and Evangelos P. Markatos. ARC: Protecting against HTTP parameter pollution attacks using application request caches. In *Proceedings of the 10th International Conference on Applied Cryptography and Network Security (ACNS)*, pages 400–417, June 2012.

29. Antonis Papadogiannakis, Michalis Polychronakis, and Evangelos P. Markatos. Tolerating overload attacks against packet capture systems (short paper). In *Proceedings of the USENIX Annual Technical Conference (ATC)*, pages 197–202, June 2012.

30. Vasilis Pappas, Michalis Polychronakis, and Angelos D. Keromytis. Smashing the gadgets: Hindering return-oriented programming using in-place code randomization. In *Proceedings of the 33rd IEEE Symposium on Security & Privacy (S&P)*, pages 601–615, May 2012.

31. Giorgos Vasiliadis, Michalis Polychronakis, and Sotiris Ioannidis. Parallelization and characterization of pattern matching using GPUs. In *Proceedings of the IEEE International Symposium on Workload Characterization (IISWC)*, pages 216–225, November 2011.

32. Michalis Polychronakis and Angelos D. Keromytis. ROP payload detection using speculative code execution. In *Proceedings of the 6th International Conference on Malicious and Unwanted Software (MALWARE)*, pages 58–65, October 2011.

33. Giorgos Vasiliadis, Michalis Polychronakis, and Sotiris Ioannidis. MIDeA: A multi-parallel intrusion detection architecture. In *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS)*, pages 297–308, October 2011.

34. Georgios Kontaxis, Michalis Polychronakis, and Evangelos P. Markatos. SudoWeb: Minimizing information disclosure to third parties in single sign-on platforms. In *Proceedings of the 14th Information Security Conference (ISC)*, pages 197–212, October 2011.

35. Sambuddho Chakravarty, Georgios Portokalidis, Michalis Polychronakis, and Angelos D. Keromytis. Detecting traffic snooping in Tor using decoys. In *Proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection (RAID)*, pages 222–241, September 2011.

36. Michalis Polychronakis, Kostas G. Anagnostakis, and Evangelos P. Markatos. Comprehensive shellcode detection using runtime heuristics. In *Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC)*, pages 287–296, December 2010.

37. Giorgos Vasiliadis, Michalis Polychronakis, and Sotiris Ioannidis. GPU-assisted malware. In *Proceedings of the 5th IEEE International Conference on Malicious and Unwanted Software (MALWARE)*, pages 1–6, October 2010.

38. Antonis Papadogiannakis, Michalis Polychronakis, and Evangelos P. Markatos. RRDtrace: Long-term raw network traffic recording using fixed-size storage. In *Proceedings of the 18th IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, pages 101–110, August 2010.

39. Giorgos Vasiliadis, Michalis Polychronakis, Spiros Antonatos, Evangelos P. Markatos, and Sotiris Ioannidis. Regular expression matching on graphics hardware for intrusion detection. In *Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection (RAID)*, pages 265–283, September 2009.

40. Antonis Theocharides, Demetres Antoniades, Michalis Polychronakis, Elias Athanasopoulos, and Evangelos P. Markatos. Topnet: A network-aware top(1). In *Proceedings of the 22nd USENIX Large Installation System Administration Conference (LISA)*, pages 145–157, November 2008.

41. Giorgos Vasiliadis, Spiros Antonatos, Michalis Polychronakis, Evangelos P. Markatos, and Sotiris Ioannidis. Gnort: High performance network intrusion detection using graphics processors. In *Proceedings of the 11th International Symposium on Recent Advances in Intrusion Detection (RAID)*, pages 116–134, September 2008.

42. Demetres Antoniades, Michalis Polychronakis, Antonis Papadogiannakis, Panos Trimintzios, Sven Ubik, Vladimir Smotlacha, Arne Øslebø, and Evangelos P. Markatos. LOBSTER: A european platform for passive network traffic monitoring. In *Proceedings of the 4th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities (TRIDENTCOM)*, March 2008.

43. Antonis Papadogiannakis, Demetres Antoniades, Michalis Polychronakis, and Evangelos P. Markatos. Improving the performance of passive network monitoring applications using locality buffering. In *Proceedings of the 15th IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, pages 151–157, October 2007.

44. Michalis Polychronakis, Kostas G. Anagnostakis, and Evangelos P. Markatos. Emulation-based detection of non-self-contained polymorphic shellcode. In *Proceedings of the 10th International Symposium on Recent Advances in Intrusion Detection (RAID)*, pages 87–106, September 2007.

45. Demetres Antoniades, Michalis Polychronakis, Spiros Antonatos, Evangelos P. Markatos, Sven Ubik, and Arne Øslebø. Appmon: An application for accurate per application network traffic characterization. In *Proceedings of the IST BroadBand Europe Conference*, December 2006.

46. Michalis Polychronakis, Kostas G. Anagnostakis, and Evangelos P. Markatos. Network-level polymorphic shellcode detection using emulation. In *Proceedings of the Third Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, volume 4064 of *Lecture Notes in Computer Science*, pages 54–73. Springer-Verlag, July 2006.

47. Panos Trimintzios, Michalis Polychronakis, Antonis Papadogiannakis, Michalis Foukarakis, Evangelos P. Markatos, and Arne Øslebø. DiMAPI: An application programming interface for distributed network monitoring. In *Proceedings of the 10th IEEE/IFIP Network Operations and Management Symposium (NOMS)*, pages 382–393, April 2006.

48. Periklis Akritidis, Evangelos P. Markatos, Michalis Polychronakis, and Kostas Anagnostakis. STRIDE: Polymorphic sled detection through instruction sequence analysis. In *Proceedings of the 20th IFIP International Information Security Conference (IFIP/SEC)*, pages 375–392. Springer, June 2005.

49. Spyros Antonatos, Michalis Polychronakis, Periklis Akritidis, Kostas G. Anagnostakis, and Evangelos P. Markatos. Piranha: Fast and memory-efficient pattern matching for intrusion detection. In *Proceedings of the 20th IFIP International Information Security Conference (IFIP/SEC)*, pages 393–408. Springer, June 2005.

50. Michalis Polychronakis, Kostas G. Anagnostakis, Evangelos P. Markatos, and Arne Øslebø. Design of an application programming interface for IP network monitoring. In *Proceedings of the 9th IEEE/IFIP Network Operations and Management Symposium (NOMS)*, pages 483–496, April 2004.

51. Spyros Antonatos, Kostas G. Anagnostakis, Evangelos P. Markatos, and Michalis Polychronakis. Performance analysis of content matching intrusion detection systems. In *Proceedings of the IEEE/IPSJ Symposium on Applications and the Internet (SAINT)*, pages 208–215, January 2004.

52. Kostas G. Anagnostakis, Evangelos P. Markatos, Spyros Antonatos, and Michalis Polychronakis. E^{2}xB: A domain-specific string matching algorithm for intrusion detection. In *Proceedings of the 18th IFIP International Information Security Conference (IFIP/SEC)*, volume 250 of *IFIP Conference Proceedings*, pages 217–228. Kluwer, May 2003.

53. Evangelos P. Markatos, Spyros Antonatos, Michalis Polychronakis, and Kostas G. Anagnostakis. ExB: Exclusion-based signature matching for intrusion detection. In *Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN)*, pages 146–152, November 2002.

Workshop Proceedings

1. Thanasis Petsas, Giannis Voyatzis, Elias Athanasopoulos, Michalis Polychronakis, and Sotiris Ioannidis. Rage against the virtual machine: Hindering dynamic analysis of mobile malware. In *Proceedings of the 7th European Workshop on System Security (EuroSec)*, April 2014.

2. Evangelos Ladakis, Lazaros Koromilas, Giorgos Vasiliadis, Michalis Polychronakis, and Sotiris Ioannidis. You can type, but you can't hide: A stealthy GPU-based keylogger. In *Proceedings of the 6th European Workshop on System Security (EuroSec)*, April 2013.

3. George Kontaxis, Michalis Polychronakis, and Angelos D. Keromytis. Computational decoys for cloud security. In *Proceedings of the ARO Workshop on Cloud Security*, March 2013.

4. Zacharias Tzermias, Giorgos Sykiotakis, Michalis Polychronakis, and Evangelos P. Markatos. Combining static and dynamic analysis for the detection of malicious documents. In *Proceedings of the 4th European Workshop on System Security (EuroSec)*, April 2011.

5. Antonis Papadogiannakis, Michalis Polychronakis, and Evangelos P. Markatos. Improving the accuracy of network intrusion detection systems under load using selective packet discarding. In *Proceedings of the 3rd European Workshop on System Security (EuroSec)*, pages 15–21, April 2010.

6. Aleš Friedl, Sven Ubik, Alexandros Kapravelos, Michalis Polychronakis, and Evangelos P. Markatos. Realistic passive packet loss measurement for high-speed networks. In *Proceedings of the 1st International Workshop on Traffic Monitoring and Analysis (TMA)*, May 2009.

7. Michalis Polychronakis, Kostas G. Anagnostakis, and Evangelos P. Markatos. An empirical study of real-world polymorphic code injection attacks. In *Proceedings of the 2nd USENIX Workshop on Large-scale Exploits and Emergent Threats (LEET)*, April 2009.

8. Michael Foukarakis, Demetres Antoniades, and Michalis Polychronakis. Deep packet anonymization. In *Proceedings of the 2nd European Workshop on System Security (EuroSec)*, March 2009.

9. Michalis Polychronakis, Kostas G. Anagnostakis, and Evangelos P. Markatos. Real-world polymorphic attack detection using network-level emulation. In *Proceedings of the 4th annual workshop on Cyber security and information intelligence research (CSIIRW)*, May 2008.

10. Michalis Polychronakis, Panayiotis Mavrommatis, and Niels Provos. Ghost turns zombie: Exploring the life-cycle of web-based malware. In *Proceedings of the 1st USENIX Workshop on Large-scale Exploits and Emergent Threats (LEET)*, April 2008.

11. Demetris Antoniades, Michalis Polychronakis, Nick Nikiforakis, Evangelos P. Markatos, and Yiannis Mitsos. Monitoring three national research networks for eight weeks: Observations and implications. In *Proceedings of the 6th IEEE Workshop on End-to-End Monitoring Techniques and Services (E2EMON)*, pages 153–156, April 2008.

12. Antonis Papadogiannakis, Alexandros Kapravelos, Michalis Polychronakis, Evangelos P. Markatos, and Augusto Ciuffoletti. Passive end-to-end packet loss estimation for Grid traffic monitoring. In *Proceedings of the 2nd CoreGRID Integration Workshop*, October 2006.

13. Augusto Ciuffoletti and Michalis Polychronakis. Architecture of a network monitoring element. In *Proceedings of the CoreGRID Workshop on Grid Middleware (held in conjunction with EuroPar 2006)*, volume 4375 of *Lecture Notes in Computer Science*. Springer-Verlag, August 2006.

14. Augusto Ciuffoletti and Michalis Polychronakis. Architecture of a network monitoring element. In *Proceedings of the 15th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, pages 220–221, June 2006. Third International Workshop on Emerging Technologies for Next-generation GRID (ETNGRID).

15. Sergio Andreozzi, Demetres Antoniades, Augusto Ciuffoletti, Antonia Ghiselli, Evangelos P. Markatos, Michalis Polychronakis, and Panos Trimintzios. Issues about the integration of passive and active monitoring for grid networks. In *Integrated Research in GRID Computing: Proceedings of the CoreGRID Integration Workshop (CGIW)*. Springer-Verlag, November 2005.

16. Jan Coppens, Evangelos P. Markatos, Jiří Novotný, Michalis Polychronakis, Vladimír Smotlacha, and Sven Ubik. SCAMPI: A scalable monitoring platform for the internet. In *Proceedings of the 2^{nd} International Workshop on Inter-Domain Performance and Simulation (IPS)*, March 2004.

Patents

1. Michalis Polychronakis and Angelos D. Keromytis. 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. US Patent 9,495,541, Issued on November 2016.

Non-refereed Publications

1. Michalis Polychronakis and Evangelos Markatos. From malicious software to malicious documents (in Greek). *The Economist (Greek Edition)*, Issue 90, July–August 2011.

2. Michalis Polychronakis. Reverse engineering of malware emulators. In *Encyclopedia of Cryptography and Security, 2nd Edition*, pages 1043–1044. Springer, 2011.

3. Michalis Polychronakis, Evangelos Markatos, Yannis Mitsos, Slavko Gajin, and Goran Muratovski. Real-world polymorphic attack detection. *ENISA Quarterly*, 4(2), Apr–Jun 2008.

4. Michalis Polychronakis, Kostas Anagnostakis, and Evangelos Markatos. LOBSTER: Detecting internet attacks (in Greek). *The Economist (Greek Edition)*, Issue 43, September 2007.

5. Evangelos Markatos, Kostas Anagnostakis, Spyros Antonatos, and Michalis Polychronakis. Real-time monitoring and detection of cyberattacks. *ENISA Quarterly*, 3(1), Jan–Mar 2007.

Invited Talks

- Defending against Advanced Return-Oriented Programming Attacks. Georgia Tech, October 2016, USA.
- Defending against Advanced Return-Oriented Programming Attacks. Qualcomm Research Silicon Valley, June 2016, USA.
- Practical Defenses Against Return-Oriented Programming. University of North Carolina at Chapel Hill, September 2015, USA.
- PixelVault: Securing Cryptographic Operations Using Graphics Processors. 34th General Meeting of the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG34), June 2015, Dublin, Ireland.
- Improving the Security and Privacy of Our Digital Life. Yahoo! Labs NYC, December 2014, USA.
- Practical Defenses Against Return-Oriented Programming. Singapore University of Technology and Design, February 2014, Singapore.
- Practical Defenses Against Return-Oriented Programming. Stevens Institute of Technology, October 2013, USA.
- Defending Against Return-Oriented Programming. Georgia Tech, October 2012, USA.
- Defending Against Return-Oriented Programming. 9th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), July 2012, Heraklion, Greece.
- From Shellcode to Return-Oriented Programming: Detecting Malicious Code using Code Emulation. AT&T Security Research Center NYC, November 2011, USA.

- Code Injection Attack Detection using Network-level Emulation. University of Pennsylvania, November 2010, USA.
- Code Injection Attack Detection using Network-level Emulation. University of North Carolina at Chapel Hill, October 2010, USA.
- Real World Detection of Polymorphic Attacks. 4th International Annual Workshop on Digital Forensics & Incident Analysis (WDFIA), June 2009, Athens, Greece.
- Polymorphic attacks: evasion techniques and detection approaches. European Conference on Computer Network Defense (EC2ND), December 2008, Dublin, Ireland.
- What's going on in our network? Traffic categorization and attack detection using passive network monitoring. Telecommunications Research Center Vienna (FTW), March 2008, Vienna, Austria.
- Passive Network Monitoring in the LOBSTER Project: A Tutorial Introduction. MetroGrid Workshop, October 2007, Lyon, France.
- Network Monitoring for Performance and Security: the LOBSTER Project. Broadband Cluster Session of the 7th IST FP6 Concertation Meeting, October 2006, Brussels, Belgium.
- Passive Monitoring for Security-Related Applications. TERENA Networking Conference, May 2006, Catania, Italy.
- Defending against Polymorphic Attacks: Recent Results and Open Questions. TERENA Networking Conference, May 2006, Catania, Italy.
- Polymorphic Attack Detection using Emulation. Institute for Infocomm Research (I^2R), January 2006, Singapore.