Michalis Polychronakis

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

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

Education

PhD 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

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

BSc 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

Associate Professor — Sep. 2019 – present
Computer Science Department, Stony Brook University

Visiting Researcher — Oct. 2021 – June 2022
Google LLC

Assistant Professor — Jan. 2015 – Aug. 2019
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

Stony Brook University

- Instructor, CSE508 - Network Security. Spring 2015, Spring 2016, Fall 2017, Spring 2021, Spring 2024.
- Instructor, CSE509 - Computer System Security. Spring 2023.
- Instructor, CSE363 - Offensive Security. Spring 2019, Spring 2020.
- Instructor, CSE331 - Computer Security Fundamentals. Fall 2017.
- Instructor, CSE590 - Offensive Security. Fall 2016.

University of Crete

- Instructor, CS345 - Operating Systems. Fall 2012.
- Teaching Assistant, CS345 - Operating Systems. Fall 2003, Fall 2004.
- Teaching Assistant, CS459 - Internet Measurement. Fall 2009.
- Teaching Assistant, CS555 - Parallel Systems and Grids. Fall 2005, Fall 2006, Fall 2007.
- Teaching Assistant, CS558 - Internet Systems and Technologies. Spring 2004, Spring 2005, Spring 2006, Spring 2007, Spring 2008.

Service at Stony Brook

- Graduate Academic Advisor, 2024 onward.
- Organizer, Distinguished Lecture Series, 2022 onward.
- Member, Network Security Working Group, 2021–2023.

Editorial Boards and Steering Committees

- Steering committee member, Information Security Conference (ISC), 2018 onward.
- Associate Editor, Encyclopedia of Cryptography, Security, and Privacy (3rd Edition), Springer, 2018.
- Steering committee member, International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2017 onward.

- Steering committee member, International Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), 2017 onward.
- Editor, IET Information Security, 2014–2018.

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

- General Chair, 22nd Information Security Conference (ISC), 2019.
- General co-Chair, 13th International Conference on Applied Cryptography and Network Security (ACNS), 2015.

Conference Support

- Publicity Chair, 15th European Conference on Computer Systems (EuroSys), 2020.
- Publicity Chair, 21th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2018.
- Publication Chair, 20th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2017.

Program Committees

- IEEE Symposium on Security and Privacy (S&P), 2019–2021, 2024.
- IEEE European Symposium on Security and Privacy (EuroS&P), 2018, 2024.
- International Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), 2013, 2014, 2020, 2023, 2024.
- ACM Conference on Computer and Communications Security (CCS), 2014, 2016, 2017, 2020, 2022, 2023.
- Annual Computer Security Applications Conference (ACSAC), 2012–2018, 2023.
- Workshop on Forming an Ecosystem Around Software Transformation (FEAST), 2020.
- Workshop on Binary Analysis Research (BAR), 2018–2020.
- Workshop on Free and Open Communications on the Internet (FOCI), 2020.
- Network and Distributed System Security Symposium (NDSS), 2018, 2019.
- International Symposium on Research in Attacks, Intrusions, and Defenses (RAID), 2013, 2014, 2016, 2019.
- IEEE International Conference on Distributed Computing Systems (ICDCS), 2016, 2018.
- International Workshop on Speculative Side Channel Analysis (WoSSCA), 2018.
- USENIX Security Symposium, 2015–2017.
- 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.
- 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 Applied Cryptography and Network Security (ACNS), 2015.
- International Conference on Privacy, Security and Trust (PST), 2013–2015.
- Internet Measurement Conference (IMC), 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

- Panelist, National Science Foundation (NSF), 2014, 2017, 2020–2022, 2024.
- Evaluation Committee Member, Hellenic Foundation for Research and Innovation (HFRI), 2022–2023.

PhD Students

- Muhammad Farrukh (February 2024 – present)
- Paschalis Bekos (January 2024 – present)
- Muhammad Sumeer Ahmad (November 2023 – present)
- Rucha Save (September 2023 – present)
- Harshvardhan Patel (September 2022 – present)
- Maryam Rostamipoor (February 2021 – present)
- Seyedhamed Ghavamnia (September 2017 – May 2023) → *Assistant Professor, University of Connecticut*
- Nguyen Phong Hoang (September 2016 – December 2021) → *Postdoctoral Researcher, University of Chicago*
- Tapti Palit (January 2017 – October 2021) → *Postdoctoral Researcher, Purdue University*
- Shachee Mishra (June 2016 – May 2021) → *Researcher, IBM Research*
- Hyungjoon Koo (January 2015 – May 2019) → *Postdoctoral Researcher, Georgia Tech* → *Assistant Professor, Sungkyunkwan University*

MS Students

- Aliakbar Mevliwala (January 2024 – present)
- Mohammad Khakhariawala (September 2023 – present)
- Swaroop Bugatha (August 2021 – May 2022)
- Md Mehedi Hasan (September 2020 – April 2023)
- Ivan Lin (June 2020 – December 2021)
- Andy Liang (August 2020 – May 2021)

- Rebecca Hassett (September 2019 – December 2019)
- Christopher Morales (June 2019 – September 2019)
- Jarin Firose Moon (February 2019 – August 2021)
- Raunak Shah (January 2018 – December 2018)
- Ishupreet Singh (December 2017 – December 2018)
- Akhil Bhutani (December 2017 – December 2018)
- Jeevan Gregory Sequeira (January 2017 – December 2017)
- Aynoor Saleem (April 2017 – August 2018)
- Aviral Nigam (January 2017 – December 2017)
- Vijay Kumar Midde (December 2016 – December 2017)
- Mahendra Dangi (August 2016 – May 2017)
- Amit Bapat (August 2016 – May 2017)
- Meghana Doppalapudi (June 2016 – May 2017)
- Aathira Prabhakar (June 2016 – December 2016)
- Anish Ahmed (January 2016 – December 2016)
- Aadarsh Jajodia (January 2016 – December 2016)
- Sumesh Balan (January 2016 – December 2016)
- Mahathi Priya Appini (June 2015 – May 2016)
- Saketa Chandra Chalamchala (June 2015 – May 2016)
- Sumit Bindal (February 2015 – January 2016)

Undergraduate Students

- Alex Snit (September 2023 – present)
- Daniel Kogan (September 2023 – present)
- Mithuna Kumar (September 2022 – December 2022)
- Ivan Lin (June 2019 – May 2020)
- Swathi Sekar (June 2018 – May 2019)
- Joseph Macaluso (January 2018 – December 2018)
- Christopher Morales (January 2018 – May 2019)
- Robert Russell (January 2018 – May 2018)
- Jayesh Ranjan (January 2018 – May 2018)

High School Students

- Alexander Zarboulas (Summer 2022)
- Nicholas Tung (Summer 2019)
- Michelle Goh (Summer 2017)
- Kevin Xu (Summer 2016)

Interns

- Christine Utz (May 2019 – September 2019)
- Manolis Karampinakis (October 2018 – February 2019)
- Sergej Proskurin (May 2018 – October 2018)
- Panagiotis Ilia (November 2016 – April 2017)

PhD Thesis Committee Service

- Dimitris Deyannis, *Full Stack Protection Leveraging User-level Enclaves*, University of Crete, July 2023.
- Eva Papadogiannaki, *Identification of Events on Encrypted Network Traffic and Characterization of Malicious Servers on the Internet*, University of Crete, June 2023.
- Brian Kondracki, *Leveraging Side-channels to Fingerprint Software Systems*, Stony Brook University, April 2023.
- Michalis Diamantaris, *Android's Security and Privacy Journey through the Lens of Access Control Policies*, University of Crete, January 2023.
- Babak Amin Azad, *Protecting Web Applications Via Software Debloating*, Stony Brook University, December 2022.
- Sergej Proskurin, *Virtualization-assisted Dynamic Binary Analysis and Operating System Security*, Technical University of Munich, November 2022.
- Reza Mirzazade Farkhani, *Understanding and Mitigating Memory Corruption Attacks*, Northeastern University, July 2022.
- Darius-Andrei Suciu, *Practical Hardware-Enforced Protections for Mobile Devices*, Stony Brook University, March 2022.
- Md Nahid Hossain, *A New Tag Based Approach for Real-Time Detection of Sophisticated Cyber Attacks*, Stony Brook University, January 2022.
- Nicholas DeMarinis, *Improving Application Security at Scale by Reducing System Call and Library Overprivilege*, Brown University, September 2021.
- Xiao Liang, *Black-Box Secure Multi-Party Computation: New Possibilities and Limitations*, Stony Brook University, August 2021.
- Piyush Sharma, *Building Performant, Privacy-Enhancing, and Blocking-Resistant Communication Systems*, Indraprastha Institute of Information Technology Delhi, August 2021.
- Shinyoung Cho, *Tackling Network-level Adversaries using Models and Empirical Observations*, Stony Brook University, August 2021.
- Meng Luo, *Evaluating Mobile-Browser Security with Dynamic Analysis Techniques*, Stony Brook University, December 2020.
- Anrin Chakraborti, *Scalable High-Throughput Systems for Practical Access Privacy*, Stony Brook University, July 2020.
- Varun Agrawal, *Instruction and Data Repetition in Applications*, Stony Brook University, June 2020.
- Najmeh Miramirkhani, *Methodologies and Tools to Study Malicious Ecosystems*, Stony Brook University, December 2019.
- Chen Chen, *Practical Plausibly Deniable Storage*, Stony Brook University, December 2019.
- Seyyedahmad Javadi, *Analytical Approaches for Dynamic Scheduling in Cloud Environments*, Stony Brook University, July 2019.
- Panagiotis Ilia, *Privacy Loss in Online Social Networks due to Access Control and Data Management Policies*, University of Crete, November 2018.

- Panagiotis Papadopoulos, *Analyzing the impact of Digital Advertising on User Privacy*, University of Crete, September 2018.
- Oleksii Starov, *The Two Sides of Web Privacy: Defending Benign Users and Detecting Malicious Actors*, Stony Brook University, May 2018.
- Rui Qiao, *Accurate Recovery of Functions in COTS Binaries*, Stony Brook University, May 2017.
- João Batista Corrêa Gomes Moreira, *Protection Mechanisms Against Control-Flow Hijacking Attacks*, University of Campinas, December 2016.
- Mingwei Zhang, *Static Binary Instrumentation with Applications to COTS Software Security*, Stony Brook University, August 2015.
- Vasileios P. Kemerlis, *Protecting Commodity Operating Systems through Strong Kernel Isolation*, Columbia University, July 2015.
- Giorgos Vasiliadis, *High-throughput Stateful Network Packet Processing Using Modern Graphics Processors*, University of Crete, December 2014.

Support for Research

- SafeTrans: AI-assisted Transcompilation to Memory-safe Languages. Amazon Research Awards, $80,000 (4/2024).
- Automated Code Translation to Memory-safe Languages. Office of Naval Research, N00014-24-1-2054, $752,096 (12/1/2023 – 11/30/2026).
- SaTC: CORE: Small: Selective Data Protection against Data-oriented and Transient Execution Attacks. NSF Secure and Trustworthy Computing (SaTC), CNS-2104148, $499,058 (7/1/2021 – 6/30/2024).
- Reducing Attack Surface through Unneeded Code Removal. Accenture (research gift), $25,000 (11/2018).
- Compiler-Assisted Software Specialization Against Vulnerability Exploitation. DARPA Young Faculty Award, D18AP00045, $893,373 (7/2/2018 – 7/2/2021).
- CAREER: Principled and Practical Software Shielding against Advanced Exploits. NSF Secure and Trustworthy Computing (SaTC), CNS-1749895, $499,899 (6/1/2018 – 5/31/2023).
- Reducing Attack Surface through Unneeded Code Removal. Accenture (research gift), $20,000 (5/2018).
- 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 (own share: $1,447,948) (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 (own share: $249,018) (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 (own share: $273,945) (7/1/2015 – 6/30/2018).
- *Total at SBU: $7,635,986; as PI: $4,139,298; own share: $4,790,337*

- 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

- ACM CCS 2022 Top Reviewer Award.
- DARPA Young Faculty Award, 2018.

- NSF CAREER award, 2018.
- Most Influential DIMVA Paper 2004-2008 Award, 9th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), 2012.
- Best Student Paper Award, 14th Information Security Conference (ISC), 2011.
- Best Paper Award, 6th International Conference on Malicious and Unwanted Software (MALWARE), 2011
- Maria M. Manassaki Bequest Scholarship, University of Crete. Given to the top PhD 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. Maryam Rostamipoor, Seyedhamed Ghavamnia, and Michalis Polychronakis. Confine: Fine-grained system call filtering for container attack surface reduction. *Computers & Security*, 132, September 2023.
2. Tapti Palit, Fabian Monrose, and Michalis Polychronakis. Mitigating data-only attacks by protecting memory-resident sensitive data. *Digital Threats: Research and Practice*, 1(4), December 2020.
3. Nguyen Phong Hoang, Arian Akhavan Niaki, Michalis Polychronakis, and Phillipa Gill. The web is still small after more than a decade. *ACM SIGCOMM Computer Communication Review (CCR)*, 50(2):24–31, May 2020.
4. 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)*, 16(2):188–203, March 2019.
5. Marios Pomonis, Theofilos Petsios, Angelos D. Keromytis, Michalis Polychronakis, and Vasileios P. Kemerlis. Kernel protection against just-in-time code reuse. *ACM Transactions on Privacy and Security (TOPS)*, 22(1):5:1–5:28, January 2019.
6. 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.
7. 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.
8. 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.
9. 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.
10. Giorgos Vasiliadis, Michalis Polychronakis, and Sotiris Ioannidis. GPU-assisted malware. *International Journal of Information Security (IJIS)*, 14(3):289–297, June 2015.
11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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. Nguyen Phong Hoang, Jakub Dalek, Masashi Crete-Nishihata, Nicolas Christin, Vinod Yegneswaran, Michalis Polychronakis, and Nick Feamster. GFWeb: Measuring the Great Firewall's Web censorship at scale. In *Proceedings of the 33rd USENIX Security Symposium*, August 2024.

2. Marius Momeu, Fabian Kilger, Christopher Roemheld, Simon Schnückel, Sergej Proskurin, Michalis Polychronakis, and Vasileios P. Kemerlis. Immutable memory management metadata for commodity operating system kernels. In *Proceedings of the 19th ACM ASIA Conference on Computer and Communications Security (AsiaCCS)*, July 2024. *(Acceptance rate: 21%)*

3. Seyedhamed Ghavamnia, Tapti Palit, and Michalis Polychronakis. C2C: Fine-grained configuration-driven system call filtering. In *Proceedings of the 29th ACM Conference on Computer and Communications Security (CCS)*, pages 1243–1257, November 2022. *(Acceptance rate: 22%)*

4. Md Mehedi Hasan, Seyedhamed Ghavamnia, and Michalis Polychronakis. Decap: Deprivileging programs by reducing their capabilities. In *Proceedings of the 25th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, pages 395–408, October 2022. *(Acceptance rate: 25%)*

5. Nguyen Phong Hoang, Michalis Polychronakis, and Phillipa Gill. Measuring the accessibility of domain name encryption and its impact on internet filtering. In *Proceedings of the Passive and Active Measurement Conference (PAM)*, pages 518–536, March 2022. *(Acceptance rate: 48%)*

6. Nguyen Phong Hoang, Arian Akhavan Niaki, Jakub Dalek, Jeffrey Knockel, Pellaeon Lin, Bill Marczak, Masashi Crete-Nishihata, Phillipa Gill, and Michalis Polychronakis. How great is the Great Firewall? measuring China's DNS censorship. In *Proceedings of the 30th USENIX Security Symposium*, pages 3381–3398, August 2021. *(Acceptance rate: 19%)*

7. Nguyen Phong Hoang, Arian Akhavan Niaki, Phillipa Gill, and Michalis Polychronakis. Domain name encryption is not enough: Privacy leakage via IP-based website fingerprinting. In *Proceedings on the 21st Privacy Enhancing Technologies Symposium (PoPETs)*, pages 420–440, July 2021. *(Acceptance rate: 19%)*

8. Tapti Palit, Jarin Firose Moon, Fabian Monrose, and Michalis Polychronakis. DynPTA: Combining static and dynamic analysis for practical selective data protection. In *Proceedings of the 42nd IEEE Symposium on Security & Privacy (S&P)*, pages 1919–1937, May 2021. *(Acceptance rate: 11.9%)*

9. Quan Chen, Panagiotis Ilia, Michalis Polychronakis, and Alexandros Kapravelos. Cookie swap party: Abusing first-party cookies for web tracking. In *Proceedings of the 30th Web Conference (WWW)*, pages 2117–2129, April 2021. *(Acceptance rate: 20.6%)*

10. Athanasios Kountouras, Panagiotis Kintis, Athanasios Avgetidis, Thomas Papastergiou, Chaz Lever, Michalis Polychronakis, and Manos Antonakakis. Understanding the growth and security considerations of ECS. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, February 2021. *(Acceptance rate: 16%)*

11. Sanjeev Das, Kedrian James, Jan Werner, Manos Antonakakis, Michalis Polychronakis, and Fabian Monrose. A flexible framework for expediting bug finding by leveraging past (mis-)behavior to discover new bugs. In *Proceedings of the 36th Annual Computer Security Applications Conference (ACSAC)*, pages 345–359, December 2020. *(Acceptance rate: 23.2%)*

12. Seyedhamed Ghavamnia, Tapti Palit, Azzedine Benameur, and Michalis Polychronakis. Confine: Automated system call policy generation for container attack surface reduction. In *Proceedings of the 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, pages 443–458, October 2020. *(Acceptance rate: 25.6%)*

13. Seyedhamed Ghavamnia, Tapti Palit, Shachee Mishra, and Michalis Polychronakis. Temporal system call specialization for attack surface reduction. In *Proceedings of the 29th USENIX Security Symposium*, pages 1749–1766, August 2020. *(Acceptance rate: 16.1%)*

14. Shachee Mishra and Michalis Polychronakis. Saffire: Context-sensitive function specialization and hardening against code reuse attacks. In *Proceedings of the 5th IEEE European Symposium on Security & Privacy (EuroS&P)*, pages 17–33, June 2020. *(Acceptance rate: 14.6%)*

15. Nguyen Phong Hoang, Arian Akhavan Niaki, Nikita Borisov, Phillipa Gill, and Michalis Polychronakis. Assessing the privacy benefits of domain name encryption. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (ASIACCS)*, pages 290–304, June 2020. *(Acceptance rate: 21.7%)*

16. Sergej Proskurin, Marius Momeu, Seyedhamed Ghavamnia, Vasileios P. Kemerlis, and Michalis Polychronakis. xMP: Selective memory protection for kernel and user space. In *Proceedings of the 41st IEEE Symposium on Security & Privacy (S&P)*, pages 603–617, May 2020. *(Acceptance rate: 12.7%)*

17. Tapti Palit, Fabian Monrose, and Michalis Polychronakis. Mitigating data leakage by protecting memory-resident sensitive data. In *Proceedings of the 35th Annual Computer Security Applications Conference (ACSAC)*, pages 598–611, December 2019. *(Acceptance rate: 22.6%)*

18. Jan Werner, Joshua Mason, Manos Antonakakis, Michalis Polychronakis, and Fabian Monrose. The severest of them all: Inference attacks against secure virtual enclaves. In *Proceedings of the 14th ACM Asia Conference on Computer and Communications Security (ASIACCS)*, pages 73–85, July 2019. *(Acceptance rate: 17%)*

19. Sanjeev Das, Jan Werner, Manos Antonakakis, Michalis Polychronakis, and Fabian Monrose. SoK: The challenges, pitfalls, and perils of using hardware performance counters for security. In *Proceedings of the 40th IEEE Symposium on Security & Privacy (S&P)*, pages 362–380, May 2019. *(Acceptance rate: 12.5%)*

20. Panagiotis Papadopoulos, Panagiotis Ilia, Michalis Polychronakis, Evangelos Markatos, Sotiris Ioannidis, and Giorgos Vasiliadis. Master of web puppets: Abusing web browsers for persistent and stealthy computation. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, February 2019. *(Acceptance rate: 17.1%)*

21. Shachee Mishra and Michalis Polychronakis. Shredder: Breaking exploits through API specialization. In *Proceedings of the 34th Annual Computer Security Applications Conference (ACSAC)*, pages 1–16, December 2018. *(Acceptance rate: 20.1%)*

22. Nguyen Phong Hoang, Panagiotis Kintis, Manos Antonakakis, and Michalis Polychronakis. An empirical study of the I2P anonymity network and its censorship resistance. In *Proceedings of the 18th Internet Measurement Conference (IMC)*, pages 379–392, October 2018. *(Acceptance rate: 24.7%)*

23. Hyungjoon Koo, Yaohui Chen, Long Lu, Vasileios P. Kemerlis, and Michalis Polychronakis. Compiler-assisted code randomization. In *Proceedings of the 39th IEEE Symposium on Security & Privacy (S&P)*, pages 472–488, May 2018. *(Acceptance rate: 13.3%)*

24. Micah Morton, Jan Werner, Panagiotis Kintis, Kevin Z. Snow, Manos Antonakakis, Michalis Polychronakis, and Fabian Monrose. Security risks in asynchronous web servers: When performance optimizations amplify the impact of data-oriented attacks. In *Proceedings of the 3rd IEEE European Symposium on Security & Privacy (EuroS&P)*, pages 167–182, April 2018. *(Acceptance rate: 22.9%)*

25. Giorgos Tsirantonakis, Panagiotis Ilia, Sotiris Ioannidis, Elias Athanasopoulos, and Michalis Polychronakis. A large-scale analysis of content modification by open HTTP proxies. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, February 2018. *(Acceptance rate: 21.5%)*

26. Mingwei Zhang, Michalis Polychronakis, and R. Sekar. Protecting COTS binaries from disclosure-guided code reuse attacks. In *Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC)*, pages 128–140, December 2017. *(Acceptance rate: 19.7%)*

27. 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)*, pages 143–160, July 2017. *(Acceptance rate: 37.5%)*

28. 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)*, pages 1009–1024, May 2017. *(Acceptance rate: 13.3%)*

29. Marios Pomonis, Theofilos Petsios, Angelos D. Keromytis, Michalis Polychronakis, and Vasileios P. Kemerlis. kR^X: Comprehensive kernel protection against just-in-time code reuse. In *Proceedings of the 12th European Conference on Computer Systems (EuroSys)*, pages 420–436, April 2017. *(Acceptance rate: 20%)*

30. 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 (EuroS&P)*, April 2017. *(Acceptance rate: 19.6%)*

31. 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. *(Acceptance rate: 13.5%)*

32. 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. *(Acceptance rate: 23.1%)*

33. 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. *(Acceptance rate: 23.1%)*

34. 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. *(Acceptance rate: 23.7%)*

35. 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. *(Acceptance rate: 24.3%)*

36. 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. *(Acceptance rate: 29.1%)*

37. 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. *(Acceptance rate: 29.1%)*

38. 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. *(Acceptance rate: 19.9%)*

39. 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. *(Acceptance rate: 19.5%)*

40. 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. *(Acceptance rate: 19.5%)*

41. 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. *(Acceptance rate: 19%)*

42. 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. *(Acceptance rate: 19%)*

43. 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. *(Acceptance rate: 18%)*

44. 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. *(Acceptance rate: 31.5%)*

45. 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. *(Acceptance rate: 19.8%)*

46. 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. *(Acceptance rate: 25.7%)*

47. Antonis Papadogiannakis, Michalis Polychronakis, and Evangelos P. Markatos. Scap: Stream-oriented network traffic capture and analysis for high-speed networks. In *Proceedings of the 13th Internet Measurement Conference (IMC)*, pages 441–454, October 2013. *(Acceptance rate: 23.6%)*

48. 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 13th Internet Measurement Conference (IMC)*, pages 277–290, October 2013. *(Acceptance rate: 23.6%)*

49. 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. *(Acceptance rate: 23.2%)*

50. 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. *(Acceptance rate: 23.2%)*

51. 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. *(Acceptance rate: 15.9%)*

52. 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. *(Acceptance rate: 32%)*

53. 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. *(Acceptance rate: 19.4%)*

54. 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. *(Acceptance rate: 17.2%)*

55. 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. *(Acceptance rate: 18.4%)*

56. 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. *(Acceptance rate: 13%)*

57. 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. *(Acceptance rate: 40%)*

58. 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. *(Acceptance rate: 37%)*

59. 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. *(Acceptance rate: 13.9%)*

60. 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. *(Acceptance rate: 26.3%)*

61. 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. *(Acceptance rate: 23%)*

62. 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. *(Acceptance rate: 17.2%)*

63. 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.

64. 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. *(Acceptance rate: 31.6%)*

65. 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. *(Acceptance rate: 28.8%)*

66. 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. *(Acceptance rate: 40.5%)*

67. 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. *(Acceptance rate: 25%)*

68. 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.

69. 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. *(Acceptance rate: 33.2%)*

70. 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. *(Acceptance rate: 16.8%)*

71. 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.

72. 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. *(Acceptance rate: 26.8%)*

73. 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. *(Acceptance rate: 28.5%)*

74. 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. *(Acceptance rate: 27.4%)*

75. 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. *(Acceptance rate: 27.4%)*

76. 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.

77. 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. *(Acceptance rate: 37.8%)*

78. Kostas G. Anagnostakis, Evangelos P. Markatos, Spyros Antonatos, and Michalis Polychronakis. E^2xB: 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. *(Acceptance rate: 27.2%)*

79. 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. Shachee Mishra and Michalis Polychronakis. SGXPecial: Specializing SGX interfaces against code reuse attacks. In *Proceedings of the 14th European Workshop on System Security (EuroSec)*, pages 48–54, March 2021. *(Acceptance rate: 56%)*

2. Nguyen Phong Hoang, Ivan Lin, Seyedhamed Ghavamnia, and Michalis Polychronakis. K-resolver: Towards decentralizing encrypted DNS resolution. In *Proceedings of the 2nd Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb)*, February 2020. *(Acceptance rate: 62%)*

3. Nguyen Phong Hoang, Sadie Doreen, and Michalis Polychronakis. Measuring I2P censorship at a global scale. In *Proceedings of the 9th USENIX Workshop on Free and Open Communications on the Internet (FOCI)*, August 2019. *(Acceptance rate: 63%)*

4. Hyungjoon Koo, Seyedhamed Ghavamnia, and Michalis Polychronakis. Configuration-driven software debloating. In *Proceedings of the 12th European Workshop on System Security (EuroSec)*, March 2019.

5. Panagiotis Papadopoulos, Antonis Papadogiannakis, Michalis Polychronakis, and Evangelos P. Markatos. Is privacy possible without anonymity? The case for microblogging services. In *Proceedings of the 12th European Workshop on System Security (EuroSec)*, March 2019.

6. 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. *(Acceptance rate: 42.8%)*

7. 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.

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

9. 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. *(Acceptance rate: 38%)*

10. 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. *(Acceptance rate: 35%)*

11. 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. *(Acceptance rate: 44.1%)*

12. 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. *(Acceptance rate: 40.1%)*

13. Michael Foukarakis, Demetres Antoniades, and Michalis Polychronakis. Deep packet anonymization. In *Proceedings of the 2nd European Workshop on System Security (EuroSec)*, March 2009. *(Acceptance rate: 32%)*

14. 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.

15. 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. *(Acceptance rate: 32.4%)*

16. 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.

17. 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.

18. 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.

19. 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).

20. 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.

21. 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 2nd International Workshop on Inter-Domain Performance and Simulation (IPS)*, March 2004.

Non-academic Refereed Conferences

1. Azzedine Benameur, Jay Chien-An Chen, Lei Ding, and Michalis Polychronakis. Container attack surface reduction beyond name space isolation. Black Hat Europe, December 2018.

2. Marios Pomonis, Theofilos Petsios, Angelos D. Keromytis, Michalis Polychronakis, and Vasileios P. Kemerlis. kRˆX: Comprehensive kernel protection against just-in-time code reuse. Black Hat USA, July 2017.

3. João Moreira, Sandro Rigo, Michalis Polychronakis, and Vasileios P. Kemerlis. Drop the ROP: Fine-grained control-flow integrity for the linux kernel. Black Hat Asia, March 2017.

4. Vasileios P. Kemerlis, Michalis Polychronakis, and Angelos D. Keromytis. ret2dir: Deconstructing kernel isolation. Black Hat Europe, October 2014.

Edited Books

1. Zhiqiang Lin, Charalampos Papamanthou, and Michalis Polychronakis, editors. *Information Security. 22nd International Conference, ISC 2019, New York City, NY, USA, September 16–18, 2019, Proceedings*, volume 11723 of *Security and Cryptology*. Springer, 2019. ISBN: 978-3-030-30215-3.

2. Marc Dacier, Michael Bailey, Michalis Polychronakis, and Manos Antonakakis, editors. *Research in Attacks, Intrusions, and Defenses. 20th International Symposium, RAID 2017, Atlanta, GA, USA, September 18–20, 2017, Proceedings*, volume 10453 of *Lecture Notes in Computer Science*. Springer, 2017. ISBN: 978-3-319-66331-9.

3. Michalis Polychronakis and Michael Meier, editors. *Detection of Intrusions and Malware, and Vulnerability Assessment. 14th International Conference, DIMVA 2017, Bonn, Germany, July 6–7, 2017, Proceedings*, volume 10327 of *Lecture Notes in Computer Science*. Springer, 2017. ISBN: 978-3-319-60875-4.

4. Michalis Polychronakis and Cristiano Giuffrida, editors. *Proceedings of the 9th European Workshop on System Security, EuroSec 2016, London, UK, April 18, 2016*. ACM, 2016. ISBN: 978-1-4503-4295-7.

5. Tal Malkin, Vladimir Kolesnikov, Allison Bishop Lewko, and Michalis Polychronakis, editors. *Applied Cryptography and Network Security. 13th International Conference, ACNS 2015, New York, NY, USA, June 2–5, 2015, Revised Selected Papers*, volume 9092 of *Lecture Notes in Computer Science*. Springer, 2015. ISBN: 978-3-319-28165-0.

6. Juan Caballero and Michalis Polychronakis, editors. *Proceedings of the 8th European Workshop on System Security, EuroSec 2015, Bordeaux, France, April 21, 2015*. ACM, 2015. ISBN: 978-1-4503-3479-2.

Book Chapters

1. Georgios Kontaxis, Michalis Polychronakis, and Angelos D. Keromytis. Computational decoys for cloud security. In *Secure Cloud Computing*, pages 261–270. Springer, 2014. ISBN: 978-1-4614-9277-1.

2. Vasilis Pappas, Michalis Polychronakis, and Angelos D. Keromytis. Practical software diversification using in-place code randomization. In Sushil Jajodia, Anup K. Ghosh, V. S. Subrahmanian, Vipin Swarup, Cliff Wang, and X. Sean Wang, editors, *Moving Target Defense II: Application of Game Theory and Adversarial Modeling*, pages 169–196. Springer, 2012. ISBN: 978-1-4614-5415-1.

3. Michalis Polychronakis. Reverse engineering of malware emulators. In Henk C.A. van Tilborg and Sushil Jajodia, editors, *Encyclopedia of Cryptography and Security, 2nd Edition*, pages 1043–1044. Springer, 2011. ISBN: 978-1-4419-5905-8.

PhD Thesis

1. Michalis Polychronakis. *Generic Detection of Code Injection Attacks using Network-level Emulation*. PhD thesis, University of Crete, October 2009.

Patents

1. Jan Jakub Werner, Kevin Zachary Snow, Nathan Michael Otterness, Robert John Dallara, Georgios Baltas, Fabian Newman Monrose, and Michalis Polychronakis. Methods, systems, and computer readable media for preventing code reuse attacks. US Patent 10,628,589, April 2020.

2. 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, 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, Evangelos Markatos, Yannis Mitsos, Slavko Gajin, and Goran Muratovski. Real-world polymorphic attack detection. *ENISA Quarterly*, 4(2), Apr–Jun 2008.
3. Michalis Polychronakis, Kostas Anagnostakis, and Evangelos Markatos. LOBSTER: Detecting internet attacks (in Greek). *The Economist (Greek Edition)*, Issue 43, September 2007.
4. 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

- [Keynote Talk] Language-enforced Data Confidentiality against Memory Disclosure and Transient Execution Attacks. ACNS 2023, June 2023, Japan.
- Defending against Memory Corruption and Transient Execution Attacks. John Jay College of Criminal Justice, March 2023, USA.
- Decap: Deprivileging Programs by Reducing Their Capabilities. FORTH-ICS, August 2022, Greece.
- Defending against Memory Corruption and Transient Execution Attacks. University of Crete, April 2022, Greece.
- Defending against Memory Corruption and Transient Execution Attacks. Sungkyunkwan University, November 2021.
- Defending against Memory Corruption and Transient Execution Attacks. Brave, August 2021.
- Defending against Memory Corruption Vulnerability Exploitation. REACT Project Workshop, May 2021.
- Software Specialization for Attack Surface Reduction. University of Crete, March 2021, Greece.
- Software Specialization for Attack Surface Reduction. Ohio State University, September 2020, USA.
- Memory Corruption Vulnerability Exploitation and Mitigations. Dagstuhl Seminar 19451 "Biggest Failures in Security," November 2019, Germany.
- Practical Software Specialization against Vulnerability Exploitation. F-Secure Consulting NYC, October 2019, USA.
- Practical Software Specialization against Vulnerability Exploitation. Brave, November 2018, USA.
- Practical Software Specialization against Vulnerability Exploitation. Accenture, November 2018, USA.
- 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.