

Georgios Portokalidis

Associate Research Professor, IMDEA Software Institute, Madrid, Spain

<https://www.portokalidis.net>

Academic Positions Held

Associate Research Professor IMDEA Software Institute, Madrid, Spain	(September 2023 – present)
Visiting Research Professor Stevens Institute of Technology, Hoboken, NJ, USA	(September 2024 – present)
Associate Professor of Computer Science Stevens Institute of Technology, Hoboken, NJ, USA	(September 2019 – August 2024)
Visiting Associate Professor of Computer Science National University of Singapore, Singapore	(January 2020 – July 2020)
Assistant Professor of Computer Science Stevens Institute of Technology, Hoboken, NJ, USA	(January 2013 – August 2019)
Postdoctoral researcher Columbia University, New York, NY, USA <i>Advisor: Angelos Keromytis</i>	(March 2010 – December 2012)

Education

PhD Computer Science, Vrije University, Amsterdam, The Netherlands Dissertation title: “Using Virtualisation Against Zero-Day Attacks” <i>Advisor: Herbert Bos, Promoter: Henri Bal</i>	(February 2010)
MSc Computer Science, Leiden University, Leiden, The Netherlands Dissertation title: “Zero Hour Worm Detection and Containment Using Honeypots” <i>Advisor: Herbert Bos</i>	(December 2004)
BSc Computer Science, University of Crete, Heraklion, Greece Dissertation title: “Study and Bridging of Peer-to-Peer File Sharing Systems” <i>Advisor: Evangelos P. Markatos, Co-advisor: Manolis Marazakis</i>	(July 2002)

Support for Research (Grants and Awards)

María de Maeztu Unit of Excellence in Research Awarded to IMDEA Software, MICIU/AEI, €3M	(April 2025 - March 2029)
Effective Software Monitoring Leveraging Hardware Debugging Extensions PI, DARPA YFA, \$492,490	(August 2021 – December 2023)
ABIDES: Adaptive BInary Debloating and Security PI (lead), ONR, \$3,243,244 (Stevens \$1,052,376)	(September 2017 – August 2022)
Adapting Static and Dynamic Program Analysis to Effectively Harden Debloated Software PI, ONR, \$467,543	(March 2016 – December 2020)
Trails: Efficient Data-Flow Tracking Through HW-assisted Parallelization PI, DARPA, \$462,419	(September 2016 – August 2019)

MINESTRONE (September 2013 – November 2014)
PI, IARPA, \$65,796
Task: Automatic Discovery of Rescue Points Using Static and Dynamic Analysis phase 3 extension

MINESTRONE (January 2013 – November 2014)
PI, IARPA, \$247,641
Task: Automatic Discovery of Rescue Points Using Static and Dynamic Analysis

Awards and Distinctions

Academic Honors

Charles Berendsen Junior Professorship in Computer Science (September 2018 – August 2021)
Stevens Institute of Technology

Provost's Award for Research Excellence (May 2018)
Stevens Institute of Technology

Paper Awards

Pwnie award for most innovative research at the Blackhat 2021 conference (August 2021)
“Speculative Probing: Hacking Blind in the Spectre Era”
Enes Gökteş, Kaveh Razavi, Georgios Portokalidis, Herbert Bos, and Cristiano Giuffrida

Outstanding paper award at ACSAC 2015 (December 2015)
“ShrinkWrap: VTable Protection without Loose Ends”
Istvan Haller, Enes Gökteş, Elias Athanasopoulos, Georgios Portokalidis, and Herbert Bos

DCSRA 2015 winner (March 2015)
Our paper was unanimously selected by the jury as excellent Dutch Cyber Security Research paper
“Out Of Control: Overcoming Control-Flow Integrity”
Enes Gökteş, Elias Athanasopoulos, Herbert Bos, and Georgios Portokalidis

Best paper award at the 6th IWSEC (November 2011)
“REASSURE: A Self-contained Mechanism for Healing Software Using Rescue Points”
Georgios Portokalidis and Angelos D. Keromytis

Publications

Peer-reviewed Conferences and Workshops

- StreamCFI: Streamed Per-Input Control-Flow Integrity**
Konstantinos Kleftogiorgos, Cristiano Giuffrida, and Georgios Portokalidis
To appear in Proceedings of the IEEE European Symposium on Security and Privacy, Lisbon, Portugal, July 2026 (15.9%)
- Lessons Learned from Five Years of Artifact Evaluations at EuroSys**
Daniele Cono D'Elia, Thaleia Doudali, Cristiano Giuffrida, Miguel Matos, Mathias Payer, Solal Pirelli, Georgios Portokalidis, Valerio Schiavoni, Salvatore Signorello, and Anjo Vahldiek-Oberwagner
Proceedings of the ACM Conference on Reproducibility and Replicability (REP), Vancouver, Canada, July 2025
- rustc++: Facilitating Advanced Analysis of Rust Code**
Antonios Louka, Georgios Portokalidis, and Elias Athanasopoulos
Proceedings of the European Workshop on Systems Security (EUROSEC), Rotterdam, The Netherlands, April 2025 (57.9%)

4. **SIDECAR: Leveraging Debugging Extensions in Commodity Processors to Secure Software**
Konstantinos Kleftogiorgos, Patrick Zielinski, Shan Huang, Jun Xu, and Georgios Portokalidis
Proceedings of the Annual Computer Security Applications Conference (ACSAC), Waikiki, Hawaii, USA, December 2024 (19.7%)
5. **Evaluating the Effect of Improved Indirect Call Resolution on System Call Debloating**
Vidya Lakshmi Rajagopalan and Georgios Portokalidis
Proceedings of the Workshop on Forming an Ecosystem Around Software Transformation (FEAST), Salt Lake City, Utah, USA, October 2024
6. **On the Dual Nature of Necessity in Use of Rust Unsafe Code**
Yuchen Zhang, Ashish Kundu, Georgios Portokalidis, and Jun Xu
Proceedings of the ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE) (Industry Track), San Francisco, USA, December 2023 (44%)
7. **SysPart: Automated Temporal System Call Filtering for Binaries**
Vidya Lakshmi Rajagopalan, Konstantinos Kleftogiorgos, Enes Göktaş, Jun Xu, and Georgios Portokalidis
Proceedings of the ACM Conference on Computer and Communications Security (CCS), Copenhagen, Denmark, November 2023 (19.9%)
8. **Eliminating Vulnerabilities by Disabling Unwanted Functionality in Binary Programs**
Mohamad Mansouri, Jun Xu, and Georgios Portokalidis
Proceedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS), Melbourne, Australia, July 2023
9. **Towards Understanding the Performance of Rust (Short paper)**
Yuchen Zhang, Yunhang Zhang, Georgios Portokalidis, and Jun Xu
Proceedings of the International Conference on Automated Software Engineering (ASE) – Industry Showcase, Oakland Center, MI, USA, October 2022
10. **Debloating Address Sanitizer**
Yuchen Zhang, Chengbin Pang, Georgios Portokalidis, Nikos Triandopoulos, and Jun Xu
Proceedings of the USENIX Security Symposium, Boston, MA, USA, August 2022 (18.1%)
11. **An In-Depth Analysis on Adoption of Attack Mitigations in Embedded Devices (invited)**
Ruotong Yu, Francesca Del Nin, Yuchen Zhang, Shan Huang, Pallavi Kaliyar, Sarah Zatzko, Mauro Conti, Georgios Portokalidis, and Jun Xu
The Learning from Authoritative Security Experiment Results (LASER) workshop, San Diego, CA, USA, April 2022
12. **Building Embedded Systems Like It's 1996**
Ruotong Yu, Francesca Del Nin, Yuchen Zhang, Shan Huang, Pallavi Kaliyar, Sarah Zatzko, Mauro Conti, Georgios Portokalidis, and Jun Xu
Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, April 2022 (16.2%)
13. **Proving LTL Properties of Bitvector Programs and Decompiled Binaries**
Yuandong Cyrus Liu, Chengbin Pang, Daniel Dietsch, Eric Koskinen, Ton Chanh Le, Georgios Portokalidis, and Jun Xu
Proceedings of the Asian Symposium on Programming Languages and Systems (APLAS), Chicago, IL, USA, October 2021
14. **Towards Optimal Use of Exception Handling Information for Function Detection**
Chengbin Pang, Ruotong Yu, Dongpeng Xu, Eric Koskinen, Georgios Portokalidis, and Jun Xu
Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Virtual, June 2021 (16.3%)
15. **SoK: All You Ever Wanted to Know About x86/x64 Binary Disassembly But Were Afraid to Ask**
Chengbin Pang, Ruotong Yu, Yaohui Chen, Eric Koskinen, Georgios Portokalidis, Bing Mao, and Jun Xu
Proceedings of the IEEE Symposium on Security and Privacy, Virtual, May 2021 (12.1%)

16. **Speculative Probing: Hacking Blind in the Spectre Era**
Enes Göktaş, Kaveh Razavi, Georgios Portokalidis, Herbert Bos, and Cristiano Giuffrida
Proceedings of the ACM Conference on Computer and Communications Security (CCS), Virtual, November 2020 (16.9%) Pwnie award for most innovative research
17. **Nibbler: Debloating Binary Shared Libraries**
Ioannis Agadacos, Di Jin, David Williams-King, Vasileios P. Kemerlis, and Georgios Portokalidis
Proceedings of the Annual Computer Security Applications Conference (ACSAC), San Juan, Puerto Rico, December 2019 (22.6%)
18. **Position-independent Code Reuse: On the Effectiveness of ASLR in the Absence of Information Disclosure**
Enes Göktaş, Benjamin Kollenda, Philipp Koppe, Eric Bosman, Georgios Portokalidis, Thorsten Holz, Herbert Bos, and Cristiano Giuffrida
Proceedings of the IEEE European Symposium on Security and Privacy, London, United Kingdom, April 2018 (22.9%)
19. **Techu: Open and Privacy-preserving Crowdsourced GPS for the Masses**
Ioannis Agadacos, Jason Polakis, and Georgios Portokalidis
Proceedings of the ACM International Conference on Mobile Systems, Applications, and Services (MobiSys), Niagara Falls, NY, USA, June 2017 (18%)
20. **Location-enhanced Authentication using the IoT**
Ioannis Agadacos, Per Hallgren, Dimitrios Damopoulos, Andrei Sabelfeld, and Georgios Portokalidis
Proceedings of the Annual Computer Security Applications Conference (ACSAC), Los Angeles, CA, USA, December 2016 (22.8%)
21. **Bypassing CLANG's Safestack for Fun and Profit**
Aggelos Oikonomopoulos, Benjamin Kollenda, Cristiano Giuffrida, Elias Athanasopoulos, Enes Göktaş, Georgios Portokalidis, Herbert Bos, and Robert Gawlik
Black Hat Europe, London, UK, November 2016
22. **NaCIDroid: Native Code Isolation for Android Applications**
Elias Athanasopoulos, Vasileios P. Kemerlis, Georgios Portokalidis, and Angelos D. Keromytis
Proceedings of the European Symposium on Research in Computer Security (ESORICS), Heraklion, Crete, Greece, September 2016 (21%)
23. **Undermining Entropy-based Information Hiding (And What to do About it)**
Enes Göktaş, Robert Gawlik, Benjamin Kollenda, Elias Athanasopoulos, Georgios Portokalidis, Cristiano Giuffrida, and Herbert Bos
Proceedings of the USENIX Security Symposium, Austin, TX, USA, August 2016 (15.55%)
24. **Speculative Memory Checkpointing**
Dirk Vogt, Armando Miraglia, Georgios Portokalidis, Herbert Bos, Andy Tanenbaum, and Cristiano Giuffrida
Proceedings of the ACM/IFIP/USENIX Middleware Conference, Vancouver, Canada, December 2015
25. **ShrinkWrap: VTable Protection without Loose Ends**
Istvan Haller, Enes Göktaş, Elias Athanasopoulos, Georgios Portokalidis, and Herbert Bos
Proceedings of the Annual Computer Security Applications Conference (ACSAC), Los Angeles, CA, USA, December 2015 (24.4%) Outstanding student paper award
26. **WYSISNWIV: What You Scan Is Not What I Visit**
Qilang Yang, Dimitrios Damopoulos, and Georgios Portokalidis
Proceedings of the International Symposium on Recent Advances in Intrusion Detection (RAID), Kyoto, Japan, November 2015 (22.69%)
27. **GPU-Disasm: A GPU based x86 Disassembler**
Evangelos Ladakis, Giorgos Vasiliadis, Michalis Polychronakis, Sotiris Ioannidis, and Georgios Portokalidis
Proceedings of the Information Security Conference (ISC), Trondheim, Norway, September 2015 (29.1%)

28. **The Devil is in the Constants: Bypassing Defenses in Browser JIT Engines**
Michalis Athanasakis, Elias Athanasopoulos, Michalis Polychronakis, Georgios Portokalidis, and Sotiris Ioannidis
Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, February 2015 (19.6%)
29. **Size Does Matter - Why Using Gadget-Chain Length to Prevent Code-reuse Attacks is Hard**
Enes Göktaş, Elias Athanasopoulos, Michalis Polychronakis, Herbert Bos, and Georgios Portokalidis
Proceedings of the USENIX Security Symposium, San Diego, CA, USA, August 2014 (19.1%)
30. **Out Of Control: Overcoming Control-Flow Integrity**
Enes Göktaş, Elias Athanasopoulos, Herbert Bos, and Georgios Portokalidis
Proceedings of the IEEE Symposium on Security and Privacy, San Jose, CA, USA, May 2014 (13.6%) DCSRA 2015 winner
31. **The Best of Both Worlds. A Framework for the Synergistic Operation of Host and Cloud Anomaly-based IDS for Smartphones**
Dimitrios Damopoulos, Georgios Kambourakis, and Georgios Portokalidis
Proceedings of the European Workshop on System Security (EUROSEC), Amsterdam, The Netherlands, April 2014 (42.9%)
32. **On the Effectiveness of Traffic Analysis Against Anonymity Networks Using Flow Records**
Sambuddho Chakravarty, Marco V. Barbera, Georgios Portokalidis, Michalis Polychronakis, and Angelos D. Keromytis
Proceedings of the Passive and Active Measurement (PAM) Conference, Los Angeles, CA, USA, March 2014 (31.5%)
33. **SAuth: Protecting User Accounts from Password Database Leaks**
Georgios Kontaxis, Elias Athanasopoulos, Georgios Portokalidis, and Angelos D. Keromytis
Proceedings of the ACM Conference on Computer and Communications Security (CCS), Berlin, Germany, November 2013 (19.8%)
34. **ShadowReplica: Efficient Parallelization of Dynamic Data Flow Tracking**
Kangkook Jee, Vasileios P. Kemerlis, Angelos D. Keromytis, and Georgios Portokalidis
Proceedings of the ACM Conference on Computer and Communications Security (CCS), Berlin, Germany, November 2013 (19.8%)
35. **Cloudopsy: an Autopsy of Data Flows in the Cloud**
Angeliki Zavou, Vasilis Pappas, Vasileios P. Kemerlis, Michalis Polychronakis, Georgios Portokalidis, and Angelos D. Keromytis
Proceedings of the International Conference on Human-Computer Interaction (HCI), Las Vegas, NV, USA, July 2013
36. **Self-Healing Multitier Architectures Using Cascading Rescue Points**
Angeliki Zavou, Georgios Portokalidis, and Angelos D. Keromytis
Proceedings of the Annual Computer Security Applications Conference (ACSAC), Orlando, FL, USA, December 2012 (19%)
37. **Exploiting Split Browsers for Efficiently Protecting User Data**
Angeliki Zavou, Elias Athanasopoulos, Georgios Portokalidis, and Angelos D. Keromytis
Proceedings of The ACM Cloud Computing Security Workshop (CCSW), Raleigh, NC, USA, October 2012
38. **Adaptive Defenses for Commodity Software through Virtual Application Partitioning**
Dimitris Geneiatakis, Georgios Portokalidis, Vasileios P. Kemerlis, and Angelos D. Keromytis
Proceedings of the ACM Conference on Computer and Communications Security (CCS), Raleigh, NC, USA, October 2012 (18.9%)
39. **kGuard: Lightweight Kernel Protection against Return-to-user Attacks**
Vasileios P. Kemerlis, Georgios Portokalidis, and Angelos D. Keromytis
Proceedings of the USENIX Security Symposium, Bellevue, WA, USA, August 2012 (19.4%)

40. **libdft: Practical Dynamic Data Flow Tracking for Commodity Systems**
Vasileios P. Kemerlis, Georgios Portokalidis, Kangkook Jee, and Angelos D. Keromytis
Proceedings of the ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments (VEE), London, UK, March 2012
41. **A General Approach for Efficiently Accelerating Software-based Dynamic Data Flow Tracking on Commodity Hardware**
Kangkook Jee, Georgios Portokalidis, Vasileios P. Kemerlis, Soumyadeep Ghosh, David I. August, and Angelos D. Keromytis
Proceedings of the Annual Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, February 2012 (17.8%)
42. **A Multilayer Overlay Network Architecture for Enhancing IP Service Availability Against DoS**
Dimitris Geneiatakis, Georgios Portokalidis, and Angelos D. Keromytis
Proceedings of the International Conference on Information Systems Security (ICISS), Kolkata, India, December 2011 (22.8%)
43. **REASSURE: A Self-contained Mechanism for Healing Software Using Rescue Points**
Georgios Portokalidis and Angelos D. Keromytis
*Proceedings of the International Workshop on Security (IWSEC), Tokyo, Japan, November 2011 **Best paper award***
44. **Taint-Exchange: a Generic System for Cross-process and Cross-host Taint Tracking**
Angeliki Zavou, Georgios Portokalidis, and Angelos D. Keromytis
Proceedings of the International Workshop on Security (IWSEC), Tokyo, Japan, November 2011
45. **Detecting Traffic Snooping in Tor Using Decoys**
Sambuddho Chakravarty, Georgios Portokalidis, Michalis Polychronakis, and Angelos D. Keromytis
Proceedings of the International Symposium on Recent Advances in Intrusion Detection (RAID), Menlo Park, CA, USA, September 2011 (23%)
46. **Global ISR: Toward a Comprehensive Defense Against Unauthorized Code Execution**
Georgios Portokalidis and Angelos D. Keromytis
Proceedings of the ARO Workshop on Moving Target Defense, Fairfax, VA, USA, January 2011
47. **Fast and Practical Instruction-Set Randomization for Commodity Systems**
Georgios Portokalidis and Angelos D. Keromytis
Proceedings of the Annual Computer Security Applications Conference (ACSAC), Austin, TX, USA, December 2010 (17%)
48. **Paranoid Android: Versatile Protection For Smartphones**
Georgios Portokalidis, Philip Homburg, Kostas Anagnostakis, and Herbert Bos
Proceedings of the Annual Computer Security Applications Conference (ACSAC), Austin, TX, USA, December 2010 (17%)
49. **iLeak: a Lightweight System for Detecting Inadvertent Information Leaks**
Vasileios P. Kemerlis, Vasilis Pappas, Georgios Portokalidis, and Angelos D. Keromytis
Proceedings of the European Conference on Computer Network Defense (EC2ND), Berlin, Germany, October 2010
50. **Eudaemon: Involuntary and On-Demand Emulation Against Zero-Day Exploits**
Georgios Portokalidis and Herbert Bos
Proceedings of the ACM SIGOPS/EuroSys European Conference on Computer Systems, Glasgow, Scotland, April 2008 (18%)
51. **Argos: Emulated Hardware Support to Fingerprint Zero-Day Attacks by Means of Dynamic Data Flow Analysis**
Georgios Portokalidis, Asia Slowinska, and Herbert Bos
Proceedings of the Annual Conference of the Advanced School for Computing and Imaging (ASCI), Belgium, June 2006

52. **Argos: an Emulator for Fingerprinting Zero-Day Attacks**
Georgios Portokalidis, Asia Slowinska, and Herbert Bos
Proceedings of ACM SIGOPS EUROSYS, Leuven, Belgium, April 2006 (20%)
53. **Argos: Securing IP Communications Against Zero-Day Attacks**
Georgios Portokalidis, Asia Slowinska, and Herbert Bos
Proceedings of NLUUG Unix Users Group Annual Conference, The Netherlands, April 2006 (invited)
54. **FFPF: Fairly Fast Packet Filters**
Herbert Bos, Willem Bruijn, Mihai Cristea, Trung Nguyen, and Georgios Portokalidis
Proceedings of the USENIX Symposium on Operating Systems Design and Implementation (OSDI), San Francisco, CA, USA, December 2004 (14%)

Patents

1. **Methods, Systems, and Media for Authenticating Users Using Multiple Services**
Angelos D. Keromytis, Elias Athanasopoulos, Georgios Kontaxis, and Georgios Portokalidis
U.S. Patent US10367797. Issued on July 30, 2019

Journals

1. **Large-Scale Debloating of Binary Shared Libraries**
Ioannis Agadakos, Nicholas Demarinis, Di Jin, Kent Williams-King, Jearson Alfajardo, Benjamin Shteinfeld, David Williams-King, Vasileios P. Kemerlis, and Georgios Portokalidis
Digital Threats: Research and Practice (DTRAP) (Volume 1, Issue 4, Pages 1–28, December 2020)
2. **Detection and Analysis of Eavesdropping in Anonymous Communication Networks**
Sambuddho Chakravarty, Georgios Portokalidis, Michalis Polychronakis, and Angelos D. Keromytis
International Journal of Information Security (IJIS) (Volume 14, Issue 3, Pages 205–220, August 2015)
3. **kGuard: Lightweight Kernel Protection**
Vasileios P. Kemerlis, Georgios Portokalidis, Elias Athanasopoulos, and Angelos D. Keromytis
USENIX/login: Magazine (Volume 37, Issue 6, Pages 7–14, December 2012)
4. **SweetBait: Zero-hour worm detection and containment using low- and high-interaction honeypots**
Georgios Portokalidis and Herbert Bos
Elsevier Journal on Computer Networks, Special Issue on Security through Self-Protecting and Self-Healing Systems (Volume 51, Issue 5, Pages 1256–1274, April 2007)

Books/Book Chapters

1. **Evaluating Control-Flow Restricting Defenses**
Enes Göktaş, Elias Athanasopoulos, Herbert Bos, and Georgios Portokalidis
In Per Larsen and Ahmad-Reza Sadeghi, editors, The Continuing Arms Race: Code-Reuse Attacks and Defenses, chapter 5, pages 117–137. ACM and Morgan & Claypool, 2018

Technical Reports

1. **On the Effectiveness of Traffic Analysis Against Anonymity Networks Using Flow Records**
Sambuddho Chakravarty, Marco V. Barbera, Georgios Portokalidis, Michalis Polychronakis, and Angelos D. Keromytis
Technical report CUCS-019-13, Columbia University, New York, NY, USA, July 2013
2. **libdft: Practical Dynamic Data Flow Tracking for Commodity Systems**
Vasileios P. Kemerlis, Georgios Portokalidis, Kangkook Jee, and Angelos D. Keromytis
Technical report CUCS-044-11, Columbia University, New York, NY, USA, October 2011
3. **Detecting Traffic Snooping in Anonymity Networks Using Decoys**
Sambuddho Chakravarty, Georgios Portokalidis, Michalis Polychronakis, and Angelos D. Keromytis
Technical report CUCS-005-11, Columbia University, New York, NY, USA, February 2011

4. **Protecting Smart Phones by Means of Execution Replication**
Georgios Portokalidis, Philip Homburg, Kostas Anagnostakis, and Herbert Bos
Technical report IR-CS-054, Vrije Universiteit, Amsterdam, The Netherlands, September 2009
5. **Multi-tier intrusion detection by means of replayable virtual machines**
Auke Folkerts, Georgios Portokalidis, and Herbert Bos
Technical report IR-CS-047, Vrije Universiteit, Amsterdam, The Netherlands, August 2008
6. **Prospector: a Protocol-Specific Detector of Polymorphic Buffer Overflows**
Asia Slowinska, Georgios Portokalidis, and Herbert Bos
Technical report IR-CS-023, Vrije Universiteit, Amsterdam, The Netherlands, June 2006
7. **Argos: an x86 Emulator for Fingerprinting Zero-Day Attacks by Means of Dynamic Data Flow Analysis**
Georgios Portokalidis, Asia Slowinska, and Herbert Bos
Technical report IR-CS-017, Vrije Universiteit, Amsterdam, The Netherlands, June 2005
8. **SweetBait: Zero-Hour Worm Detection and Containment Using Honeypots**
Georgios Portokalidis and Herbert Bos
Technical report IR-CS-015, Vrije Universiteit, Amsterdam, The Netherlands, May 2005
9. **Packet Monitoring at High Speed with FFPF**
Georgios Portokalidis and Herbert Bos
Technical report 2004-01, LIACS, Leiden University, Leiden, The Netherlands, January 2004
10. **Study and Bridging of Peer-to-Peer File Sharing Systems**
Georgios Portokalidis, Evangelos P. Markatos, and Manolis Marazakis
Technical report 312, ICS-FORTH, Heraklion, Crete, Greece, October 2002

Unpublished

1. **Redirect2Own: Protecting the Intellectual Property of User-uploaded Content through Off-site Indirect Access**
Georgios Kontaxis, Angelos D. Keromytis, and Georgios Portokalidis
arXiv:1810.04779, October 2018
2. **Hands-Free One-Time and Continuous Authentication Using Glass Wearable Devices**
Dimitrios Damopoulos and Georgios Portokalidis
arXiv:1810.02496, October 2018

Talks and Panels

Talks

1. **Offloading Security Policy Enforcement Using Processor Debugging Extensions**
7th Huawei Forum on Trust and Privacy for the Future Digital World, Singapore, November 2024
2. **Securing Software by Mitigating Risks through System Call-Based Compartmentalization**
3rd Huawei Paris Workshop on Building Open Trust Systems, Paris, France, May 2024
3. **Harder, Better, Faster, Stronger: Establishing Trustworthy Software and Systems**
IMDEA Software Institute, Madrid, Spain, April 2023
Host: Juan Caballero
4. **Harder, Better, Faster, Stronger: Establishing Trustworthy Software and Systems**
North Carolina State University, Raleigh, NC, USA, March 2023
Host: William Enck
5. **New Challenges and Solutions for Kernel Security in the Spectre Era**
Telefonica Research, Barcelona, Spain, December 2022
Host: Ioannis Arapakis

6. **Effective Software Monitoring Leveraging Hardware Debugging Extensions**
CAREER Club Symposium, Stevens Institute of Technology, NJ, USA, November 2021
7. **Improving Software Security and Reliability**
SES Virtual Research Forum, Stevens Institute of Technology, NJ, USA, November 2020
8. **Hardening Binary Software Through Debloating**
United Technologies Research Center, Rome, Italy, December 2019
Host: Valerio Senni
9. **Hardening Binary Software Through Debloating**
Institute of Computer Science, FORTH, Heraklion, Crete, Greece, December 2019
Host: Evangelos Markatos
10. **Hardening Binary Software Through Debloating**
Athens University of Economics, Athens, Greece, December 2019
Host: Georgios Polyzos
11. **Better Security by Debloating Binary Shared Libraries**
Vrije University, Amsterdam, The Netherlands, October 2019
Host: Herbert Bos
12. **Improving Systems Security through Software Debloating**
University of California Santa Barbara, CA, USA, June 2018
Host: Christopher Kruegel
13. **Improving Systems Security through Attack Surface Reduction and Execution Transparency**
Ohio State University, Columbus, OH, USA, April 2018
Host: Zhiqiang Lin
14. **Improving Systems Security through Attack Surface Reduction and Execution Transparency**
National and Kapodistrian University of Athens, Athens, Greece, November 2017
Host: Mema Roussopoulos
15. **Improving Systems Security through Attack Surface Reduction and Execution Transparency**
Vrije Universiteit, Amsterdam, The Netherlands, November 2017
Host: Herbert Bos
16. **Improving Systems Security through Attack Surface Reduction and Execution Transparency**
University of Padova, Padua, Italy, November 2017
Host: Mauro Conti
17. **Code-Reuse Attacks and Software Surface**
Security & Privacy Day, Stony Brook University, New York, NY, USA, October 2017
18. **Understanding Code-Reuse Attacks and Reducing Attack Surface**
MIT, Boston, MA, USA, October 2017
Host: Stelios Sidiroglou-Douskos
19. **Understanding Code-Reuse Attacks and Reducing Attack Surface**
Northeastern University, Boston, MA, USA, October 2017
Host: Engin Kirda
20. **Securing Financial Transactions with IoT-powered Location-based Authentication**
FinCyberSec Conference, Stevens Institute of Technology, May 2017
21. **Out of Control**
Vrije Universiteit, Amsterdam, The Netherlands, October 2016

22. **Improving Software Resiliency Against Code-Reuse Attacks**
Athens University of Economics and Business, October 2016
23. **Improving Software Resiliency Against Code-Reuse Attacks**
Aristotle University of Thessaloniki, October 2016
24. **WYSISNWIV: What You Scan Is Not What I Visit**
International Symposium on Recent Advances in Intrusion Detection (RAID), Kyoto, Japan, November 2015
25. **WYSISNWIV: What You Scan Is Not What I Visit**
Stony Brook University's CEWIT 2015 conference, Stony Brook, NY, USA, October 2015
26. **Using the Internet of Things to Augment Security Decisions**
International Workshop on Cyber Threat Resilience, IIITM-K, Kerala, India, October 2015
27. **Evaluation Tools and Metrics for Control-flow Integrity Defenses**
Dagstuhl seminar "The Continuing Arms Race: Code-Reuse Attacks and Defenses", Dagstuhl, Germany, July 2015
28. **How about some control-flow integrity**
FORTH-ICS, Heraklion, Crete, Greece, July 2014
29. **From Hacking for Fun to Cyber-crime and Cyber-warfare, and How Can We Stop It**
Kaspersky "CyberSecurity for the Next Generation", The Americas Round 2014, Washington D.C., April 2014
30. **From Hacking for Fun to Cyber-crime and Cyber-warfare, and How Can We Stop It**
Vrije Universiteit, Amsterdam, The Netherlands, November 2013
31. **Protecting Commodity Software**
Northeastern University, Boston, MA, USA, April 2013
32. **Protecting Commodity Software**
University of Twente, Enschede, The Netherlands, June 2012
33. **Protecting Commodity Software**
University of California, Riverside, CA, USA, March 2012
34. **Protecting Commodity Software**
Stevens Institute of Technology, Hoboken, NJ, USA, January 2012
35. **Paranoid Android: Versatile Protection For Smartphones**
AT&T Security Research Center, New York, NY, USA, December 2011
36. **Using Rescue Points**
International Workshop on Security (IWSEC), Tokyo, Japan, November 2011
37. **Paranoid Android: Versatile Protection For Smartphones**
Annual Computer Security Applications Conference (ACSAC), Austin, TX, USA, December 2010
38. **iLeak: a Lightweight System for Detecting Inadvertent Information Leaks**
European Conference on Computer Network Defense (EC2ND), Berlin, Germany, October 2010
39. **Heavyweight Protection for Lightweight Devices**
Internet Research Group, Telefonica Research, Barcelona, Spain, May 2009
40. **Tutorial on Information Flow Tracking**
European Conference on Computer Network Defense (EC2ND), Dublin, Ireland, December 2008
41. **Eudaemon: Involuntary and On-Demand Emulation Against Zero-Day Exploits**
ACM SIGOPS/EuroSys European Conference on Computer Systems, Glasgow, Scotland, April 2008
42. **Argos: an Emulator for Fingerprinting Zero-Day Attacks**
IBM Research, Zürich, Switzerland, July 2006

43. **Argos: Emulated Hardware Support to Fingerprint Zero-Day Attacks by Means of Dynamic Data Flow Analysis**
Annual Conference of the Advanced School for Computing and Imaging (ASCI), Belgium, June 2006
44. **Argos: Securing IP Communications Against Zero-Day Attacks**
NLUUG Unix Users Group Annual Conference, The Netherlands, April 2006
45. **Argos: an Emulator for Fingerprinting Zero-Day Attacks**
ACM SIGOPS EUROSYS, Leuven, Belgium, April 2006

Panels

1. **Panel on Security in Wireless Networks and Mobile Devices (Panelist)**
In the 28th IEEE Annual Computer Communications Workshop (CCW), November 2014
2. **Panel on Emerging Research Directions (Panelist)**
European Workshop on System Security (EUROSEC), March 2009
3. **Panel on Future and Emerging Threats in Information and Communication Technology Infrastructures (Panelist)**
European Conference on Computer and Network Defense (December EC2ND), December 2008

Students and Postdocs

PhD Students

- Risto Kivilahti, IMDEA Software Institute, Madrid, Spain** (November 2024 – present)
- Vidya Lakshmi Rajagopalan, Stevens Institute of Technology, NJ, USA** (January 2019 – December 2025)
Dissertation title: "Automated Generation of System Call Based Sandboxes in Binaries"
Post-graduation: Postdoctoral Researcher New York University
- Konstantinos Kleftogiorgos, Stevens Institute of Technology, NJ, USA** (September 2018 – July 2025)
Dissertation title: "Decoupling Security via Software-Driven Logging"
Post-graduation: GE Vernova, NY, USA
- Ruotong Yu, University of Utah, UT, USA** (September 2020 – March 2024)
Co-advised with Prof. Jun Xu, University of Utah
Dissertation title: "Evaluating, Improving, and Applying Modern Binary Analysis for Security"
Post-graduation: Postdoctoral Researcher Virginia Tech
- Yuchen Zhang, Stevens Institute of Technology, NJ, USA** (September 2019 – May 2023)
Co-advised with Prof. Jun Xu, University of Utah
Dissertation title: "Balancing the Security and Performance of Modern Programming Languages"
Post-graduation: Postdoctoral Researcher New York University
- Yifan Wang, Stevens Institute of Technology, NJ, USA** (September 2019 – December 2022)
Co-advised with Prof. Jun Xu, University of Utah
Dissertation title: "Improving Efficiency, Effectiveness, and Evaluation of Fuzz Testing"
- Ioannis Agadakos, Stevens Institute of Technology, NJ, USA** (January 2015 – May 2019)
Dissertation title: "Improving Software Hardening by Disabling Unused Code in Dynamically Linked Applications"
Post-graduation: SRI New York
- Enes Göktaş, Vrije Universiteit Amsterdam, NL** (July 2015 – April 2019)
Visiting scholar at Stevens (July 2015 – October 2015, January 2017 – July 2017)
Co-advised with Prof. Herbert Bos & Prof. Cristiano Giuffrida Vrije Universiteit Amsterdam
- Kangkook Jee, Columbia University, NY, USA** (January 2013 – May 2015)
Co-advised with Prof. Angelos Keromytis, Columbia University
Currently (2022): Assistant Professor, UT Dallas
Dissertation title: "On Efficiency and Accuracy of Data Flow Tracking Systems"

Sambuddho Chakravarty, Columbia University, NY, USA (January 2013 – May 2014)
Co-advised with Prof. Angelos Keromytis, Columbia University
Currently (2022): Associate Professor, IIIT Delhi
Dissertation title: “Traffic Analysis Attacks and Defenses in Low Latency Anonymous Communication”

Angeliki Zavou, Columbia University, NY, USA (January 2013 – May 2014)
Co-advised with Prof. Angelos Keromytis, Columbia University
Currently (2022): Senior Director, Northwestern Mutual
Dissertation title: “Information Flow Auditing In the Cloud”

Vasileios P. Kemerlis, Columbia University, NY, USA (January 2013 – December 2013)
Co-advised with Prof. Angelos Keromytis, Columbia University
Currently (2022): Assistant Professor, Brown University
Dissertation title: “Protecting Commodity Operating Systems through Strong Kernel Isolation”

Postdocs/Researchers

Enes Göktaş (May 2019 – August 2021)

Dimitrios Damopoulos (September 2013 – August 2015)

Interns

Emilien Fourgnier, IMDEA Software Institute (April 2026 – present)

Eleftherios Georgiadis, IMDEA Software Institute (October 2025 – present)

Rupesh Punna, IMDEA Software Institute (February 2025 – present)

Mathieu Michel, IMDEA Software Institute (April 2025 – October 2025)

Fatih Durmaz, IMDEA Software Institute (April 2024 – March 2025)

MS Students with Thesis

Fatih Durmaz, University of Southern Brittany & Université Libre de Bruxelles (April 2024 – September 2024)
Thesis title: “Enhancing System Security Through Binary and Static Analysis by Detecting Dormant Vulnerabilities”

Francesca Del Nin, University of Padova, IT (March 2019 – December 2019)
Co-advised with Dr Mauro Conti, University of Padova
Thesis title: “IoT Software Defenses Assessment”

Mohamad Mansouri, EURECOM, FR (March 2019 – September 2019)
Co-advised with Dr Davide Balzaroti, University of Padova
Interned at Stevens
Thesis title: “Disabling Unwanted Program Functionalities for Reducing Attack Surface”

Konstantinos Kleftogiorgos, University of Crete, GR (April 2016 – May 2018)
Co-advised with Dr Sotiris Ioannidis and Dr Evangelos Markatos, ICS/FORTH
Visiting scholar at Stevens October 2017 – May 2018
Thesis title: “Hardware Accelerated Control-Flow Reconstruction in JIT Environments”

Evangelos Ladakis, University of Crete, GR (July 2014 – September 2014)
Co-advised with Dr Sotiris Ioannidis, ICS/FORTH
Visiting scholar at Stevens
Thesis title: “GPU-Disasm: A GPU-based x86 Disassembler”

Enes Göktaş, Vrije Universiteit Amsterdam, NL (June 2013 – November 2013)
Co-advised with Prof. Herbert Bos, Vrije Universiteit Amsterdam
Visiting scholar at Stevens
Thesis title: “Out Of Control: Overcoming Control-Flow Integrity”

MS Students

Patrick Zielinski, Stevens Institute of Technology, NJ, USA	(June 2022 – present)
Yanjie Xu, Stevens Institute of Technology, NJ, USA	(June 2022 – November 2022)
Xi Luo, Stevens Institute of Technology, NJ, USA	(September 2013 – May 2014)

Undergraduate Students

Matthew Turner, Stevens Summer Scholar & Student Researcher	(June 2022 – present)
Peter Krasinsky, Research Assistant	(June 2017 – August 2017)
Nicholas Cyprus, Research Assistant	(June 2017 – August 2017)
Daniel Vinakovsky, Stevens CS Major	(September 2016 – December 2016)
Yongxin Feng, Stevens I&E scholar	(May 2016 – August 2016)
Dylan Iuzzolino, Stevens Pinnacle scholar	(May 2016 – July 2016)
Min Su Park, Stevens CS Major	(May 2016 – June 2016)
Zara Graves, Stevens summer scholar	(June 2013 – August 2013)

High-school Students

Paul Jung , high-school student intern	(September 2020 – May 2021)
Benjamin Iofel , high-school student intern	(September 2014 – May 2015)

Academic Service

Program Organization

ACM Conference on Reproducibility and Replicability (REP) (Program Chair)	(2026)
4th Workshop on Active Defense and Deception (AD&D) (Program Chair)	(2025)
European Conference on Computer Systems (EuroSys) (Artifact Evaluation Committee Co-chair)	(2025)
37th IEEE Symposium on Security and Privacy (Posters Chair)	(2016)
17th International Symposium on Research in Attacks, Intrusions and Defenses (RAID) (Publication Co-chair)	(2014)
Security and Privacy Day, Stevens Institute of Technology (Organizing Committee)	(2013)

Program Committee Service

Annual Computer Security Applications Conference (ACSAC)	(2026)
International Symposium on Research in Attacks, Intrusions and Defenses (RAID)	(2026)
ACM Conference on Computer and Communications Security (CCS)	(2026)
USENIX Security Symposium (USENIX Security)	(2025)
USENIX Security Symposium (USENIX Security)	(2024)
IEEE Symposium on Security and Privacy (S&P)	(2024)
IEEE European Symposium on Security and Privacy (EuroS&P)	(2024)
International Conference on Advanced Information Networking and Applications (AINA)	(2024)
International Conference on Distributed Computing Systems (ICDCS)	(2023)
Information Security Conference (ISC)	(2023)

ACM ASIA Conference on Computer and Communications Security (ASIACCS)	(2022)
ACM ASIA Conference on Computer and Communications Security (ASIACCS)	(2021)
ACM Conference on Computer and Communications Security (CCS)	(2021)
ACNS Workshop on Security in Mobile Technologies (SecMT)	(2021)
ACM Conference on Computer and Communications Security (CCS)	(2020)
ACM Conference on Computer and Communications Security (CCS) Poster Session	(2020)
International Symposium on Research in Attacks, Intrusions and Defenses (RAID)	(2020)
Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)	(2020)
ACM Conference on Computer and Communications Security (CCS) Poster Session	(2019)
Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)	(2019)
ACM ASIA Conference on Computer and Communications Security (ASIACCS)	(2018)
Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)	(2018)
International Conference on Distributed Computing Systems (ICDCS)	(2018)
ACM ASIA Conference on Computer and Communications Security (ASIACCS)	(2017)
ACM Conference on Computer and Communications Security (CCS)	(2017)
USENIX Security Symposium (USENIX Security)	(2017)
IEEE European Symposium on Security and Privacy (EuroS&P)	(2017)
International Conference on Distributed Computing Systems (ICDCS)	(2016)
USENIX Security Symposium (USENIX Security)	(2016)
ACM Cloud Computing Security Workshop (CCSW)	(2016)
ACM ASIA Conference on Computer and Communications Security (ASIACCS)	(2015)
International Symposium on Research in Attacks, Intrusions and Defenses (RAID)	(2015)
USENIX Security Symposium (USENIX Security)	(2015)
European Workshop on System Security (EUROSEC)	(2015)
Network and Distributed System Security Symposium (NDSS)	(2015)
Annual Computer Security Applications Conference (ACSAC)	(2015)
International Symposium on Engineering Secure Software and Systems (ESSoS)	(2015)
ACM ASIA Conference on Computer and Communications Security (ASIACCS)	(2014)
International Symposium on Research in Attacks, Intrusions and Defenses (RAID)	(2014)
European Workshop on System Security (EUROSEC)	(2014)
Annual Computer Security Applications Conference (ACSAC)	(2014)
APWG Symposium on Electronic Crime Research (eCrime)	(2014)
International Conference on Security and Privacy in Communication Networks (SecureComm)	(2014)
Kaspersky “CyberSecurity for the Next Generation”, The Americas Round	(2014)
Annual Computer Security Applications Conference (ACSAC)	(2013)
International Conference on Security and Privacy in Communication Networks (SecureComm)	(2013)
IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC)	(2013)
Annual Computer Security Applications Conference (ACSAC)	(2012)

European Conference on Computer Network Defense (EC2ND) (2011)
International Conference on Cryptology And Network Security (CANS) (2010)
ACM EuroSys Conference (*Shadow PC*) (2010)

Grant Proposal Review

National Research Center for Applied Cybersecurity ATHENE Reviewer (2025)
European Research Council (ERC) Reviewer (2025)
Fonds Wetenschappelijk Onderzoek – Vlaanderen (FWO) Panelist (2025)
NSF Reviewer and panellist (2015, 2017, 2018, 2021)
Vienna Science and Technology Fund (WWTF) Reviewer (2019, 2023)

Other Reviewing

External reviewer

IWSEC'10, ACSAC'11, ESORICS'11, RAID'11, ACNS'12, CANS'12, NDSS'12, CCS'12, FC2013

Journal reviewer

IET Information Security '10, '11, '12, Information Security Journal '12, ACM transactions of Information and System Security (TISSEC) '12 & '13, KSII Transactions on Internet and Information Systems '13, IEEE Transactions on Reliability '13, IEEE Communications Letters '13 and '14, IEEE Transactions on Dependable and Secure Computing '14, IEEE S&P '14, De gruyter it - Information Technology '16, Elsevier Computers & Security (COSE) '13, '17, & '18, and IEEE Transactions on Information Forensics and Security (TIFS) '18.

Editorships

Special issue on Security on Mobile and IoT devices (July 2020)
Elias Athanasopoulos, Georgios Portokalidis, and Martina Lindorfer (editors)
IET Information Security (Volume 14, Issue 4, pages 367–481)

Special Issue on Security and Privacy in Unified Communications: Challenges and Solutions (September 2015)
Georgios Karopoulos, Georgios Portokalidis, Josep Domingo-Ferrer, Ying-Dar Lin, Dimitris Geneiatakis, and Georgios Kambourakis (editors)
Computer Communications, Elsevier

Research in Attacks, Intrusions, and Defenses (RAID) (September 2014)
Angelos Stavrou, Herbert Bos, and Georgios Portokalidis (editors)
Lecture Notes in Computer Science (LNCS), Springer

PhD-Defense Committee Service

Vidya Lakshmi Rajagopalan, Stevens Institute of Technology (member) (December 2025)
Dissertation title: "Automated Generation of System Call Based Sandboxes in Binaries"

Konstantinos Kleftogiorgos, Stevens Institute of Technology (member) (July 2025)
Dissertation title: "Decoupling Security via Software-Driven Logging"

Koustubha Bhat, Vrije Universiteit Amsterdam (member) (May 2025)
Dissertation title: "Fast Automatic Software Survivability"

Erik Bosman, Vrije Universiteit Amsterdam (member) (November 2024)
Dissertation title: "Attacker-defined Abstractions: Programming Benign System Functionality For Subversive Purposes"

Ruotong Yu, University of Utah (member) (March 2024)
Dissertation title: "Evaluating, Improving, and Applying Modern Binary Analysis for Security"

Antreas Dionysiou, University of Cyprus (member) (March 2024)
Dissertation title: "Hardening Modern Systems and Services for Protecting User Privacy"

Yuchen Zhang , Stevens Institute of Technology (chair) <i>Dissertation title: "Balancing the Security and Performance of Modern Programming Languages"</i>	(May 2023)
Yifan Wang , Stevens Institute of Technology (chair) <i>Dissertation title: "Improving Efficiency, Effectiveness, and Evaluation of Fuzz Testing"</i>	(December 2022)
Shachee Mishra , Stony Brook University (member) <i>Dissertation title: "Multi-Layer API Specialization for Attack Surface Reduction"</i>	(April 2021)
Ioannis Agadakos , Stevens Institute of Technology (chair) <i>Dissertation title: "Improving Software Hardening by Disabling Unused Code in Dynamically Linked Applications"</i>	(May 2019)
Keith D. Willet , Stevens Institute of Technology (member) <i>Dissertation title: "Cybersecurity Decision Patterns as Adaptive Knowledge Encoding in Cybersecurity Operations"</i>	(November 2016)
Kangkook Jee , Columbia University (member) <i>Dissertation title: "On Efficiency and Accuracy of Data Flow Tracking Systems"</i>	(June 2015)
Angeliki Zavou , Columbia University (member) <i>Dissertation title: "Information Flow Auditing In the Cloud"</i>	(May 2014)
Asia Slowinska , Vrije Universiteit Amsterdam (member) <i>Dissertation title: "Using Information Flow Tracking to Protect Legacy Binaries"</i>	(May 2012)
Other	
Bergen County Technical High School Member of the advisory board for the Computer Science major	(2016 – 2019)

Professional Organisations

ACM Senior Member
IEEE Senior Member
USENIX Member

Press

Authored Articles in Popular Media

¿Y si el apagón fue un ciberataque? Responde un experto en ciberseguridad (June 2025)
The Conversation, Spanish version

Media Coverage and Interviews

TechXplore: "Redirect2Own: A new approach to protect the intellectual property of user-uploaded content." (October 2018)
TechXplore writes about our work.

"Practical Binary Analysis", Nostarch Press (September 2018)
Dennis Andriessse writes about using libdft to perform taint analysis.

Observer: "Do Captchas Make it Easy to ID Anonymous Web Users?" (July 2016)
Brady Dale talks about CloudFlare captchas for Tor users and our work on Tor-traffic de-anonymization.

New York Post: "How the US is losing the escalating cyberwar" (December 2014)
I spoke to Jonathon M. Trugman after the 2014 SONY hack.

Slashdot, Hackernews, nu.nl, etc. (November 2014)
The web talks about our work on Tor traffic de-anonymization.

- “Virtual Honeypots: From Botnet Tracking to Intrusion Detection”** (July 2007)
Niels Provos and Thorsten Holz have written a book about Honeypots that writes in some detail about Argos.
- USENIX ‘;Login:’** (October 2007)
Sam Stover writes about Argos
- Bright magazine: Feature: “Labrats”** (April 2006)
Another Dutch article about Argos.
- Computable: Opsporing Verzocht** (February 2006)
Dutch article about Argos.

Other Professional Experience

- Visiting researcher** (September 2019 – December 2019)
Mobile Multimedia Laboratory, Athens University of Economics and Business, Athens, Greece
- Visiting Researcher** (August 2008)
ERTOS group at Neville Roach Lab (NRL), NICTA, Sydney, Australia
- Visiting Researcher** (May 2008 – July 2008)
Internet Security Lab, Institute for Infocomm Research, Singapore, Singapore
- Intern** (April 2007 – June 2007)
Microsoft Research, Cambridge, UK
- Intern** (September 2004 – January 2005)
Intel Research, Cambridge, UK
- Research Assistant** (September 2003 – July 2004)
Leiden University, Leiden, The Netherlands
- Summer Trainee** (June 2001 – August 2001)
Internet Hellas, Athens, Greece
- Full-Stack Web Developer/Linux System Administrator** (November 1999 – February 2002)
ATLANTIS group, Heraklion, Greece
- Assistant Linux System Administrator** (March 2000 – September 2000)
UCnet University of Crete, Heraklion, Greece
- Assistant Windows System Administrator** (December 1999 – February 2000)
E.L.K.E. University of Crete, Heraklion, Greece

Teaching

Universidad Politécnica de Madrid

- Computer Security** (Fall 2024)
19 students (on campus)

Stevens Institute of Technology

- CS-676 Advanced Topics in Systems Security** (Spring 2023)
4 students (on campus)
- CS-676 Advanced Topics in Systems Security** (Spring 2019)
11 students (on campus)
- CS-676 Advanced Topics in Systems Security** (Spring 2018)
2 students (on campus)

CS-676 Advanced Topics in Systems Security 2 students (on campus)	(Spring 2017)
CS-960 Research in Computer Science 2 students (on campus)	(Spring 2023)
CS-960 Research in Computer Science 2 students (on campus)	(Fall 2022)
CS-960 Research in Computer Science 2 students (on campus)	(Spring 2022)
CS-960 Research in Computer Science 1 student (on campus)	(Fall 2021)
CS-960 Research in Computer Science 1 student (on campus)	(Spring 2021)
CS-960 Research in Computer Science 2 students (on campus)	(Fall 2020)
CS-960 Research in Computer Science 2 students (on campus)	(Spring 2020)
CS-960 Research in Computer Science 2 students (on campus)	(Fall 2019)
CS-960 Research in Computer Science 2 students (on campus)	(Spring 2019)
CS-960 Research in Computer Science 1 student (on campus)	(Fall 2018)
CS-960 Research in Computer Science 2 students (on campus)	(Spring 2017)
CS-960 Research in Computer Science 2 students (on campus)	(Fall 2016)
CS-960 Research in Computer Science 2 students (on campus)	(Spring 2016)
CS-960 Research in Computer Science 2 students (on campus)	(Fall 2015)
CS-960 Research in Computer Science 2 students (on campus)	(Spring 2015)
CS-960 Research in Computer Science 1 student (on campus)	(Fall 2014)
CS-960 Research in Computer Science 1 student (on campus)	(Spring 2014)
CS-960 Research in Computer Science 1 student (on campus)	(Fall 2013)
CS-801 Special Problem in CS for PhD students 1 student (on campus)	(Fall 2022)
CS-801 Special Problem in CS for PhD students 1 student (on campus)	(Fall 2018)
CS-801 Special Problem in CS for PhD students 1 student (on campus)	(Spring 2017)

CS-801 Special Problem in CS for PhD students 1 student (on campus)	(Fall 2014)
CS-800 Special Problem in Computer Science for MS students 1 student (on campus)	(Fall 2022)
CS-800 Special Problem in Computer Science for MS students 1 student (on campus)	(Spring 2018)
CS-800 Special Problem in Computer Science for MS students 1 student (on campus)	(Spring 2017)
CS-800 Special Problem in Computer Science for MS students 1 student (on campus)	(Fall 2013)
CS-576 Systems Security 14 students (on campus)	(Spring 2022)
CS-576 Systems Security 37 students (online)	(Fall 2020)
CS-576 Systems Security 26 students (on campus)	(Fall 2018)
CS-576 Systems Security 27 students (on campus)	(Spring 2018)
CS-576 Systems Security 16 students (on campus)	(Fall 2016)
CS-492 Operating Systems Section-A: 48 students, Section-B: 49 students (on campus)	(Spring 2021)
CS-392-A Systems Programming 21 students (on campus)	(Spring 2017)
CS-392-A Systems Programming 25 students (on campus)	(Spring 2016)
CS-497-S Independent Study 1 student (on campus)	(Fall 2016)
CS-576 Secure Systems 15 students (on campus)	(Fall 2015)
CS-576 Secure Systems 15 students (on campus)	(Fall 2014)
CS-577 Cybersecurity Lab 15 students (on campus)	(Fall 2015)
CS-577 Cybersecurity Lab 15 students (on campus)	(Fall 2014)
CS-397 Outreach Participation 1 student (on campus)	(Spring 2015)
CS-397 Outreach Participation 4 students (on campus)	(Fall 2014)
CS-397 Outreach Participation 4 students (on campus)	(Spring 2014)
CS-397 Outreach Participation 5 students (on campus)	(Fall 2013)

CS-695 Host Forensics 6 students (on campus)	(Spring 2014)
CS-695 Host Forensics 3 students (on campus)	(Spring 2013)
CS-181 Introduction to Computer Science, Honors I 19 students (on campus)	(Fall 2013)
<u>Vrije Universiteit Amsterdam</u>	
Practical computer security courses for high-school students (course for high-school students)	(Spring 2006)
Practical computer security courses for high-school students (course for high-school students)	(Spring 2007)
Practical computer security courses for high-school students (course for high-school students)	(Spring 2009)
<u>Guest Lectures</u>	
CS-101 Research and Entrepreneurship in Computing Stevens Institute of Technology	(September 2020)
CS-188 Seminar in Computer Science Stevens Institute of Technology	(April 2020)