Georgios Portokalidis

Associate Research Professor, IMDEA Software Institute, Madrid, Spain
Associate Professor, Dept. of Computer Science, Stevens Institute of Technology, NJ, USA
https://www.portokalidis.net

Academic Positions Held

Associate Research Professor (September 2023 – present)
IMDEA Software Institute, Madrid, Spain

Associate Professor of Computer Science (September 2019 – present)
Stevens Institute of Technology, Hoboken, NJ, USA

Visiting Associate Professor of Computer Science (January 2020 – July 2020)
National Univerity of Singapore, Singapore

Assistant Professor of Computer Science (January 2013 – August 2019)
Stevens Institute of Technology, Hoboken, NJ, USA

Postdoctoral researcher (March 2010 – December 2012)
Columbia University, New York, NY, USA
Advisor: Angelos Keromytis

Education

PhD Computer Science, Vrije University, Amsterdam, The Netherlands (February 2010)
Dissertation title: "Using Virtualisation Against Zero-Day Attacks"
Advisor: Herbert Bos, Promoter: Henri Bal

MSc Computer Science, Leiden University, Leiden, The Netherlands (December 2004)
Dissertation title: "Zero Hour Worm Detection and Containment Using Honeypots"
Advisor: Herbert Bos

BSc Computer Science, University of Crete, Heraklion, Greece (July 2002)
Dissertation title: "Study and Bridging of Peer-to-Peer File Sharing Systems"
Advisor: Evangelos P. Markatos, Co-advisor: Manolis Marazakis

Support for Research (Grants and Awards)

Effective Software Monitoring Leveraging Hardware Debugging Extensions (August 2021 – July 2023)
PI, DARPA YFA, $492,490

ABIDES: Adaptive BInary Debloating and Security (September 2017 – August 2022)
PI (lead), ONR, $3,243,244 (Stevens $1,052,376)

Adapting Static and Dynamic Program Analysis to Effectively Harden Debloated Software (March 2016 – December 2020)
PI, ONR, $467,543

Trails: Efficient Data-Flow Tracking Through HW-assisted Parallelization (September 2016 – August 2019)
PI, DARPA, $462,419

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 Göktaş, 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 Göktaş, Elias Athanasopoulos, Georgios Portokalidis, and Herbert Bos

DCSRA 2015 winner (March 2015)
Our paper was was unanimously selected by the jury as excellent Dutch Cyber Security Research paper
"Out Of Control: Overcoming Control-Flow Integrity"
Enes Göktaş, 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

1. **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%)

2. **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%)

3. **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

4. **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

5. **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%)

6. **Building Embedded Systems Like It's 1996**
   Ruotong Yu, Francesca Del Nin, Yuchen Zhang, Shan Huang, Pallavi Kaliyar, Sarah Zatko, 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%)

7. **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 Zatko, Mauro Conti, Georgios Portokalidis, and Jun Xu
   The Learning from Authoritative Security Experiment Results (LASER) workshop, San Diego, CA, USA, April 2022

8. **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

9. **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%)

10. **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%)

11. **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***

12. **Nibbler: Debloating Binary Shared Libraries**
    Ioannis Agadakos, 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%)

13. **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%)

14. **Techu: Open and Privacy-preserving Crowdsourced GPS for the Masses**
    Ioannis Agadakos, 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%)

15. **Location-enhanced Authentication using the IoT**
    Ioannis Agadakos, 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%)

16. **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

17. **NaClDroid: 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%)

18. **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%)

19. **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

20. **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***

21. **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%)

22. **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%)

23. **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%)

24. **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%)

25. **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***

26. **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%)

27. **On the Effectiveness of Traffic Analysis Against Anonymity Networks Using Flow Records**
Sambuddho Chakravarty, Marco V. Barbera, Georgios Portokalidis, Michalis Polychronakis, and Angelos D. Keromytis
Proceedings of the Passive and Active Measurement (PAM) Conference, Los Angeles, CA, USA, March 2014 (31.5%)

28. **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%)

29. **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%)

30. **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

31. **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%)

32. **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%)

33. **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

34. **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%)

35. **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

36. **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%)

37. **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%)

38. **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***

39. **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

40. **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%)

41. **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

42. **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%)

43. **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%)

44. **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

45. **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%)

46. **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

47. **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%)

48. **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)

49. **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. **Harder, Better, Faster, Stronger: Establishing Trustworthy Software and Systems**
   IMDEA Software Institute, Madrid, Spain, April 2023
   Host: Juan Caballero

2. **Harder, Better, Faster, Stronger: Establishing Trustworthy Software and Systems**
   North Carolina State University, Raleigh, NC, USA, March 2023
   Host: William Enck

3. **New Challenges and Solutions for Kernel Security in the Spectre Era**
   Telefonica Research, Barcelona, Spain, December 2022
   Host: Ioannis Arapakis

4. **Effective Software Monitoring Leveraging Hardware Debugging Extensions**
   CAREER Club Symposium, Stevens Institute of Technology, NJ, USA, November 2021

5. **Improving Software Security and Reliability**
   SES Virtual Research Forum, Stevens Institute of Technology, NJ, USA, November 2020

6. **Hardening Binary Software Through Debloating**
   United Technologies Research Center, Rome, Italy, December 2019
   Host: Valerio Senni

7. **Hardening Binary Software Through Debloating**
   Institute of Computer Science, FORTH, Heraklion, Crete, Greece, December 2019
   Host: Evangelos Markatos

8. **Hardening Binary Software Through Debloating**
   Athens University of Economics, Athens, Greece, December 2019
   Host: Georgios Polyzos

9. **Better Security by Debloating Binary Shared Libraries**
   Vrije University, Amsterdam, The Netherlands, October 2019
   Host: Herbert Bos

10. **Improving Systems Security through Software Debloating**
    University of California Santa Barbara, CA, USA, June 2018
    Host: Christopher Kruegel

11. **Improving Systems Security through Attack Surface Reduction and Execution Transparency**
    Ohio State University, Columbus, OH, USA, April 2018
    Host: Zhiqiang Lin

12. **Improving Systems Security through Attack Surface Reduction and Execution Transparency**
    National and Kapodistrian University of Athens, Athens, Greece, November 2017
    Host: Mema Roussopolos

13. **Improving Systems Security through Attack Surface Reduction and Execution Transparency**
Vrije Universiteit, Amsterdam, The Netherlands, November 2017
Host: Herbert Bos

14. **Improving Systems Security through Attack Surface Reduction and Execution Transparency**
University of Padova, Padua, Italy, November 2017
Host: Mauro Conti

15. **Code-Reuse Attacks and Software Surface**
Security & Privacy Day, Stony Brook University, New York, NY, USA, October 2017

16. **Understanding Code-Reuse Attacks and Reducing Attack Surface**
MIT, Boston, MA, USA, October 2017
Host: Stelios Sidiroglou-Douskos

17. **Understanding Code-Reuse Attacks and Reducing Attack Surface**
Northeastern University, Boston, MA, USA, October 2017
Host: Engin Kirda

18. **Securing Financial Transactions with IoT-powered Location-based Authentication**
FinCyberSec Conference, Stevens Institute of Technology, May 2017

19. **Out of Control**
Vrije Universiteit, Amsterdam, The Netherlands, October 2016

20. **Improving Software Resiliency Against Code-Reuse Attacks**
Athens University of Economics and Business, October 2016

21. **Improving Software Resiliency Against Code-Reuse Attacks**
Aristotle University of Thessaloniki, October 2016

22. **WYSISNWIV: What You Scan Is Not What I Visit**
International Symposium on Recent Advances in Intrusion Detection (RAID), Kyoto, Japan, November 2015

23. **WYSISNWIV: What You Scan Is Not What I Visit**
Stony Brook University's CEWIT 2015 conference, Stony Brook, NY, USA, October 2015

24. **Using the Internet of Things to Augment Security Decisions**
International Workshop on Cyber Threat Resilience, IIITM-K, Kerala, India, October 2015

25. **Evaluation Tools and Metrics for Control-flow Integrity Defenses**
Dagstuhl seminar "The Continuing Arms Race: Code-Reuse Attacks and Defenses", Dahstuhl, Germany, July 2015

26. **How about some control-flow integrity**
FORTH-ICS, Heraklion, Crete, Greece, July 2014

27. **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

28. **From Hacking for Fun to Cyber-crime and Cyber-warfare, and How Can We Stop It**
Vrije Universiteit, Amsterdam, The Netherlands, November 2013

29. **Protecting Commodity Software**
Northeastern University, Boston, MA, USA, April 2013

30. **Protecting Commodity Software**
University of Twente, Enschede, The Netherlands, June 2012

31. **Protecting Commodity Software**
University of California, Riverside, CA, USA, March 2012

32. **Protecting Commodity Software**
Stevens Institute of Technology, Hoboken, NJ, USA, January 2012

33. **Paranoid Android: Versatile Protection For Smartphones**
AT&T Security Research Center, New York, NY, USA, December 2011

34. **Using Rescue Points**
International Workshop on Security (IWSEC), Tokyo, Japan, November 2011

35. **Paranoid Android: Versatile Protection For Smartphones**
Annual Computer Security Applications Conference (ACSAC), Austin, TX, USA, December 2010

36. **iLeak: a Lightweight System for Detecting Inadvertent Information Leaks**
European Conference on Computer Network Defense (EC2ND), Berlin, Germany, October 2010

37. **Heavyweight Protection for Lightweight Devices**
Internet Research Group, Telefonica Research, Barcelona, Spain, May 2009

38. **Tutorial on Information Flow Tracking**
European Conference on Computer Network Defense (EC2ND), Dublin, Ireland, December 2008

39. **Zero-Day Exploits**
ACM SIGOPS/EuroSys European Conference on Computer Systems, Glasgow, Scotland, April 2008

40. **Argos: an Emulator for Fingerprinting Zero-Day Attacks**
IBM Research, Zürich, Switzerland, July 2006

41. **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

42. **Argos: Securing IP Communications Against Zero-Day Attacks**
NLUUG Unix Users Group Annual Conference, The Netherlands, April 2006

43. **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

Postdocs/Researchers

Enes Göktaş (May 2019 – August 2021)

Dimitrios Damopoulos (September 2013 – August 2015)

PhD Students

Vidya Lakshmi Rajagopalan, Stevens Institute of Technology, NJ, USA (January 2019 – present)
Co-advised by Prof. Jun Xu, University of Utah

Konstantinos Kleftogiorgos, Stevens Institute of Technology, NJ, USA (September 2018 – present)
Co-advised by Prof. Jun Xu, University of Utah

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"

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 (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"

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)

Co-advised MS Students

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"

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 Committee Service

2024

USENIX Security Symposium (USENIX Security)

IEEE Symposium on Security and Privacy (S&P)

IEEE European Symposium on Security and Privacy (EuroS&P)

International Conference on Advanced Information Networking and Applications (AINA)

2023

International Conference on Distributed Computing Systems (ICDCS)

Information Security Conference (ISC)

2022

ACM ASIA Conference on Computer and Communications Security (ASIACCS)

2021

ACM ASIA Conference on Computer and Communications Security (ASIACCS)

ACM Conference on Computer and Communications Security (CCS)

ACNS Workshop on Security in Mobile Technologies (SecMT)

2020

ACM Conference on Computer and Communications Security (CCS)

ACM Conference on Computer and Communications Security (CCS) Poster Session

International Symposium on Research in Attacks, Intrusions and Defenses (RAID)

Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)

2019

ACM Conference on Computer and Communications Security (CCS) Poster Session

Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)

2018

ACM ASIA Conference on Computer and Communications Security (ASIACCS)

Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)

International Conference on Distributed Computing Systems (ICDCS)

2017

ACM ASIA Conference on Computer and Communications Security (ASIACCS)

ACM Conference on Computer and Communications Security (CCS)

USENIX Security Symposium (USENIX Security)

IEEE European Symposium on Security and Privacy (EuroS&P)

2016

International Conference on Distributed Computing Systems (ICDCS)

USENIX Security Symposium (USENIX Security)

ACM Cloud Computing Security Workshop (CCSW)

2015

ACM ASIA Conference on Computer and Communications Security (ASIACCS)

International Symposium on Research in Attacks, Intrusions and Defenses (RAID)

USENIX Security Symposium (USENIX Security)

European Workshop on System Security (EUROSEC)

Network and Distributed System Security Symposium (NDSS)

Annual Computer Security Applications Conference (ACSAC)

International Symposium on Engineering Secure Software and Systems (ESSoS)

2014

ACM ASIA Conference on Computer and Communications Security (ASIACCS)

International Symposium on Research in Attacks, Intrusions and Defenses (RAID)

European Workshop on System Security (EUROSEC)

Annual Computer Security Applications Conference (ACSAC)

APWG Symposium on Electronic Crime Research (eCrime)

International Conference on Security and Privacy in Communication Networks (SecureComm)

Kaspersky "CyberSecurity for the Next Generation", The Americas Round

2013

Annual Computer Security Applications Conference (ACSAC)

International Conference on Security and Privacy in Communication Networks (SecureComm)

IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC)

2012

Annual Computer Security Applications Conference (ACSAC)

2011

European Conference on Computer Network Defense (EC2ND)

2010

International Conference on Cryptology And Network Security (CANS)

ACM EuroSys Conference *(Shadow PC)*

Grant Proposal Review

NSF Reviewer and panelist (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.

Program Organization

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) (2014)
(Publication Co-chair)

Security and Privacy Day, Stevens Institute of Technology (Organizing Committee) (Spring 2013)

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

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) (May 2023)
Dissertation title: "Balancing the Security and Performance of Modern Programming Languages"

Yifan Wang, Stevens Institute of Technology (chair) (December 2022)
Dissertation title: "Improving Efficiency, Effectiveness, and Evaluation of Fuzz Testing"

Shachee Mishra, Stony Brook University (member) (April 2021)
Dissertation title: "Multi-Layer API Specialization for Attack Surface Reduction"

Ioannis Agadakos, Stevens Institute of Technology (chair) (May 2019)
Dissertation title: "Improving Software Hardening by Disabling Unused Code in Dynamically Linked Applications"

Keith D. Willet, Stevens Institute of Technology (member) (November 2016)
Dissertation title: "Cybersecurity Decision Patterns as Adaptive Knowledge Encoding in Cybersecurity Operations"

Kangkook Jee, Columbia University (member) (June 2015)
Dissertation title: "On Efficiency and Accuracy of Data Flow Tracking Systems"

Angeliki Zavou, Columbia University (member) (May 2014)
Dissertation title: "Information Flow Auditing In the Cloud"

Asia Slowinska, Vrije Universiteit Amsterdam (member) (May 2012)
Dissertation title: "Using Information Flow Tracking to Protect Legacy Binaries"

Other

Bergen County Technical High School (Fall 2016 – current)
Member of the advisory board for the Computer Science major

Press

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 Andriesse 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

Stevens Institute of Technology

CS-676 Advanced Topics in Systems Security
Spring 2023 (on campus): 4 students, Spring 2019 (on campus): 11 students, Spring 2018 (on campus): 2 students, Spring 2017 (on campus): 2 students

CS-960 Research in Computer Science
Spring 2023 (on campus): 2 students, Fall 2022 (on campus): 2 students, Spring 2022 (on campus): 2 students, Fall 2021 (on campus): 1 student, Spring 2021 (on campus): 1 student, Fall 2020 (on campus): 2 students, Spring 2020 (on campus): 2 students, Fall 2019 (on campus): 2 students, Spring 2019 (on campus): 2 students, Fall 2018 (on campus): 1 students, Spring 2017 (on campus): 2 students, Fall 2016 (on campus): 2 students, Spring 2016 (on campus): 2 students, Fall 2015 (on campus): 2 students, Spring 2015 (on campus): 2 students, Fall 2014 (on campus): 1 student, Spring 2014 (on campus): 1 student, Fall 2013 (on campus): 1 student

CS-801 Special Problem in CS for PhD students
Fall 2022 (on campus): 1 student, Fall 2018 (on campus): 1 student, Spring 2017 (on campus): 1 student, Fall 2014 (on campus): 1 student

CS-800 Special Problem in Computer Science for MS students
Fall 2022 (on campus): 1 student, Spring 2018 (on campus): 1 student, Spring 2017 (on campus): 1 student, Fall 2013 (on campus): 1 student

CS-576 Systems Security
Spring 2022 (on campus): 14 students, Fall 2020 (online): 37 students, Fall 2018 (on campus): 26 students, Spring 2018 (on campus): 27 students, Fall 2016 (on campus): 16 students

CS-492 Operating Systems
Spring 2021 (on campus): Section-A 48 students, Section-B 49 students

CS-392-A Systems Programming
Spring 2017 (on campus): 21 students, Spring 2016 (on campus): 25 students

CS-497-S Independent Study
Fall 2016 (on campus): 1 student

CS-576 Secure Systems
Fall 2015 (on campus): 15 students, Fall 2014 (on campus): 15 students

CS-577 Cybersecurity Lab
Fall 2015 (on campus): 15 students, Fall 2014 (on campus): 15 students

CS-397 Outreach Participation
Spring 2015 (on campus): 1 student, Fall 2014 (on campus): 4 students, Spring 2014 (on campus): 4 students, Fall 2013 (on campus): 5 students

CS-695 Host Forensics
Spring 2014 (on campus): 6 students, Spring 2013 (on campus): 3 students

CS-181 Introduction to Computer Science, Honors I
Fall 2013 (on campus): 19 students

Vrije Universiteit Amsterdam

Practical computer security courses for high-school students
Spring 2006, Spring 2007, Spring 2009

Guest Lectures

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