

Georgios Portokalidis

Schaefer School of Engineering & Science, Dept. of Computer Science,
Stevens Institute of Technology, NJ, USA

E-mail: gportoka@stevens.edu, URL: <https://www.portokalidis.net>

Academic Positions Held

Stevens Institute of Technology, New Jersey, USA (January 2013 – present)
Assistant Professor of Computer Science

Stevens Institute of Technology, New Jersey, USA (September 2016 – December 2016)
Program director MS in Cybersecurity

Columbia University, New York, USA (March 2010 – December 2012)
Postdoctoral researcher in the Network Security Lab (NSL)
Advisor: Angelos Keromytis

Education

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

MSc Computer Science, Leiden University, The Netherlands (April 2005)
Dissertation title: “Zero Hour Worm Detection and Containment Using Honeypots”
Advisor: Herbert Bos

BSc Computer Science, University of Crete, Greece (July 2002)
Dissertation title: “Study and Bridging of Peer-to-Peer File Sharing Systems”
Advisor: Evangelos P. Markatos

Support for Research (Grants)

PI (lead), “ABIDES: Adaptive BINARY Debloating and Security” (September 2017 – August 2020)
ONR, **\$3,243,244** (Stevens \$1,052,376)

PI, “Trails: Efficient Data-Flow Tracking Through HW-assisted Parallelization” DARPA, **\$462,419** (September 2016 – August 2018)

PI, “Adapting Static and Dynamic Program Analysis to Effectively Harden Debloated Software”, ONR, **\$467,543** (March 2016 – February 2019)

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

PI (lead Columbia University), “MINESTRONE (September 2012 – November 2014)
Task: Automatic Discovery of Rescue Points Using Static and Dynamic Analysis”, IARPA, **\$247,641**

Awards and Distinctions

Academic Honors

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

Paper Awards

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 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

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%)

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)

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%)

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

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%)

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

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%)

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%)

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

Detecting Traffic Snooping in Tor Using Decoys

Sambuddho Chakravarty, Michalis Polychronakis, Georgios Portokalidis, and Angelos D. Keromytis

Proceedings of the International Symposium on Recent Advances in Intrusion Detection (RAID), Menlo Park, CA, USA, September 2011 (23%)

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

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***

A Multilayer Overlay Network Architecture for Enhancing IP Service Availability Against DoS

Dimitris Geneiataki, Georgios Portokalidis, and Angelos D. Keromytis

Proceedings of the International Conference on Information Systems Security (ICISS), Kolkata, India, December 2011 (22.8%)

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%)

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

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%)

Exploiting Split Browsers for Efficiently Protecting User Data

Angeliki Zavou, Elias Athanasopoulos, Georgios Portokalidis, and Angelos D. Keromytis

Proceedings of CCSW: The ACM Cloud Computing Security Workshop, Raleigh, NC, USA, October 2012

Adaptive Defenses for Commodity Software through Virtual Application Partitioning

Dimitris Geneiataki, Georgios Portokalidis, Vasileios P. Kemerlis, and Angelos D. Keromytis

Proceedings of the ACM Conference on Computer and Communications Security, Raleigh, NC, USA, October 2012 (18.9%)

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%)

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

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%)

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%)

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%)

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%)

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%)

Size Does Matter - Why Using Gadget-Chain Length to Prevent Code-reuse Attacks is Hard

Enes Göktaş, Elias Athanasopoulos, Herbert Bos, Michalis Polychronakis, and Georgios Portokalidis

Proceedings of the USENIX Security Symposium, San Diego, CA, USA, August 2014 (19.1%)

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 (NDSS) Symposium, San Diego, CA, USA, February 2015 (19.6%)

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%)

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%)

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

Speculative Memory Checkpointing

Dirk Vogt, Armando Miraglia, Georgios Portokalidis, Herbert Bos, Andrew S Tanenbaum, and Cristiano Giuffrida

Proceedings of the ACM/IFIP/USENIX Middleware Conference, Vancouver, Canada, December 2015

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%)

NaCIDroid: Native Code Isolation for Android Applications

Elias Athanasopoulos, Vasileios P. Kemerlis, Georgios Portokalidis, and Angelos Keromytis

Proceedings of the European Symposium on Research in Computer Security (ESORICS), Heraklion, Crete, Greece, September 2016 (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

Location-enhanced Authentication using the IoT

Ioannis Agadakis, 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%)

Techu: Open and Privacy-preserving Crowdsourced GPS for the Masses

Ioannis Agadakis, 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%)

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

To appear in Proceedings of the IEEE European Symposium on Security and Privacy, London, United Kingdom, April 2018 (22.9%)

Journals

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)

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)

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, June 2015)

Books/Book Chapters

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

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

Packet Monitoring at High Speed with FFPF

Georgios Portokalidis and Herbert Bos

Technical report 2004-01, LIACS, Leiden University, Leiden, The Netherlands, January 2004

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

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

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

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

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

Detecting Traffic Snooping in Anonymity Networks Using Decoys

Sambuddho Chakravarty, Michalis Polychronakis, Georgios Portokalidis, and Angelos D. Keromytis

Technical report CUCS-005-11, Columbia University, New York, NY, USA, February 2011

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

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

Talks and Panels

Talks

Argos: an Emulator for Fingerprinting Zero-Day Attacks (April 2006)

ACM SIGOPS EUROSYS, Leuven, Belgium

Argos: Securing IP Communications Against Zero-Day Attacks (April 2006)

NLUUG Unix Users Group Annual Conference, The Netherlands

Argos: Emulated Hardware Support to Fingerprint Zero-Day Attacks (June 2006)

by Means of Dynamic Data Flow Analysis

Annual Conference of the Advanced School for Computing and Imaging (ASCI), Belgium

Argos: an Emulator for Fingerprinting Zero-Day Attacks (July 2006)

Invited talk IBM Research, Zürich, Switzerland

Eudaemon: Involuntary and On-Demand Emulation Against (April 2008)

Zero-Day Exploits

ACM SIGOPS/EuroSys European Conference on Computer Systems, Glasgow, Scotland

Tutorial on Information Flow Tracking (December 2008)

European Conference on Computer Network Defense (EC2ND), Dublin, Ireland

Heavyweight Protection for Lightweight Devices (May 2009)

Internet Research Group, Telefonica Research, Barcelona, Spain

- iLeak: a Lightweight System for Detecting Inadvertent Information Leaks** (October 2010)
European Conference on Computer Network Defense (EC2ND), Berlin, Germany
- Paranoid Android: Versatile Protection For Smartphones** (December 2010)
Annual Computer Security Applications Conference (ACSAC), Austin, TX, USA
- Paranoid Android: Versatile Protection For Smartphones** (December 2011)
AT&T Security Research Center, New York, NY, USA
- REASSURE: A Self-contained Mechanism for Healing Software Using Rescue Points** (November 2011)
International Workshop on Security (IWSEC), Tokyo, Japan
- Protecting Commodity Software** (January 2012)
Stevens Institute of Technology, Hoboken, NJ, USA
- Protecting Commodity Software** (March 2012)
University of California, Riverside, CA, USA
- Protecting Commodity Software** (June 2012)
University of Twente, Enschede, The Netherlands
- Protecting Commodity Software** (April 2013)
Northeastern University, Boston, MA, USA
- From Hacking for Fun to Cyber-crime and Cyber-warfare, and How Can We Stop It** (November 2013)
Vrije Universiteit, Amsterdam, The Netherlands
- From Hacking for Fun to Cyber-crime and Cyber-warfare, and How Can We Stop It** (April 2014)
Kaspersky “CyberSecurity for the Next Generation”, The Americas Round 2014, Washington D.C.
- How about some control-flow integrity** (July 2014)
FORTH-ICS, Heraklion, Crete, Greece
- Evaluation Tools and Metrics for Control-flow Integrity Defenses** (July 2015)
Dagstuhl seminar “The Continuing Arms Race: Code-Reuse Attacks and Defenses”, Dahstuhl, Germany
- WYSISNWIV: What You Scan Is Not What I Visit** (October 2015)
Stony Brook University’s CEWIT 2015 conference, Stony Brook, NY, USA
- Using the Internet of Things to Augment Security Decisions** (October 2015)
International Workshop on Cyber Threat Resilience, IIITM-K, Kerala, India
- WYSISNWIV: What You Scan Is Not What I Visit** (November 2015)
International Symposium on Recent Advances in Intrusion Detection (RAID), Kyoto, Japan
- Out of Control** (October 2016)
Vrije Universiteit, Amsterdam, The Netherlands
- Improving Software Resiliency Against Code-Reuse Attacks** (October 2016)
Athens University of Economics and Business
- Improving Software Resiliency Against Code-Reuse Attacks** (October 2016)
Aristotle University of Thessaloniki
- Securing Financial Transactions with IoT-powered Location-based Authentication** (May 2017)
FinCyberSec Conference, Stevens Institute of Technology
- Understanding Code-Reuse Attacks and Reducing Attack Surface** (October 2017)
Northeastern University, Boston, MA, USA
Host: Engin Kirda

- Understanding Code-Reuse Attacks and Reducing Attack Surface** (October 2017)
MIT, Boston, MA, USA
Host: Stelios Sidiroglou-Douskos
- Code-Reuse Attacks and Software Surface** (October 2017)
Security & Privacy Day, Stony Brook University, New York, NY, USA
- Improving Systems Security through Attack Surface Reduction and Execution Transparency** (November 2017)
Vrije Universiteit, Amsterdam, The Netherlands
Host: Herbert Bos
- Improving Systems Security through Attack Surface Reduction and Execution Transparency** (November 2017)
University of Padova, Padua, Italy
Host: Mauro Conti
- Improving Systems Security through Attack Surface Reduction and Execution Transparency** (November 2017)
National and Kapodistrian University of Athens, Athens, Greece
Host: Mema Roussopolos
- Improving Systems Security through Attack Surface Reduction and Execution Transparency** (April 2018)
Ohio State University, Columbus, OH, USA
Host: Zhiqiang Lin

Panels

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

Students and Postdocs

Current PhD Students

- Ioannis Agadakos (January 2015 – present)
- Samaneh Berenjian (September 2016 – present)
- Abdullah Samarkandi (January 2018 – present)

Postdoctoral Students/Researchers

- Dimitrios Damopoulos** (September 2013 – August 2015)
Currently a teaching professor at Stevens Institute of Technology

Co-advised PhD Students

- Angeliki Zavou, Columbia University, NY, US** (January 2013 – May 2014)
Co-advised with Prof. Angelos Keromytis, Columbia University
- Kangkook Jee, Columbia University, NY, US** (January 2013 – May 2015)
Co-advised with Prof. Angelos Keromytis, Columbia University

Sambuddho Chakravarty, Columbia University, NY, US (January 2013 – May 2014)
Co-advised with Prof. Angelos Keromytis, Columbia University

Vasileios P. Kemerlis, Columbia University, NY, US (January 2013 – December 2013)
Co-advised with Prof. Angelos Keromytis, Columbia University

Enes Göktaş, Vrije Universiteit Amsterdam, NL (July 2015 – present)
Visiting scholar at Stevens (July 2015 – October 2015, January 2017 – July 2017)
Co-advised with Prof. Herbert Bos & Prof. Cristiano Giuffrida Vrije Universiteit Amsterdam

MS Students

Xi Luo, Stevens (September 2013 – May 2014)

MS Students Co-advised

Enes Göktaş, Vrije Universiteit Amsterdam, NL (June 2013 – November 2013)
Visiting scholar at Stevens for the same period (supported by a grant)
Co-advised with Prof. Herbert Bos, Vrije Universiteit Amsterdam

Evangelos Ladakis, University of Crete, GR (July 2014 – September 2014)
Visiting scholar at Stevens for the same period (supported by a grant)
Co-advised with Dr Sotiris Ioannidis, ICS/FORTH

Konstantinos Kleftogiorgos University of Crete, GR (April 2016 – May 2018)
Visiting scholar at Stevens October 2017 – May 2018 (supported by a grant)
Co-advised with Dr Sotiris Ioannidis, ICS/FORTH

Undergraduate Students

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

Benjamin Iofel, high-school student intern (September 2014 – May 2015)

Academic Service/Reviewing

Program Committee Service

Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) (2018)

ACM Symposium on Information, Computer and Communications Security (ASIACCS) (2014, 2015, 2017, 2018)

ACM Conference on Computer and Communications Security (CCS) (2017)

USENIX Security Symposium (2015 – 2017)

IEEE European Symposium on Security and Privacy (EuroS&P) (2017)

ACM Cloud Computing Security Workshop (CCSW) (2016)

International Conference on Distributed Computing Systems (ICDCS) (2016, 2018)

European Workshop on System Security (EUROSEC)	(2014 – 2015)
Network and Distributed System Security Symposium (NDSS)	(2015)
Annual Computer Security Applications Conference (ACSAC)	(2012 – 2015)
International Symposium on Research in Attacks, Intrusions and Defenses (RAID)	(2014 – 2015)
International Symposium on Engineering Secure Software and Systems (ESSoS)	(2015)
APWG Symposium on Electronic Crime Research (eCrime)	(2014)
Kaspersky “CyberSecurity for the Next Generation”, The Americas Round	(2014)
International Conference on Security and Privacy in Communication Networks (SecureComm)	(2013 – 2014)
IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC)	(2013)
European Conference on Computer Network Defense (EC2ND)	(2011)
International Conference on Cryptology And Network Security (CANS)	(2010)
ACM EuroSys Conference (<i>Shadow PC</i>)	(2010)

Grant Proposal Review

NSF	(2015, 2017, 2018)
Reviewer and panelist for NSF	

Other Reviewing

I have been invited to review and have reviewed papers for the following conferences and journals: IWSEC’10, ACSAC’11, ESORICS’11, RAID’11, ACNS’12, CANS’12, NDSS’12, CCS’12, FC2013, *and* journals: IET Information Security ’10, ’11, ’12, Information Security Journal ’12, ACM transactions of Information and System Security (TISSEC) ’12 and ’13, KSII Transactions on Internet and Information Systems ’13, Elsevier Computers & Security 2013 & 2017 , IEEE Transactions on Reliability ’13, IEEE Communications Letters ’13 and ’14, IEEE Transactions on Dependable and Secure Computing ’14, IEEE S&P ’14, and De gryuter it - Information Technology ’16.

Program Organization

Posters Chair, 37th IEEE Symposium on Security and Privacy	(2016)
Publication co-chair, 17th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)	(2014)
Organizing Committee, Security and Privacy Day, Stevens Institute of Technology	(Spring 2013)

PhD Committee Service

Keith D. Willet, Stevens Institute of Technology	(November 2016)
Kangkook Jee, Columbia University	(June 2015)
Angeliki Zavou, Columbia University	(May 2014)
Asia Slowinska, Vrije Universiteit Amsterdam	(May 2012)

Editorships

Research in Attacks, Intrusions, and Defenses (RAID)

Angelos Stavrou, Herbert Bos, and Georgios Portokalidis (editors)

Lecture Notes in Computer Science (LNCS), Springer, September 2014

Special Issue on Security and Privacy in Unified Communications: Challenges and Solutions

Georgios Karopoulos, Georgios Portokalidis, Josep Domingo-Ferrer, Ying-Dar Lin, Dimitris Geneiatakis, and

Georgios Kambourakis (editors)
Computer Communications, Elsevier, September 2015

Other

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

Press

“Practical Binary Analysis” (September 2018)
Nostarch Press

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

NICTA, Sydney, Australia (August 2008)
Visiting researcher in the ERTOS group at the Neville Roach Lab (NRL)

Institute for Infocomm Research, Singapore (May 2008 – July 2008)
Visiting Researcher in the Internet Security Lab

Microsoft Research at Cambridge, UK (April 2007 – June 2007)
Intern

Intel Research at Cambridge, UK (September 2004 – January 2005)
Intern

Leiden University, The Netherlands (September 2003 – July 2004)
Research assistant

Internet Hellas, Greece (June 2001 – August 2001)
Summer trainee

ATLANTIS group, Greece (November 1999 – February 2002)
Web and application developer, system administrator

UCnet University of Crete, Greece (March 2000 – September 2000)
Assistant system administrator

E.L.K.E. University of Crete, Greece
Assistant system administrator

(December 1999 – February 2000)

Teaching

Stevens Institute of Technology

CS-676 Advanced Topics in Systems Security

Spring 2017 (on campus): 2 students, Spring 2018 (on campus): 2 students

CS-576 Systems Security

Fall 2016 (on campus): 16 students, Spring 2018 (on campus): 27 students

CS-497-S Independent Study

Fall 2016 (on campus): 1 student

CS-392-A Systems Programming

Spring 2016 (on campus): 25 students, Spring 2017 (on campus): 21 students

CS-576 Secure Systems

Fall 2014 (on campus): 15 students, Fall 2015 (on campus): 15 students

CS-577 Cybersecurity Lab

Fall 2014 (on campus): 15 students, Fall 2015 (on campus): 15 students

CS-695 Host Forensics

Spring 2013 (on campus): 3 students, Spring 2014 (on campus): 6 students

CS-181 Introduction to Computer Science, Honors I

Fall 2013 (on campus): 19 students

CS-801-S Special Problem in CS for PhD students

Fall 2014 (on campus): 1 student Spring 2017 (on campus): 1 student

CS-800-S Special Problem in Computer Science for MS students

Fall 2013 (on campus): 1 student, Spring 2017 (on campus): 1 student, Spring 2018 (on campus): 1 student

CS-960-S Research in Computer Science

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-397 Outreach Participation

Fall 2013 (on campus): 5 students, Spring 2014 (on campus): 4 students, Fall 2014 (on campus): 4 students, Spring 2015 (on campus): 1 student

Vrije Universiteit Amsterdam

Practical courses for high-school students

(Spring 2006, 2007 & 2009)

Computer Science Department, Vrije Universiteit, The Netherlands

Stevens Service

Institutional

SES Committee on Committees

(2014 – 2016)

Departmental

Undergraduate advisor for CS majors

(Fall 2015 – Spring 2016, Fall 2017 – present)

Communications committee (chair)	(Fall 2016 – present)
MS in Cybersecurity admissions committee (chair)	(Fall 2016)
PhD committee (member)	(Spring 2013 – present)
Graduate advisor for MS in cybersecurity	(Fall 2016)
Hiring committee (member)	(2015 – 2016, 2018)
Undergraduate advisor for cybersecurity majors	(Fall 2016)
Seminar coordinator	(Fall 2013 – Spring 2016)
Communications committee (member)	(Spring 2013 – Spring 2016)
Admissions committee (member)	(Fall 2015)