

Z. BERKAY CELIK

336 Westgate Building University Park, PA, 16802, USA
zbc102@psu.edu ◇ <https://berkay.github.io/> ◇ 814-777-1060

EDUCATION

- | | |
|----------------|---|
| 2014 - Present | The Pennsylvania State University , Ph.D. in Computer Science and Engineering <ul style="list-style-type: none">• Thesis: Automated IoT Security and Privacy Analysis• Advisor: Professor Patrick McDaniel |
| 2009 - 2011 | The Pennsylvania State University , M.S. in Computer Science <ul style="list-style-type: none">• Minor in Computational Science• Thesis: Salting Public Traces with Attack Traffic to Test Flow Classifiers• Advisor: Professor George Kesidis |
| 2002 - 2006 | Naval Academy (Istanbul, Turkey) , B.S. in Computer Science (<i>summa cum laude</i>) |

ACADEMIC AND RESEARCH APPOINTMENTS

- | | |
|----------------|--|
| 2018 - present | Lead Graduate Student
Systems and Internet Infrastructure Security (SIIS) Laboratory, Pennsylvania State University <ul style="list-style-type: none">• Conduct weekly lab meetings of nine graduate students• Provide students with mentoring, research guidance and leadership skills |
| 2014 - 2018 | Computer Security Graduate Research Assistant
Systems and Internet Infrastructure Security (SIIS) Laboratory, Pennsylvania State University <ul style="list-style-type: none">• Designed algorithms to automate IoT security and privacy analysis• Proposed defense for sensitive data leaks and safety and security violations in IoT• Introduced detection under privileged information to improve detection accuracy• Disseminated research through a survey article and open-source contributions |
| 2011 - 2014 | Visiting Research Associate
Computer Networks Research Laboratory, Istanbul Technical University <ul style="list-style-type: none">• Worked Prof. Sema Oktug's group on ML and malware detection systems• Gave seminars in machine learning algorithms for security• Developed ML algorithms for malware detection• Published results on early-detection of fast-flux botnets at IEEE ISCC'13 |
| 2009 - 2011 | Research Assistant
Advanced Network Sciences and Communications Laboratory, Pennsylvania State University <ul style="list-style-type: none">• Advised by Prof. George Kesidis and Prof. David J. Miller• Worked on NSF NeTSE: Unsupervised Flow-Based Clustering project• Developed machine learning models for flow-based malware detection systems• Published results on botnet detection at USENIX Security CSET'11 |

INDUSTRIAL EXPERIENCE

- | | |
|----------------|---|
| May - Aug 2017 | VMware, Software Engineer in Research Intern
VMware Monitor Team, Cambridge, MA <ul style="list-style-type: none">• Hosted by Josh Simmons and Ronn Mann at VMware's Office of the CTO• Applied Deep Learning to evaluate VMware software for security and efficacy• Developed ML and NLP algorithms to automate software security analysis• Researched VMware's IoT agent for security and privacy issues |
|----------------|---|

- May - Aug 2015 Vencore Labs in Research Intern**
Cybersecurity and Data Analytics Team, Basking Ridge, NJ
- Hosted by Dr. Ritu Chadha (Security) and Rauf Izmailov (ML)
 - Developed malware simulation scenarios in a controlled testbed
 - Designed Learning Using Privileged Information (LUPI) models for security
 - Implemented algorithms to retain classifier accuracy when users redact private data
- 2011 - 2014 Turkish Naval Forces**
Software Developer
- Developed algorithms for Naval and NATO software systems
 - Implemented naval inventory management system serving thousands of users
 - Attended multiple international and NATO-related software trainings
- 2007 - 2009 Turkish Naval Forces**
First Officer
- Exercised command over Naval and NATO software systems
 - Led 87 petty officers and enlisted men under my command

HONORS & AWARDS

Best Paper: Security and Privacy in Communications Networks (SecureComm) (2018)
Most Amusing Talk: Program Analysis of IoT Implementations, USENIX Security HoTSec (2018)
Best Demonstration: Sensitive Information Tracking in Commodity IoT, Florida Institute for Cybersecurity Research (FICS) (2018)
Student Travel Awards: ACM ASIACCS (2018), Military Communications Conference (2015)
Summer Grant Award: PSU Summer Tuition Assistance Program Fellowship (2015, 2017)
Research Assistantship: The Pennsylvania State University (2014-2019)
Exceptional Academic Achievement: Turkish Naval Academy Honor List (2002-2006)

PROFESSIONAL ACTIVITIES

Session Chair

- 2018: SecureComm Conference (Session on Web Security)

Program Committee Member

- 2019: ASIA Conference on Computer and Communications Security (ASIACCS)
- 2018: NIPS Workshop on Security in Machine Learning
- 2018: CCS Poster/Demonstration Session
- 2018: Privacy-Aware Computing Symposium (IEEE PAC)
- 2017: Internet of Things Security and Privacy Workshop (IoT S&P) (co-located with CCS)
- 2017: Cyber-Physical Systems Security Workshop (CPS-Sec) (co-located with CNS)
- 2016: Conference for Military Communications (MILCOM)

External Reviewer

- 2019: USENIX Security Symposium
- 2018: ACM Computing Surveys (CSUR)
- 2018: Conference on Decision and Game Theory for Security (GameSec)
- 2018: ACM Conference on Computer and Communications Security (CCS)
- 2018: USENIX Security Symposium
- 2018: IEEE Symposium on Security and Privacy (S&P)
- 2018: Neural Information Processing Systems (NIPS)
- 2017: IEEE Security and Privacy Magazine
- 2017: IEEE Symposium on Security and Privacy (S&P)

- 2017: ACM Computing Surveys (CSUR)
- 2017: Neural Processing Letters
- 2017: IEEE Transactions on Information Forensics and Security
- 2016: Computers Open Access Journal
- 2016: Journal of Network and Computer Applications (JNCA)

Community Outreach and Research Dissemination

- Co-authored and maintain the IoT Bench open-source test-suite for IoT apps
 - The repository has 20+ stars on GitHub.
 - Code was written by 5+ contributors
- Co-authored and maintain the source code of the ultimate Java Multithreading course
 - The repository has 300+ stars and 350+ forks on GitHub.

TEACHING EXPERIENCE

Co-instructor

CSE 597: Security and Privacy of Machine Learning (Fall 2016)

CSE 597: Advanced Topics in the Security and Privacy of Machine Learning (Spring 2017)

Guest lecturer

CMPSC 443: Introduction to Computer and Network Security (Spring 2017, Fall 2018)

CMPSC 311: Introduction to Systems Programming (Fall 2016)

CSE 597: Wireless and Mobile Security (Fall 2017)

CSE 543: Computer Security (Fall 2018)

PRESENTATIONS AND INVITED TALKS

Automated IoT Security and Privacy Analysis

- November 2018: University of Florida
- October 2018: Worcester Polytechnic Institute
- September 2018: Northeastern University
- August 2018: USENIX Security Lighting Talk Session
- August 2018: USENIX HotSec Workshop
- April 2018: CSE 597 Wireless and Mobile Security, Penn State University
- April 2018: Army Research Laboratory
- March 2018: CMPSC 443 Computer Security, Penn State University
- June 2017: University of California, Davis
- April 2017: Great Lakes Security Day, Rochester Institute of Technology

Generating Machine Learning Models under Privileged Information

- December 2016: Istanbul Technical University
- September 2016: Florida International University
- September 2016: Institute for Networking and Security Research, Penn State University
- May 2016: Indiana University

Security and Privacy in Machine Learning

- December 2018: CSE 543 Computer Security, Penn State University (Adversarial ML lecture)
- August 2018: VMware Monitor Team
- July 2018: VMware CTO Office
- July 2017: College of Engineering Symposium, Penn State University

Malware Detection and Modeling Operations in Cyberspace

- March 2016: Army Research Laboratory

- March 2016: George Mason University
- August 2015: Vencore Labs
- June 2015: University of California, Riverside

PUBLICATIONS

Complete list of publications is maintained at <https://berkay.github.io/>.

Journal Publications

[J1]. Z. Berkay Celik, Patrick McDaniel, and Thomas Bowen, **Malware Modeling and Experimentation through Parameterized Behavior**, In Journal of Defense Modeling and Simulation, 2018

Conference Publications

[C1]. Z. Berkay Celik, Gang Tan, and Patrick McDaniel **IoTGuard: Dynamic Enforcement of Security and Safety Policy in Commodity IoT**, Proceedings of the Network and Distributed System Security Symposium (NDSS), 2019 Acceptance Rate: 17%

[C2]. Z. Berkay Celik, Abbas Acar, Hidayet Aksu, Ryan Sheatsley, Patrick McDaniel, and Selcuk Uluagac, **Curie: Policy-based Secure Data Exchange**, ACM Conference on Data and Application Security and Privacy (CODASPY), 2019 Acceptance Rate: 23.5%

[C3]. Z. Berkay Celik, Patrick McDaniel, and Gang Tan, **Soteria: Automated IoT Safety and Security Analysis**, Proceedings of the USENIX Annual Technical Conference (USENIX ATC), 2018, Acceptance Rate: 19% (4 citations)

[C4]. Z. Berkay Celik, Leonardo Babun, Amit K. Sikder, Hidayet Aksu, Gang Tan, Patrick McDaniel, and Selcuk Uluagac, **Sensitive Information Tracking in Commodity IoT**, Proceedings of the USENIX Security Symposium, 2018, Acceptance Rate: 18% (8 citations)

[C5]. Z. Berkay Celik, Patrick McDaniel, Rauf Izmailov, Nicolas Papernot, Ryan Sheatsley, Raquel Alvare, and Ananthram Swami, **Detection under Privileged Information**, Proceedings of the Asia Conference on Computer and Communications Security (ASIACCS), 2018, Acceptance Rate: 20%

[C6]. Sayed Saghaian, Tom La Porta, Trent Jaeger, Z. Berkay Celik, and Patrick McDaniel, **Mission-oriented Security Model, Incorporating Security Risk, Cost and Payout**, Proceedings of the Security and Privacy in Communication Networks (SecureComm), 2018, (Best Paper Award)

[C7]. Z. Berkay Celik, David Lopez-Paz, and Patrick McDaniel, **Patient-Driven Privacy Control through Generalized Distillation**, Proceedings of the IEEE Privacy-aware Computing (PAC), 2017

[C8]. Nicolas Papernot, Patrick McDaniel, Ian Goodfellow, Somesh Jha, Z. Berkay Celik et al., **Practical Black-Box Attacks against Machine Learning**, Proceedings of the Asia Conference on Computer and Communications Security (ASIACCS), 2017, Acceptance Rate: 20% (427 citations)

[C9]. Abbas Acar, Z. Berkay Celik, Hidayet Aksu, A. Selcuk Uluagac, and Patrick McDaniel, **Achieving Secure and Differentially Private Computations in Multiparty Settings**, Proceedings of the IEEE Privacy-aware Computing (PAC), 2017, Acceptance Rate: 33%

[C10]. Z. Berkay Celik, Nan Hu, Yun Li et al., **Mapping Sample Scenarios to Operational Models**, Proceedings of the IEEE Conference for Military Communications (MILCOM), 2016

[C11]. Nicolas Papernot, Patrick McDaniel, Somesh Jha, Matt Fredrikson, Z. Berkay Celik et al., **The Limitations of Deep Learning in Adversarial Settings**, Proceedings of the European Symposium on Security and Privacy (Euro S&P), 2016, Acceptance Rate: 17.3% (469 citations)

[C12]. Z. Berkay Celik, Robert J Walls, Patrick McDaniel, and Ananthram Swami, **Malware Traffic**

Detection using Tamper Resistant Features, Proceedings of the IEEE Military Communications (MILCOM) Conference, 2015, (17 citations)

[C13]. Z. Berkay Celik and Sema Oktug, **Detection of Fast-flux Networks using Various DNS Feature Sets**, Proceedings of the IEEE Computers and Communications Symposium (ISCC), 2013, (19 citations)

Workshop Publications

[W1]. Z. Berkay Celik and Patrick McDaniel, **Extending Detection with Privileged Information via Generalized Distillation**, IEEE Workshop on Deep Learning and Security (colocated with S&P), 2018, Acceptance Rate: 27%

[W2]. Z. Berkay Celik, Jayaram Raghuram, George Kesidis, and David J. Miller, **Salting Public Traces with Attack Traffic to Test Flow Classifiers**, Proceedings of USENIX Security Workshop on Cyber Security and Experimentation (CSET), 2011, (31 citations)

[W3]. Z. Berkay Celik, Patrick McDaniel, and Rauf Izmailov, **Feature Cultivation in Privileged Information augmented Detection**, Proceedings of the Security And Privacy Analytics Workshop (CODASPY, IWSPA), 2017 (Invited paper)

Columns

[CL1]. Patrick McDaniel, Nicolas Papernot and Z. Berkay Celik, **Machine Learning in Adversarial Settings**, IEEE Security & Privacy Magazine (May/June 2016), (31 citations)

Technical Reports

[T1]. Z. Berkay Celik, Patrick McDaniel, and Rauf Izmailov, **Proof and Implementation of Algorithmic Realization of Learning Using Privileged Information (LUPI) Paradigm: SVM+**, NSCR, Department of CSE, Pennsylvania State University, Tech. Rep. NAS-TR-0187-2015

Papers Under Review

[S1]. Z. Berkay Celik, Earlence Fernandes, Eric Pauley, Gang Tan, and Patrick McDaniel, **Program Analysis of Commodity IoT Apps for Security and Privacy: Opportunities and Challenges**, 2018, (<https://arxiv.org/pdf/1809.06962.pdf>)

[S2]. Amit Sikder, Leonardo Babun, Z. Berkay Celik, Abbas Acar, Engin Kirda, Patrick McDaniel, and Selcuk Uluagac, **Kratos: Multi-User Multi-Device-Aware Access Control System for Smart Home**, 2018

[S3]. Nan Hu, Novella Bartollini, Tom La Porta, Z. Berkay Celik, and Patrick McDaniel, **On the Optimization of Cyber Missions under Risk**, 2018

REFERENCES

Available upon request.