Z. BERKAY CELIK

Assistant Professor of Department of Computer Science, Purdue University

LWSN 1187, 305 N. University Street West Lafayette, IN 47907-2107, USA

zcelik@purdue.edu ◇ https://beerkay.github.io/ ◇ (765) 496-1761

Updated: May 3, 2020

CURRENT ACADEMIC APPOINTMENT

2019 - present **Purdue University**, Assistant Professor, Computer Science Department

EDUCATION

2014 - 2019 **The Pennsylvania State University**, Ph.D. in Computer Science and Engineering
- Thesis: *Automated IoT Security and Privacy Analysis*
- Advisor: Professor Patrick McDaniel

2009 - 2011 **The Pennsylvania State University**, M.S. in Computer Science
- 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 (*summa cum laude*)

PREVIOUS RESEARCH APPOINTMENTS

2018 - 2019 **Lead Graduate Student**
Systems and Internet Infrastructure Security (SIIS) Laboratory, Pennsylvania State University

2014 - 2018 **Computer Security Graduate Research Assistant**
Systems and Internet Infrastructure Security (SIIS) Laboratory, Pennsylvania State University

2011 - 2014 **Visiting Research Associate**
Computer Networks Research Laboratory, Istanbul Technical University
- Worked Prof. Sema Oktug's group on ML and malware detection systems

2009 - 2011 **Graduate Student Member**
Advanced Network Sciences and Communications Laboratory, Pennsylvania State University
- Advised by Prof. George Kesidis and Prof. David J. Miller

INDUSTRIAL EXPERIENCE

May - Aug 2017 **VMware, Software Engineer in Research Intern**
VMware Monitor Team, Cambridge, MA
- Hosted by Josh Simmons and Ronn Mann at VMware's Office of the CTO

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)

2011 - 2014 **Turkish Naval Forces**
Software Developer

HONORS & AWARDS

- 2020, Purdue Graduate Student Board (GSB) Most Influential Professor in Computer Science
- 2018, 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: NDSS (2019), ACM ASIACCS (2018), MILCOM (2015)
- 2015, 2017, Summer Research Grant Award: PSU Summer Tuition Assistance Program Fellowship
- 2014-2019, Research Assistantship, The Pennsylvania State University
- Exceptional Academic Achievement, Turkish Naval Academy Honor List (2002-2006)

PUBLICATIONS

Journal Articles

[J1]. 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**, ACM Computing Surveys (CSUR), 2019, (`https://arxiv.org/pdf/1809.06962.pdf`)

[J2]. Z. Berkay Celik, Patrick McDaniel, and Thomas Bowen, **Malware Modeling and Experimentation through Parameterized Behavior**, In Journal of Defense Modeling and Simulation, 2018

Peer-reviewed Conference Publications

[C3]. Leonardo Babun, Z. Berkay Celik, Patrick McDaniel, and Selcuk Uluagac, **Real-time Analysis of Privacy-(un)aware IoT Applications**, Privacy Enhancing Technologies Symposium (PETS), 2021,

[C4]. 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 the Smart Home**, 2020, ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec)

[C5]. Michael Norris, Z.Berkay Celik, Prasanna Venkatesh, Shulin Zhao, Gang Tan, Patrick McDaniel, and Anand Sivasubramaniam, **IoTRepair: Systematically Addressing Device Faults in Commodity IoT**, ACM/IEEE Conference on Internet of Things Design and Implementation (IoTDI), 2020

[C6]. 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%

[C7]. 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%

[C8]. 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%

[C9]. 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%

[C10]. Z. Berkay Celik, Patrick McDaniel, Rauf Izmailov, Nicolas Papernot, Ryan Sheatsley, Raquel

Alvarez, and Ananthram Swami, **Detection under Privileged Information**, Proceedings of the Asia Conference on Computer and Communications Security (ASIACCS), 2018, Acceptance Rate: 20%

[C11]. 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)**

[C12]. 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

[C13]. Nicolas Papernot, Patrick McDaniel, Ian Goodfellow, Somesh Jha, Z. Berkay Celik, and Ananthram Swami, **Practical Black-Box Attacks against Machine Learning**, Proceedings of the Asia Conference on Computer and Communications Security (ASIACCS), 2017, Acceptance Rate: 20%

[C14]. 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%

[C15]. 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

[C16]. Nicolas Papernot, Patrick McDaniel, Somesh Jha, Matt Fredrikson, Z. Berkay Celik and Ananthram Swami, **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%

[C17]. 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

[C18]. 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

Refereed Workshop Publications

[W19]. Paul Berges, Basavesh A. Shivakumar, Timothy Graziano, Ryan Gerdes, and Z. Berkay Celik, **On the Feasibility of Exploiting Traffic Collision Avoidance System Vulnerabilities**, IEEE Workshop on Cyber-Physical Systems Security (CPS-Sec) (colocated with IEEE CNS), 2020.

[W20]. 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,

[W21]. 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)

[W22]. 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

Refereed Magazine Articles

[CL23]. Z. Berkay Celik, Patrick McDaniel, Gang Tan, Selcuk Uluagac, and Leonardo Babun, **Verifying IoT Safety and Security in Physical Spaces**, IEEE Security & Privacy Magazine, 2019

[CL24]. Patrick McDaniel, Nicolas Papernot and Z. Berkay Celik, **Machine Learning in Adversarial Settings**, IEEE Security & Privacy Magazine (May/June 2016),

Technical Reports

[T25]. 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

Thesis

[Th26]. Z. Berkay Celik, **Automated IoT Security and Privacy Analysis**, PhD Thesis, Pennsylvania State University, August 2019.

[Th27]. Z. Berkay Celik, **Salting Public Traces with Attack Traffic to Test Flow Classifiers**, Master Thesis, Pennsylvania State University, August 2011.

PRESENTATIONS AND INVITED TALKS

- **Safety and Security Analysis of IoT Systems**
  - April 2019: University of Rochester
  - April 2019: Lehigh University
  - March 2019: Boston University
  - March 2019: The University of Texas at Dallas
  - March 2019: Oregon State University
  - March 2019: Duke University
  - March 2019: George Washington University
  - March 2019: Syracuse University
  - March 2019: University of Arizona
  - February 2019: Drexel University
  - February 2019: The College of William & Mary
  - February 2019: Stevens Institute of Technology
  - February 2019: Dartmouth College
  - February 2019: Worcester Polytechnic Institute
  - February 2019: The University of California, Irvine
  - January 2019: University of Pittsburgh
- **Program Analysis of IoT Systems for Security and Privacy**
  - 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
- **Training 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 of Machine Learning Systems**
  - 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 Cyber Operation Modeling**
  - March 2016: Army Research Laboratory
  - March 2016: George Mason University
  - August 2015: Vencore Labs
  - June 2015: University of California, Riverside

PROFESSIONAL ACTIVITIES

- **Session Chair**
  - 2018: SecureComm Conference (Session on Web Security)
- **Program Committee Member**
  - 2020: SecureComm Conference
  - 2020, Workshop on Trustworthy ML (co-located with ICLR)
  - 2020, European Symposium on Research in Computer Security (ESORICS)
  - 2020, Uncertainty in Artificial Intelligence (UAI)
  - 2020, IEEE Computer Security Foundations Symposium (CSF)
  - 2019, CCS Workshop on the Internet of Things Security and Privacy (IoT S&P)
  - 2019, MILCOM 2019 (Track 3 - Cyber Security and Trusted Computing)
  - 2019, Workshop on ML for Security and Cryptography (co-located with IEEE PIMRC)
  - 2019, Uncertainty in Artificial Intelligence (UAI)
  - 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)
- **Journal and External Reviewer**
  - 2020, IEEE Transactions on Dependable and Secure Computing
  - 2019, IEEE Security & Privacy Magazine
  - 2019, IEEE Transactions on Mobile Computing
  - 2019, ACM Transactions on Internet of Things
  - 2019, IEEE Transactions on Dependable and Secure Computing
  - 2019, IEEE Transactions on Neural Networks and Learning Systems
  - 2019, 2018, USENIX Security Symposium
  - 2019, 2018, 2017, IEEE Symposium on Security and Privacy (S&P)
  - 2018, ACM Conference on Computer and Communications Security (CCS)
  - 2018, ACM Computing Surveys (CSUR)
  - 2018, Conference on Decision and Game Theory for Security (GameSec)
  - 2018, Neural Information Processing Systems (NIPS)
  - 2017, IEEE Security and Privacy Magazine
  - 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)

- 2020, NSF Experimental Program to Stimulate Competitive Research (EPSCoR) extranal reviewer
- 2019, NSF SaTC panelist (virtual)
- 2020, Computing Research Association (CRA), Career Mentoring Workshop (Selected Attendee)
- 2020, NSF CISE CAREER Workshop, April 6-8 (Virtual, Selected Attendee)
- 2020, Faculty Success Program, May 17 - August 8 (12-week, online)

UNIVERSITY ACTIVITIES

Service to CS Department of Purdue University

- 2019, 2020: Departmental Graduate Admission Committee, Member

Presentations

- September 2020, CS 397, Honors Seminar, IoT Systems Security
- March 2020, General Motors, Intentional Electomagnetic Attacks and Defenses against Sensors/Actuators
- October 2019, Tsukuba University visitors, IoT and Machine Learning Security
- October 2019, Air Force Research Laboratory visitors, IoT/CPS Safety and Security
- October 2019, Seminar for First-year PhD students, IoT and Machine Learning Security
- October 2019, Naval Surface Warfare Center-Crane Division, IoT and Machine Learning Security
- August 2019, CS 397, Honors Seminar, Trustworthy Machine Learning
- August 2019, CS Grad Orientation Week, IoT/CPS Safety and Security
- July 2019, Boeing, Verification of IoT Software for Safety and Security

STUDENT ADVISING

Current Students

- M. Ozgur Ozmen, PhD, Spring'20
- Yi-Shan Lin, PhD, Fall'20
- Basavesh Shivakumar, Msc
- Michael Reeves, Msc
- Siddharth Divi, Msc

Co-advising

- Abdulellah Alsaheel, PhD (co-advised with Prof. Dongyan Xu)
- Khaled Serag, PhD (co-advised with Prof. Dongyan Xu)

Undergraduate Students

- Andrew Chun-An Chu, senior, Purdue CS
- Ruoyu Song, senior, Purdue CS

Advisory Committee Member

- Khaled Serag (Chair: Prof. Xu), Li Jiacheng (Chair: Prof. Li), Le Yu (Chair: Prof. Zhang), Hong Jun Cho (Chair: Prof. Zhang), Weicheng Wang (Chair: Prof. Li)

Past PhD Committees

- Rohit Bhatia, Purdue University, Fall'19.
  Thesis: On Cyber-Physical Forensics, Attacks, and Defenses

TEACHING

Unless noted otherwise, all courses are 3-credit courses.

Purdue University

- Fall 2020: CS 529: Security Analytics
- Spring 2020: CS 590: IoT/CPS Security (9 students)
- Fall 2019: CS 529: Security Analytics (Significantly redesigned, 23 students), Evaluation: 4.7/5

Penn State University (During Ph.D.)

- **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)

Community Outreach and Research Dissemination

- Co-authored and maintain the `IoTBench` open-source test-suite for IoT apps
  - The repository has 40+ 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 400+ stars and 350+ forks on GitHub.