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: September 1, 2021

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*)

ACADEMIC AND RESEARCH APPOINTMENTS

Computer Science, Purdue University — West Lafayette, IN, USA
Assistant Professor — Aug 2020–*present*

Systems and Internet Infrastructure Security (SIIS) Laboratory — University Park, PA, USA
Lead Graduate Student — Jan 2019–Aug 2020

Pennsylvania State University, SIIS Laboratory — University Park, PA, USA
Computer Security Graduate Research Assistant — Aug 2014–Aug 2020

Computer Networks Research Laboratory, Istanbul Technical University — Istanbul, Turkey
Researcher — Aug 2011–Aug 2014

Pennsylvania State University, Network Sciences and Communications Lab — University Park, PA, USA
Graduate Student Member — Jan 2010–Aug 2011

INDUSTRIAL EXPERIENCE

VMware, CTO Office, Hypervisor Team — Cambridge, MA, USA
Research Intern, Mentored by Josh Simmons — May 2017–Aug 2017

Vencore Labs — Basking Ridge, NJ, USA
Research Intern, Mentored by Dr. Ritu Chadha and Dr. Rauf Izmailov — May 2015–Aug 2015

Turkish Naval Forces — Turkey
Software Engineer — Aug 2011–May 2014

AWARDS AND HONORS

Internal to Purdue

◇ Most Influential Professor in Computer Science, Purdue Graduate Student Board (GSB), April 2020.

External to Purdue

◇ Best paper award, Security and Privacy in Communications Networks (SecureComm) Conference, August 2018.
◇ The most amusing talk award, Program Analysis of IoT Implementations, USENIX Summit on Hot Topics in Security (colocated with USENIX Security), August 2018.
◇ Best demonstration award, Sensitive Information Tracking in Commodity IoT, Florida Institute for Cybersecurity Research (FICS), March 2017.
◇ Student travel awards, NDSS (2019), ACM ASIACCS (2018), MILCOM (2015).
◇ Summer research grant award, PSU Summer Tuition Assistance Fellowship, 2015 and 2017.
◇ Research assistantship, The Pennsylvania State University, 2014–2019.
◇ Exceptional academic achievement, Turkish Naval Academy Honor List, 2002–2006.

REFEREED PUBLICATIONS

Journal Articles

[J1]. Amit Sikder, Leonardo Babun, Z. Berkay Celik, Abbas Acar, Engin Kirda, Patrick McDaniel, and Selcuk Uluagac, **Who's Controlling My Device? Multi-User Multi-Device-Aware Access Control System for Shared Smart Home**, ACM Transactions on Internet of Things (ACM TIOT), 2021

[J2]. Kyle Denney, Leonardo Babun, Z. Berkay Celik, Patrick McDaniel, and Selcuk Uluagac, **A Survey on IoT Platforms: Communication, Security, and Privacy Perspectives**, Computer Networks, Volume 192, 108040, ISSN 1389-1286, 2021

[J3]. 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), 52, 4, Article 74, 2019

[J4]. Z. Berkay Celik, Patrick McDaniel, and Thomas Bowen, **Malware Modeling and Experimentation through Parameterized Behavior**, In Journal of Defense Modeling and Simulation, vol. 15(1), pages 31-48, 2018

Peer-reviewed Conference Publications

[C5]. Yi-Shan Lin[G], Wen-Chuan Lee, and Z. Berkay Celik, **What Do You See? Evaluation of Explainable Artificial Intelligence (XAI) Interpretability through Neural Backdoors**, ACM SIGKDD Conference on Knowledge Discovery & Data Mining (KDD), 2021, (Acceptance Rate 15.4%).

[C6]. Khaled Serag[G], Rohit Bhatia, Vireshwar Kumar,Z. Berkay Celik, and Dongyan Xu, **Exposing New Vulnerabilities of Error Handling Mechanism in CAN**, Proceedings of the USENIX Security Symposium, 2021, (Acceptance Rate: 18.8%).

[C7]. Abdulellah Alsaheel[G], Yuhong Nan, Shiqing Ma, Le Yu, Gregory Walkup, Z. Berkay Celik, Dongyan Xu, and Xiangyu Zhang, **ATLAS: A Sequence-based Learning Approach for Attack Investigation**, Proceedings of the USENIX Security Symposium, 2021, (Acceptance Rate: 18.8%).

[C8]. Hyungsub Kim[G], M. Ozgur Ozmen[G], Antonio Bianchi, Z. Berkay Celik, and Dongyan Xu, **PGFUZZ: Policy-Guided Fuzzing for Robotic Vehicles**, Proceedings of the Network and Distributed System

Security Symposium (NDSS), 2021, (Acceptance Rate: 15.2%).

[C9]. Rohit Bhatia, Vireshwar Kumar, Khaled Serag[G], Z. Berkay Celik, Mathias Payer, and Dongyan Xu, **Evading Voltage-Based Intrusion Detection on Automotive CAN**, Proceedings of the Network and Distributed System Security Symposium (NDSS), 2021, (Acceptance Rate: 15.2%)

[C10]. Habiba Farrukh[G], Tinghan Yang, Yuxuan Yin, Hanwen Xu, He Wang, and Z. Berkay Celik, **S3: Side-channel Attack on Stylus Pencil Through Sensors**, The ACM Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT/UbiComp), 5, 1, Article 8, March, 2021

[C11]. Leonardo Babun, Z. Berkay Celik, Patrick McDaniel, and Selcuk Uluagac, **Real-time Analysis of Privacy-(un)aware IoT Applications**, Proceedings on Privacy Enhancing Technologies (PoPETS), no.1, pp.145-166, 2021, (Acceptance Rate: 18.6%)

[C12]. Adrien Cosson, Amit Sikder, Leonardo Babun, Z. Berkay Celik, Patrick McDaniel and Selcuk Uluagac , **Sentinel: A Robust Intrusion Detection System for IoT Networks Using Kernel-Level System Information**, ACM/IEEE Conference on Internet of Things Design and Implementation (IoTDI), 2021, (Acceptance Rate: 25%)

[C13]. 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**, ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec), 2020

[C14]. 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

[C15]. 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%)

[C16]. 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%)

[C17]. 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%)

[C18]. 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%)

[C19]. 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%)

[C20]. 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)**

[C21]. 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

[C22]. 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%)

[C23]. 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

[C24]. Z. Berkay Celik, Nan Hu, Yun Li, Nicolas Papernot, Patrick McDaniel, Robert Walls, Jeff Rowe, Karl Lewitt, Novella Bartolini, Tom LaPorta, and Ritu Chadha, **Mapping Sample Scenarios to Operational Models**, Proceedings of the IEEE International Conference for Military Communications (MILCOM), 2016

[C25]. 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%)

[C26]. 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

[C27]. 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

[W28]. Siddharth Divi[G], Yi-Shan Lin[G], Habiba Farrukh[G], and Z. Berkay Celik, **New Metrics to Evaluate the Performance and Fairness of Personalized Federated Learning**, International Workshop on Federated Learning for User Privacy and Data Confidentiality, FL-ICML (colocated with ICML), Poster and Oral presentation, 2021

[W29]. Furkan Goksel[U], M. Ozgur Ozmen[G], Michael Reeves[G], B. Shivakumar[G], and Z. Berkay Celik, **On the Safety Implications of Misordered Events and Commands in IoT Systems**, IEEE S&P SafeThings Workshop (colocated with IEEE S&P), 2021

[W30]. Paul Berges, B. Shivakumar[G], 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

[W31]. Z. Berkay Celik and Patrick McDaniel, **Extending Detection with Privileged Information via Generalized Distillation**, IEEE Workshop on Deep Learning and Security (colocated with IEEE S&P), 2018

[W32]. 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)

[W33]. 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

[CL34]. 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

[CL35]. Patrick McDaniel, Nicolas Papernot and Z. Berkay Celik, **Machine Learning in Adversarial Settings**, IEEE Security & Privacy Magazine, 2016

Technical Reports

[T36]. 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

[Th37]. Z. Berkay Celik, **Automated IoT Security and Privacy Analysis**, PhD Thesis, Pennsylvania State University, August 2019

[Th38]. Z. Berkay Celik, **Salting Public Traces with Attack Traffic to Test Flow Classifiers**, Master Thesis, Pennsylvania State University, August 2011

PROFESSIONAL LEADERSHIP AND SERVICE

Technical Program Committee

- ◇ 2022, NDSS
- ◇ 2022, 2021, USENIX Security
- ◇ 2021, ACSAC
- ◇ 2021, CCS (Hardware, Side Channels, and Cyber-Physical Systems Track)
- ◇ 2021, Workshop on Internet of Safe Things (co-located with IEEE S&P)
- ◇ 2021, European Symposium on Research in Computer Security (ESORICS)
- ◇ 2020, SecureComm
- ◇ 2020, Workshop on Trustworthy ML (co-located with ICLR)
- ◇ 2020, European Symposium on Research in Computer Security (ESORICS)
- ◇ 2020, 2019, 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, 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)

Session Chair

- ◇ 2018: SecureComm Conference (Web Security Chair)

Journal and External Reviewer

- ◇ 2022, INFOCOM (External Reviewer on Fuzzing and Explainable AI)

◇ 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)

Other Activities and Services

◇ 2020, Faculty Success Program, May 17 - August 8 (online), supported by Purdue Faculty Affairs
◇ 2020, SaTC Town Hall, December 15 (Attendee)
◇ 2020, NSF Experimental Program to Stimulate Competitive Research (EPSCoR) (External Reviewer)
◇ 2020, Computing Research Association (CRA), Career Mentoring Workshop (Selected Attendee)
◇ 2020, NSF CISE CAREER Workshop, April 6-8 (Virtual, Selected Attendee)
◇ 2019, NSF SaTC panelist (virtual)

STUDENT ADVISING

Current PhD Students

◇ Habiba Farrukh, Fall'20
Dissertation topic: Side-Channel Attacks through Sensors (Prelim Exam Completed)
Bilsland Dissertation Fellowship Award 2021-2022.
◇ Reham Mohamed Aburas, Fall'20
◇ M. Ozgur Ozmen, Spring 20
◇ Arjun Arunaslam, Fall 20

Co-advising PhD Students

◇ Ruoyu Song, Spring 21 (co-Advised with Antonio Bianchi)
◇ Abdulellah Alsaheel, PhD (co-advised with Dongyan Xu)
◇ Khaled Serag, PhD (co-advised with Dongyan Xu)

Current Msc Students

◇ Eliz Tekcan
◇ Jackson Bizjak
◇ Abhinav Gupta

◇ Gaurav Jadhav

Current Undergraduate Students

◇ Jason Perry, senior, Purdue CS
◇ Haozhe Zhou, senior, Purdue CS
◇ Varun Gannavarapu, junior, Purdue CS

Graduated Master Thesis Students

◇ Siddharth Divi, 2021
  – Thesis title: Unifying Distillation with Personalization in Federated Learning
  – Thesis Committee: Ming Yin and Kamyar Azizzadenesheli
  – Last Employment: Amazon
◇ Michael Reeves, 2021
  – Thesis title: Investigating Escape Vulnerabilities in Container Runtimes
  – Thesis committee: Dave Tian and Antonio Bianchi
  – Last Employment: Sandia Labs

SERVICE ON MS/PHD COMMITTEES

Preliminary Exam/Final Committee Membership

◇ Choi, Jongouk (Chair: Changhee Jung)
◇ Abdullah Imran (Chair: Antonio Bianchi)
◇ Zhiyuan Cheng (Chair: Xiangyu Zhang)
◇ Ibrahim Muhammad (Chair: Antonio Bianchi)
◇ Kyungtae Kim (Chair: Dongyan Xu)
◇ Hongjun Choi (Chair: Xiangyu Zhang)
◇ Hyungsub Kim (Chair: Dongyan Xu)
◇ Khaled Serag (Chair: Dongyan Xu)
◇ Abdulellah Alsaheel (Chair: Dongyan Xu)
◇ Ruoyu Wu (Chair: Dongyan Xu)
◇ Li Jiacheng (Chair: Ninghui Li)
◇ Le Yu (Chair: Xiangyu Zhang)
◇ Weicheng Wang (Chair: Ninghui Li)

Past PhD Committees

◇ Rohit Bhatia, CS, Fall'19 (Last Employment: Google)

OTHER MENTORING (SUPERVISED UNDERGRADUATE AND MSC RESEARCH)

Graduate Students

◇ Yi-Shan Lin (Msc), Research Advisor, 2021
◇ Basavesh Shivakumar (Msc), Research Advisor (PhD at MPI-SP), 2020
◇ Zhanfu Yang (Msc), Research Advisor (PhD at Stevens Institute of Technology), 2020
◇ Akhil Bandarupalli (Msc), Research Advisor, (PhD at Purdue CS), 2020
◇ Andrew Chun-An Chu (Senior, CS, Fall 20/Summer 20)
  – Honorable mention for the 2021 NSF GRFP fellowship
  – PhD at University of Chicago (Fall 21)

- ◇ Rouyu Song (Senior, CS, Fall 20/Summer 20)
  - PhD under my supervision
- ◇ William Carter Bell (Junior, Data Science, Summer 20)
- ◇ Anirudh Giridhar (Junior, CS minor in Mathematics and Statistics, Summer'20)
- ◇ Kaushik Ramachandran (Senior, CS, Summer 20)
- ◇ Yizhen (Yuen) Yuan, (Junior, Purdue CS, Summer 20)
- ◇ Ishan Kaul (Senior, CS, Summer 20)
- ◇ Sidhartha Agrawal (Sophomore, CS minor in Mathematics, Summer'20)
- ◇ Jason Perry (Junior, CS, Summer 20/Fall 20)
- ◇ Yuxuan Yang (Junior, CS minor in Mathematics and Economics, Summer'20)
- ◇ Rafael Zhu (Freshman, CS, Summer 20/Fall 20)
- ◇ Nail Tarcan Gul (Senior, CS, Fall 20)

External Research Interns

- ◇ Furkan Goksel (Senior, Computer Science, METU (Turkey), Summer'20, Online)
- ◇ Kerem Ors (Msc, Computer Science, Sabanci University (Turkey), Summer'20, Online)

TEACHING EXPERIENCE

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

Purdue University

- ◇ Fall 2021: CS 529: Security Analytics (33 students)
- ◇ Spring 2021: CERIAS Seminar, CS-591-SEC, 1 credit, (17 students)
- ◇ Spring 2021: CS 529: Security Analytics (Online Course Preparation)
- ◇ Fall 2020: CS 529: Security Analytics (16 students)
- ◇ Spring 2020: CS 590: IoT/CPS Security (9 students)
- ◇ Fall 2019: CS 529: Security Analytics (Significantly redesigned, 23 students)

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)

ENGAGEMENT AND SERVICE

Departmental Engagement

- ◇ Started the Systems Security Reading Group, (weekly meetings), Attendance: 20 graduate/undergraduate students and faculty members, Fall 2019-present
- ◇ Co-founder of `PurSec Research Group` (with Dongyan Xu, Antonio Bianchi, and Dave Tian)
- ◇ GoBoiler Internships (2 students, 2020)
- ◇ **Committees**
  - ◇ 2019, 2020: Departmental Graduate Admission Committee, Member

◇ **Presentation for Engagement Seminars**
- September 2020: CS 591, Graduate Research Seminar, IoT/CPS Safety and Security
- 2021, 2020, 2019: CS 397, Honors Seminar, IoT/CPS Safety and Security
- September 2019: Seminar for First-year PhD students, IoT and Machine Learning Security
- August 2019, CS Grad Orientation Week, IoT/CPS Safety and Security

Other Activities

◇ October 2020: Saab Autonomy Workshop, IoT/CPS Safety and Security
◇ September 2020: CERIAS External Advisory Board (EAB), Cyber Experimentation in Sandia SOL4CE
◇ 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: Naval Surface Warfare Center-Crane Division, IoT and Machine Learning Security
◇ July 2019: Boeing, Verification of IoT Software for Safety and Security

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.

Media Coverage

◇ Mid-air Collision Spoofing Attacks, Traffic Collision Avoidance Systems (TCAS) Security, `The Register`, June 2020
◇ Purdue teams up with DENSO to teach undergraduates about autonomous vehicles, `Purdue Engineering`, August 2020

PRESENTATIONS AND SELECTED 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

Learning in Security Systems 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