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/ ◇ +1 (765) 496-1761

Updated: December 5, 2022

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 2019–*present*

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

Pennsylvania State University, SIIS Laboratory — University Park, PA, USA
Computer Security Graduate Research Assistant — Aug 2014–Aug 2019

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
MSc 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

◇ 2020, Ross-Lynn Research Scholars Grant for the project "Security and Privacy of Intermittent Devices in Physical Spaces".

◇ 2020, Selected the most influential Professor by Purdue CS Graduate Student Board (GSB).

External to Purdue

◇ 2022, Google ASPIRE (Android Security and PrIvacy REsearch) award for the project "Improving the Security and Usability of the Wear OS Permission Model".
◇ 2022, NSF CAREER Award for the project "Compositional IoT Safety and Security in Physical Spaces".
◇ 2022, General Motors AutoDriving Security Award for the paper "DriveTruth: Automated Autonomous Driving Dataset Generation for Security Applications" to recognize research that makes substantial contributions to securing today's emerging autonomous driving technology.
◇ 2021, Google ASPIRE (Android Security and PrIvacy REsearch) award for the project "Improving the Usability of Android APIs for Conformity of Standard Security Practices".
◇ 2021, Graduate advisee Habiba Farrukh received Bilsland Dissertation Fellowship Award.
◇ 2021, Undergraduate research advisee Andrew Chu received an Honorable mention for the 2021 NSF Graduate Research Fellowships Program (GRFP).
◇ 2018, Best paper award at 14th Security and Privacy in Communications Network (SecureComm) Conf. for the paper "Mission-oriented Security Model, Incorporating Security Risk, Cost and Payout".
◇ 2018, The most amusing talk award at USENIX Summit on Hot Topics in Security (colocated with USENIX Security) for "Program Analysis of IoT Implementations".
◇ 2017, Best demonstration award at Florida Institute for Cybersecurity Research (FICS) for the demo "Sensitive Information Tracking in Commodity IoT".
◇ Student travel awards for NDSS (2019), ACM ASIACCS (2018), MILCOM (2015).
◇ 2015, 2017, Summer research grant award, PSU Summer Tuition Assistance Fellowship
◇ 2014–2019, Research assistantship, The Pennsylvania State University
◇ 2002–2006, Exceptional academic achievement, Turkish Naval Academy Honor List

PUBLICATIONS

My undergraduate (^{U}) and graduate (^{G}) advisees and co-advisees are shown with dashed underline for clarity. Acceptance rates are shown where available.

Refereed Journal Articles

[J56] Michael Norris, Z.Berkay Celik, Prasanna Venkatesh, Shulin Zhao, Patrick McDaniel, Anand Sivasubramaniam, and Gang Tan, **IoTRepair: Flexible Fault Handling in Diverse IoT Deployments**, ACM Transactions on Internet of Things (TIOT), pages 1-32, 2022.

[J55] 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), pages 1-30, 2022.

[J54] Kyle Denney, Leonardo Babun, Z. Berkay Celik, Patrick McDaniel, and Selcuk Uluagac, **A Survey on IoT Platforms: Communication, Security, and Privacy Perspectives**, Computer Networks, Vol 192, 108040, ISSN 1389-1286, pages 1-50, 2021.

[J53] 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), V:52, Nr:4, Article 74, pages 1-30, 2019.

[J52] Z. Berkay Celik, Patrick McDaniel, and Thomas Bowen, **Malware Modeling and Experimentation through Parameterized Behavior**, Defense Modeling and Simulation, Vol 15(1), pages 31-48, 2018.

Refereed Conference Proceedings

[C51] Reham Mohamed[G], Habiba Farrukh[G], He Wang, Yidong Lu, and Z. Berkay Celik, **iStelan: Disclosing Sensitive User Information by Mobile Magnetometer from Finger Touches**, In Proceedings of the Privacy Enhancing Technologies (PoPETS), 2023. (Acceptance Rate: TBD%)

[C50] M. Ozgur Ozmen[G], Ruoyu Song[G], Habiba Farrukh[G]and Z. Berkay Celik, **Evasion Attacks on Smart Home Physical Event Verification and Defenses**, In Proceedings of the Network and Distributed System Security Symposium (NDSS), pages 1-18, 2023. (Acceptance Rate: TBD%)

[C49] Hyungsub Kim[G], M. Ozgur Ozmen[G], Z. Berkay Celik, Antonio Bianchi, and Dongyan Xu, **PatchVerif: Discovering Faulty Patches in Robotic Vehicles**, In Proceedings of the USENIX Security Symposium, pages 1-18, 2023. (Acceptance Rate: TBD%)

[C48] Yanmao Man, Raymond Muller[G], Ming Li, Z. Berkay Celik and Ryan Gerdes, **That Person Moves Like A Car: Misclassification Attack Detection for Autonomous Systems using Spatiotemporal Consistency**, In Proceedings of the USENIX Security Symposium, pages 1-18, 2023.

[C47] M. Ozgur Ozmen[G], Xuansong Li, Andrew Chun-An Chu[U], Z. Berkay Celik, Bardh Hoxha, and Xiangyu Zhang, **Discovering IoT Physical Channel Vulnerabilities**, In Proceedings of the ACM Conference on Computer and Communications Security (CCS), pages 1-13, 2022. (Acceptance Rate: 22%)

[C46] Raymond Muller[G], Yanmao Man, Z. Berkay Celik, Ryan Gerdes, and Ming Li, **Physical Hijacking Attacks against Object Trackers**, In Proceedings of the ACM Conference on Computer and Communications Security (CCS), pages 1-13, 2022. (Acceptance Rate: 22%)

[C45] Hyungsub Kim[G], M. Ozgur Ozmen[G], Z. Berkay Celik, Antonio Bianchi, and Dongyan Xu, **PGPatch: Policy-Guided Logic Bug Patching for Robotic Vehicles**, In Proceedings of the IEEE Security and Privacy (S&P), pages 1-18, 2022. (Acceptance Rate: 14.5%)

[C44] Andrew Chun-An Chu[U], Arjun Arunasalam[G], M. Ozgur Ozmen[G], and Z. Berkay Celik, **Behind the Tube: Exploitative Monetization of Content on YouTube**, In Proceedings of the USENIX Security, pages 1-18, 2022. (Acceptance Rate: 17.2%)

[C43] Abdullah Imran, Habiba Farrukh[G], Muhammad Ibrahim, Z. Berkay Celik, and Antonio Bianchi, **SARA: Secure Android Remote Authorization** , In Proceedings of the USENIX Security Symposium, pages 1-18, 2022. (Acceptance Rate: 17.2%)

[C42] 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**, In Proceedings of the ACM SIGKDD Conference on Knowledge Discovery & Data Mining (KDD), pages 1027-1035, 2021. (Acceptance Rate 15.4%)

[C41] Michael Reeves[G], Dave (Jing) Tian, Antonio Bianchi, and Z. Berkay Celik, **Towards Improving Container Security by Preventing Runtime Escapes**, In Proceedings of the IEEE Secure Development Conference (SECDEV), 2021.

[C40] Khaled Serag[G], Rohit Bhatia, Vireshwar Kumar,Z. Berkay Celik, and Dongyan Xu, **Exposing New Vulnerabilities of Error Handling Mechanism in CAN**, In Proceedings of the USENIX Security Symposium, pages 4241-4258, 2021. (Acceptance Rate: 18.8%).

[C39] 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**, In

Proceedings of the USENIX Security Symposium, pages 3005-3022, 2021. (Acceptance Rate: 18.8%)

[C38] Hyungsub Kim[G], M. Ozgur Ozmen[G], Antonio Bianchi, Z. Berkay Celik, and Dongyan Xu, **PGFUZZ: Policy-Guided Fuzzing for Robotic Vehicles**, In Proceedings of the Network and Distributed System Security Symposium (NDSS), pages 1-18, 2021. (Acceptance Rate: 15.2%)

[C37] Rohit Bhatia, Vireshwar Kumar, Khaled Serag[G], Z. Berkay Celik, Mathias Payer, and Dongyan Xu, **Evading Voltage-Based Intrusion Detection on Automotive CAN**, In Proceedings of the Network and Distributed System Security Symposium (NDSS), pages 1-17, 2021. (Acceptance Rate: 15.2%)

[C36] Habiba Farrukh[G], Tinghan Yang, Yuxuan Yin, Hanwen Xu, He Wang, and Z. Berkay Celik, **S3: Side-channel Attack on Stylus Pencil Through Sensors**, In Proceedings of the ACM Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT/UbiComp), 5, 1, Article 8, pages 1-25, March, 2021.

[C35] Leonardo Babun, Z. Berkay Celik, Patrick McDaniel, and Selcuk Uluagac, **Real-time Analysis of Privacy-(un)aware IoT Applications**, In Proceedings of the Privacy Enhancing Technologies (PoPETS), no.1, pages 145-166, 2021. (Acceptance Rate: 18.6%)

[C34] 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**, In Proceedings of the ACM/IEEE Conference on Internet of Things Design and Implementation (IoTDI), pages 53-66, 2021. (Acceptance Rate: 25%)

[C33] 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**, In Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec), pages 1-12, 2020. (Acceptance rate: 28%)

[C32] Michael Norris, Z.Berkay Celik, Prasanna Venkatesh, Shulin Zhao, Gang Tan, Patrick McDaniel, and Anand Sivasubramaniam, **IoTRepair: Systematically Addressing Device Faults in Commodity IoT**, In Proceedings of the ACM/IEEE Conference on Internet of Things Design and Implementation (IoTDI), pages 142-148, 2020.

[C31] Z. Berkay Celik, Gang Tan, and Patrick McDaniel, **IoTGuard: Dynamic Enforcement of Security and Safety Policy in Commodity IoT**, In Proceedings of the Network and Distributed System Security Symposium (NDSS), pages 1-15, 2019. (Acceptance Rate: 17%)

[C30] Z. Berkay Celik, Abbas Acar, Hidayet Aksu, Ryan Sheatsley, Patrick McDaniel, and Selcuk Uluagac, **Curie: Policy-based Secure Data Exchange**, In Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY), pages 121-132, 2019. (Acceptance Rate: 23.5%)

[C29] Z. Berkay Celik, Patrick McDaniel, and Gang Tan, **Soteria: Automated IoT Safety and Security Analysis**, In Proceedings of the USENIX Annual Technical Conference (USENIX ATC), pages 147-158, 2018. (Acceptance Rate: 19%)

[C28] Z. Berkay Celik, Leonardo Babun, Amit K. Sikder, Hidayet Aksu, Gang Tan, Patrick McDaniel, and Selcuk Uluagac, **Sensitive Information Tracking in Commodity IoT**, In Proceedings of the USENIX Security Symposium, pages 1687-1704, 2018. (Acceptance Rate: 19%)

[C27] Z. Berkay Celik, Patrick McDaniel, Rauf Izmailov, Nicolas Papernot, Ryan Sheatsley, Raquel Alvarez, and Ananthram Swami, **Detection under Privileged Information**, In Proceedings of the Asia Conference on Computer and Communications Security (ASIACCS), pages 199-206, 2018. (Acceptance Rate: 20%)

[C26] Sayed Saghaian, Tom La Porta, Trent Jaeger, Z. Berkay Celik, and Patrick McDaniel, **Mission-oriented Security Model, Incorporating Security Risk, Cost and Payout**, In Proceedings of the Security

and Privacy in Communication Networks (SecureComm), pages 192-212, 2018. **(Best Paper Award)**

[C25] Z. Berkay Celik, David Lopez-Paz, and Patrick McDaniel, **Patient-Driven Privacy Control through Generalized Distillation**, In Proceedings of the IEEE Privacy-aware Computing (PAC), pages 1-12, 2017.

[C24] Nicolas Papernot, Patrick McDaniel, Ian Goodfellow, Somesh Jha, Z. Berkay Celik, and Ananthram Swami, **Practical Black-Box Attacks against Machine Learning**, In Proceedings of the Asia Conference on Computer and Communications Security (ASIACCS), pages 506-519, 2017. (Acceptance Rate: 18%)

[C23] Abbas Acar, Z. Berkay Celik, Hidayet Aksu, A. Selcuk Uluagac, and Patrick McDaniel, **Achieving Secure and Differentially Private Computations in Multiparty Settings**, In Proceedings of the IEEE Privacy-aware Computing (PAC), pages 49-59, 2017.

[C22] 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**, In Proceedings of the IEEE International Conference for Military Communications (MILCOM), pages 7-12, 2016.

[C21] Nicolas Papernot, Patrick McDaniel, Somesh Jha, Matt Fredrikson, Z. Berkay Celik and Ananthram Swami, **The Limitations of Deep Learning in Adversarial Settings**, In Proceedings of the European Symposium on Security and Privacy (Euro S&P), pages 372-387, 2016. (Acceptance Rate: 17.3%)

[C20] Z. Berkay Celik, Robert J Walls, Patrick McDaniel, and Ananthram Swami, **Malware Traffic Detection using Tamper Resistant Features**, In Proceedings of the IEEE Military Communications (MILCOM) Conference, pages 330-335, 2015.

[C19] Z. Berkay Celik and Sema Oktug, **Detection of Fast-flux Networks using Various DNS Feature Sets**, In Proceedings of the IEEE Computers and Communications Symposium (ISCC), pages 868-873, 2013.

Refereed Workshop Publications

[W18] Raymond Muller[G], Yanmao Man, and Z. Berkay Celik, Ming Li and Ryan Gerdes, **DRIVETRUTH: Automated Autonomous Driving Dataset Generation for Security Applications**, International Workshop on Automotive and Autonomous Vehicle Security (AutoSec), collocated with NDSS, 2022. **(General Motors AutoDriving Security Award)**

[W17] Abdullah Zubair Mohammed, Yanmao Man, Ryan Gerdes, Ming Li, and Z. Berkay Celik, **Physical Layer Data Manipulation Attacks on the CAN Bus**, International Workshop on Automotive and Autonomous Vehicle Security (AutoSec), collocated with NDSS, 2022.

[W16] 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.

[W15] 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), pages 235-241, 2021.

[W14] 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), pages 1-6, 2020.

[W13] Z. Berkay Celik and Patrick McDaniel, **Extending Detection with Privileged Information via Gen-**

eralized Distillation, IEEE Workshop on Deep Learning and Security (colocated with IEEE S&P), pages 83-88, 2018.

[W12] 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), pages 73-80, 2017 (Invited paper).

[W11] 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), pages 1-8, 2011.

Refereed Demos/Abstracts/Posters

[D10] Yanmao Man, Raymond Muller[G], Ming Li, Z. Berkay Celik and Ryan Gerdes, **Evaluating Perception Attacks on Prediction and Planning of AVs** (Poster), USENIX Security, 2022.

[D9] Upinder Kaur, Z. Berkay Celik, and Richard Voyles, **Robust and Energy Efficient Malware Detection for Robotic Cyber-Physical Systems**, International Conference on Cyber-Physical Systems (ICCPS), WIP Session (Abstract + Demo), 2022.

[D8] Hyungsub Kim, Muslum Ozgur Ozmen[G], Antonio Bianchi, Z. Berkay Celik and Dongyan Xu, **DEMO: Policy-based Discovery and Patching of Logic Bugs in Robotic Vehicles**, International Workshop on Automotive and Autonomous Vehicle Security (AutoSec), collocated with NDSS, 2022.

[D7] Khaled Serag[G], Vireshwar Kumar, Z. Berkay Celik, Rohit Bhatia, Mathias Payer and Dongyan Xu, **DEMO: Attacks on CAN Error Handling Mechanism**, International Workshop on Automotive and Autonomous Vehicle Security (AutoSec), collocated with NDSS, 2022.

[D6] Leonardo Babun, Z. Berkay Celik, Amit K. Sikder, Hidayet Aksu, Gang Tan, Patrick McDaniel, and A. Selcuk Uluagac, **DEMO: Sensitive Information Tracking for IoT Apps** at the Annual Research Conference at the University of Florida's Florida Institute of Cybersecurity Research (FICS), Gainesville, FL, March 1, 2018. **(Best Demo Award)**

Refereed Magazine Articles

[CL5] Z. Berkay Celik, Patrick McDaniel, Gang Tan, Selcuk Uluagac, and Leonardo Babun, **Verifying IoT Safety and Security in Physical Spaces**, IEEE Security & Privacy Magazine, Vol 17, Nr 5, pages 30-37, 2019.

[CL4] Patrick McDaniel, Nicolas Papernot and Z. Berkay Celik, **Machine Learning in Adversarial Settings**, IEEE Security & Privacy Magazine, Vol 14, Nr 3, pages 68-72, 2016.

Technical Reports

[T3] 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., pages 1-6, NAS-TR-0187-2015.

Thesis

[Th2] Z. Berkay Celik, **Automated IoT Security and Privacy Analysis**, PhD Thesis, Pennsylvania State University, August 2019.

[Th1] Z. Berkay Celik, **Salting Public Traces with Attack Traffic to Test Flow Classifiers**, Master Thesis, Pennsylvania State University, August 2011.

INVITED TALKS

National and International Meetings

- November 2022: Speaker, Rolls Royce Cyber Technology Research Network (CTRN) Conference, Developing Software Sensors for Digital Twin based Cybersecurity (virtual event)
- November 2022, Talk on Automated Autonomous Driving Dataset Generation for Security Applications at the Road to Future Automotive Research Datasets: Challenges and Opportunities (virtual workshop), invited by David Balenson at USC.
- October 2022: Speaker at Google, ASPIRE Seminar on Security of Mobile Ecosystem (virtual meeting)
- June 2022: Invited Panelist, ACM Symposium on Access Control Models and Technologies (SACMAT), Enforcing Security and Privacy Policies in Emerging Systems and Networks (virtual event), invited by Omar Chowdhury at Stony Brook.
- November 2021: Speaker, Rolls Royce Cyber Technology Research Network (CTRN) Conference, "Developing Software Sensors for Digital Twin based Cybersecurity" (virtual event)

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

Detection for Security 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 Bloomington

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

STUDENT ADVISING

Current PhD Students

◇ Habiba Farrukh, Fall 20
◇ Reham Mohamed Aburas, Fall 20
◇ M. Ozgur Ozmen, Spring 20
◇ Arjun Arunaslam, Fall 20
◇ Raymond Muller, Spring 21,
◇ Faik Kerem Ors, Fall 22

Current co-advising PhD Students

◇ Khaled Serag (co-advised with Dongyan Xu)
  – Dissertation: Securing CAN Bus Through Vulnerability Identification and Defense Construction
◇ Abdulellah Alsaheel (co-advised with Dongyan Xu)
  – Dissertation: Cyber Forensics and Cyber-physical Hardening
◇ Ruoyu Song, Spring 21 (co-advised with Antonio Bianchi)

Current Msc Students

◇ Jackson Bizjak (Fall 20 - Present)
◇ Chandrika Mukherjee (Spring 21 - Present)
◇ Chandrika Mukherjee (Spring 21 - Present)
◇ Rwitam Bandyopadhyay (Spring 21 - Present)
◇ Ben Chen (Fall 22 - present)

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

Independent Study Msc Students

◇ Gaurav Jadhav, 2022
  - Security issues in Web and Mobile Ad Ecosystem

◇ Abhishek Shah (Amazon), 2022
  - Security of AR/VR Devices

◇ Aniket Nare (Amazon), 2022
  - Scene Classification and Semantic Segmentation on 3D Point Cloud Dataset

◇ Abhinav Gupta (Facebook), 2022
  - Account Selling as a Fraud

◇ Eliz Tekcan (Vestel), 2022
  - Online Hate and Harassment in Social Platforms

◇ Yi-Shan Lin (Google), 2021
  - Evaluation of Explainable Artificial Intelligence (XAI) Interpretability

◇ Akram Ahmed Faqihr (Msc), 2021
  - Security of CAN Bus Error Handling Protocol

◇ Basavesh Shivakumar (PhD student at MPI-SP), 2020
  - Safety and Security of Event Ordering on IoT Systems

◇ Zhanfu Yang (PhD student at Stevens Institute of Technology), 2020
  - Physical Modelling of Events in IoT Systems

◇ Akhil Bandarupalli (PhD student at Purdue CS), 2020
  - Program Syntesis of IoT Applications

SUPERVISED UNDERGRADUATE RESEARCH

Current Undergraduate Students

◇ Jason Perry (Senior, CS), Modeling and Verification of Binaural Beats Tracks

◇ Varun Gannavarapu (Junior, CS), Analysis of Illicit Account Marketplaces

◇ Xueyuan Cao (Senior, CS), Secure Pairing in VR/AR Devices

Past Undergraduate Students

◇ Andrew Riordan (Senior, CS, Fall 21/Spring 22)
  - **Topic:** Side Channel Attacks on Intermittent Energy Harvesting Devices (CS Honors project)

◇ Haozhe Zhou (Senior, CS, 2020-2022)
  - **Topic:** Side-Channel Attacks on Mobile Devices
  - College of Science Alumni Summer Research Fellowship, 2021
  - PhD student at Carnegie Mellon University (Fall 22)

◇ Andrew Chun-An Chu (Senior, CS, 2019-2021),
  - **Topic:** Security and Privacy of Online Entities
  - Honorable mention for the 2021 NSF GRFP fellowship
  - PhD student at University of Chicago (Fall 21)

◇ Rouyu Song (Senior, CS, Fall 20/Summer 20),
  - **Topic:** Evasion of Anomaly detection algorithms for IoT Systems
  - PhD student under my supervision and Antonio Bianchi

◇ William Carter Bell, (Junior, Data Science, Summer 20)
  – **Topic:** Automated Evaluation of Explainable AI
◇ Anirudh Giridhar (Junior, CS, Summer 20)
  – **Topic:** System Events Generation for Realistic Cyber Experimentation on SOL4CE
◇ Sidhartha Agrawal (Sophomore, CS, Summer 20)
  – **Topic:** System Event and Network Traffic Generation for Realistic Cyber Experimentation on SOL4CE (Scalable Open Laboratory for Cyber Experimentation)
◇ Yizhen Yuan, (Junior, Purdue CS, Summer 20)
  – **Topic:** Author-Topic Modelling with Latent Dirichlet Allocation
  – PhD student at Tsinghua university
◇ Ishan Kaul, (Senior, CS, Summer 20)
  – **Topic:** Physical Event Verification in Smart Homes
◇ Yuxuan Yang (Junior, Summer'20)
  – **Topic:** Understanding the threat model of Autonomous Vehicles
◇ Rafael Zhu, (Freshman, CS, Summer 20/Fall 20)
  – **Topic:** Security of Intermittent Computing Devices
◇ Nail Tarcan Gul (Senior, CS, Fall 20)
  – **Topic:** Security of Intermittent Devices (CS Honors program project)

External Research Interns

◇ Burak Koroglu (Senior, CS, METU (Turkey), Summer'22, Online)
◇ Berk Aydogmus (Senior, CS, METU (Turkey), Summer'22, Online)
◇ Yahya Sungur (Senior, CS, METU (Turkey), Summer'22, Online)
◇ Burak Ucar (Senior, CS, METU (Turkey), Summer'22, Online)
◇ Berkin Kerim Konar (Senior, CS, METU (Turkey), Summer'22, Online)
◇ Kerem Serttas, (Senior, CS, METU (Turkey), Summer'22, Online)
◇ Furkan Goksel (Senior, CS, METU (Turkey), Summer'20, Online – GoBoiler Internship program)
◇ Kerem Ors (Msc, CS, Sabanci University (Turkey), Summer'20, Online – GoBoiler Internship program)
◇ Yigit Varli (Senior, CS, METU (Turkey), Summer'21, Voluntary, Online)
◇ Bharat Chandra (Senior, Vellore Institute of Technology (India), Summer'21, Voluntary, Online)
◇ Anirudh Gupta and Mohit Thakur (Junior, IIT Delhi (India), Summer'21, Voluntary, Online)

RESEARCH GRANTS

Funded Proposals

[1] **Title of Project: Improving the Security and Usability of the Wear OS Permission Model (Unrestricted Gift)**

Agency/Company: Google ASPIRE (Android Security and PrIvacy REsearch) Award
Total Dollar Amount: $80,850
Role: PI
Collaborators: Antonio Bianchi (co-PI)
Period of Performance: 10/26/22 -
Share: %50

[2] **Hardening PLC Programs with Physical Causal Invariants from Code & Trace Analysis**

Agency/Company: (Contract with) Cisco

Total Dollar Amount: $186,614
Role: PI
Collaborators: Dongyan Xu (co-PI)
Period of Performance: 10/01/22- 09/30/23
Share: %50

[3] **Title of Project: Deploying Cyber Emulation, Modeling, and Analysis Tools on the SOL4CE**
Agency/Company: Sandia National Laboratories
Total Dollar Amount: $75,000
Role: PI
Collaborators: Sonia Fahmy (co-PI)
Period of Performance: 5/1/22-9/30/22
Share: %50

[4] **Title of Project: CAREER: Compositional IoT Safety and Security in Physical Spaces**
Agency/Company: National Science Foundation
Total Dollar Amount: $558,375
Role: PI
Collaborators: —
Period of Performance: 7/1/22-7/1/27
Share: %100

[5] **Title of Project: Improving the Usability of Android APIs for Conformity of Standard Security Practices (Unrestricted Gift)**
Agency/Company: Google ASPIRE (Android Security and PrIvacy REsearch) Award
Total Dollar Amount: $95,000
Role: PI
Collaborators: Antonio Bianchi (co-PI)
Period of Performance: 11/4/21 -
Share: %50

[6] **Title of Project: Developing Software Sensors for Digital Twin based Cybersecurity**
Agency/Company: Rolls-Royce Cyber Technology Research Network
Total Dollar Amount: $51,000
Role: PI
Collaborators: –
Period of Performance: 11/15/21-12/15/22
Share: %100

[7] **Title of Project: Bringing Fuzzing to the Cyber-Physical World**
Agency/Company: Office of Naval Research (ONR)
Total Dollar Amount: $799,876
Role: PI
Collaborators: Antonio Bianchi, Dave Tian, and Dongyan Xu (co-PIs)
Period of Performance: 01/15/20-1/15/23
Share: %30

[8] **Title of Project: System Events and Network Traffic Generation for Realistic Cyber Experimentation**

Agency/Company: Sandia, National Security Funding (from DoE)
Total Dollar Amount: $55,000
Role: PI
Collaborators: –
Period of Performance: 4/1/20-9/3/20
Share: %100

[9] **Title of Project: Security and Privacy of Intermittent Devices in Physical Spaces**

Agency/Company: Ross-Lynn Research Scholars Grant
Total Dollar Amount: (0.50 FTE) Graduate Research Assistant
Role: PI
Collaborators: –
Period of Performance: 09/15/20-02/28/22
Share: %100

[10] **Title of Project: Undergraduate Student 4.0: A Convergent Training Program for Autonomous Connected Mobility Networks**

Agency/Company: Denso North America Foundation
Amount: $110,000
Role: Co-PI
Collaborators: Ajay Malshe (PI, Mechanical Engineering), John Sutherland (Environmental & Ecological Engineering, co-PI), Prof. Dongyan Xu (co-PI)
Period of Performance: 05/01/20-04/31/21
Share: %25

[11] **Title of Project: IoT-D: Towards Internets of Dialect-Speaking Things**

Agency/Company: Office of Naval Research (ONR)
Senior Personnel,
Amount: $6,000,000
Role: Senior Personnel
Collaborators: Dongyan Xu (PI), Xiangyu Zhang, Mathias Payer, Byoungyoung Lee (co-PIs)
Period of Performance: 01/18-01/2024

TEACHING EXPERIENCE

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

Courses Taught at Purdue University

Courses Taught at 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)

Semester	Course Number	Course Title	Enrollment	Course (5.0)	Instructor (5.0)	Response
Fall 2022	CS 529	Security Analytics (link)	54			
Spring 2022	CS 592ICS	IoT/CPS Security (link)	15	4.9	4.9	8/15
Fall 2021	CS 529	Security Analytics (link)	32	4.6	4.7	21/32
Spring 2021	CS 591-SEC	CERIAS Seminar (Online due to Covid) (link)	16	4.4	4.6	10/16
Spring 2021	CS 529	Security Analytics (Online Course Preparation)	—	—	—	—
Fall 2020	CS 529	Security Analytics (Online due to Covid) (link)	16	4.5	4.7	11/16
Spring 2020	CS 590ICS	IoT/CPS Security (link)	9	–	–	–
Fall 2019	CS 529	Security Analytics* (link)	23	4.9	4.7	10/23

* Significantly redesigned the syllabus of the CS 529 Security Analytics course to include topics on security and privacy of machine learning.

  - CMPSC 311: Introduction to Systems Programming (Fall 2016)
  - CSE 597: Wireless and Mobile Security (Fall 2017)
  - CSE 543: Computer Security (Fall 2018)

PROFESSIONAL SERVICE AND ENGAGEMENT

Professional Service

- Chair/Co-Chair
  - ◇ 2023, Program Co-chair, Symposium on Vehicle Security and Privacy (VehicleSec 2023) (co-located with NDSS)
  - ◇ 2022, Automotive/Autonomous Vehicle Security (AutoSec) Workshop (co-located with NDSS)
  - ◇ 2022, Workshop Co-chair, IEEE Conference on Communications and Network Security (CNS)
  - ◇ 2018, SecureComm Conference (Web Security Session Chair)
- Technical Program Committee
  - ◇ 2023, Security and Privacy in Wireless and Mobile Networks (WiSec)
  - ◇ 2023, 2022, NDSS
  - ◇ 2023, IEEE Symposium on Security and Privacy
  - ◇ 2023, 2022, 2021, USENIX Security
  - ◇ 2023, Secure and Trustworthy Machine Learning (SATML)
  - ◇ 2022, 2019, Workshop on the Internet of Things Security and Privacy (colocated with CCS)
  - ◇ 2022, IEEE SmartGridComm (Security and Privacy track)
  - ◇ 2022, IEEE Secure Development Conference (SecDev)
  - ◇ 2022, Workshop on Internet of Safe Things (co-located with IEEE S&P)
  - ◇ 2021, CCS (Hardware, Side Channels, and Cyber-Physical Systems Track)
  - ◇ 2021, ACSAC
  - ◇ 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)

- Journal and External Reviewer
  - ◇ 2022, 2019, IEEE Transactions on Mobile Computing
  - ◇ 2022, 2018, 2017, ACM Computing Surveys (CSUR)
  - ◇ 2022, INFOCOM (External Reviewer on Fuzzing and Explainable AI)
  - ◇ 2022, IEEE Transactions on Software Engineering
  - ◇ 2020, 2019, IEEE Transactions on Dependable and Secure Computing
  - ◇ 2019, IEEE Security & Privacy Magazine
  - ◇ 2019, ACM Transactions on Internet of Things
  - ◇ 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, Conference on Decision and Game Theory for Security (GameSec)
  - ◇ 2018, Neural Information Processing Systems (NIPS)
  - ◇ 2017, IEEE Security and Privacy Magazine
  - ◇ 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
  - ◇ 2022, 2020, SaTC Town Hall (Attendee)
  - ◇ 2020, participated the Faculty Success Program by National Center for Faculty Development & Diversity, May 17-August 8 (online), supported by Purdue Faculty Affairs
  - ◇ 2020, NSF Experimental Program to Stimulate Competitive Research (EPSCoR) (Ex. 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)

Engagement

- University-Level Engagement
  - ◇ 2022, ManTech (CERIAS corporate partners) campus visit, talk on Secure Autonomy
  - ◇ 2022 CERIAS Balkan Fellowship, mentoring a senior security professional from the Balkans
  - ◇ 2021, Cerias Security Symposium Panelist, Topic: "Aero-Cyber: The challenges of resource-constrained embedded systems"
  - ◇ April 2022: Eli Lilly, Security of Industrial Control Systems (hosted by CERIAS)

- ◇ October 2020: Saab Autonomy Workshop, IoT/CPS Safety and Security
- ◇ September 2020: CERIAS External Advisory Board Meeting presentation, System Events and Network Traffic Generation in Sandia SOL4CE
- ◇ March 2020: General Motors, Intentional Electromagnetic Attacks and Defenses against Sensors/Actuators
- ◇ October 2019: Tsukuba University visitors, talk on IoT and Machine Learning Security
- ◇ October 2019: Air Force Research Laboratory visitors, IoT/CPS 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

- College-Level and Departmental Engagement
  - ◇ 2022, Women in Science Program (WISP) at Purdue, Invited talk to educate on basic principles of internet of things security, and make members understand the importance of cybersecurity and how to implement strategies to keep their technology safe
  - ◇ 2022, Primary Advisor of Computer Science Graduate Student Board (GSB)
  - ◇ 2022, Grad Day Visit (virtual) organizer
  - ◇ 2021, Speaker for professional writing Workshop series for Purdue undergrads - writing a research statement for grad school (with Ellie Broughton, Undergraduate Programs Specialist)
  - ◇ 2021, Co-adviser of Computer Science Graduate Student Board (GSB)
  - ◇ 2019 (Fall), Started the Systems Security Reading Group (weekly meetings), attendance: ∼20 graduate/undergraduate students and faculty members (with Dongyan Xu, Antonio Bianchi, and Dave Tian)
  - ◇ Co-founder of `PurSec Research Group` (with Dongyan Xu, Antonio Bianchi, and Dave Tian)
  - ◇ 2020, GoBoiler Internships (2 students)
  - ◇ **Departmental Committees**
    - ∗ 2022, ISCP Admissions Committee Summer/Fall, Member
    - ∗ 2019, 2020: Departmental PhD Admission Committee, Member
- 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.

Research Coverage

- ◇ Celik earns NSF CAREER award, `Purdue CS news`, February 2021.
- ◇ Three professors receive funding with the Rolls-Royce Cybersecurity Technology Research Network, `Purdue CS news`, December 2020.
- ◇ Bianchi and Celik win 2021 Google ASPIRE Award, `Purdue CS news`, November 2021.
- ◇ Undergraduate Research at Purdue CS, Student Stories, Volunteering for research leads to first paper `Purdue CS news`, September 2021.
- ◇ 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.