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: July 17, 2023

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

Department of 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

- 2023, Elevated to the grade of IEEE Senior member.
- 2023, Graduate advisee Raymond Muller received the Graduate Teaching award from Purdue Computer Science Department.
- 2023, Graduate advisee Raymond Muller is awarded an X-Force Fellowship through the National Security Innovation Network to solve national security problems in collaboration with the U.S. military.
- 2023, Qualcomm Best Demo Runner-up Award for the Demo "Physically Hijacking Object Trackers" at Vehicle Security and Privacy (VehicleSec) Symposium collocated with NDSS.
- 2022, Graduate co-advise Khaled Serag received Emil Stefanov Fellowship Award.
- 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, Undergraduate advisee Haozhe Zhou (now Ph.D. at CMU) received the College of Science Alumni Summer Research Fellowship.
- 2021, Graduate advisee Habiba Farrukh received Bilsland Dissertation Fellowship Award.
- 2021, Undergraduate advisee Andrew Chu (now Ph.D. at University of Chicago) 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. Software Tools and Datasets are available at `PurSec GitHub Repository`.

Refereed Journal Articles

[J63] 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.

[J62] 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.

[J61] 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.

[J60] 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.

[J59] 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

[C58] **[USENIX Security'23]** Ruoyu Song[G], M. Ozgur Ozmen[G], Hyungsub Kim[G], Raymond Muller[G], Z. Berkay Celik, and Antonio Bianchi, **Discovering Adversarial Driving Maneuvers against Autonomous Vehicles**. In Proceedings of the USENIX Security Symposium, 2023. (Acceptance Rate: TBD%)

[C57] **[USENIX Security'23]** Habiba Farrukh[G], Reham Mohamed[G], Aniket Nare[G], Antonio Bianchi, and Z. Berkay Celik, **LocIn: Inferring Semantic Location from Spatial Maps in Mixed Reality**. In Proceedings of the USENIX Security Symposium, 2023. (Acceptance Rate: TBD%)

[C56] **[USENIX Security'23]** Khaled Serag[G], Rohit Bhatia, Akram Faqih, Muslum Ozgur Ozmen[G], Vireshwar Kumar, Z. Berkay Celik, and Dongyan Xu, **ZBCAN: A Zero-Byte CAN Defense System**. In Proceedings of the USENIX Security, pages 1-18, 2023. (Acceptance Rate: TBD%)

[C55] **[USENIX Security'23]** 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%)

[C54] **[USENIX Security'23]** 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. (Acceptance Rate: TBD%)

[C53] **[PETS'23]** 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: 25%)

[C52] **[IEEE S&P'23]** Habiba Farrukh[G], M. Ozgur Ozmen[G], Faik Kerem Ors[G], and Z. Berkay Celik, **One Key to Rule Them All: Secure Group Pairing for Heterogeneous IoT Devices**. In Proceedings of the IEEE Security and Privacy (S&P), pages 1693-1709, 2023. (Acceptance Rate: TBD%)

[C51] **[NDSS'23]** M. Ozgur Ozmen[G], Ruoyu Song[G], Habiba Farrukh[G] and Z. Berkay Celik, **Evasion Attacks and Defenses on Smart Home Physical Event Verification**. In Proceedings of the Network and Distributed System Security Symposium (NDSS), pages 1-18, 2023. (Acceptance Rate: 16.2%)

[C50] **[CCS'22]** M. Ozgur Ozmen[G], Xuansong Li, Andrew 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%)

[C49] **[CCS'22]** 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%)

[C48] **[IEEE S&P'22]** 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%)

[C47] **[USENIX Security'22]** Andrew 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%)

[C46] **[USENIX Security'22]** 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%)

[C45] **[USENIX Security'22]** 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%).

[C44] **[KDD'22]** 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%)

[C43] **[SecDev'22]** 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.

[C42] **[USENIX Security'21]** 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%)

[C41] **[NDSS'21]** 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%)

[C40] **[NDSS'21]** 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%)

[C39] **[IMWUT/UbiComp'21]** 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.

[C38] **[PETS'21]** 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%)

[C37] **[IoTDI'21]** 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%)

[C36] **[WiSec'21]** 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%)

[C35] **[IoTDI'20]** 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.

[C34] **[NDSS'19]** 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%)

[C33] **[CODASPY'19]** 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%)

[C32] **[USENIX ATC'18]** 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%)

[C31] **[USENIX Security'18]** 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%)

[C30] **[ASIACCS'18]** 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%)

[C29] **[SecureComm'18]** 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)**

[C28] **[IEEE PAC'17]** 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.

[C27] **[IEEE PAC'17]** 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.

[C26] **[ASIACCS'17]** 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%)

[C25] **[MILCOM'17]** 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.

[C24] **[Euro S&P'17]** 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%)

[C23] **[MILCOM'15]** 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.

[C22] **[ISCC'13]** 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

[W21] **[VehicleSec'23]** Muslum Ozgur Ozmen[G], Habiba Farrukh[G], Hyungsub Kim, Antonio Bianchi, Z. Berkay Celik, **Short: Rethinking Secure Pairing in Drone Swarms (Position Paper)**. In Proceedings of the Vehicle Security and Privacy (VehicleSec) Symposium, 2023 (collocated with NDSS).

[W20] **[VehicleSec'23]** Raymond Muller[G], Yanmao Man, and Z. Berkay Celik, Ming Li and Ryan Gerdes, **DRIVETRUTH: Automated Autonomous Driving Dataset Generation for Security Applications**. In Proceedings of the International Workshop on Automotive and Autonomous Vehicle Security (AutoSec), 2022 (collocated with NDSS). **(General Motors AutoDriving Security Award)**

[W19] **[AutoSec'22]** Abdullah Zubair Mohammed, Yanmao Man, Ryan Gerdes, Ming Li, and Z. Berkay Celik, **Physical Layer Data Manipulation Attacks on the CAN Bus**. In Proceedings of the International Workshop on Automotive and Autonomous Vehicle Security (AutoSec), 2022 (collocated with NDSS).

[W18] **[FL-ICML'21]** 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**. In Proceedings of the International Workshop on Federated Learning for User Privacy and Data Confidentiality (FL-ICML) 2021 (colocated with ICML).

[W17] **[SafeThings'22]** 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**, In Proceedings of the IEEE S&P SafeThings Workshop pages 235-241, 2021 (colocated with IEEE S&P).

[W16] **[CPS-Sec'20]** Paul Berges, B. Shivakumar[G], Timothy Graziano, Ryan Gerdes, and Z. Berkay Celik, **On the Feasibility of Exploiting Traffic Collision Avoidance System Vulnerabilities**. In Proceedings of the IEEE Workshop on Cyber-Physical Systems Security (CPS-Sec) pages 1-6, 2020 (colocated with IEEE CNS).

[W15] **[DLSP'18]** Z. Berkay Celik and Patrick McDaniel, **Extending Detection with Privileged Information via Generalized Distillation**. In Proceedings of the IEEE Workshop on Deep Learning and Security, pages 83-88, 2018 (colocated with IEEE S&P).

[W14] **[IWSPA'17]** Z. Berkay Celik, Patrick McDaniel, and Rauf Izmailov, **Feature Cultivation in Privi-**

leged Information augmented Detection. In Proceedings of the Security And Privacy Analytics Workshop (IWSPA), pages 73-80, 2017 (colocated with CODASPY), Invited Paper.

[W13] **[CSET'11]** Z. Berkay Celik, Jayaram Raghuram, George Kesidis, and David J. Miller, **Salting Public Traces with Attack Traffic to Test Flow Classifiers**. In Proceedings of the Workshop on Cyber Security and Experimentation (CSET), pages 1-8, 2011 (colocated with USENIX Security).

Refereed Demos/Abstracts/Posters

[D12] **[VehicleSec'23]** Raymond Muller[G], Yanmao Man, Z. Berkay Celik, Ryan Gerdes, and Ming Li, **Demo: Physically Hijacking Object Trackers**, Vehicle Security and Privacy (VehicleSec) Symposium, 2023 (collocated with NDSS). **(Qualcomm Best Demo Runner-up Award)**

[D11] **[VehicleSec'23]** Hyungsub Kim, Muslum Ozgur Ozmen[G], Antonio Bianchi, Z. Berkay Celik and Dongyan Xu, **DEMO: Discovering Faulty Patches in Robotic Vehicle Control Software**, Vehicle Security and Privacy (VehicleSec) Symposium, 2023 (collocated with NDSS).

[D10] **[USENIX Security'22]** 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] **[ICCPS'22]** 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] **[AutoSec'22]** 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] **[AutoSec'22]** 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] **[FICS'18]** 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

- Current Landscape of IoT Security Research: A Path to Secure Autonomy
  Invited Speaker at Sp4rkCon (April 2023)
- Physical Hijacking Attacks against Object Trackers
  Qualcomm (Computer Vision Group), with Raymond Muller (January 2023)
- Industrial Control System Modeling with SCEPTRE Framework
  Sandia National Laboratories (January 2023)
- Software Sensors to Mitigate Physical Threats in IoT Environments
  Rolls Royce Cyber Technology Research Network Conference (November 2022)
- Automated Autonomous Driving Dataset Generation for Security Applications
  Road to Future Automotive Research Datasets: Challenges and Opportunities, with Raymond Muller (November 2022)
- Security of Mobile and Wearable Devices
  Google ASPIRE Seminar (October 2022)
- Enforcing Security and Privacy Policies in Emerging Systems and Networks
  Invited Panelist, ACM Symposium on Access Control Models and Technologies (June 2022)
- Developing Software Sensors for Digital Twin based Cybersecurity
  Rolls Royce Cyber Technology Research Network Conference (November 2021)

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
- Hongyu Cai, Fall 23

Current co-advising PhD Students

- Hyungsub Kim (co-advised with Dongyan Xu and Antonio Bianchi)
  - Dissertation: Defeating Logic Bugs in Robotic Vehicles
- Khaled Serag (co-advised with Dongyan Xu)
  - Dissertation: Proactive Vulnerability Identification and Defense Construction – The Case for CAN

  - Emil Stefanov Fellowship, 2022
- 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

- Ananth Shreekumar (Summer 2023 - Present)
- Jyun-Jhu Syu (Summer 2023 - Present)
- Chandrika Mukherjee (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

- Yufan Chen, 2023
  - Exploration of Security and Privacy Concerns in Large Language Models
- Rwitam Bandyopadhyay (Amazon), 2023
  - Auto-Tuning PID Controllers in Robotic Vehicles
- 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 Synthesis of IoT Applications

Current Undergraduate Students

- Varun Gannavarapu (Junior, CS), Analysis of Illicit Account Marketplaces
- Xueyuan Cao (Senior, CS), Secure Pairing in VR/AR Devices

Past Undergraduate Students

- Jason Perry (Senior, CS)
  - **Topic:** Modeling and Verification of Binaural Beats Tracks
  - Software Engineer at Google Youtube Music Team
- 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

- Blaise Swartwood (Junior, CS), Rose-Hulman Institute of Technology, Summer'23
- Burak Koroglu (Senior, CS, METU (Turkey), Summer'22, Online)
- 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, Online)
- Bharat Chandra (Senior, Vellore Institute of Technology (India), Summer'21, Online)
- Anirudh Gupta and Mohit Thakur (Junior, IIT Delhi (India), Summer'21, Online)

RESEARCH GRANTS

Funded Proposals

[1] **Institute for Artificial Cyber Threat Intelligence and OperatioN (ACTION)**

Agency/Company: National Science Foundation
Amount: $20M, $3M (Purdue's share)
PI: Giovanni Vigna. Purdue Team: Dongyan Xu (Co-PI), Ninghui Li, Elisa Bertino, Ming Yin, Yung-Hsiang Lu
Period of Performance: 6/1/2023 - 5/31/2028

[2] **Enabling Secure and Resilient XFC: A Software/Hardware-Security Co-Design Approach**

Agency/Company: Department of Energy (DOE) Subaward
Amount: $80K + $20K cost share
Role: Co-PI with Antonio Bianchi
Period of Performance: TBD

[3] **National Center for Transportation Cyber Security and Resiliency (TraCR), University Transportation Centers Programs**

Agency/Company: Department of Transportation (USDOT)
Total: $20 Million, Purdue's Share: TBD
Lead: Clemson University. Purdue Team: Satish Ukkusuri (Civil Eng.), Yiheng Feng (Civil Eng.), Dongyan Xu, and Aniket Kate
Period of Performance: TBD

[4] **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)
Date Awarded: 11/4/21
Share: %50

[5] **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

[6] **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

[7] **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

[8] **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)
Date Awarded: 11/4/2021
Share: %50

[9] **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

[10] **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

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

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

[12] **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

[13] **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

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

Agency/Company: Office of Naval Research (ONR)
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

Table 1 summarizes the courses I thought at Purdue University from 2019 to 2023.

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)

Table 1: Courses Taught at Purdue University

Semester	Course Number	Course Title	Enrollment	Course (5.0)	Instructor (5.0)	Response
Spring 2023	CS 426	Computer Security (link)	69	4.0	4.5	33/69
Fall 2022	CS 529	Security Analytics (link)	54	4.5	4.6	38/54
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 (1 credit hours) (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 the security and privacy of machine learning.

- **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)

PROFESSIONAL SERVICE

Journal Editorial Positions

- 2023-Present, Associate Editor, IEEE Transactions on Information Forensics and Security (T-IFS)

Conference/Workshop Organization

- **Program Co-chair:** Symposium on Vehicle Security and Privacy (VehicleSec), 2023
- **Program Co-chair:** IEEE/ACM Workshop on the Internet of Safe Things, 2023
- **Workshop Co-chair:** IEEE Conference on Communications and Network Security (CNS), 2022
- **Program Co-chair:**, Automotive/Autonomous Vehicle Security (AutoSec) Workshop, 2022
- **Session Chair of Web Security:** SecureComm, 2018

Technical Program Committee

- **USENIX Security:** 2024, 2023, 2022, 2021
- **IEEE Symposium on Security and Privacy:** 2024, 2023
- **NDSS:** 2024, 2023, 2022
- **CCS (Hardware, Side Channels, and CPS – ML and Security Tracks)**: 2023, 2021
- **IEEE Secure Development Conference (SecDev):** 2023, 2022
- **ACM Security and Privacy in Wireless and Mobile Networks (WiSec)**: 2023
- **Secure and Trustworthy Machine Learning (SATML):** 2023
- **CCS Workshop on the Internet of Things Security and Privacy:** 2022, 2019, 2017
- **SmartGridComm (Security and Privacy track):** 2022
- **Workshop on the Internet of Safe Things:** 2022, 2021
- **ACSAC:** 2021
- **European Symposium on Research in Computer Security (ESORICS):** 2021, 2020
- **SecureComm:** 2020
- **Workshop on Trustworthy ML (co-located with ICLR):** 2020
- **Uncertainty in Artificial Intelligence (UAI)**: 2020, 2019

- **IEEE Computer Security Foundations Symposium (CSF):** 2020
- **MILCOM:** 2019, 2016
- **Workshop on ML for Security and Cryptography (co-located with IEEE PIMRC):** 2019
- **ASIACCS:** 2019
- **NIPS Workshop on Security in Machine Learning:** 2018
- **CCS Poster/Demonstration Session:** 2018
- **Privacy-Aware Computing Symposium (IEEE PAC):** 2018
- **IEEE CNS Cyber-Physical Systems Security Workshop (CPS-Sec):** 2017

Journal and External Reviewer

- **ACM Computing Surveys (CSUR):** 2023, 2022, 2018, 2017
- **IEEE Communications Magazine:** 2023
- **IEEE Transactions on Information Forensics & Security (TIFS)** 2023, 2017
- **IEEE Transactions on Mobile Computing:** 2022, 2019
- **INFOCOM (External Reviewer on Fuzzing and Explainable AI):** 2022
- **IEEE Transactions on Software Engineering:** 2022
- **IEEE Transactions on Dependable and Secure Computing:** 2020, 2019
- **IEEE Security & Privacy Magazine:** 2019
- **ACM Transactions on Internet of Things:** 2019
- **IEEE Transactions on Neural Networks and Learning Systems:** 2019
- **USENIX Security Symposium:** 2019, 2018
- **IEEE S&P:** 2019, 2018, 2017
- **CCS:** 2018
- **Decision and Game Theory for Security (GameSec):** 2018
- **NeurIPS:** 2018
- **IEEE Security and Privacy Magazine:** 2017
- **Neural Processing Letters:** 2017
- **Computers Open Access Journal:** 2016
- **Journal of Network and Computer Applications (JNCA):** 2016

Other Services and Activities

- Invited participants for the Quad Countries (Australia, India, Japan, USA) event organized by NSF and National Security Council (The White House), 2023
- NSF Review Panel, 2023 and 2019
- NSF SaTC Town Hall (Attendee), 2022 and 2020
- Faculty Success Program participant by National Center for Faculty Development & Diversity, (May 17-August 8, supported by Purdue Faculty Affairs), 2020
- NSF Experimental Program to Stimulate Competitive Research (External Reviewer), 2020
- Computing Research Association, Career Mentoring Workshop (Selected Attendee), 2020
- NSF CISE CAREER Workshop (Selected Attendee), 2020

ENGAGEMENT, DIVERSITY, AND OUTREACH

University-Level Engagement

Presentations were given during company/organization visits to Purdue University.

- Attack Modeling and Attack Investigation
  Lockheed Martin, 2023
- Semantic Bug Discovery and Patching on Robotic Vehicle Control Programs
  ONR/Naval Surface Warfare Center - Crane Division visit for UAS Research and Test Facility, 2023
- Secure Autonomy and Cyber Security Experimentation and Test
  Chris Rawlings, cybersecurity division group leader at Los Alamos National Laboratory, 2023
- Sol4CE and Emulytics Laboratory Directed Research & Development
  Sandia National Laboratories (Jennifer Gaudioso, Director of Computation and Analysis for National Security), 2022
- Deploying Cyber Emulation, Modeling, and Analysis Tools on the SOL4CE
  Sandia National Laboratories and Naval Surface Warfare Center - Crane Division (Reno L. Sanchez, Director of RF & Electronic Systems Center), 2022.
- Secure Autonomous Systems
  ManTech, 2022
- The challenges of resource-constrained embedded systems
  CERIAS Security Symposium Panelist, 2021
- Security of Industrial Control Systems
  Eli Lily, 2022
- IoT/CPS Safety and Security
  Saab Autonomy Workshop, 2020
- System Events and Network Traffic Generation in SOL4CE
  CERIAS External Advisory Board Meeting, 2020
- Intentional Electromagnetic Attacks and Defenses against Sensors/Actuators
  General Motors, 2020
- IoT and Machine Learning Security
  Tsukuba University, 2019
- Cyber-Physical Systems Security
  Air Force Research Laboratory, 2019
- IoT and Machine Learning Security
  Naval Surface Warfare Center-Crane Division
- Verification of IoT Software for Safety and Security
  Boeing Company, 2019

College-Level and Departmental Engagement

- Presenter for online MS in Information and Cybersecurity (ISCY) webinar, 2023
- Prospective PhD visit day organizer, 2023, 2022
- Primary Advisor of Computer Science Graduate Student Board (GSB), 2023, 2022
- Co-adviser of Computer Science Graduate Student Board (GSB), 2021
- Started the Systems Security reading group (weekly meetings), attendance: $\sim$20 graduate/undergraduate students (with Dongyan Xu, Antonio Bianchi, and Dave Tian), 2019 Fall
- Co-founder of `PurSec Laboratory` (with Dongyan Xu, Antonio Bianchi, and Dave Tian), 2020

- **Departmental Committees**
  - Admission Committee, Interdisciplinary Graduate Program in Information Security, 2023
  - Admission Committee, Professional MS Program, Information and Cyber Security, 2023
  - Admission Committee, Information Security for Computing Professionals, 2022
  - PhD Admission Committee, 2020, 2019

Community Outreach and Diversity Activities

- Advisor for `Summer Research Opportunity Program (SROP)`, Purdue Office of Graduate Diversity Initiatives, 2023
- Invited talk on basic principles of IoT security at `Women in Science Program (WISP)` to educate and make members understand the importance of cybersecurity and how to implement strategies to keep their technology safe, 2022
- CERIAS Balkan Fellowship, mentoring a senior security professional from the Balkans, 2022.
- Speaker for professional writing workshop series for Purdue undergrads' writing a research statement for grad school (with Ellie Broughton, Undergraduate Programs Specialist), 2021
- Advised 2 students through `GoBoiler Internships program`, 2020

Research Dissemination

- Code and data release of papers available at `PurSec Lab Git Repository`
- Co-authored and maintain the `IoTBench` open-source test-suite for IoT apps
  - The repository has 60+ 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 600+ stars and 500+ forks on GitHub.

Research Coverage

- Purdue CS graduate student Raymond Muller secures X-Force Fellowship, `Purdue news` June 2023 and `Purdue Today` July 2023.
- NSF funds institute to research AI-powered cybersecurity, `Purdue news`, May 2023.
- Antonio Bianchi, Z. Berkay Celik, and their research group in the PurSecLab have won the 2022 Android Security and PrIvacy REsearch (ASPIRE) Award, `Purdue CS news`, January 2023.
- Supercharged research boosts cybersecurity, `Virginia Tech Engineering` Stories, December, 2022.
- 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.