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 7, 2024

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*)

RESEARCH INTEREST

I am a systems security researcher. My research investigates the design and evaluation of security for software and systems, particularly on emerging computing platforms and the complex physical environments in which they operate. To achieve my research goal, I tie theoretical and practical questions to new algorithmic methods on a variety of computing platforms. These security-driven scientific questions present challenging problems that include representing the behavior of multiple interacting system components, synthesizing distinct physical processes into code analysis, identifying their complex security and privacy policies, and formally reasoning about a system's compositional security.

In my group, we address these challenges by architecting and prototyping system platforms that leverage ideas at the confluence of program analysis, hybrid modeling, formal methods, and machine learning. My research is exemplified by my extensive work in the security and privacy of Internet of Things (IoT)/Cyber-Physical Systems (CPS), including robotic vehicles, automobiles, self-driving cars, industrial control systems, and mobile systems, such as smartphones, wearables (e.g., smartwatches, AR/VR headsets).

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 Simons — 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

- 2024, Acorn Awardee of Purdue Research x 2, in recognition of accomplishment in obtaining an external sponsored award exceeding $1 million.
- 2024, Selected the most influential Professor by the Purdue CS Graduate Student Board (GSB).
- 2024, Received College of Science Faculty Leadership Award.
- 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 the Purdue CS Graduate Student Board (GSB).

External to Purdue

- 2024, Distinguished Paper award at ACM Conference on Computer and Communications Security (CCS)
- 2024, Outstanding Editorial Board Member award for IEEE Transactions on Information Forensics and Security (TIFS)
- 2024, Amazon Research award (AI for Information Security)
- 2023, Google ASPIRE award
- 2023, Elevated to the grade of IEEE Senior member
- 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, Google ASPIRE award
- 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 award
- 2018, Best paper award at the 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 the 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

Awards and Honors of My Students

- 2024, Graduate advisee Muslum Ozgur Ozmen received the CERIAS Diamond Award for his outstanding acadamic achievement.
- 2024, Graduate advisee Raymond Muller selected for CPS Rising Stars.
- 2024, Graduate advisee Raymond Muller received the Emil Stefanov Fellowship Award.
- 2023-Fall, Graduate advisees Ruoyu Song and Arjun Arunasalam received the Graduate Teaching award from Purdue Computer Science Department.
- 2023, Graduate advisee Muslum Ozgur Ozmen is invited as a panelist to NSA's Center of Academic Excellence in Cybersecurity Research Symposium to present his dissertation research on IoT/CPS security to practitioners and government agencies for real-world adoption
- 2023-Spring, Graduate advisee Raymond Muller received the Graduate Teaching award from the 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
- 2022, Graduate co-advise Hyungsub Kim selected for CPS Rising Stars.
- 2022, Graduate co-advise Khaled Serag received Emil Stefanov Fellowship Award.
- 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 the 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)

PUBLICATIONS

My undergraduate (^{U}) and graduate (^{G}) advisees and co-advisees are shown with dashed underline.

26 papers (2 Pre-Purdue Hire and 24 Post-Purdue Hire) are published at the top-4 Security conferences (USENIX Security, IEEE S&P, CCS, and NDSS), as shown in the Table below. The acceptance rate is 10-25% in these conferences. Software tools and datasets are available at `PurSec GitHub Repository`.

Total Citations: 12, 878, H-Index: 24, i10-Index: 46 (Google Scholar, as of December 2024)

Year	Publication Summary											
	Security	**S&P**	**CCS**	**NDSS**	**PETS**	**IROS**	**KDD**	**UBICOMP**	**ATC**	**ACSAC**	**Euro S&P**	**AsiaCCS**
2024	4	2	1	1	1	2				1		
2023	5	1		1	1					1		
2022	2	1	2									
2021	2			2	1		1	1				
Total	**13**	**4**	**3**	**4**	**3**	**2**	**1**	**1**	–	**2**	–	–
Pre Purdue	1			1					1		1	2
	Total Number of Top-4 Security Papers: 26 (2 Pre-Purdue and 24 Post-Purdue)											

Pre-prints

[P85] Claire Le Goues, Sebastian Elbaum, David Anthony, Z. Berkay Celik, Mauricio Castillo-Effen, Nikolaus Correll, Pooyan Jamshidi, Morgan Quigley, Trenton Tabor, Qi Zhu, **Software Engineering for**

Robotics: Future Research Directions; Report from the 2023 Workshop on Software Engineering for Robotics, arXiv:2401.12317, pages 1-16, 2024.

Refereed Journal Articles

[J84] 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.

[J83] 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.

[J82] 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.

[J81] 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.

[J80] Z. Berkay Celik, Patrick McDaniel, and Thomas Bowen, **Malware Modeling and Experimentation through Parameterized Behavior**. Defense Modeling and Simulation, Vol 15(1), pages 1-18, 2018.

Refereed Conference Proceedings

[C79] **[NDSS'25]** Derin Cayir, Reham Mohamed Aburas[G], Riccardo Lazzeretti, Marco Angelini, Abbas Acar, Mauro Conti, Z. Berkay Celik, and Selcuk Uluagac, **Speak Up, I'm Listening: Extracting Speech from Zero-Permission VR Sensors**. In Proceedings of the Network and Distributed System Security (NDSS) Symposium, pages 1-17, 2025.

[C78] **[NDSS'25]** Zeyu Lei, Güliz Seray Tuncay, Beatrice Carissa Williem, Z. Berkay Celik, and Antonio Bianchi, **ScopeVerif: Analyzing the Security of Android's Scoped Storage via Differential Analysis**. In Proceedings of the Network and Distributed System Security (NDSS) Symposium, pages 1-17, 2025.

[C77] **[SANER'25]** Hanxiao Lu[G], Hongyu Cai[G], Yiming Liang[G], Antonio Bianchi, and Z. Berkay Celik, **A Progressive Transformer for Unifying Binary Code Embedding and Knowledge Transfer**, In Proceedings of the IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), pages 1-10, 2025. (Acceptance Rate: 23.11%)

[C76] **[ICWSM'25]** Arjun Arunasalam, Jason Tong, Habiba Farrukh, Muslum Ozgur Ozmen, Koustuv Saha, and Z. Berkay Celik, **Deceptive Sound Therapy on Online Platforms: Do Mental Wellbeing Tracks Conform to User Expectations?**. In Proceedings of the International AAAI Conference on Web and Social Media (ICWSM), pages 1-10, 2025.

[C75] **[PETS'25]** M. Ozgur Ozmen[G], M. Oguz Sakaoglu[G], Jackson Bizjak[G], Jianliang Wu, Antonio Bianchi, Dave (Jing) Tian, and Z. Berkay Celik, **Why Am I Seeing Double? An Investigation of Device Management Flaws in Voice Assistant Platforms** In Proceedings of the Privacy Enhancing Technologies (PoPETS), pages 1-15, 2025.

[C74] **[CSCW'24]** Arjun Arunasalam[G], Jason Tong[U], Habiba Farrukh[G], Muslum Ozgur Ozmen[G], Koustuv Saha, and Z. Berkay Celik, **Expectation Conformance in Online Sound Therapy: Designing Tools for Users of Mental Wellbeing Applications**. In Companion Publication of Conference on Computer-Supported

Cooperative Work and Social Computing (CSCW), pages 1-6, 2024.

[C73] **[CCS'24]** Zhaozhou Tang, Khaled Serag[G], Z. Berkay Celik, Saman Zonouz, Dongyan Xu, and Raheem Beyah, **ERACAN: Defending Against an Emerging CAN Threat Model**. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), pages 1-15, 2024. **(Distinguished Paper Award)**

[C72] **[ACSAC'24]** Chenyi Wang, Yanmao Man, Raymond Muller[G], Ming Li, Z. Berkay Celik, Ryan Gerdes, and Jonathan Petit **Physical ID-Transfer Attacks against Multi-Object Tracking via Adversarial Trajectory** Annual Computer Security Applications Conference (ACSAC), pages 1-17, 2024. (Acceptance Rate: 19.7%)

[C71] **[IROS'24]** Upinder Kaur, Z. Berkay Celik, and Richard Voyles, **RoboCop: A Robust Zero-Day Cyber-Physical Attack Detection Framework for Robots**. In Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), pages 1-6, 2024.

[C70] **[IROS'24]** Upinder Kaur, Z. Berkay Celik, and Richard Voyles, **RoboGuardZ: A Scalable Zero-Shot Framework for Detecting Zero-Day Malware in Robots**. In Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), pages 1-6, 2024.

[C69] **[USENIX Security'24]** Syed Ghazanfar Abbas[G], Muslum Ozgur Ozmen[G], Abdulellah Alsaheel[G], Arslan Khan, Z. Berkay Celik, and Dongyan Xu, **SAIN: Improving ICS Attack Detection Sensitivity via State-Aware Invariants**. In Proceedings of the USENIX Security Symposium, pages 1-18, 2024. (Acceptance Rate: 18.3%)

[C68] **[USENIX Security'24]** Raymond Muller[G], Yanmao Man, Ming Li, Ryan Gerdes, Jonathan Petit, and Z. Berkay Celik, **VOGUES: Validation of Object Guise using Estimated Components**. In Proceedings of the USENIX Security Symposium, pages 1-18, 2024. (Acceptance Rate: 18.3%)

[C67] **[USENIX Security'24]** Reham Mohamed[G], Arjun Arunasalam[G], Habiba Farrukh[G], Jason Tong[U], Antonio Bianchi, and Z. Berkay Celik, **ATTention Please! An Investigation of the App Tracking Transparency Permission**. In Proceedings of the USENIX Security Symposium, pages 1-18, 2024. (Acceptance Rate: 18.3%)

[C66] **[USENIX Security'24]** Arjun Arunasalam[G], Habiba Farrukh[G], Eliz Tekcan[G], and Z. Berkay Celik, **Understanding the Security and Privacy Implications of Online Toxic Content on Refugees**, In Proceedings of the USENIX Security Symposium, pages 1-18, 2024 (Acceptance Rate: 18.3%)

[C65] **[PETS'24]** Muslum Ozgur Ozmen[G], Habiba Farrukh[G], and Z. Berkay Celik, **Physical Side-Channel Attacks against Intermittent Devices**. In Proceedings of the Privacy Enhancing Technologies (PoPETS), pages 1-18, 2024. (Acceptance Rate: 19.5%)

[C64] **[IEEE S&P'24]** Hyungsub Kim[G], Rwitam Bandyopadhyay[G], M. Ozgur Ozmen[G], Z. Berkay Celik, Antonio Bianchi, Yongdae Kim, and Dongyan Xu **A Systematic Study of Physical Sensor Attack Hardness**. In Proceedings of the IEEE Security and Privacy (S&P), pages 1-18, 2024. (Acceptance Rate: 17.8%)

[C63] **[IEEE S&P'24]** Doguhan Yeke[G], Muhammad Ibrahim, Guliz Seray Tuncay, Habiba Farrukh[G], Abdullah Imran, Antonio Bianchi, and Z. Berkay Celik, **Wear's my Data? Understanding the Cross-Device Runtime Permission Model in Wearables**. In Proceedings of the IEEE Security and Privacy (S&P), pages 1-18, 2024. (Acceptance Rate: 17.8%)

[C62] **[NDSS'24]** Arjun Arunasalam[G], Andrew Chu[U], M. Ozgur Ozmen[G], Habiba Farrukh[G], and Z. Berkay Celik, **The Dark Side of E-commerce: Dropshipping Abuse as a Business Model**, In Proceedings

of the Network and Distributed System Security Symposium (NDSS), pages 1-18, 2024 (Acceptance Rate: 15.8%)

[C61] **[ACSAC'23]** Yufan Chen[G], Arjun Arunasalam[G], and Z. Berkay Celik, **Can Large Language Models Provide Security & Privacy Advice? Measuring the Ability of LLMs to Refute Misconceptions**. In Proceedings of the Annual Computer Security Applications Conference (ACSAC), pages 1-15, 2023. (Acceptance Rate: 24%)

[C60] **[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, pages 1-18, 2023. (Acceptance Rate: 29%)

[C59] **[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, pages 1-18, 2023. (Acceptance Rate: 29%)

[C58] **[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: 29%)

[C57] **[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: 29%)

[C56] **[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: 29%)

[C55] **[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), pages 1-18, 2023. (Acceptance Rate: 25%)

[C54] **[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 1-17, 2023. (Acceptance Rate: 17.1%)

[C53] **[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%)

[C52] **[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%)

[C51] **[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%)

[C50] **[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%)

[C49] **[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%)

[C48] **[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%)

[C47] **[USENIX Security'21]** 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 1-18, 2021. (Acceptance Rate: 18.8%).

[C46] **[KDD'21]** 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 1-9, 2021. (Acceptance Rate 15.4%)

[C45] **[SecDev'21]** 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), pages 1-9, 2021.

[C44] **[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 1-19, 2021. (Acceptance Rate: 18.8%)

[C43] **[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%)

[C42] **[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%)

[C41] **[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), pages 1-25, 2021.

[C40] **[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 1-22, 2021. (Acceptance Rate: 18.6%)

[C39] **[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 1-14, 2021. (Acceptance Rate: 25%)

[C38] **[WiSec'20]** 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%)

[C37] **[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 1-7, 2020.

[C36] **[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%)

[C35] **[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 1-12, 2019. (Acceptance Rate: 23.5%)

[C34] **[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 1-12, 2018. (Acceptance Rate: 19%)

[C33] **[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 1-18, 2018. (Acceptance Rate: 19%)

[C32] **[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 1-8, 2018. (Acceptance Rate: 20%)

[C31] **[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 1-13, 2018. **(Best Paper Award)**

[C30] **[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.

[C29] **[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 1-11, 2017.

[C28] **[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 1-14, 2017. (Acceptance Rate: 18%)

[C27] **[MILCOM'16]** 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 1-6, 2016.

[C26] **[Euro S&P'16]** 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 1-16, 2016. (Acceptance Rate: 17.3%)

[C25] **[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 1-6, 2015.

[C24] **[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 1-6, 2013.

Refereed Workshop Publications

[W23] **[USEC'24]** Arjun Arunasalam[G], Habiba Farrukh[G], Eliz Tekcan[G], and Z. Berkay Celik, **An Exploration of Online Toxic Content Against Refugees**. In Proceedings of the Symposium on Usable Security (USEC) 2024, (colocated with NDSS).

[W22] **[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).

[W21] **[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)**

[W20] **[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).

[W19] **[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**. International Workshop on Federated Learning for User Privacy and Data Confidentiality (FL-ICML) 2021 (colocated with ICML).

[W18] **[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).

[W17] **[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).

[W16] **[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).

[W15] **[IWSPA'17]** Z. Berkay Celik, Patrick McDaniel, and Rauf Izmailov, **Feature Cultivation in Privileged Information Augmented Detection**. In Proceedings of the Security And Privacy Analytics Workshop (IWSPA), pages 73-80, 2017 (colocated with CODASPY), Invited Paper.

[W14] **[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

[D13] **[VehicleSec'24]** Ashwin Nambiar[G], Z. Berkay Celik, Ryan Gerdes, Antonio Bianchi, **Poster: PLUG&CHECK: Finding Bugs in ISO15118 Implementations with EVFUZZ**, Vehicle Security and Privacy

(VehicleSec) Symposium, 2024 (collocated with NDSS).

[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

- ◇ Secure Autonomy: Vulnerability Discovery and Mitigation
  Qualcomm AI Lectures. December, 2024
- ◇ Finding and Mitigating Vulnerabilities of Autonomous Vehicle Control Software to Physical Adversaries
  Research Institute for Transportation Safety and Security at Sandia National Laboratories (RITS3). September, 2024
- ◇ Challenges in Compositional Secure Autonomy
  Dagstuhl Seminar on Security and Privacy of Current and Emerging IoT Devices and Systems (August, 2024)
- ◇ Generative AI and Autonomous Vehicle Security
  DENSO North America Cybersecurity Research and Development Team (June 2024)
- ◇ From Perception to Control: Compositional Security Analysis of Autonomous Systems
  Workshop on Cyber Security in Smart Grid, Electric Vehicles, and Autonomous Vehicles organized by Google Research and Cardiff University (June 2024)
- ◇ Unlocking the Potential of Generative AI for Security Applications
  MITRE, AI-Cyber Convergence Technical Exchange Meeting (April 2024)
- ◇ Towards Compositional Secure Autonomy: From Perception to Control
  - *National Center for Transportation Cybersecurity and Resiliency (TraCR), USDOT National University Transportation Center, Scholar Webinar (October 2024)*
  - *Akademiska Föreningen, Lund University Sweden for the ELLIIT focus period Symposium on Security and Fault Tolerance of Cyber-Physical Systems (April 2024)*
  - *Ohio State University, Institute for Cybersecurity & Digital Trust (March 2024)*
  - *University of California Santa Cruz Baskin School of Engineering, Cyber-Physical Systems Research Center (CPSRC) (February 2024)*
  - *Computer Science Distinguished speaker at the University of Virginia (December 2023)*
  - *Keynote Speaker at the Workshop on Security and Privacy of Sensing Systems (Sensors S&P) colocated with ACM SenSys (November 2023)*
- ◇ An Overview of Cyber-Physical Systems Research at Purdue Security Laboratory (PurSec)
  Rose-Hulman Institute of Technology (November 2023)
- ◇ Current Landscape of IoT Security Research: A Path to Secure Autonomy
  Sp4rkCon - Information Security Conference presented by Walmart Global Tech (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
  Workshop on 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

Ph.D. STUDENTS

Past PhD Students

- 2024, Muslum Ozgur Ozmen, Assistant Professor in the School of Computing and Augmented Intelligence at Arizona State University
  - Thesis: Achieving Compositional Security and Privacy in IoT Environments
- 2024, Reham Aburas, Assistant Professor in the Department of Computer Science and Engineering at the American University of Sharjah
  - Thesis: User-Centered Data Access Control Techniques for Secure and Privacy-Aware Mobile Systems
- 2023, Habiba Farrukh, Assistant Professor in the Department of Computer Science at the University of California, Irvine
  - Thesis: Leveraging Multimodal Sensing for Enhancing the Security and Privacy of Mobile Systems

Past Co-advised PhD Students

- 2024, Hyungsub Kim, Assistant Professor in the Department of Computer Science at Indiana University (co-advised with Dongyan Xu and Antonio Bianchi)
  - Thesis: Defeating Logic Bugs in Robotic Vehicles
- 2023, Khaled Serag, Research Scientist at Qatar Computing Research Institute (co-advised with Dongyan Xu)
  - Thesis: Proactive Vulnerability Identification and Defense Construction – The Case for CAN
- 2023, Abdulellah Alsaheel, now private Security Consultant (co-advised with Dongyan Xu)
  - Thesis : Trace Data-driven Defense Against Cyber And Cyber-physical Attacks

Current PhD Students

- Arjun Arunaslam, Fall 20
- Raymond Muller, Spring 21
- Hongyu Cai, Fall 23
- Chandrika Mukherjee, Fall 23

Current co-advising PhD Students

- Ruoyu Song, Spring 21 (co-advised with Antonio Bianchi)
- Doguhan Yeke, Fall 21 (co-advised with Antonio Bianchi)
- Ananth Shreekumar, Fall 23 (co-advised with Dongyan Xu)

MSc and UNDERGRADUATE STUDENTS

Current Msc Students

- Devin Ersoy (Spring 2024 - Present)
  - Devin will start his PhD under my supervision in Fall 2024

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 National Laboratories

Independent Study Msc Students

- Jevin Amit Modi, 2024
  - **Topic:** Security Analysis of Robotic Vehicles
- Ananth Shreekumar, 2023
  - **Topic:** Attacks on Object Detection and Tracking
  - PhD student under my supervision and Dongyan Xu
- Chandrika Mukherjee, 2023
  - **Topic:** Security of Mixed Reality
  - PhD student under my supervision
- Jyun-Jhu Syu, 2023
  - **Topic:** Self-Explaining AI Models
- Ben Chen, 2023
  - **Topic:** Attack Investigation with Hyribd Models
- Yufan Chen, 2023
  - **Topic:** Exploration of Security and Privacy Concerns in Large Language Models
- Rwitam Bandyopadhyay (Amazon), 2023
  - **Topic:** Auto-Tuning PID Controllers in Robotic Vehicles
- Gaurav Jadhav, 2022
  - **Topic:** Security issues in Web and Mobile Ad Ecosystem
- Abhishek Shah (Amazon), 2022
  - **Topic:** Security of AR/VR Devices
- Aniket Nare (Amazon), 2022
  - **Topic:** Scene Classification and Semantic Segmentation on 3D Point Cloud Dataset
- Abhinav Gupta (Facebook), 2022
  - **Topic:** Account Selling as a Fraud
- Eliz Tekcan (Vestel), 2022
  - **Topic:** Online Hate and Harassment in Social Platforms
- Yi-Shan Lin (Google), 2021
  - **Topic:** Evaluation of Explainable Artificial Intelligence (XAI) Interpretability

- Akram Ahmed Faqihr (Msc), 2021
  - **Topic:** Security of CAN Bus Error Handling Protocol
- Basavesh Shivakumar (PhD student at MPI-SP), 2020
  - **Topic:** Safety and Security of Event Ordering on IoT Systems
- Zhanfu Yang (PhD student at Stevens Institute of Technology), 2020
  - **Topic:** Physical Modelling of Events in IoT Systems
- Akhil Bandarupalli (PhD student at Purdue CS), 2020
  - **Topic:** Program Synthesis of IoT Applications

Current Undergraduate Students

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

Past Undergraduate Students

- Varun Gannavarapu (Junior, CS)
  - **Topic:** Analysis of Illicit Account Marketplaces
  - Software Engineer at Sandia National Laboratories
- 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 of 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
- 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

- David Felipe Ramirez (CS, Universidad Nacional de Colombia, 2024) – GoBoiler Internship program
- Felipe Barreto (CS, Icesi University (Colombia), 2024) – GoBoiler Internship program
- Blaise Swartwood (Junior, CS), Rose-Hulman Institute of Technology, Summer'23
- 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)

TEACHING EXPERIENCE

Courses Taught at Purdue University

Semester	Course Number	Course Title	Enrollment	Course (5.0)	Instructor (5.0)	Response
Fall 2023	CS 390-GIS	Great Issues in Computing (link)	83	4.2	4.4	24/82
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.

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)
  - 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)
- 2024-Present, **Co-moderator** for cs.CR, the Cryptography and Security subject area in arXiv

Conference/Workshop Organization

- **General Chair:** Symposium on Vehicle Security and Privacy (VehicleSec), 2025
- **General Chair:** Symposium on Vehicle Security and Privacy (VehicleSec), 2024
- **Program Co-chair:** IEEE/ACM Workshop on the Internet of Safe Things, 2024
- **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

- Workshop on Security and Privacy in Standardized IoT (SDIoTSec), 2025
  CCS (Hardware, Side Channels, and CPS – ML and Security Tracks): 2025, 2024, 2023, 2021
- **NDSS:** 2025, 2024, 2023, 2022
- **USENIX Security:** 2024, 2023, 2022, 2021
- **IEEE Symposium on Security and Privacy:** 2024, 2023
- **ACM Security and Privacy in Wireless and Mobile Networks (WiSec)**: 2024, 2023
- **IEEE Secure Development Conference (SecDev):** 2023, 2022
- **Secure and Trustworthy Machine Learning (SATML):** 2023
- **IEEE International Symposium on Secure and Private Execution Environment Design:** 2024
- **Workshop on IoT Security and Cyber Threat Intelligence (co-located at ACSAC):** 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
- **Journal of Software Practice and Experience** 2023
- **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 to attend the Dagstuhl Seminar on Security and Privacy of Current and Emerging IoT Devices and Systems (Jul 28 – Aug 02) 2024.
- Invited mentor at the NSF SaTC Aspiring PI Workshop, 2024 (University of Chicago).
- Invited participants for the NSF-sponsored Workshop on Software Engineering for Robotics, 2023. The event brings together leaders from academia and industry to identify key problems in software engineering for robotics that we should tackle in the next 5 years.
- Invited participants for the Quad Countries (Australia, India, Japan, USA) event on leveraging machine learning research to enhance cyber security organized by NSF and National Security Council (The White House), 2023
- NSF Review Panel, 2024, 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.

- Integrating Human Reasoning into Autonomous Systems for Secure Control
  Sandia National Laboratories, Digital Assurance for High Consequence Computing (DAHCS), 2024
- Vulnerability Discovery in Cyber-Physical Systems and Defenses
  Airbus, 2024
- IoT/CPS Research at PurSec Laboratory
  MITRE, 2023
- IoT/CPS Research at PurSec Laboratory
  Perspecta, 2023
- Attack Modeling and Attack Investigation through a Sequence-based Learning Approach
  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
- Security of Industrial Control Systems
  Eli Lily, 2022
- Aero Cyber: The challenges of resource-constrained embedded systems
  CERIAS Annual Security Symposium Panelist, 2021
- 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, 2019
- Verification of IoT Software for Safety and Security
  Boeing Company, 2019

College-Level and Departmental Engagement

- Organizer for GoBoiler Program Welcome Event, 2024
- Member of PhD Fellowship Review Panel, Office of the Vice Provost for Graduate Students and Postdoctoral Scholars, 2024
- Presenter for online MS in Information and Cybersecurity (ISCY) webinar, 2023
- Prospective PhD visit day organizer, 2024, 2023, 2022
- Primary Advisor of Computer Science Graduate Student Board (GSB), 2024, 2023, 2022
- Co-adviser of Computer Science Graduate Student Board (GSB), 2021
- Started the Systems Security reading group (weekly meetings), attendance: ∼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, 2024, 2023
  - Admission Committee, Professional MS Program, Information and Cyber Security, 2024, 2023
  - Admission Committee, Information Security for Computing Professionals, 2022
  - PhD Admission Committee, 2020, 2019

Community Outreach and Diversity Activities

- My group has contributed to the `4-H Academy @ Purdue` on August 2024 by developing and leading a hands-on, two-hour session on cyber-physical systems security for high school students My research group highlighted the security of robotic vehicles, AR/VR devices, autonomous vehicles, and industrial control systems through videos, posters, and interactive demonstrations with devices and research prototypes.
- Selected to deliver two lectures on cyber-physical systems security for the `Cybersecurity Youth Academy for Jordan (Cyber Academy)` organized by Purdue Applied Research Institute and CERIAS. The goal of this academy is to support the strengthening of Jordan's overall cybersecurity posture through increasing resilience to cyberattacks and cyber workforce strengthening, 2024.
- Attended webinar for Egypt University of Informatics (EUI) students, the faculty representative to answer any technical or security course content-related questions, 2024
- 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
- Speaker for professional writing workshop series for Purdue undergrads; writing a research statement for grad school (with Ellie Broughton, Undergraduate Programs Specialist), 2021
- Advised 4 students through `GoBoiler Internships program`, which aims to provide students from targeted regions with research experience. 2 students from Latin (South) American Universities (2020) and 2 students from European Universities (2024).

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

- Addressing cybersecurity issues, Celik earned Amazon Research Award, `Purdue CS News`, October 2024.
- Defense award launches Purdue project to strengthen cyber-physical systems, `Purdue Office of Research`, April 2024.
- Purdue Marketing and Communications recorded a video in which I discussed the security and privacy of wearable devices. So far, this video has been picked up by more than 10 news channels and outlets in Terre Haute, Lafayette, and Indianapolis, March 2024.
- Protecting Privacy in Wearable Devices, `Purdue Today`, March 2024.
- Can Large Language Models Provide Security & Privacy Advice? Measuring the Ability of LLMs to Refute Misconceptions, `Montreal AI Ethics Institute`, August 2023.
- Purdue part of a national research center aimed at hardening transportation systems against cyberattacks, `Purdue CS News` and `College of Engineering News`, August 2023.
- Purdue CS graduate student Raymond Muller secures X-Force Fellowship, `Purdue CS 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 News`, August 2020.