RUOYU SONG

305 N University St, West Lafayette, IN, 47906
ry@purdue.edu ⋄ ruoyu.sh ⋄ (562) 324-1253

EDUCATION

Purdue University Jan 2021 - August 2026 (Expected)

- Ph.D. in Computer Science
- Advisor: Professor Z.Berkay Celik and Professor Antonio Bianchi
- Research Focus: Autonomous Vehicle Software Security

Purdue University August 2016 - December 2020

- Bachelor of Science in Computer Science (*Honor*)
- Bachelor of Art in Philosophy

RESEARCH INTERESTS

My research focuses on **system security**, employing methodologies in **system design, formal methods**, and **machine learning** to improve security and privacy in **autonomous systems** and their interactions with physical environments. This approach is best exemplified through my contributions to **Autonomous Vehicle** safety and security.

RESEARCH EXPERIENCE

Graduate Research Assistant in Dr.Celik's Research Group May 2020 - Present
Purdue University *West Lafayette, IN*

- Developed an LLM-Based AD reasoning agent that enhances the robustness of the Autonomous Driving system against perception attack on a dataset collected from ***CARLA*** simulator, achieving 83.3% accuracy on identifying the attack and 86.4% on defending the attack.
- Developed *Acero*, which systematically discovers the maneuvers an adversarial vehicle can make to cause the ***Autoware*** (based on ROS) and ***openpilot*** (end-to-end AD software) to fail their intended operations while ensuring that the adversary remains safe and achieves low liability, resulting in finding over 28 unique attacks.
- Developed a system that predicts the motion behavior of agents on the highway by extracting and normalizing characteristics using MLP and training on the US-101 highway data set, achieving 99.88% accuracy in lateral prediction and 81.22% accuracy in longitudinal prediction.
- Modeled an IoT environment with ten sensors and six actuators, developed an algorithm using the LTL formula, and refined parameter mining method, which enabled the framework to find 17 physical constrain violations in this environment

Undergraduate Research Assistant in Dr.Walid Aref's Research Group Feb 2019 - May 2019
Purdue University *West Lafayette, IN*

- Implemented a vertex-cover algorithm for the GRFusion, a combination of database and graph system, which greatly improved the capability and functionality of the system.

PUBLICATIONS

Conference Publications

C4 Chenyi Wang, Raymond Muller, **Ruoyu Song**, Jean-Philippe Monteuuis, Jonathan Petit, Yanmao Man, Ryan Gerdes, Z Berkay Celik, Ming Li. *From Threat to Trust: Exploiting Attention Mechanisms for Attacks and Defenses in Cooperative Perception.* Usenix Security 2025 (Acceptance Rate: 17%)

C3 Raymond Muller, **Ruoyu Song**, Chenyi Wang, Yuxia Zhan, Jean-Philippe Monteuuis, Yanmao Man, Ming Li, Ryan Gerdes, Jonathan Petit, and Z Berkay Celik. *Investigating Physical Latency Attacks against Camera-based Perception* . IEEE Security and Privacy Symposium (Oakland) 2024 (Acceptance Rate: 14.8%)

C2 **Ruoyu Song**, Muslum Ozgur Ozmen, Hyungsub Kim, Raymond Muller, Z. Berkay Celik, and Antonio Bianchi. *Discovering Adversarial Driving Maneuvers against Autonomous Vehicles.* Usenix Security 2023. (Acceptance Rate: 29%)

C1 Muslum Ozgur Ozmen, **Ruoyu Song**, Habiba Farrukh, and Z. Berkay Celik. *Evasion Attacks on Smart Home Physical Event Verification and Defenses.* Network and Distributed System Security Symposium (NDSS), 2023. (Acceptance Rate: 19%)

TEACHING EXPERIENCE

Guest Lecturer:

• AT532 - Contemporary Issues In Transportation Security	Spring 2025
• CS390 - Great Issues in Computing	Fall 2023
• CS592ICS - IoT & CPS Security, Purdue University	Spring 2022

Teaching Assistant:

• CS426 - Computer Security, Purdue University	Fall 2024
• CS527 - Software Security, Purdue University	Spring 2024, 2023, 2022
• CS490-SWS - Software Security Graduate Teaching Assistant	Fall 2022
• CS381 - Algorithm	Fall 2020
• CS190 - Dev Pool	Spring 2021
• CS240 - Programming in C	Fall 2018

SERVICE

Program Committee Member

- 2nd Cyber Security in Cars Workshop (CSCS) 2025
- IEEE Secure Development Conference (SecDev) 2025
- 3rd USENIX Symposium on Vehicle Security and Privacy (VehicleSec) 2025
- 1st International Workshop on Software Engineering for Autonomous Driving Systems (SE4ADS) 2025

Reviewer

- IEEE Transactions on Vehicular Technology (IEEE TVT) 2025

External Reviewer

- Network and Distributed System Security Symposium (NDSS) 2025, 2022
- ACM Conference on Computer and Communications Security (CCS) 2024
- ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) 2023
- USENIX Security 2025, 2024, 2023
- IEEE Symposium on Security and Privacy (S&P) 2026, 2023

Outreach

- Presented my research to about 20 high school students as part of a 4-H event.

STUDENT RESEARCH ADVISING

- Neeraj Gopalakrishnan M.S. CS, Purdue University 2024
- Berk Aydogmus M.S. CS, Middle East Technical University 2022

AWARDS AND GRANTS

- 2025 Usenix VehicleSec Student Travel Grant
- 2025 Qualcomm Innovation Fellowship Finalist (North America)

PRESENTATIONS

Conference and Workshop Talks

T2 Discovering Adversarial Driving Maneuvers against Autonomous Vehicles, CERIAS security symposium, IN, USA, April 2024

T1 Discovering Adversarial Driving Maneuvers against Autonomous Vehicles, USENIX Security, CA, USA, August 2023

TECHNICAL SKILLS

- **Programming Languages:** Python, C++, Matlab, Scenic
- **Methods:** Formal Verification, Fuzzing, Motion Planning, Computer Vision, GFlowNet, LLM Fine tuning
- **Systems:** CARLA, Autoware, openpilot, Apollo, PyTorch, Gymnasium, QLoRA