RUOYU SONG

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

EDUCATION

Purdue University 2020 - present

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

Purdue University 2016 - 2020

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

RESEARCH EXPERIENCE

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

- Developing an LLM-Based AD system that enhances the robustness of the AD system against perception attack by fine-tuning the LLaMa2 model using LoRA on a dataset collected from **CARLA** simulator. (Ongoing)
- 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.

TEACHING EXPERIENCE

- Served as graduate teaching assistant for 5 courses (Undergraduate Dev-Pool, Undergraduate Software Security, Graduate Software Security, Algorithm, C-Programming) over 7 semesters.
- Lead laboratory/recitation session of ∼30 students and graded ∼7 assignments per semester.

PUBLICATIONS

Conference Publications

C1 **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%)

C2 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%)