Department of Computer Science

Achieving Compositional Safety and Security in IoT Environments

Muslum Ozgur Ozmen
Purdue University

Hosted by Yiannis Koutis

Date: Monday, February 12, 2024
Coffee: 2:15 PM – 2:30 PM
Time: 2:30 PM – 3:30 PM
Location: GITC 4402 (4th floor Seminar Lecture Hall)
Zoom Link: https://njit-edu.zoom.us/j/92374083925?pwd=RWc2NUk4Rm1FN2NCUVd5YjFTOGRLQT09

Abstract:
The Internet of Things (IoT) systems include sensors that measure the physical world, actuators that influence it, and IoT apps that automate these sensors and actuators. While IoT environments have revolutionized our lives by integrating digital connectivity into physical processes, they have also become attractive targets for adversaries. In this talk, I will explore emerging safety and security issues arising from the complex physical interactions in IoT environments. I will then demonstrate how to identify and mitigate these issues through systems design, formal methods, and applied cryptography. In particular, I will present three systems for compositional (system-wide) IoT safety and security: (1) a system that discovers physical app interaction vulnerabilities through hybrid modeling and falsification, (2) evasion attacks against physical event verification systems and preventing such attacks through patching and sensor placement, (3) and a secure group pairing method for devices with heterogeneous sensing modalities. Through these efforts, we develop formal techniques and tools that enable developers to build safe and secure IoT environments.

Bio:
Muslum Ozgur Ozmen is a Ph.D. candidate in the Department of Computer Science at Purdue University, where he is advised by Professor Z. Berkay Celik. Prior to joining Purdue, Ozgur earned his Master of Science degree in computer science from Oregon State University. He has researched a variety of topics, including IoT security and privacy, mobile robot and self-driving car security, and lightweight cryptography. His dissertation focuses on developing tools and algorithms that ensure compositional safety and security in IoT systems through formal methods. He served at the student advisory council of NSF AI Institute for Agent-based Cyber Threat Intelligence and Operation (ACTION) as the Purdue representative in 2023. He also interned with the cyber-physical systems research team at the Toyota Research Institute North America. He anticipates completing his Ph.D. in the Spring of 2024.

More information can be obtained at https://ozgurozmen.github.io/.