CPS: Medium: Collaborative Research: Security vs. Privacy in Cyber-Physical Systems

Submitted by jkatz on Mon, 05/06/2019 - 4:59pm

Project Details

Lead PI:	Jonathan Katz
Performance Period:	10/01/18 - 09/30/21
Institution(s):	University of Maryland College Park
Sponsor(s):	National Science Foundation
Award Number:	1837517

Abstract: This research examines the scientific foundations for modeling security and privacy trade-offs in cyber-physical systems, focusing in particular on settings where privacy-protection technologies might be abused by malicious parties to hide their attacks. The goal is to provide both security and privacy guarantees for a variety of cyber-physical systems including intelligent transportation systems, smart energy, and autonomous vehicles. Privacy and security in cyber-physical systems have been studied independently before, but often they have not been addressed jointly. This project will study privacy-protection mechanisms such as differential privacy, and explore how using such mechanisms can affect the state-of-art integrity and attack-detection mechanisms. The project will also develop novel defenses including: 1) Identifying fundamental trade-offs between privacy and security based theoretical analyses of privacy, control theory, and optimization methods, with applications such as traffic-density estimation and smart grids; 2) incorporating game-theoretic considerations in analyzing adversarial strategies; and 3) Proposing new privacy-preserving techniques applicable in cyber-physical systems and beyond.

Related Artifacts

Presentations

- Security vs. Privacy in Cyber-Physical Systems | Download

Posters

- Security vs. Privacy in Cyber-Physical Systems | Download
