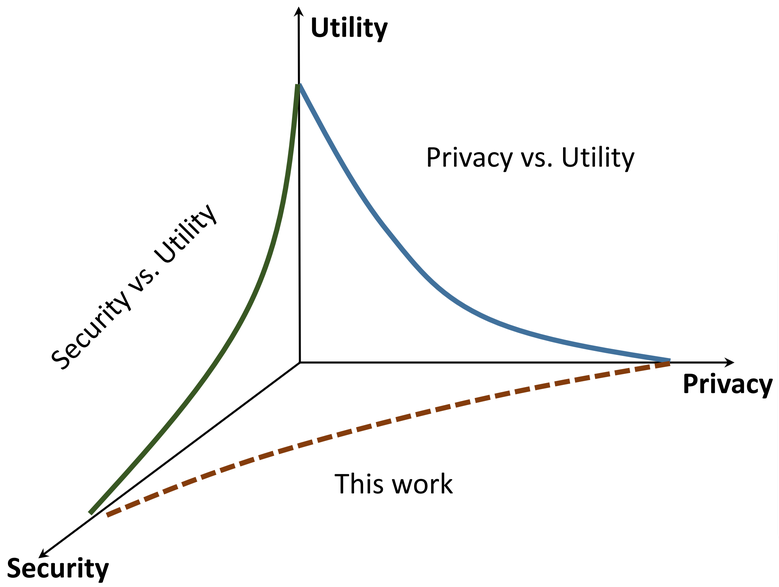
CPS: Medium: Collaborative Research: Security vs. Privacy in Cyber-Physical Systems

PIs: Alvaro Cardenas, University of California at Santa Cruz
Murat Kantarcioglu, University of Texas at Dallas
Jonathan Katz, University of Maryland



This research examines the scientific foundations for modeling security and privacy trade-offs in cyber-physical systems, focusing 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.

Challenges

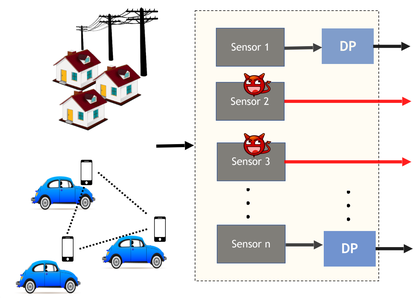
- Preserve confidentiality and security of sensor data.
- Minimize the overhead of confidentiality-preserving techniques for a real-time control system.

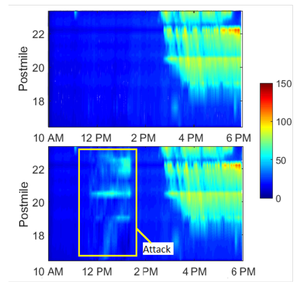
Security and Privacy with Differential Privacy in Cyber-Physical Systems

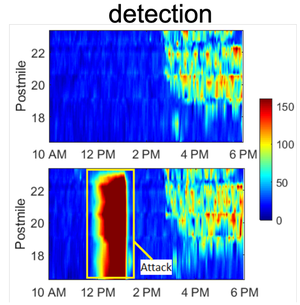
Classical Utility: Usable Statistics, Reason for data collection

Privacy: Protect consumer data

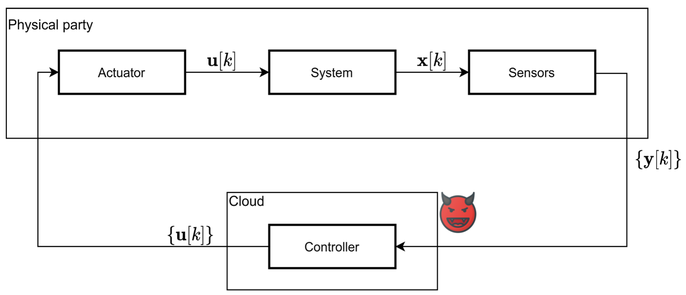
Security: Trustworthy data, Detect data poisoning, Different from classical utility because this is an adversarial setting







Ongoing Work:
Security and Privacy
Privacy-Preserving
Crypto



Recent Publications

- Giraldo, Cardenas, Kantarcioglu, Katz. Adversarial Classification Under Differential Privacy. **NDSS 2020**
- Ozdayi, Kantarcioglu, Gel. Defending Against Backdoors in Federated Learning with Robust Learning Rate. **AAAI 2021**

Broader Impacts

- Interdisciplinary theoretical advances (security/control) to consider privacy and security in the design of cyber-physical systems.
- Outreach and mentoring activities supporting underrepresented students in STEM at both graduate and undergraduate levels

2021 NSF Cyber-Physical Systems Principal Investigators' Meeting
June 2-4, 2021

Award ID#: 1929410 (UCSC)
1837517 (UMD)