Challenges of Timing Attacks

- CPS functionality is affected by both the data values of operations and the time those operations are conducted.
- Timing-based security attacks: compromise functionality by changing the timing of computation or communication operations.
- Broad attack surface across cyber and physical domains.
- Timing attacks could be stealthy, and difficult to defend against at real time under limited resources.

Framework

Thrust A: Analyze Timing-based Attack Surface and Strategies

A1. Identification and Analysis of Timing-based Attack Surface
- Wireless jamming and flooding at physical layer; denial-of-service on TCP/IP or WAVE; compromised nodes on CAN, Ethernet or other buses; partially compromised computation nodes.

A2. Investigate Precise and Stealthy Timing-based Attack Strategies
- Attack on clock synchronization algorithms (e.g., NTP); Multipronged attacks; Flow-in-the-Middle (FIM) attacks.

Thrust B: Cross-Layer Analysis of Timing Attacks

B1. Analysis of System Properties under Timing Aberration
- Analyze the impact of timing aberration on system properties, e.g., safety, performance, liveness, deadlock-free, fairness, robustness.
- Safety and mobility applications for vehicular networks.

- Correlate system-level timing changes with local timing changes.

Thrust C: Cybersecurity and Control-based Defense

- Design of protocols that are robust to timing aberration.
- System interconnection adaptation for improving resilience to timing attacks. System level control-based detection mechanisms.

Scientific Impacts

- Discover new timing-based attack surface and threat models.
- Develop novel cross-layer methodologies for analyzing the impact of timing attacks on system properties.
- Develop novel run-time detection and mitigation techniques as well as design-time protection strategies for timing attacks.
- Provide insights to address robustness under general timing variations.

Broader Impacts

- Address little-studied timing attacks and design secure CPS in critical sectors, e.g., automotive and transportation systems, industrial automation, robotic systems.
- Enable close collaboration with industry and explore potential technology transfer.
- Integrate findings into Northwestern and UCR curriculum and extend to K-12 through Lego Mindstorm.

CPS: Synergy: Securing the Timing of Cyber-Physical Systems

Qi Zhu (Northwestern); Nael Abu-Ghazaleh, Zhiyun Qian, Fabio Pasqualetti, Matthew Barth (UC Riverside)
2018 NSF Cyber-Physical Systems Principal Investigators’ Meeting