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

Qi Zhu (Northwestern); Nael Abu-Ghazaleh, Zhiyun Qian, Fabio Pasqualetti, Matthew Barth (UC Riverside)

2021 NSF Cyber-Physical Systems Principal Investigators' Meeting

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 operation timing.
- Broad attack surface across cyber and physical domain, and difficult to defend at real time under limited resources.

Framework

Thrust A: Timing-based Attack Surface and Strategies

A1. Identification and Analysis of Timing-based Attack Surface

- Jamming and flooding at physical layer; denial-of-service on TCP/IP or WAVE; compromised nodes on CAN, Ethernet.

A2. Investigate Precise and Stealthy Timing-based Attack

- Attack on clock synchronization (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-level properties, e.g., safety, performance, robustness.

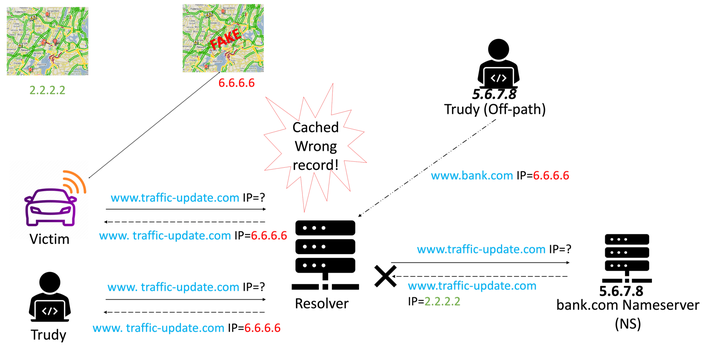
B2. Cross-Layer Timing Analysis for Timing Attacks

- Correlate system-level timing with local timing changes.

Thrust C: Cybersecurity and Control-based Defense

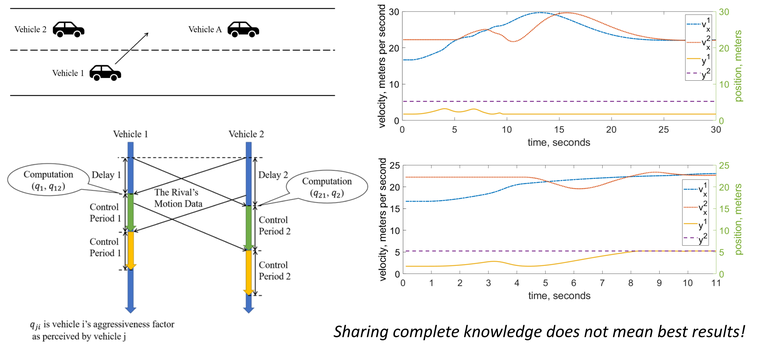
- Design of protocols that are robust to timing aberration.
- System adaptation for improving resilience to timing attacks. System level control-based detection mechanisms.

DNS Cache Poisoning: Impact on Connected Vehicles



*[K. Man, et al. DNS Cache Poisoning Attack Reloaded: Revolutions with Side Channels. ACM Conference on Computer and Communications Security (CCS), 2020. **Distinguished Paper Award**]*

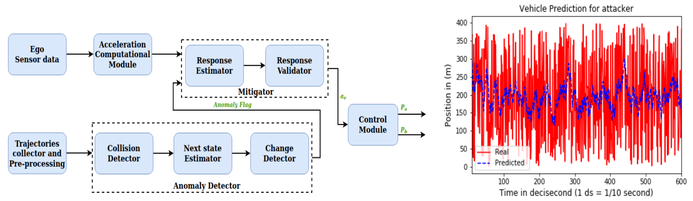
Performance & Safety Impact of Sharing Driving Attitude



Sharing complete knowledge does not mean best results!

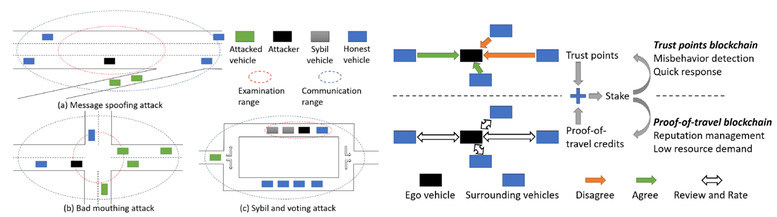
[X. L, et al. Impact of Sharing Driving Attitude Information: A Quantitative Study on Lane Changing. IEEE Intelligent Vehicles (IV), 2020.]

CVGuard: Mitigating Application Level Attacks on Connected Vehicles



- *Validate incoming DSRC data with an anomaly detector.*
- *Use reinforcement learning for detecting stealthy attacks.*
- *Evaluate the approach on a real vehicle with DSRC module, and use hardware-in-the-loop connected vehicles emulator.*

Securing Connected Vehicle Applications with an Efficient Dual Cyber-Physical Blockchain Framework



A framework that incorporates blockchain technology and physical sensing capabilities of vehicles to build trust and secure communication for CV applications.

[X. L, et al. Securing Connected Vehicle Applications with an Efficient Dual Cyber-Physical Blockchain Framework. IEEE Intelligent Vehicles (IV), 2021.]

Scientific Impacts

- Discover timing-based attack and threat models.
- Develop cross-layer methodologies for analyzing the impact of timing attacks on system properties.
- Develop run-time mitigation techniques and 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, transportation, industrial automation, robotics.
- Enable close collaboration with industry and explore potential technology transfer.
- Integrate findings into Northwestern and UCR curriculum. Extend to K-12 through Lego Mindstorm.

Award ID#: 1839511