CAREER: Foundations for Real-Time System Security

CNS-2046705

Gedare Bloom, University of Colorado Colorado Springs (gbloom@uccs.edu)

https://www.real-time-security.com

Abstract

Real-time systems must respond to a stimulus within a bounded time known as a deadline. When the deadline is missed, disaster can happen. Safety-critical systems, cyber-physical systems (CPS), and critical infrastructure all rely upon the correct, safe functioning of the underlying, embedded real-time systems. When their security is compromised, the improper functioning of a real-time system can cause hazardous and deadly consequences. The objective of this project is to protect real-time systems from cyberattack. The outcomes of this project advance theory and practice of real-time security as a burgeoning field that promises deep explorations.

Challenge

Real-time systems have latency deadlines

- General computing sacrifices latency for thruput
- Security mechanisms ignore worst-case timing
- Time predictability is a problem and an opportunity

The significance of this project is to stimulate a comprehensive understanding of the new field of real-time security to bring it from its nascent beginnings into a mature discipline.

Scientific Impact

Stimulating the formation of a rigorous new subdiscipline focusing on the real-time aspects of security

Better understanding of the relationship between inherent properties of real-time systems and their cybersecurity posture

New understanding of attacks stimulates further discovery

Technical Approach

Schedule-Based Security – Cyber attacks and mitigations that leverage the real-time guarantees and schedule predictability inherent to real-time systems.

Real-Time Trusted Execution Environments (TEEs) – Integration of TEE management capabilities into real-time operating systems to leverage TEE-based security for real-time embedded systems.

Securing Real-Time Fault Tolerance – Cyber attacks and mitigations that leverage the fault tolerance capabilities found in safety-critical, real-time cyber-physical systems.

Broader Impacts

On Society

- Increase resilience of infrastructure
- Strong engagement with industry
- Broadening Participation
  - 1 Black PhD student
  - 1 US veteran PhD student

On Education/Outreach

- Mentoring in open-source software
- 2 PhD students supported
- Writing a new textbook to distill the knowledge of real-time security as a discipline.

Other Broader Impacts

- Share datasets and research tools
- New collaborations formed
  - NXP Semiconductors, Italian National Research Council, L3Harris Technologies, Vultara, TU Eindhoven