CPS: TTP Option: Medium: Collaborative Research: Trusted CPS from Untrusted Components

Submitted by Aditya Mathur on Thu, 05/02/2019 - 4:23pm

Project Details

Lead PI:	Aditya Mathur
Performance Period:	10/01/18 - 09/30/21
Institution(s):	Purdue University
Sponsor(s):	National Science Foundation
Award Number:	1837352

359 Reads. Placed 505 out of 803 NSF CPS Projects based on total reads on all related artifacts.

Abstract: The nation's critical infrastructures are increasingly dependent on systems that use computers to control vital physical components, including water supplies, the electric grid, airline systems, and medical devices. These are all examples of Cyber-Physical Systems (CPS) that are vulnerable to attack through their computer systems, through their physical properties such as power flow, water flow, chemistry, etc., or through both. The potential consequences of such compromised systems include financial disaster, civil disorder, even the loss of life. The proposed work significantly advances the science of protecting CPS by ensuring that the systems "do what they are supposed to do" despite an attacker trying to make them fail or do harm. In this convergent approach, the key is to tell the CPS how it is supposed to behave and build in defenses that make sure each component behaves and works well with others. The proposed work has a clear transition to industrial practice. It will also enhance education and opportunity by opening up securing society as a fascinating discipline for K-12 students to follow. The objective of the proposed project is to produce, from untrusted components, a trusted Cyber-physical system (CPS) that is resilient to security attacks and failures. The approach will rely on information flows in both the cyber and physical subsystems, and will be validated experimentally on high fidelity water treatment and electric power CPS testbeds. The project brings together concepts from distributed computing, control theory, machine learning, and estimation theory to synthesize a complete mitigation of the security and operational threats to a CPS. The proposed method's key difference from current methods is that security holes will be identified and plugged automatically at system design time, then enforced during runtime without relying solely on secure boundaries or firewalls. The system will feature the ability to identify and isolate a malfunctioning device or cyber-physical intrusion in real-time by validating its operation against

fundamental scientific/engineering principles and learned behavior. A combined mathematical/data science approach will be used to generate governing invariants that are enforced at system runtime. Invariants are a scientific approach grounded in the system's physics coupled with machine learning and real-time scheduling approaches embedded in the CPS. Robust state estimation will account for errors in measurement and automated security domain construction and optimization to reduce the cost of evaluation without sacrificing coverage. The successful outcome of this research will lead to improved national security across various CPS infrastructures which, in turn, will improve economic and population health and security. The work can be taken to industry for deployment in critical infrastructures. The project will stimulate interest in Science, Technology, Engineering and Mathematics (STEM) through the development of a water-themed tabletop exercise for K-12 and helping current college students develop an interest in outreach through the experiential learning aspects of developing the tabletop exercise.

Related Artifacts

Posters

- CPS: TTP Option: Medium: Collaborative Research: Trusted CPS from Untrusted Components | Download
- Trusted CPS from Untrusted Components | Download