Synergy: Collaborative Research: Security and Privacy-Aware Cyber-Physical Systems

Submitted by Insup Lee on Mon, 02/01/2016 - 5:36am. Contributors:
Insup LeeAndreas HaeberlenBill HansonNadia HeningerRoss KoppelMiroslav PajicGeorge PappasLinh T.X. PhanRita PowellKang ShinOleg SokolskyJeffrey Vagle Christopher YooJesse Walker

Abstract:

Security and privacy concerns in the increasingly interconnected world are receiving much attention from the research community, policymakers, and general public. However, much of the recent and on-going efforts concentrate on privacy in communication and social interactions. The advent of cyber-physical systems, which aim at tight integration between distributed computational intelligence, communication networks, physical world, and human actors, opens new possibilities for developing intelligent systems with new capabilities. Autonomous cars may reduce number of accidents and increase throughputs of transportation networks. Interoperable medical devices can improve patient safety, mitigate caregiver errors, enable personalized treatments, and allow older adults to age in their places. People are increasingly finding themselves in sensor-rich environments that can provide health-related feedback or warn about potential dangers in the environment. At the same time, cyber-physical systems introduce new challenges and concerns about safety, security, and privacy. Cyber-physical systems (CPS) involve tight integration of computational nodes, connected by one or more communication networks, the physical environment of these nodes, and human users of the system, who interact with both the computational part of the system and the physical environment. Attacks on a CPS system may affect all of its components: computational nodes and communication networks are subject to malicious intrusions, and physical environment may be maliciously altered. CPS-specific security challenges arise from two perspectives. On the one hand, conventional information security approaches can be used to prevent intrusions, but attackers can still affect the system non-invasively via the physical environment. On the other hand, resource constraints, inherent in many CPS domains, may prevent heavy-duty security approaches from being deployed. These two considerations lead us to explore how to tolerate attacks in addition to prevent them. Thus, this proposal is to develop a framework in which the mix of prevention, detection and recovery, and robust techniques to work together to improve the security and privacy of CPS. The intellectual merits are as follows: (1) the development of techniques to prevent security attacks to CPS and to detect and recover from malicious attacks to CPS; (2) to develop techniques for security-aware control design by develop attack resilient state estimator; (3) ensuring privacy of data collected and used by CPS, and (4) develop an assurance cases framework for ensuring the security and privacy of CPS with evidence. In addition, our techniques will be evaluated in several case studies on autonomous features of vehicles, internal and external vehicle networks, medical device interoperability, and smart connected medical home. The broader impacts are safer CPS through improved trustworthiness of CPS. As our daily lives depend more CPS (including IoT), the proposed research and development results will provide rigorous foundations and techniques for ensuring the security and privacy of CPS. The potential CPS applications include automotive systems, healthcare systems, medical devices, smart power grids, industrial process control systems,

Insup Lee | Andreas Haeberlen | Bill Hanson | Nadia Heninger | Ross Koppel |Miroslav Pajic | George Pappas | Linh T.X. Phan | Rita Powell | Kang Shin | Oleg Sokolsky | Jeffrey Vagle | Christopher Yoo | Jesse Walker

Other available formats:

Synergy: Collaborative Research: Security and Privacy-Aware Cyber-Physical Systems

Switch to normal viewerSwitch to experimental viewer

Automotive CPS Domains Medical Devices Control Platforms Modeling Health Care Resilient Systems Transportation CPS Technologies Foundations CPS Privacy CPS Security Duke University Intel Internet of Things (IoT) security University of Michigan University of Pennsylvania 2015 CPS PI MTG Videos, Posters, and Abstracts National CPS PI Meeting 2015 2015 Academia Industry Abstract Poster