NORTHWEST INSTITUTE FOR CYBERSECURITY EDUCATION AND RESEARCH

CySER Virtual Seminar

Monowar Hasan
Washington State University

Exploring Platform Reboot as a Security Measure for Cyber-Physical Systems

Mar. 20, 2023, 3:10 – 4PM PDT

Team Link: Click here to join the meeting
Meeting ID: 287 304 495 40 | Passcode: wdM7Vw
Call in (audio only) +1 509-498-6399 | Phone Conference ID: 834 528 822#

Abstract:

A successful cyber attack on a cyber-physical platform can trigger actions that may destabilize (or even damage) the underlying physical systems. In this talk, we will discuss how to ensure the safety of the physical plant even when the platform is compromised. The key idea is proactively cleaning the system through "platform-level reset" and reloading uncompromised copies of cyber components (e.g., OS image and application binaries). We leverage that due to "physical inertia," an adversary cannot instantaneously destabilize the plant (even with complete control over the software), thus allowing the system to perform reboot operations systematically. We will present two approaches to ensure the integrity of these computations in an untrusted environment: 1) a custom design: entire platform-wide restarts coupled with a root-of-trust timer, and 2) an alternate approach using COTS hardware: utilizing trusted execution environment (TEE) features available modern systems. We will further discuss ongoing research to enable platform reboot for various classes of cyber-physical applications.

Bio:

Dr. Monowar Hasan is a Computer Science Assistant Professor at Washington State University (WSU). Before joining WSU, he held an Assistant Professor position at Wichita State University from 2021-2022. Dr. Hasan received his Ph.D. in Computer Science from University of Illinois at Urbana-Champaign (UIUC) in 2020 and an M.S. in Electrical and Computer Engineering in 2015 from University of Manitoba (UM). Dr. Hasan's research interests include exploring security and resiliency techniques of cyber-physical system domains. He has published over 30 peer-reviewed papers at top academic venues and is a recognized expert in real-time cyber-physical systems, cybersecurity, and wireless communication networks.

cyser.wsu.edu