CECS Seminar

"Searching for Digital Evidence in Industrial Control Systems"

Professor Irfan Ahmed

Associate Professor of Computer Science at Virginia Commonwealth University

Tuesday, February 20th
10:30-11:30 a.m.
Location: EH 2430

Abstract: Industrial control systems (ICS) control significant portions of the U.S. critical infrastructure (e.g., power grid, pipelines, and water management). These systems are known to be vulnerable to cyberattacks, as demonstrated in the past, such as CrashOverride, Havex, and HatMan. More recently, DHS CISA reported Russian state-sponsored cyber operations against Ukrainian critical infrastructure, causing denial-of-service and deployment of KillDisk and other destructive malware. In case of a security breach or catastrophic event, digital forensics investigation is crucial to answering questions about an attack. This talk will explore how malicious actors can exploit the vulnerabilities in common design features in real-world field devices into successful attacks on physical processes. It will further discuss research challenges and opportunities to investigate an ICS environment effectively.

Biography: Irfan Ahmed is a VCU NIRA scholar and an Associate Professor of Computer Science at Virginia Commonwealth University (VCU), where he runs the Security and Forensics Engineering (SAFE) Lab in the College of Engineering, focusing on the cybersecurity of industrial control systems (ICS). He has an extensive track record of ICS offensive and defensive research, including eleven ICS-CERT CVEs for the programmable logic controllers of five vendors, i.e., Siemens, Schneider Electric, Rockwell Automation, SEL, and Automation Direct. Ahmed is a steering team member of the DHS Industrial Control Systems Joint Working Group (ICSJWG) to engage asset owners, vendors, state and local governments, industry associations, and consultants/integrators to improve ICS cybersecurity. His work has received three Best Paper Awards, three Best Student Paper Awards, and two Outstanding Poster Awards in digital forensics and cybersecurity conferences. He is also the recipient of an Outstanding Research Award from the American Academy of Forensic Sciences, the ORAU Ralph E. Powe Junior Faculty Enhancement Award, and the CCI Innovation Award from the Virginia Commonwealth Cyber Initiative. Ahmed has also developed laboratory-scale, fully functional ICS testbeds on a gas pipeline and a wastewater treatment plant initially funded by the Army Research Office. His research work is regularly funded by the DHS, NSA, DOE, and NSF. For more information, https://people.vcu.edu/~iahmed3/

Hosted By: Prof. Yasser Shoukry and Prof. Mohammad Al Faruque