SUPPLY CHAIN SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

WEDNESDAY: SESSION 4, TRACK 1

SESSION CHAIR

Quanyan Zhu, New York University

PRESENTERS

- Jennifer Pederson, Cybersecurity and Infrastructure Agency (CISA)
- Charmaine Sample, MTSI
- Sachin Schetty, Old Dominion University
- Junaid Farooq, University of Michigan

SESSION ABSTRACT

The security of industrial control systems (ICS) depends on not only the security of the software and hardware components but also the organizations that created them. An ICS integrates a variety of existing subcomponents created by disconnected actors through a complex supply chain network. The insecurity of one subcomponent in the supply chain can have downstream effects on the security and resiliency of the ICS that integrates many components. This special session aims to understand the supply chain threats on ICS, quantify the risks, and find ways to mitigate them. This special session will consist of invited talks, paper presentations, and panel discussions to provide promising scientific methodologies and tools to improve the current supply chain practices.

Topics of Focus Include:

- Methods for analysis of the supply chain for control systems
- Risk models for management of supply chains, either in the chain or in the end device
- Integration of complexity models highlighting aspects such as emergent behaviors, self-organization, sudden transitions, large events, self-organization, evolutionary dynamics and fundamental uncertainty.
- Supply chain research and empirical studies affecting embedded, 10T, or specialty computing systems, or research highlighting distinctions in the associated supply chains
- Tools for analyzing supply chain risk to assist in risk analysis at scale
- The role and risks of policy tools such as transparency and accountability to better secure the supply chain
- Direct and indirect security and privacy effects of manipulation of computer system supply chain elements