Designed-in Cybersecurity for Cyber-Physical Systems Workshop

Thursday, April 4, 2013

8:00 Breakfast

9:00 Plenary – Green Auditorium
Donna Dodson – NIST introduction

Lee Holcomb – CSRA introduction

Suzanne Lightman on the structure of the workshop and NIST's interest

9:45 Breakout sessions (see below for preliminary descriptions)

- **Buying the Black Box: Security in Acquisition and Implementation** – Lecture Room A

  Mike Baldi, Honeywell Process Systems
  Scott Saunders, Sacremento Municipal Utility District
  Emile Monette, U.S. General Services Administration
  Blaine Burnham, USC /ISI

- **Getting Reliable Information on Vulnerabilities and Threats** – Lecture Room B

  David Dagon, Damballa
  Lisa Kaiser, Department of Homeland Security
  Edward Bonver, Symantec

10:45-11:00 Coffee break

11:45 Plenary – Wrap up of first sessions – Green Auditorium

12:30 Lunch

1:30 Breakout sessions

- **Working with What We Have: Securing the Base** – Lecture Room A

  Glenn Feidelholtz, Department of Homeland Security
  John Cusimano, exida

- **Supply Chain: Its Impact on Securing CPS** – Lecture Room B

  Jon Boyens, NIST
  Nadya Bartol, Utilities Telecom Council

2:45-3:00 Coffee break

3:30 Plenary – Wrap up for second sessions – Green Auditorium

4:00 Adjourn

Friday, April 5, 2012

8:00 Breakfast

9:00 Plenary – Red Auditorium
Lee Holcomb, CSRC -- Discussion of First Day; Introduction to Second Day

9:15 Breakout Sessions

- **Approaches to Assurance and Assurance Composition for CPS** – Lecture Room D

  Michael Peters, Lockheed Martin
  Virgil Gligor, Carnegie Mellon University
  Hal Aldridge, Sypris

- **Enabling Trustworthy Operation Readiness** – Heritage Room

  Steve Kester, AMD
  Sean Smith, Dartmouth University

10:45 – 11:00 Coffee break

11:45 Plenary – Wrap up of Morning Sessions – Red Auditorium

12:30 Lunch

1:30 Plenary – Wrap up of the Workshop – Red Auditorium

3:00 Coffee and Networking

Breakout Sessions

Buying the Black Box: Security in Acquisition and Implementation

This session will consider the best practices, tools and methods that the CPS user community employs when they are purchasing and implementing CPS.

Getting Reliable Information on Vulnerabilities and Threats

Identification of threats and vulnerabilities is the foundation of threat analysis and essential to securing a system. How do CPS users find out about vulnerabilities? Do users feel there is a need for an authoritative source?

Working With What We Have: Securing the Base

Given the complexity of most CPS and the safety concerns, they do not lend themselves to the rapid upgrade cycles of traditional IT systems. However, the threat environment changes as rapidly for CPS as for traditional IT systems. This session will focus on identifying current tools, practices and techniques for securing current systems, their limitations, and gaps.

Supply Chain: Its Impact on Securing CPS

This session will try and identify the processes, questions and procedures that companies can consider when trying to achieve a degree of assurance with their CPS supply chain. Finally, the session will consider desired tools and practices for this area.

Approaches to Assurance and Assurance Composition for CPS

The session will focus on defining properties to be included in the design of the CPS systems of the future to support assurance and their trustworthy operations. This may include the trusted path to the device and the trusted device itself. We will also define approaches to creating composite metrics for individual trustworthy features as well as the unified standard framework for assurance properties across information and control systems.

Enabling Trustworthy Operation Readiness

This session will focus on developing and embedding capabilities into CPS built on verifiable models that upon system deployment allow generation of traceable evidence of trustworthiness at run time. In addition to extracting system trustworthiness features, the models need to be extensible and include information about threats and threat agents. Verification is understood as a formalized way for evaluating the model; the model also needs to be extensible. Practical mechanisms are needed that can be integrated into deployed CPS systems for operational use resulting in resilient systems.