

## AGENDA (FINAL)

### Tuesday August 30, 2016 – Green Auditorium

7:30 am Registration

8:00 am Opening Session (Moderator: Dave Wollman, NIST)

- **Welcome** ~ Chris Greer, NIST
- **Importance and Context of Trustworthiness** ~ Ron Ross, NIST
- **Workshop Objectives** ~ Edward Griffor, NIST

8:30 am Keynote

- **CPS/IoT Trustworthiness – Future Vision and Challenges** ~ Vint Cerf, Google

9:15 am Elements of Risk management for Trustworthiness (Moderator: N. Ivy, NIST)

#### Trustworthiness Risk Management in Connected, Interacting Environments

- Todd Grams, Deloitte and Touche LLC
- Karen Hardy, U.S. Department of Commerce
- Michael Huth, Imperial College London

*What are the key elements of risk management frameworks that are useful to consider in the context of the various Trustworthiness concerns?*

*How can risk management frameworks support consideration of risks across the various Trustworthiness concern areas?*

*How can existing risk management frameworks assist in measuring risks in Trustworthiness?*

10:30 am White House Priorities for trustworthy CPS/IoT Systems

- Greg Shannon, Assistant Director for Cyber Strategy, Office of Science and Technology Policy

10:50 am Break

#### Trustworthiness Concerns Working Sessions

**Working sessions will review current approaches to the trustworthiness concerns in question (e.g., standards and best practices that are process- or certification-based). Each session will consist of remarks by subject matter experts followed by a general Q&A session addressing:**

*How is safety/ security/ privacy/ resilience/ reliability currently addressed and how is that affected by new CPS/IoT challenges?*

*What types of metrics exist for safety/ security/ privacy/ resilience/reliability and what data/information is needed to develop or improve these metrics?*

*How do current methodologies for safety/security/privacy/resilience/reliability interact with those of the other dimensions of trustworthiness? What dependencies are recognized between these areas/disciplines?*

**Additional discussion will take place following initial remarks focusing on the challenges to the approaches posed by CPS and IoT. Key issues include:**

- *Conflicts and Collaborations between CPS Concerns*
- *Cyber-Physical Interactions*
- *Unmanaged Composition in Future CPS/IoT*

11:05 am Session I: CPS Safety (Moderator: C. Vishik, Intel)

#### Safety Challenges in Freely Composed CPS

- James Boehm, McKinsey
- Albert Wavering, NIST

### Tuesday August 30, 2016 – Green Auditorium

- Joe Miller, TRW/ZF
- Ravi Jain, FAA
- Pieter Mosterman, Mathworks

1:00 pm Lunch NIST Cafeteria, Bldg. 101

2:00 pm Session II: CPS Privacy (Moderator: N. Lefkowitz, NIST)

#### Privacy in a Highly Connected World of CPS

- Lorrie Cranor, Federal Trade Commission
- Stacey Gray, Future of Privacy Forum
- Ellen Nadeau, NIST
- Alvaro Cardenas, University of Texas, Dallas

3:15 pm First Day Review of Results and Next Day Objectives

4:00 pm Adjourn Day 1

### Wednesday Morning, August 31, 2016 – Green Auditorium

8:30 am First Day Review

9:00 am Keynote

- **Trustworthiness – Government Perspectives** ~ Tony Scott, U.S. Chief Information Officer

9:45 am Session III: CPS Resilience and Reliability (Moderator: T. McAllister, NIST)

#### Resilience and Reliability Challenges and CPS Game-Changers

- Bruce McMillin, Missouri University of Science and Technology
- Pat Muoio, G2 Inc.
- Janos Sztipanovits, Vanderbilt University
- Deb Bodeau, The MITRE Corporation

11:15 am Session IV: CPS Security (Moderator: R. Ross, NIST)

#### Challenges and Opportunities – Building Trustworthy Secure Systems

- Cynthia Irvine, Naval Postgraduate School
- Michael McEvelley, The MITRE Corporation
- Steve Lipner, Formerly Microsoft Corporation

12:30 pm Lunch NIST Cafeteria, Bldg. 101

1:30 pm Dialogue on Guiding Principles for Securing IoT

- Robert Silvers, Assistant Secretary for Cyber Policy, U.S. Department of Homeland Security

2:15 pm Crosscutting Scenario for Trustworthiness (Moderator: E. Griffor)

A high-profile, trustworthiness risk scenario, chosen at the end of the first day of the workshop, will be analyzed along the dimensions of safety/security/privacy/ resilience/reliability. The session participants will point out the tradeoffs between those concerns and assess the impact of the CPS and IoT challenges. On stage will be individuals representing the different Trustworthiness concerns.

- 'Pacemaker Syndrome' - ('Homeland Video')
- 'Deceiving the Operator: Hollywood Scenario' – ('Power Plant Gone Wild Video')
- 'Hacked Vehicle' – ('Vehicle Hijack Video')

Tuesday August 30, 2016 – Green Auditorium

3:15 pm Closing Summary - Wrap up and Next Steps

3:45 pm Adjourn

## Questions/Challenges/Scenario Lists for Workshop Sessions

### Trustworthiness Risk Management

- What are the key elements of risk management frameworks that are useful to consider in the context of the various Trustworthiness concerns?
- How can risk management frameworks support consideration of risks across the various trustworthiness concern areas?
- How can existing risk management frameworks assist in measuring risks in Trustworthiness?

### CPS and IoT Challenges

- Conflicts and collaborations between CPS Concerns
- Cyber-Physical Interactions
- Unmanaged Composition in Future CPS/IoT

### Trustworthiness Dimension Sessions

#### (Safety/Security/Privacy/Resilience/Reliability)

- How is safety/security/privacy/resilience/reliability currently addressed and how is that affected by new CPS/IoT challenges?
- What types of metrics exist for safety/security/privacy/resilience/reliability and what data/information is needed to develop or improve these metrics?
- How do current methodologies for safety/security/privacy/resilience/reliability interact with those of the other dimensions of trustworthiness? What dependencies are recognized between these areas/disciplines?

### Crosscutting Scenarios

- 'Pacemaker Syndrome' - ('Homeland Video')
- 'Deceiving the Operator: Hollywood Scenario' – ('Power Plant Gone Wild Video')
- 'Hacked Vehicle' – ('Vehicle Hijack Video')