End to End Trust and Security Workshop for the Internet of Things

The goal of this workshop would be for researchers, IT architects and security professionals from industry, government and academia to discuss and agree the scope of an end to end trust and security open architecture for IOT, resulting in a report out and point of view with recommended next steps.

Target audience is 100 to 150 attendees representing:

- Universities including researchers, IT, IOT, CISO
- Agencies including NIST, DHS, DOE, NSF, OSTP
- IOT and Standards Organizations including IEEE and IIC
- U.S. Regional Research & Education Network (e.g., NYSERNET)
- Industry Players such as IBM, Cisco, ARM, Intel, STMicro
- Internet2 staff and E2ET&S and IOT innovation working groups

Pre-work: There will be a call for presentations to deliver during the workshop.

Proposed one day agenda:

8:00am Coffee

8:30am Welcome and introductions

- Present Goal: Develop a deep understanding of the needs and agreement on a framework for end to end trust and security open architecture for IOT. Agree to work in unison and aligned as partners to change the game in end to end trust and security.
- Open architecture so everyone can execute it, is the way you execute that makes it secure. Keep humans safe as possible in the IOT world.
- Challenges and opportunities we must address:
  - Show jeep hack video
  - https://www.youtube.com/watch?v=MK0SrxBC1xs
  - Show Kaiser aspirational healthcare video http://www.kp-itcomms.org/mm/digitalhealth/index.html
- How do we address TIPPSS needs – Trust, Identify, Privacy, Protection, Security, Safety (includes application aware security)
- Focus on a few use cases based on invitee input. For example, Connected Healthcare, Connected Vehicles, Smart Grid

9:00am Opening moderated panel

  - IIC, IEEE, Internet2, NSF, DHS, OSTP, Cisco on the importance of this topic and scope
  - Show converging efforts of thought leaders and do leaders

9:45am Break

10:00am Presentations on Requirements of what we need to do for E2ET&S 4 IOT

- Top 5 presentations submitted present for 15 minutes each

11:15am Presentations on Viewpoints and use cases of potential E2ET&S open architecture and elements

- Top 5 presentations submitted present for 15 minutes each

12:30pm Lunch

1:30pm Breakout working session by focus area to develop proposal for end to end trust and security framework

- By use case — e.g., Healthcare, smart grid, connected vehicles
  - For that use case, what are **categories of devices and software systems to be considered for an end to end trust and security architecture for IOT,** for example for healthcare…does it include biomedical devices, bedside technology, EMR/EHR, home nursing systems, in home medical alert systems?
  - For that use case, what are the **IT and device components and industry players** for a true End to End Trust and Security Architecture for the Internet of Things? Hardware, firmware, software, services, from chip to cloud.
  - Determine **technology elements and actions** needed for the end to end trust and security solution, including Trust, Identity, Privacy, Security — e.g., Hardware/Chip/Device, Firmware/Software/Middleware, Service level
- While an open architecture, ensure the individual implementations make it secure
  - Key players to be engaged to develop this open architecture and execute it (researchers, U.S. Agencies, industry players)

3:30pm Break

4:00pm Bring all the recommendations together in defining and developing an Open Architecture for End to End Trusty and Security for IOT

- Presentations by each breakout group for 20 minutes

5:00pm Closing and next steps

5:30pm End of day