Internet2 CINO End-to-End Trust & Security (E2ET&S) Working Group Collaborative Innovation Community Meeting

19 February 2016

Chairs:
Mark Cather, UMBC
Scot Ransbottom, Va. Tech
Donna Tatro, Princeton

Meeting Objectives

- E2ET&S Focus for 2016
- E2ET&S Working Group Plan Update
- E2ET&S for IoT Workshop Debrief
- Launching the Smart Cities/Smart Campus Focus Group
- Next steps

E2ET&S Innovation Working Group Focus for 2016

- *Develop an advanced architectural roadmap and recommended implementation approach to enable future "End-to-End Trust & Security" innovations for the Research & Education community*
- *Leverage existing resources and capabilities including TIER and InCommon*
- *Address trust, identity, privacy, physical & cyber security, compliance, etc.*
- **Focus areas include**
  - **Internet of Things (IoT)**
  - **Smart Cities/Campus**
  - **Coherent trust & identity protocols across multiple enterprises and networks**
  - **Healthcare & Life Sciences (HCLS)**

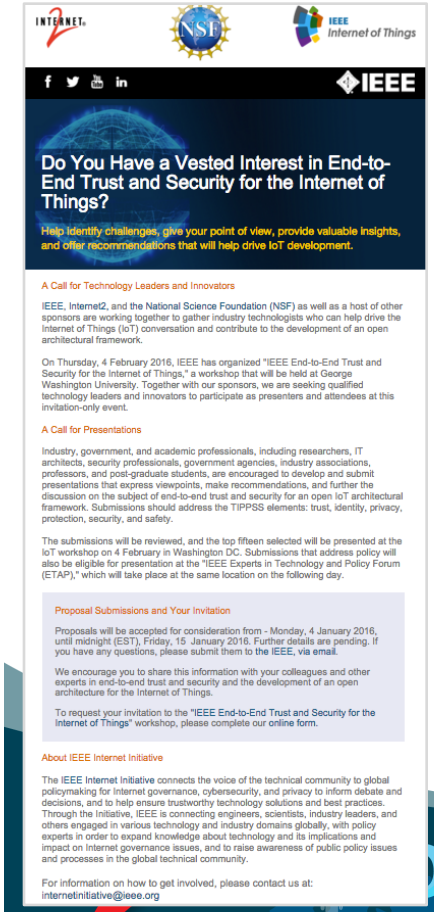
E2ET&S Use Cases and Plans (Page 1 of 2)

Initiative/Use Case	Description	Plan
IoT		
Network Segmentation for IoT	Network segmentation for IoT connected devices not compromising overall network security.	• Webinar held February 2, 2016. Slides and recording available: http://bit.ly/1Q2eDcI • Cisco blog post http://bit.ly/1A1acwl
End to End Trust & Security Open Architecture for IoT (including HCLS)	Create a point of view and next steps for a comprehensive E2ET&S Open Architecture for the Internet of Things.	• February 4, 2016, workshop in cooperation with IEEE, NSF, and GW University • Discussion at the CSG meeting in April 2016
Smart Cities/Campus (include HCLS)		
Launch Smart Cities/Campus CIO Advisory Council and Initiative	Enable Internet2 members to deploy Smart Cities/Campus initiatives by sharing best practices and develop next practices, use cases, and innovations.	• Launch February 2016
Provision strong credentials in the form of a virtual campus ID card	Mobile device as central access to all aspects of a campus – physical and digital. Applied at all levels within a campus: student, faculty, & administration.	• Determine requirements for solution • Identify testbed campuses

E2ET&S Use Cases and Plans (Page 2 of 2)

Initiative/Use Case	Description	Plan
Coherent trust & identity protocols across multiple enterprises & networks		
IPsec and Identity based firewalls	Develop an 'Identity Based Firewall' technology based on the identity of authorized people rather than device IP numbers.	• Steve Wallace engaging SDN/Security WG • Potential to combine with External access to "research zone" systems use case
Assign, manage, and revoke permissions on a platform to support collaborative work	An international unified ID system utilizing existing secure credentials.	• Potential to combine with IPsec & ID-Based Firewalls • InCommon work Int'l Federations • Link with DBDA Digital Humanities focus
External access to "research zone" systems	Subset of the above. An international unified ID system utilizing existing secure credentials.	• Potential to combine with IPsec & ID-Based Firewalls • InCommon work Int'l Federations • Link with DBDA Digital Humanities focus
Improved interoperability among university and hospital networks	Consider use of Security Group Tags and Cisco's TrustSec policy management framework to integrate "cyberinfrastructure islands".	• Identify universities with AMCs to discover needs and create potential solutions

E2ET&S for IoT Workshop: February 4, 2016



Do You Have a Vested Interest in End-to-End Trust and Security for the Internet of Things?

Help identify challenges, give your point of view, provide valuable insights, and offer recommendations that will help drive IoT development.

A Call for Technology Leaders and Innovators

IEEE, Internet2, and the National Science Foundation (NSF) as well as a host of other sponsors are working together to gather industry technologists who can help drive the Internet of Things (IoT) conversation and contribute to the development of an open architectural framework.

On Thursday, 4 February 2016, IEEE has organized "IEEE End-to-End Trust and Security for the Internet of Things," a workshop that will be held at George Washington University. Together with our sponsors, we are seeking qualified technology leaders and innovators to participate as presenters and attendees at this invitation-only event.

A Call for Presentations

Industry, government, and academic professionals, including researchers, IT architects, security professionals, government agencies, industry associations, professors, and post-graduate students, are encouraged to develop and submit presentations that express viewpoints, make recommendations, and further the discussion on the subject of end-to-end trust and security for an open IoT architectural framework. Submissions should address the TIPPSS elements: trust, identity, privacy, protection, security, and safety.

The submissions will be reviewed, and the top fifteen selected will be presented at the IoT workshop on 4 February in Washington DC. Submissions that address policy will also be eligible for presentation at the "IEEE Experts in Technology and Policy Forum (ETAP)," which will take place at the same location on the following day.

Proposal Submissions and Your Invitation

Proposals will be accepted for consideration from - Monday, 4 January 2016, until midnight (EST), Friday, 15 January 2016. Further details are pending. If you have any questions, please submit them to the IEEE, via email.

We encourage you to share this information with your colleagues and other experts in end-to-end trust and security and the development of an open architecture for the Internet of Things.

To request your invitation to the "IEEE End-to-End Trust and Security for the Internet of Things" workshop, please complete our online form.

About IEEE Internet Initiative

The IEEE Internet Initiative connects the voice of the technical community to global policymaking for Internet governance, cybersecurity, and privacy to inform debate and decisions, and to help ensure trustworthy technology solutions and best practices. Through the Initiative, IEEE is connecting engineers, scientists, industry leaders, and others engaged in various technology and industry domains globally, with policy experts in order to expand knowledge about technology and its implications and impact on Internet governance issues, and to raise awareness of public policy issues and processes in the global technical community.

For information on how to get involved, please contact us at: internetinitiative@ieee.org

- **Event at the George Washington University Marvin Center in Washington, DC in conjunction with IEEE, NSF, and George Washington University**
  - Followed by IEEE Experts in Technology & Policy event (http://bit.ly/1PXCPBI)
- **150+ participants (190+ registrants), 30+ presentations (40 paper submissions)**
- **Agenda:**
  - Opening panel with participants from the US DoE, IEEE, IIC, NSF, and M2MI
  - Afternoon break outs on Access Control & Identity Management; Architectural Framework; Policy & Standards; and Scenarios & Use Cases
- **Next Steps:**
  - Opportunity for IoT-related education a key theme (E2ET&S, educating future leaders)
  - Presentations will be available in the next few weeks on the IEEE website
  - Report out from workshop to be available Spring 2016 to identify future next steps
  - Potential follow on events and collaborations to keep the conversation going
  - IEEE conference on Connected Health: Applications, Systems & Engineering Technology (CHASE) event, June 27-29 in Washington, DC (http://bit.ly/1W6x1Wt)

Launching Smart Cities/Campus CIO Advisory Council and Initiative

- **Goal**: Enable interested Internet2 members to deploy Smart Cities/Campus initiatives by sharing best practices and develop next practices, use cases, and innovations. Include opportunity to leverage the Internet2 network as a test bed and backbone for smart campus/cities, incorporating end-to-end trust and security elements.
- **Timing**: Launch February 2016
- **Inaugural Participants**:

ASU Arizona State University
Division of Science & Research West Virginia Higher Education Policy Commission
Indiana University Bloomington
Johns Hopkins University
Marshall University
MIT
Princeton University
usignite
UMBC An Honors University in Maryland
University of Pittsburgh
University of Washington
Wisconsin University of Wisconsin-Madison
VirginiaTech Invent the Future
CUNY The City University of New York

INTERNET2 POWERED BY COMMUNITY

E2ET&S Innovation Working Group Next Steps

- Smart Cities/Campus Initiative participation – let us know if you want to participate or have potential use cases
- Determine how to best leverage other initiatives
  - Proposed White House Cybersecurity National Action Plan (CNAP) released (http://bit.ly/1RHhc9v), how does your institution anticipate participating?
  - IEEE conference on Connected Health: Applications, Systems & Engineering Technology (CHASE) event, June 27-29 in Washington, DC (http://bit.ly/1W6x1Wt)
- Internet2 Open Id Connect workshops scheduled next week
  - February 22nd: http://bit.ly/24cl3jQ
  - February 24th: http://bit.ly/1RR0sNh

Questions & Answers…
Thank You

e2etschairs@Internet2.edu

CINO@Internet2.edu

@FloInternet2

@EmilyNInternet2

E2ET&S Use Cases for Future Action

Initiative/Use Case	Description	Plan
Software Defined Perimeter (SDP)	Leverage SDP against attacks to provide security for cloud, mobile computing, and IoT applications.	• SDP Webinar held 9/1/2015 • SDP session held at SC15 • Opportunity to work with CSA on SDP Spec V2
		Plan: Connecting with Other Initiatives
Security for web-based mobile applications	Adding support for OpenID Connect to Shibboleth IdPv3 allows secure authentication for mobile applications.	• Connected with the University of Chicago • Awaiting further maturation • Engage the TIER community
Preserving student privacy while enabling use of InCommon federated services	Allow students to access InCommon federated identity services while preserving student confidentiality and privacy.	• Dependent upon University Policy, and relationships between services & institutions • Awaiting further maturation • Engage InCommon community