



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

15 January 2016

Chairs:

Mark Cather, UMBC

Scot Ransbottom, Va. Tech

Donna Tatro, Princeton

INTERNET²

POWERED BY
COMMUNITY



Meeting Objectives

- E2ET&S Working Group Plan Update
- E2ET&S for IoT Workshop Update – February 4, 2016
- Launching the Smart Cities/Smart Campus Focus Group
- E2ET&S Focus for 2016
- 2016 Plans and Next Steps

INTERNET[®]
2

POWERED BY
COMMUNITY



E2ET&S Use Cases and Plans (Page 1 of 3)

Initiative/Use Case	Description	Plan
End to End Trust & Security Open Architecture for IoT	Create a point of view and recommended next steps to develop a comprehensive End to End Trust & Security Open Architecture for the Internet of Things	<ul style="list-style-type: none"> February 4, 2016, workshop in cooperation with IEEE, NSF, and George Washington University
Network Segmentation for IoT	Use of network segmentation to ensure additional IoT connected devices don't undermine overall network security; Cisco blog post in <i>The Security Ledger</i> http://bit.ly/1A1acwI	<ul style="list-style-type: none"> Scheduling webinar with Scott Harrell, Cisco VP Product Management, Security Business Group early 2016 to increase awareness within the Community Webinar likely 2/2 at 3PM ET
Easily provision strong credentials in the form of a virtual campus ID card backed by a set of high-assurance personal X.509 certs	Mobile device as central access to all aspects of a campus – physical and digital. Multi-layered security required for a secure environment: biometric, PIN, device encryption. Applied at all levels within a campus: student, faculty, and administration. Has the potential to be applied in the commercial world: hospitality, retail, benefits, etc.	<ul style="list-style-type: none"> Engage interested campuses to determine requirements for solution Agree actions, maybe engage vendors? Identify testbed campuses Integrating with Smarter Cities/Campus Pilot Group
Improved interoperability among university and hospital networks	Consider use of Security Group Tags and Cisco's TrustSec policy management framework to integrate "cyberinfrastructure islands"	<ul style="list-style-type: none"> Identify universities with academic medical centers to discover needs and create potential solutions

E2ET&S Use Cases and Plans (Page 2 of 3)

Initiative/Use Case	Description	Plan: Connecting with Other Initiatives
IPsec and Identity based firewalls	Develop an 'Identity Based Firewall' technology based on the identity of authorized people rather than on the IP numbers of their devices.	<ul style="list-style-type: none"> • 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	Need for international cross-access permissions amongst universities, fine arts institutions, and research institutions to have a unified ID system utilizing existing secure credentials	<ul style="list-style-type: none"> • Potential to combine with IPsec & ID-Based Firewalls • InCommon is working on portions with International Federations • Opportunity to link with the Digital Humanities focus of DBDA
External access to "research zone" systems	Subset of the above. Need for international cross-access permissions amongst universities, fine arts institutions, and research institutions to have a unified ID system utilizing existing secure credentials	<ul style="list-style-type: none"> • Potential to combine with IPsec and Identity Based Firewalls • InCommon is working on portions with International Federations • Opportunity to link with the Digital Humanities focus of DBDA




E2ET&S Use Cases for Future Action (Page 3 of 3)

Initiative/Use Case	Description	Plan
Software Defined Perimeter (SDP)	Leverage SDP (Software Defined Perimeter) against real life attack scenarios to provide the highest level of security for cloud, mobile computing, and IoT applications	<ul style="list-style-type: none"> • SDP Webinar held 9/1/2015 • SDP session held at SC15 • Opportunity to work with Cloud Security Alliance (CSA) on SDP Spec V2
Plan: Connecting with Other Initiatives		
Security for web-based mobile applications	Adding support for OpenID Connect to Shibboleth IdPv3 would allow secure authentication for mobile applications, and enhance end to end security	<ul style="list-style-type: none"> • Connected with the University of Chicago's project currently underway • Awaiting further maturation • Engage the TIER community for additional support
Preserving student privacy while enabling use of InCommon federated services	Allow students to access InCommon federated identity services while preserving student confidentiality and privacy	<ul style="list-style-type: none"> • Dependent upon University Policy, and relationships between services & institutions • Awaiting further maturation • Engage InCommon community for additional support



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

- **2 day event at the George Washington University Marvin Center in Washington, DC in conjunction with IEEE, NSF, and George Washington University**
 - Day 1, February 4, 2016: Deep technical workshop on E2ET&S for IoT open architecture needs, viewpoints, use cases
 - Day 2, February 5, 2016: IEEE ETAP ([Experts in Technology and Policy](#)) – *IEEE Invitation Only*
- **Goal:** 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, identified research challenges, and point of view with recommended next steps.
- **Target audience of 100 to 150 attendees:** Universities, Agencies, IoT related Standards Organizations, U.S. Regional Research & Education Networks, Industry Players, Internet2 staff and Collaborative Innovation Community
 - Over 130 registrant requests and interest expressed by about a dozen for paper submissions
- **Updated Agenda available on the event website** <http://bit.ly/1RG95Jo>
- **Interested in attending?** <http://bit.ly/1Rb29p7>
- **Interested in submitting a paper? Send via email by January 15:** d.ceruto@ieee.org

POWERED BY
COMMUNITY



Launching Smart Cities/Campus Pilot Group

- **Tentative Goal:** Identify current best practices and develop next practices, use cases, and innovations in Smart Cities/Campus testbeds. 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 January 2016, followed by regular cadence of collaborative calls
- **Inaugural Participants:**



Others Interested? Email Emily Nichols
enichols@Internet2.edu

INTERNET²

POWERED BY
COMMUNITY



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: IoT, Smart Campus/Cities, HCLS, and coherent trust & identity protocols across multiple enterprises and networks**

INTERNET[®]
2

POWERED BY
COMMUNITY



Collaborative Innovation Community Operations

Timeline: 2016 – We evolve and grow

1H

- E2ET&S for IoT workshop(s)
- Smart Grid testbed planning
- Smart Campus focus group
- Expand IoT Sandbox
- Develop Healthcare/Life Sciences (HCLS) strategy
- Increase researcher engagement
- Develop DBDA Digital Humanities/Humanists strategy
- Continue education & awareness for new innovation opportunities

2H

- Assess/extend Sandbox approach
- Smart Grid testbed
- Smart Campus enablement
- Continued IoT and DBDA strategy development
- E2ET&S collaboration across extended community
- HCLS strategy execution
- DBDA Digital Humanities strategy continuation
- Constant market insight gathering
- Innovation input from community

Ongoing Community Input

INTERNET[®]

POWERED BY
COMMUNITY



E2ET&S Innovation Working Group Next Steps

- Register to attend the E2ET&S for IoT Workshop, presentation submissions due January 15th , 11:59pm ET
- Smart Cities/Campus focus group participation – let us know if you want to participate or have potential use cases
- E2ET&S for Healthcare and Life Science (HC/LS)
 - Improved interoperability among university and hospital networks
 - Identify universities with hospitals/AMCs to participate in discussion
 - Let us know if you want to be involved in this discussion
 - Internet of Medical Things

INTERNET[®]
2

POWERED BY
COMMUNITY



Questions & Answers...
Thank You
e2etschairs@Internet2.edu
CINO@Internet2.edu
[@FIInternet2](https://twitter.com/FIInternet2)
[@EmilyNInternet2](https://twitter.com/EmilyNInternet2)



INTERNET[®]
2

POWERED BY
COMMUNITY

