INTERNET2®

2015 TECHNOLOGY exchange

OCTOBER 4–7
CLEVELAND OH

END-TO-END TRUST & SECURITY (E2ET&S): INNOVATION WORKING GROUP MEETING

FLORENCE HUDSON
Senior Vice President & Chief Innovation Officer

EMILY NICHOLS
Innovation Program Manager

INTERNET2

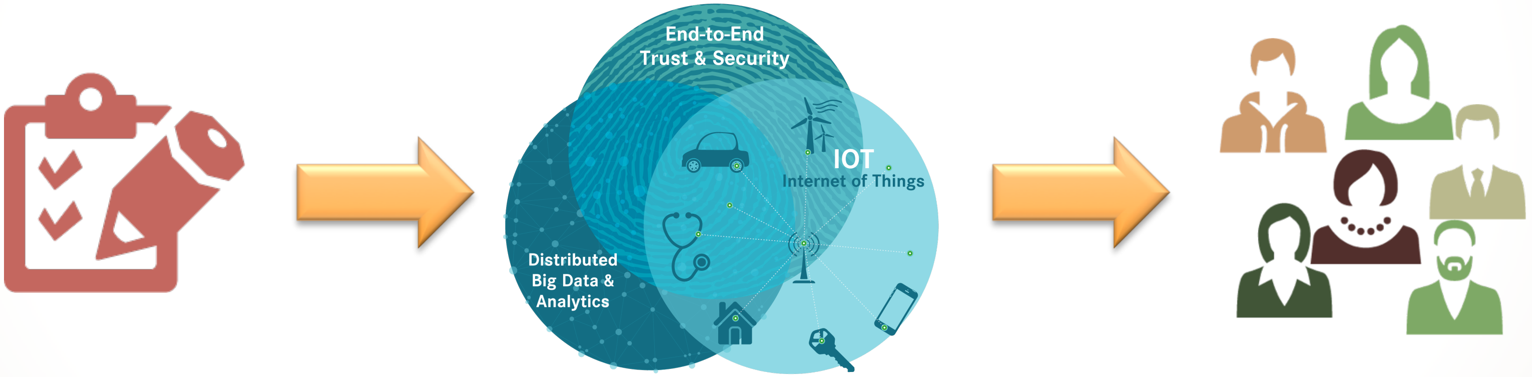
E2ET&S: INNOVATION WORKING GROUP MEETING

AGENDA

- Welcome and Introductions
  - Review of the Collaborative Innovation Community
- Status of Current Plans & Next Steps
- Other Innovations
- Closing

Collaborative Innovation Program

Established three new Collaborative Innovation Working Groups based on March 2015 Member Survey



End-to-End Trust & Security

IOT Internet of Things

Distributed Big Data & Analytics

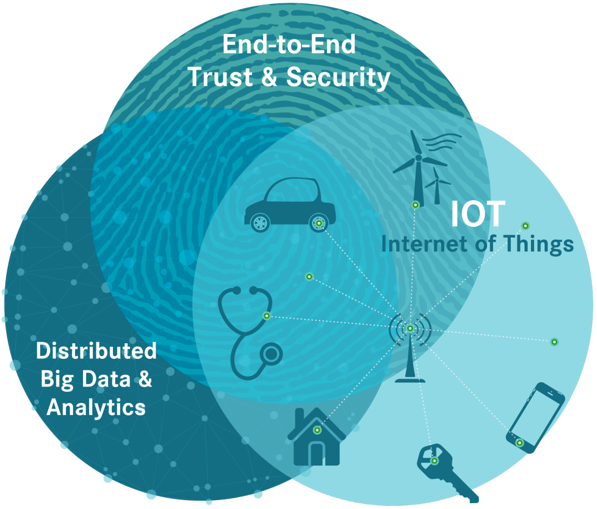
Collaborative Innovation Program Current Focus Areas

E2E Trust & Security:

- End to End Trust and Security for IOT
- TIPS – Trust, Identity, Privacy & Security
- SDP (Software Defined Perimeter), Network Segmentation

Distributed Big Data & Analytics:

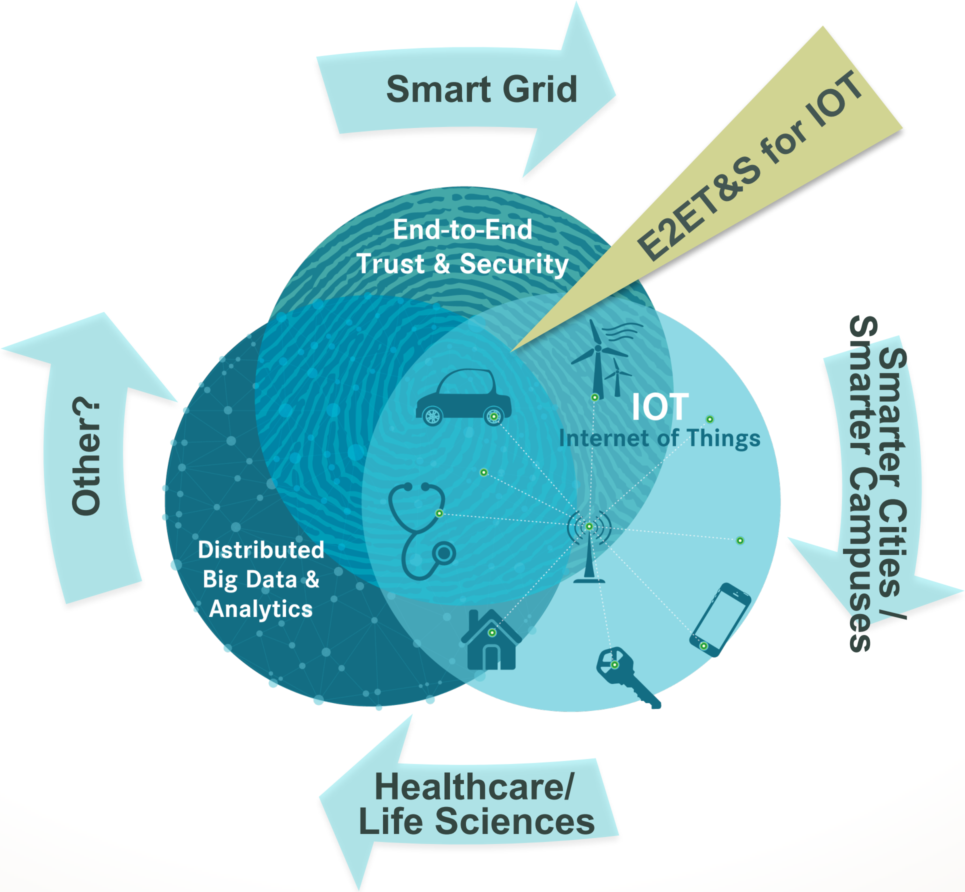
- Genomics
- Smarter Cities / Smarter Campuses
- Digital Humanities



Internet of Things:

- IOT Sandbox
- Smarter Cities / Smarter Campuses
- Smart Grid Testbed

Members Can Participate in Collaboration Opportunities Across the Collaborative Innovation Community Working Groups



Smarter Cities and Healthcare/Life Sciences are beacons of the future economy, and will provide the use cases that bring new applications and technologies to life

Smarter Cities

- **Grid**
- **Campus**

Healthcare/ Life Sciences

Collaborative Innovation Program Working Group: E2ET&S

Co-Chairs

- Mark Cather, University of Maryland, Baltimore County
- Mary Dunker, Virginia Tech
- Donna Tatro, Princeton University

80+ Members Representing Universities, Industry, Affiliates, Regional & International R&E Networks

Scope:

- *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.*

The Vision for E2ET&S Innovation Working Group

Distribute Security Functionality to the Edge with Central Management

- We are seeing the following trends:
  - The number of connected devices and volume of data to store and process continue to grow rapidly
  - The data processing and storage will continue to become more and more distributed
- We must distribute our security and privacy infrastructure to the endpoints to address these trends
- Even though the trends may require the distribution of our security infrastructure to the endpoints, political and contractual requirements will require the centralized management of security and privacy policy

Scope of what E2ET&S could address…

- **Contexts & Security Architecture**
  - People belong to multiple societal contexts, restricted by IT systems configured for only one context
  - Maintaining and using separate, disparate solutions for each context difficult
  - Multi-device use requires different security and privacy policies for each context within a device
  - System Virtualization technologies and SDN may be useful to securely and dynamically link contexts between systems
- **Middleware (MW) and Encryption**
  - MW could allow authentication to any end point and securely access all contexts
    - MW to manage details for each context and distribute details to each participating endpoint
    - MW, like TIER, needed to authenticate and authorize a person to each of their contexts.
    - MW to manage encryption of system processing, storage, and communications channels
  - Encryption key to maintain security: data in transit and within system context
- **What's Next? Possible Technologies On the Path to the Vision**
  - Chip technology to distribute security processing / filtering to the end point NIC
    - Ex: 10GE / 100GE NIC with Line-Rate Intrusion Prevention and Firewall on the NIC
  - Standards based protocols for distributing security and privacy rules to end points
  - Virtualization by context rather than virtual host
  - Software Defined Networking by context
  - Dynamic encryption of communications channels between end points
  - Encryption of data while stored and processed within a context on an end point

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

- Thank you to our members for submitting use cases – Brown University, Clemson University, MCNC, North Dakota State University, University of Pittsburgh, Virginia Tech

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	• SDP Webinar 9/1/2015 • Opportunity to work with Cloud Security Alliance (CSA) on SDP Spec V2
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 academic medical centers to discover needs and create potential solutions
Network Segmentation for IOT	Use of network segmentation to ensure additional IOT connected devices don't undermine overall network security; Cisco blog post in *The Security Ledger* http://bit.ly/1A1acwl	• Identify experts, prepare potential whitepaper or webinar • Increase awareness
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	• Develop proposal for a workshop in 1H16 in cooperation with NSF, NIST, IEEE, DHS, OSTP, IIC

End-to-End Trust & Security

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

Initiative/Use Case	Description	Plan
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.	• 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	• 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
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	• 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 and Plans (Page 3 of 3)

Initiative/Use Case	Description	Plan
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	• Connect with the University of Chicago's project currently underway • 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	• Dependent upon University Policy, and relationships between services & institutions • Engage InCommon community for additional support
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.	• Identify campuses interested in capability • Determine requirements for solution • Identify testbed campuses • Opportunity to integrate with Smarter Cities / Campus initiative

Workshop Proposal: “End to End Trust & Security Open Architecture for the Internet of Things”

- **Goal:** 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

- **Outcomes:** Report and initial plan on the definition and scope of an open architecture for End to End Trust and Security for IOT, and next steps to enable the development of this architecture, across the ecosystem

- **Participants:** Attendees from U.S. based Universities, U.S. Government Agencies (e.g., NIST, NSF, OSTP, DHS), U.S. Regional Networks, Industry Members, IOT standards bodies (e.g., IEEE, IIC), and Internet2 staff
  - Want to participate? Send email to CINO@Internet2.edu

Brainstorm Other E2ET&S Innovations

- End to End Trust and Security for IOT
- TIPS – Trust, Identity, Privacy & Security
- SDP, Network Segmentation
- The use cases just reviewed
- What's missing?

- OSU – Cross collaboration of data sets: data obfuscation – not scalable, disparate data solutions. Solution or protocol?
  - Nick L. DHI, differentiate amongst the data sets
- MEMS
- PCI, Tokenization: data benefits AND regulatory compliance
- Working group: privacy & the data the flows up from HC/LS, IOT related info, beyond climatology, etc – longer term horizon, applied research
- As data grows from IOT, HC/LS, will need to look at privacy
- Insider threat issues & how to deal with for sensitive research
  - Internet2 Working Group on Security focused on Ddos, likely to go further & look at the perimeter
  - IBM speaker on pattern recognitions

Forge Rock Industry member doing work on SmartGrid & Smart Cities, how to align with IOT

One last thing…

Security Incident and Assurance in FIM
Licia Floria, GEANT Association
TODAY, 11:20AM-1:00PM
Room 13

Closing: How You Can Get Involved

- **Interested in participating in the E2E Trust and Security Open Architecture for IOT workshop?**
  - Let us know! Email CINO@Internet2.edu
- **Does your University include an Academic Medical Center?**
  - Participate in our upcoming case study on interoperability among university and hospital networks
  - Email CINO@Internet2.edu
- **Provide feedback on the Smart Grid white paper**
  - http://bit.ly/1iJ0N5V
  - Email CINO@Internet2.edu
- **Know an SDP or Network Segmentation expert?**
  - Let us know! Email CINO@Internet2.edu
- **Join the E2ET&S Working Group**
  - Email CINO@Internet2.edu
- **Check out our Wiki for more detailed E2ET&S information:**
  - http://bit.ly/1PJgRiP

Collaborative Innovation Program

E2ET&S Co-Chairs

e2etschairs@Internet2.edu

Florence Hudson

CINO@Internet2.edu
fhudson@Internet2.edu
@FloInternet2

Emily Nichols

CINO@Internet2.edu
enichols@Internet2.edu

INTERNET2®

2015 TECHNOLOGY exchange

OCTOBER 4-7
CLEVELAND OH

END-TO-END TRUST & SECURITY (E2ET&S): INNOVATION WORKING GROUP MEETING

FLORENCE HUDSON
Senior Vice President & Chief Innovation Officer

EMILY NICHOLS
Innovation Program Manager

INTERNET2