End to End Trust & Security

Internet2 CINO Initiative Working Group Kickoff Meeting

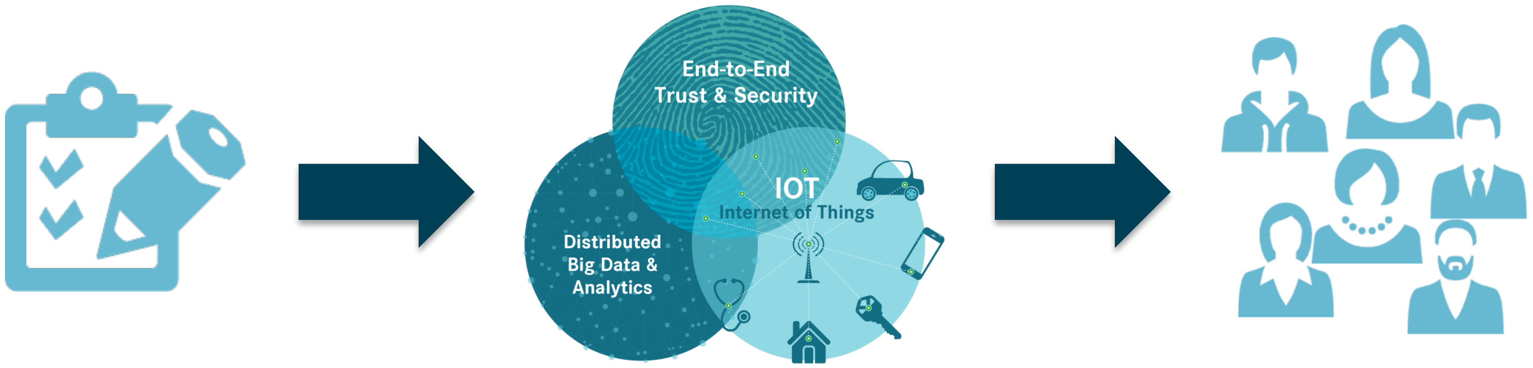
May 26, 2015

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

End-to-End
Trust & Security

Collaborative Innovation Program

Three new collaborative
Innovation Working Groups



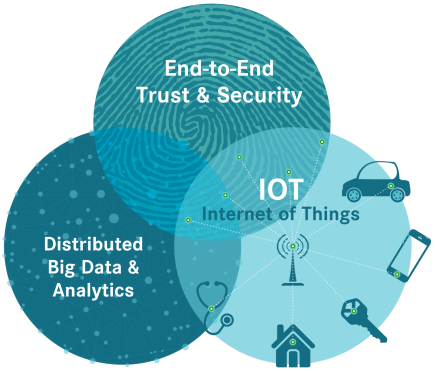
End-to-End
Trust & Security

IOT
Internet of Things

Distributed
Big Data &
Analytics

Establishing Three New Collaborative Innovation Working Groups

- Each will formulate specific recommendations for a particular innovation initiative, including scope, value, milestones
  - Clarify value to members
  - Ensure the innovation is economically viable
  - Develop a scalable model to positively impact a significant segment of Internet2 membership
- Led by member representatives
  - May leverage member programs and facilities
  - Participation encouraged for all Internet2 members
- Working groups will operate within a broader Internet2 Collaborative Innovation Community with representatives from member organizations



End to End Trust & Security Working Group Kickoff

- Goals of the kickoff call today
  - Discuss the mission, scope, schedules, and operations of this working group
  - Discuss major developments and trends that form the context for the working group activities – concepts to consider when formulating possible subgroups or projects
  - Gather your input on the plans for this WG as discussed in this material today
- Next steps
  - Email your input by June 1, 2015 to WG chairs at e2etschairs@internet2.edu
  - You can offer to lead potential sub-groups based on topical areas for E2ET&S
  - WG chairs will pull together your recommendations for review and agreement on our next call
- E2ET&S Working Group Chairs
  - Mark Cather, Chief Information Security Officer - University of Maryland, Baltimore County
  - Scot Ransbottom, Chief of Staff, Deputy CIO - Virginia Tech
  - Donna Tatro, Associate CIO and Director, Enterprise Infrastructure Services - Princeton

Introduction

The need exists in Research and Education networks for scalable and extensible approaches to integrating capabilities for trust, identify, privacy, security, and compliance beyond individual enterprise networks.

WG recommendations may include establishing a group to create software and/or services which address end-to-end security, privacy, and/or identity for the research and education community's specific requirements..

- Potential Use Cases may include:
  - Protection of sensitive and regulated research data
  - Mitigation of risks to enterprise administrative operations
  - Material for new educational programs

Mission and Scope

- Mission
  - Develop an architecture and implementation approach to enable “End-to-End Trust & Security” for the Research & Education community.
- Scope of Activities
  - Formulate specific recommendations for End-to-End Trust & Security innovation initiative
  - Identify and develop feasible recommendation(s) for review by Internet2 community that are informed by current state of the art trust and security technical, policy and process operational and research
  - Coordinate and differentiate innovative initiative with ongoing TIER WG
  - Engage in formal and informal collaborations with Internet2 members. These collaborations may include research, pilot implementations, standards development, policy development, etc.

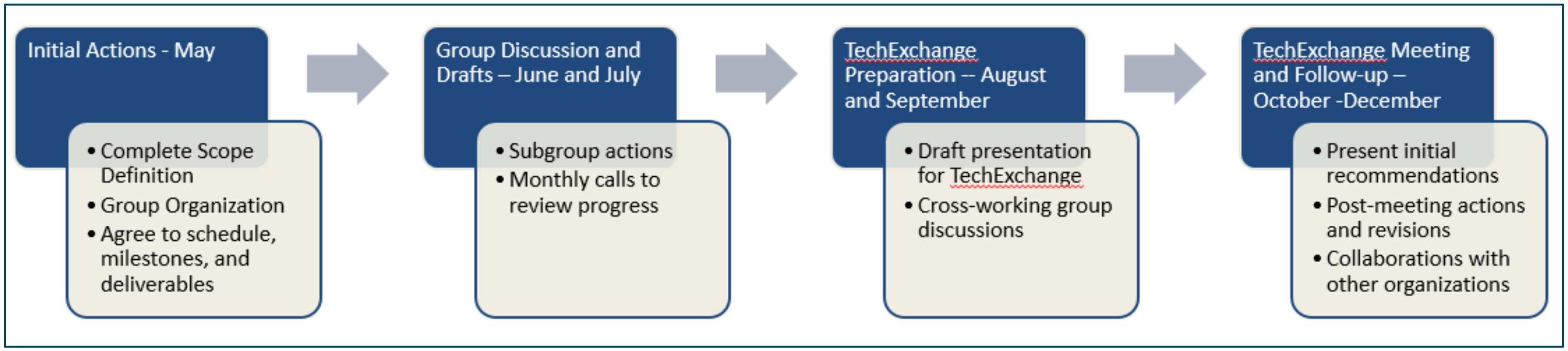
Working Group Operations

- Operating principles – open membership, open meetings, open source results
- Make maximum feasible use of available prior related work
  - In particular, close coordination with InCommon, TIER, and Internet2 CCSO
  - Representatives from these activities are participants in this working group
- Working group deliverables
  - List of projects to include owners, expectations, and timelines.
  - Develop and publish white papers and standards for use cases, research and implementation of End-to-End Trust & Security

Working Group Communications

- Communications
  - Monthly meetings with teleconference capabilities – held in various locations
  - Mailing list for email communications to entire E2ET&S working group – cino-e2e@internet2.edu
  - Mailing list for chairs of E2ET&S working group - e2etschairs@internet2.edu
  - Wiki site for collaborative work - https://spaces.internet2.edu/x/jYdHBQ
  - Bi-monthly meetings with all CINO working groups aka Collaborative Innovation Community
  - In-person meetings and presentations at related events (e.g., at TechEx in Ohio in October 2015)

Working Group Operations Timeline



Initial Actions - May

- Complete Scope Definition
- Group Organization
- Agree to schedule, milestones, and deliverables

Group Discussion and Drafts – June and July

- Subgroup actions
- Monthly calls to review progress

TechExchange Preparation -- August and September

- Draft presentation for TechExchange
- Cross-working group discussions

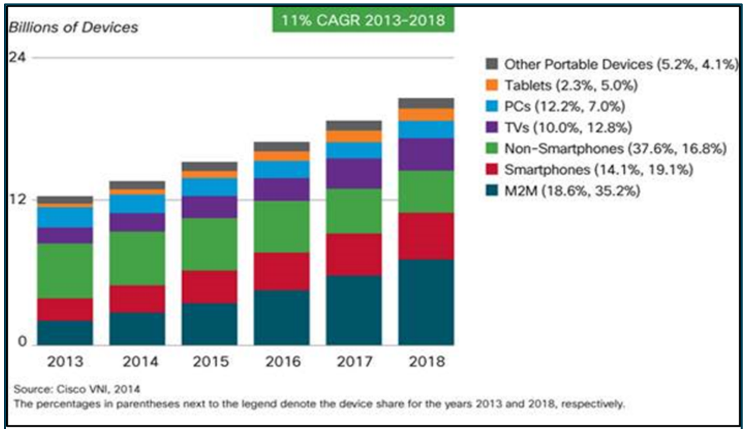
TechExchange Meeting and Follow-up – October -December

- Present initial recommendations
- Post-meeting actions and revisions
- Collaborations with other organizations

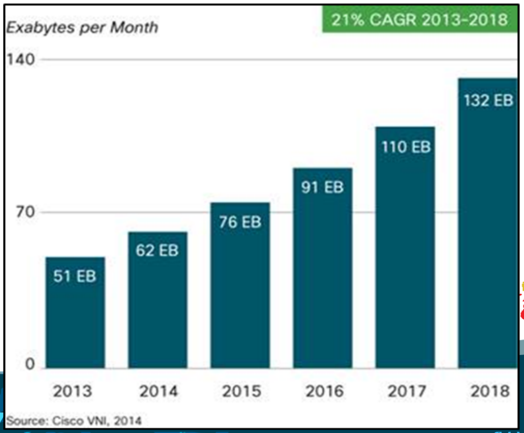
- June 1: Need your input to agree to scope, schedule, milestones, and deliverables
- Plan to present initial results at the October Technology Exchange (TechEx) Meeting
- Recommendations may include
  - Creating an approach to build an end to end platform with community-acceptable capabilities for trust, identify, privacy, security
  - Creating educational material
  - Proposing research projects
- Considerations for innovation planning
  - What could we do that is not being addressed elsewhere?
  - What types of resources would be required and how might we get them?
  - Why is the Internet2 community the right place for this activity?

Context for Working Group Actions – Key Trends

- Growth and distribution of devices and data
  - The number of connected devices and volume of data to store and process will continue to grow rapidly
  - Globally, devices and connections (10.7% CAGR) are growing faster than the population (1.1% CAGR)
  - Annual global IP traffic will pass the zettabyte (1000 exabytes) threshold by YE2016, and will reach 1.6 zettabytes per year by 2018
  - 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*



Source: Cisco VNI, 2014
The percentages in parentheses next to the legend denote the device share for the years 2013 and 2018, respectively.



Source: Cisco VNI, 2014

Context for Working Group Actions - Convergence

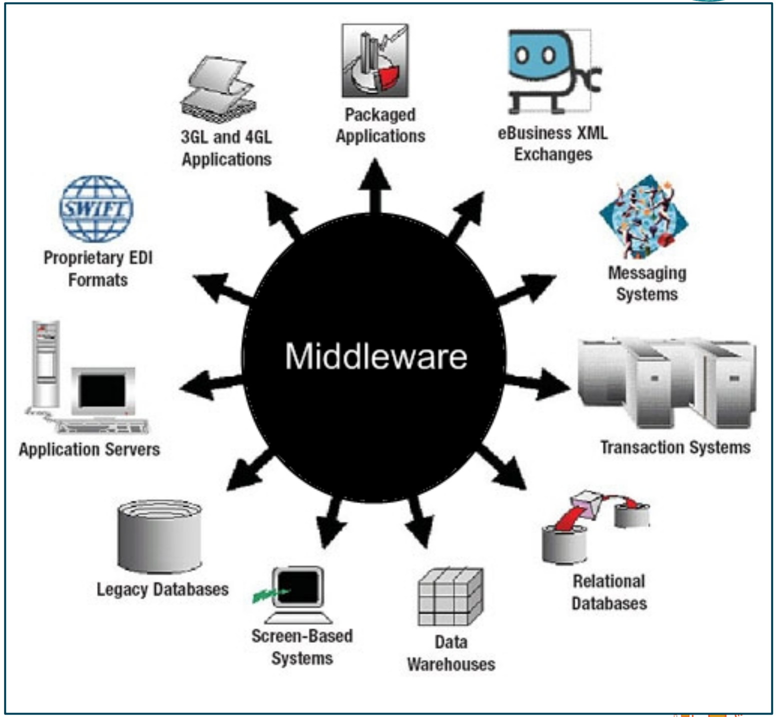
- Many early attempts to integrate multiple profiles into single devices
  - BYOD is one of many examples
- Need to meet requirements of different security and privacy policies for each context within a device.
  - Virtualization may help
- SDN may be a useful way to securely and dynamically link contexts between systems
  - Devices will be connected to many other SDN networks for each context on each device

kindle FreeTime
Multiple Profiles
Multiple WhatsApp Accounts
NOW USE MULTIPLE WHATSAPP ACCOUNTS IN SINGLE ANDROID DEVICE...
Multiple Clash Of Clans Accounts In 1 Device
Cancel
Okay
B.Y.O.D.
(Bring Your Own Device)

Context for Working Group Actions - Middleware

End-to-End Trust & Security

- Robust middleware layer required to manage details for each context
  - Distribute details of each context’s security and privacy policies to participating endpoints
- Middleware, like TIER, will be needed to authenticate and authorize a person to each of their contexts.
- Encryption will be a key requirement for maintaining the security of all data
- Middleware needed to manage encryption of processing, storage, and communications
- A future robust middleware layer could allow anyone to authenticate to any end point and securely access all contexts anywhere.



Context for Working Group Actions – What's next?

End-to-End Trust & Security

- Chip technology to distribute the 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
- TIER / Federated authentication & authorization to contexts
- Global PKI to manage data encryption on communications channels and within contexts

Challenges to Address – Innovations Needed

End-to-End Trust & Security

- Distributed security and privacy infrastructure with centralized management
- Linking contexts and devices to meet federated trust, identify, security and privacy (TIPS) policies and needs
- Use case specific needs – e.g., Healthcare IT with HIPAA
- Need for an open and extensible end to end trust and security architecture
  - From chip to device to network to cloud
  - Hardware, firmware, software, service levels of security
  - Device and data level security

Next Steps

- Provide feedback on scope, schedule, deliverables, milestones, sub-groups/ projects by June 1 to e2etschairs@internet2.edu
- Provide input and offer to lead/participate in sub-groups/projects. Initial ideas:
  - Distributed security and privacy with centralized management
  - Cloud services for E2ET&S
  - Healthcare IT E2ET&S
  - High performance e2e trust and security needs – Internet2 network, big data, Physics, Genomics…
  - TIPS architecture - Open and extensible end to end architecture for Trust, Identify, Privacy, Security
  - Other possibilities
- Next meetings --
  - Monthly team meeting – next one late June
  - Joint Collaborative Innovation Community call with all 3 working groups bi-monthly

Thank You