End to End Trust & Security

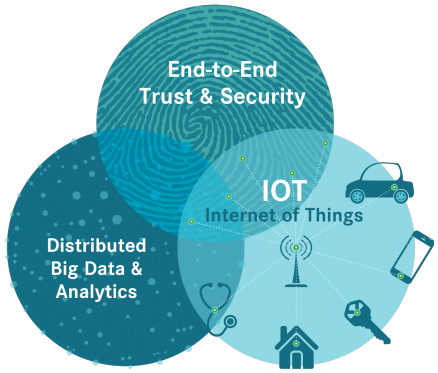
Internet2 CINO Initiative Working Group Meeting #2

June 22, 2015

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

Established Three 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 Mission, Scope, Deliverables

- Mission
  - Develop an architecture and implementation approach to enable “End-to-End Trust & Security” for R&E community.
- Scope of Activities
  - Identify and develop feasible recommendation(s)
  - Engage in formal and informal collaborations with Internet2 members and partners, which may include research, pilot implementations, standards development, policy development, etc.
- Deliverables
  - List of projects based on use case and project input from WG to include owners, expectations, timelines
  - Develop and publish white papers and standards for use cases, research, implementation of E2ET&S
  - Recommendations which may include establishing a group to create software and/or services which address end-to-end security, privacy, and/or identity for the R&E community’s specific requirements

Goals of E2ET&S Meeting June 22, 2015

- Review the use cases submitted by working group members
- Discuss and capture potential additional use cases from working group members
- Discuss draft “categories” and maturity model for end to end trust & security use cases
- Gather your input on the plans for this WG as discussed in this material today

- Discuss Next steps
  - Email your input to WG chairs at e2etschairs@internet2.edu
  - You can offer to lead potential sub-groups based on topical areas and use cases for E2ET&S
  - WG chairs will pull together your recommendations for review and agreement on our next call

Use case input from the working group – Page 1 of 2

Use Case #	Use Case Title	Summary Comments	Name	Institution
1	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.	Mary Dunker	Virginia Tech
2	Preserving student privacy while enabling use of InCommon federated services	Allow students to access InCommon federated identity services while preserving student confidentiality and privacy.	Mary Dunker	Virginia Tech
3	Assign, manage, and revoke permissions on a platform to support collaborative work	The Center is kicking off a three year project funded by US/NEH and by the European Commission. Representative of many other research community use cases.	Steve Carmody	Brown
4	External access to "research zone" systems	The Center wants their external partners to be able to do this using Federated Authentication. They do NOT want to have to issue local credentials to people based at other campuses.	Steve Carmody	Brown
5	Improved interoperability among university and hospital networks	Possible use of Security Group Tags and Cisco's TrustSec policy management framework to integrate "cyberinfrastructure islands"	Brian Stengel	University of Pitt

Use case input from the working group – Page 2 of 2

Use Case #	Use Case Title	Summary Comments	Name	Institution
6	Campus-Based Computational Research Support	Funded NSF project at U.Utah and Clemson. By building a cloud-like environment for advanced computing and infrastructure support, the project seeks to create a community that fosters seamless integration of cyberinfrastructure and domain researchers and expand the reach of researchers involved in the use of advanced cyberinfrastructure across campuses. (www.nsf.gov -- Award Abstract #1341935)	Jill Gemmill	Clemson
7	Network Segmentation for IoT	Blog post from Cisco available at https://securityledger.com/2015/01/why-network-segmentation-is-imperative-on-the-internet-of-things/. Relevant to IoT and E2ET&S discussion.	Chris Beal	MCNC
8	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 the Internet of Things applications.	Bruce Curtis	North Dakota State Univ.
9	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.	Bruce Curtis	North Dakota State Univ.
10	Easily provision strong credentials in the form of a **virtual campus ID card** backed by a set of high-assurance personal X.509 certs	Uses include: Authentication (private, non-escrowed key) ; Encryption (escrowed private key); Signing (private, non-escrowed key). All certs should be protected by a user-selectable and changeable PIN. Can be used to sign, encrypt and authenticate to systems via ISO/IEC 14443 near-field communication identity card protocols, provide similar functionality to a PIV-I card. Able to be used for all of the functions outlined above at a workstation, other mobile device, or via interaction with "proximity" door access panels. **VA Tech experience:** Virginia Tech's InCommon Silver credential is an X.509 certificate on a USB hardware token validated at FIPS 140-2 level 2. See http://www.incommonfederation.org/assurance/approved/20131022-1.1-AM.pdf	Nick Roy	Internet2 now (was at Penn State and University of Iowa)

DRAFT E2ET&S "Categories" and Maturity Model

(Includes E2ET&S Use cases 1-10)

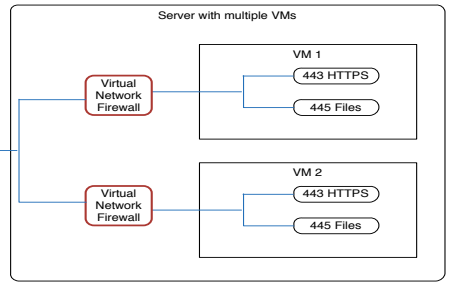
EETS Architecture "Categories"	Mature Technologies / Capabilities	Nascent Technologies / Capabilities	Future
A - Distributing Security Capabilities / Filtering to the Endpoint	• Traditional Network Security Models	• Software-Defined Networking	• (10) Virtual Campus ID Card
B - Partitioning of Devices by Context		• Docker application containerization • Mobile virtualization • Device containerization	• (7) Network segmentation for IOT
C - Contexts and Peer Relationships Drive Security Architecture	• Direct trust relationships between and among campus networks		• (3) Assign, manage, and revoke permissions to support collaborative work • (5) Improved interoperability among university & hospital networks • (8) Software-Defined Perimeters
D - Middleware / AAA of IT Resources and People by Context	• InCommon	• TIER	• (1) OpenID • (2) InCommon Student Confidentiality • (4) External access to "research zone" systems • (6) Campus based computational research support • (9) Identity Based Firewall
E - Internet2 "S"		• Virtual dark fiber	

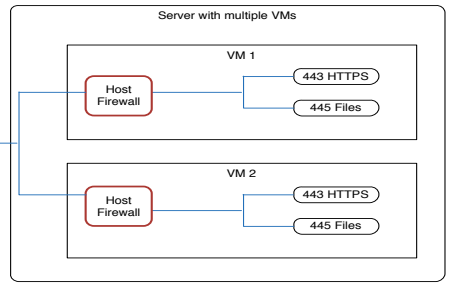
Sample Use Case Template: IPsec and Identity Based Firewalls

- **Concept**: Develop an 'Identity Based Firewall" technology based on the identity of authorized people rather than on the IP numbers of their devices. This host based firewall would be a standard part of Operating Systems that could attach something smaller than a full IP header (bloated with redundant source and destination addresses etc. in every packet) to each packet that could be used to verify that the packets came from devices operated by authorized users.
- **Value proposition:** Such a technology would have been largely immune to both heart bleed & shellshock, only being vulnerable to packets from devices operated by authorized users, & would be totally immune to poodle since poodle depends on a man-in-the-middle attack.

Details:

- Diagram 1 – A virtual firewall in front of every virtual server. When a VM is moved to a different server the virtual firewall must be moved with the VM.
- Diagram 2 - It is logically equivalent to just have a host firewall on the VM. The host firewall blocks packets from arriving at the software listening on the illustrated port 443 just as well as the virtual firewall, and the host firewall has less administrative overhead.
- Basing security on IP numbers does not scale and continues to become more difficult as devices become more mobile, easily switching between IP numbers on numerous WiFi and Cellular networks. (And with MPTCP even using multiple IP numbers at once.)





- **References**: Social or P2P VPN, e.g. Hamachi and Pertino. (see use case in notes)
- **Contact**: Bruce Curtis, North Dakota State University, Certified NetAnalyst II, bruce.curtis@ndsu.edu

Next Steps

- Provide input & offer to lead/participate in sub-groups/projects for use cases
  - Submit additional use cases using the sample use case template in this deck
  - Email your input and offer to lead a sub-group or project to either:
    - Entire E2ET&S working group – cino-e2e@internet2.edu
    - Chairs of E2ET&S working group - e2etschairs@internet2.edu
  - Wiki site for collaborative work - https://spaces.internet2.edu/x/jYdHBQ

- Next meetings --
  - Monthly team meeting – next one late July
  - Joint Collaborative Innovation Community call with all 3 working groups this summer
  - In person workshop at TechEx in Cleveland Oct 4-7, 2015

Thank You

End-to-End Trust & Security

INTERNET2®

POWERED BY COMMUNITY

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
  - 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

Sample Use case Template: SDP (Software Defined Perimeter)

Concept: Leverage the multi-layer SDP (Software Defined Perimeter) security model against real life attack scenarios to provide the highest level of security for cloud, mobile computing and the Internet of Things applications.

Value Proposition: Identify and enable SDP capabilities and services collaboratively for Internet2 members, to provide the highest level of security for cloud, mobile computing and the Internet of Things applications.

Details: The SDP Hackathon Results Report Whitepaper provides a detailed explanation of the SDP concept, its multiple layers of security controls, and the results of the hacking contest. The Hackathon, announced by Alan Boehme of Coca Cola at the CSA Summit at RSA 2014, invited hackers worldwide to attack a server defended by the SDP. While more than 10 billion packets were fired at the SDP from around the world, no attacker broke through even the first of five layers of security controls specified by the SDP architecture.

"The Hackathon provides critical validation for the multi-layer SDP security model. Even after 10 billion attack packets, no one was able to crack even the first layer of SDP security controls during the event," said Junaid Islam, co-chair of the SDP Working Group and CTO of new CSA corporate member Vidder, Inc. "It's the goal of this research initiative to keep testing SDP against real life attack scenarios to provide the highest level of security for cloud, mobile computing and the Internet of Things applications."

References

- https://cloudsecurityalliance.org/research/sdp/#_overview
- https://downloads.cloudsecurityalliance.org/initiatives/sdp/SDP_Specification_1.0.pdf
- https://cloudsecurityalliance.org/research/sdp/#_downloads
- https://cloudsecurityalliance.org/media/news/cloud-security-alliance-releases-update-to-software-defined-perimeter-sdp/
- https://cloudsecurityalliance.org/media/news/csa-software-defined-perimeter-details/

Contact: Bruce Curtis, North Dakota State University, Certified NetAnalyst II, bruce.curtis@ndsu.edu

Comments for DRAFT E2ET&S Classification and Maturity Model

Docker application containerization	Docker containers wrap up a piece of software in a complete filesystem that contains everything it needs to run: code, runtime, system tools, system libraries – anything you can install on a server. *https://www.docker.com/whatisdocker*
Mobile virtulization - device containerization	Mobile OS virtualization can divide one smartphone into multiple virtual smartphones. Since instances run within their own namespace, they are secure and scalable, and they preserve the overall user experience. *http://www.networkcomputing.com/wireless-infrastructure/mobile-virtualization-the-future-of-security/a/d-id/1318324*
Software-defined perimeters	The Software Defined Perimeter creates a cryptographic perimeter for each protected application so that applications only receive traffic from authenticated and authorized users whose device, software, and location have been pre-validated and deemed acceptable. Such end devices are given a unique and temporal cryptographic connection to an obfuscated location that houses the protected application. The service is not visible to any other traffic. *https://cloudsecurityalliance.org/research/sdp/#_overview*
OpenID	OpenID is an open standard and decentralized protocol by the non-profit OpenID Foundation that allows users to be authenticated by certain co-operating sites (known asRelying Parties) using a third party service. This eliminates the need for webmasters to provide their own ad hoc systems and allowing users to consolidate their digital identities. *http://openid.net/*
Virtual dark fiber	Virtual dark fiber is a layer 1 service developed by Internet2. VDF provides nearly all the advantages of a completely private dark-fiber network: traffic isolation, scalability, flexibility and control, with a cost and management profile that is closer to that of a lit circuit service. With the VDF architecture, Internet2 consortium members acquire and manage their own premise optical network systems (terminals); once connected through their own terminal infrastructure, an Internet 2 member injects its traffic into the Internet2 optical system at the photonic level as a specific optical channel or frequency for transmission, bypassing any of the Internet2 equipment and systems that could either detect data or control traffic.

DRAFT Potential Categories of E2ET&S Innovations

SDN/Software controlled delivery of trust and security configs

Docker/Containers

Other trust and security components

Authorization Services

Authentication Services

Internet2 “s”