Internet2 Security Activities: The Security Fruitcake

Rev. 24-July-2006

Traditional Internet2 Security Goals

- Advanced network security
  - Security on advanced networks
  - Advanced applications and security
- Fit into overall R&E security activities
  - Complement existing work, particularly in the Educause/Internet2 Security Task Force (STF)
  - Avoid basic research
- Much of our middleware work addresses security and privacy issues

Internet 2 Security – Feb 1, 2005

- Salsa, composed of leading campus networkers with security interests. Chaired by Mark Poepping, CMU, with representatives from MIT, Duke, Pennsylvania, Oregon, Educause, Washington, etc.
- Appointment of people within Internet2 to staff the effort
- Coordination of role within the Educause/Internet2 Security Task Force
- Successful WGs formed in NetAuth, Federated Wireless NetAuth, CSI2
- Commitment of flywheels, scribes, etc.

Community self-assessment

- Salsa as a place for some cross communication
- NetAuth and FWNA WG in NetAuth and derivative federated wireless network access efforts
  - White paper, taxonomy well received and disseminated
  - Next step is detailed specs of desirable components
  - Federated network access experimentation also underway
- CSI2 WG
  - organize activities to identify how security incidents can be better identified
  - how to be shared to improve the overall security of the network
  - information sharing frameworks as a background for future systems.
- Ad hoc conversations about very timely topics (e.g. botnets, netflow privacy) that serve as an informed opinion for lists like security@educause

What we heard from NPPAC

- Security is one of a very limited set of key areas for Internet2
- A top priority is to assist campus personnel in their current needs in addition to traditional focus on next generation needs
- Both intracampus and intercampus issues, including central ISAC-type services, need to be considered
- Make sure that security is a consistent planning thread across all of Internet2 activities, from current Abilene operational procedures through middleware tools that can improve network security
- Need to increase investment significantly
  - leverage campus capabilities more than acquire central staff

Developing the response

- Salsa – campus leaders in networking and security that advise Internet2 on network security initiatives
- Internet2/Educause Security Task Force Exec
- Discussions with Indiana/REN-ISAC
- Internal Internet2 planning
- Coordinated through this deck - the security fruitcake:
  - See http://security.internet2.edu/docs/fruitcake.pdf

Security Initiative Themes

- Strengthen campus capabilities now and in the future
- Improve Internet2 security procedures with campuses and internally
- Coordinate the inclusion of security in the development of new technologies at all levels of the stack
- Tap into the expertise in the community in security and network operations for new data streams and tools
- Work deeply and in an ongoing way with other initiatives in security and the R&E community

Some things left out of the response

- International issues
- Privacy and policy issues
- Trust issues
- Business model
- Assuming direction from DHS

Overview of Activities Going Forward

- Community Based
  - An immediate set of services and tools for improved prevention and better incident handling with intra-campus and inter-campus components
  - “Tools for tomorrow” delivers, in 1-3 years, improved NetAuth (in campus and federated flavors) and other products and services
  - “Rethinking the problem” workshop in the fall kicks off a researcher-practitioner-vendor partnership to radically change long-term approaches to Internet security

Community-based security activities

- Salsa as an overarching advisory and coordinating group for Internet2 member security activities
- Tools and processes for today
  - Intra-campus incident handling tools
  - Inter-campus and inter-sector information and tools
- Tools for 1-3 years – activities to produce security infrastructure tools that can be deployed relatively soon
  - Net-auth
  - Federated network access
  - Integration with middleware
- Big Picture – activities to rethink our approaches to networking integrated with security

Community-based Timelines

- Tools for tomorrow WG well underway, producing deliverables
- Tools and services for today
  - Discussions under way with Indiana; customer focus group convening shortly
  - WG for ISO to be announced at 3Q2005, along with security-announce, briefings at CIO gatherings
  - Additional WG will form as need and opportunity presents
  - Coordination on dissemination with EDUCAUSE Effective Practices
- Rethinking the problem workshop in the fall

Salsa

- Key networking/security leaders and Area/WG chairs, will be reconstituted somewhat from existing group
- Decides on WG areas, recommends on priorities, policies, etc.
- Informs each other and the community on other related activities on a periodic basis
- Sorts issues for attention (e.g. sec path discovery)
- Does timely topics discussions and “to sense” doc review
- Coordinates closely with other direction setting mechanisms

Tools for tomorrow

- Area Director: Chris Misra (UMass)
- Charter:
  - Using the scenarios-requirements-specifications-development cycle, create documents, frameworks, subsystems, etc. that will improve network security while facilitating the research and education missions of our members…
- Major themes
  - Authenticated and authorized networks
  - Meet those needs not likely to be met by the marketplace
  - Collaborative security approaches
  - Delivery of tools in 1-3 year time frames, with intermediate products along the way
- Working Groups
  - NetAuth – managing the connection of a device to a network
  - FNWA – extending connection management to a federated community

Salsa – Net Authentication

- Co-Chaired by Kevin Amorin (Harvard) and Chris Misra (UMass)
- White paper/taxonomy first deliverable, with webcasts and wide circulation
  - Investigation of requirements and implementations of network database and registration services in support of network security management
  - Investigation of extensions to these services including: proactive detection of unauthorized or malicious network activity; containment and prevention of such activity; identification and remediation of the sources of such activity
  - Strategies and Future Architectures documents
- Next step is investigation of the value/cost of developing a network auth framework and open source BoB modules
- Watching the NAC/NAP/IETF NEA spaces
- http://security.internet2.edu/netauth/

Federated Wireless Network Access

- Chaired by Kevin Miller (Duke) and Philippe Hanset (Tennessee)
- Enable members of one institution to authenticate to the wireless network at another institution using their home credentials. Often called the “roaming scholar” problem in HiEd. Work with EduRoam
- Deployed Radius pilot
- Use cases and requirements development under way
- Ultimately might leverage InCommon as a “collegial service”
- Workplan, documents and minutes at http://security.internet2.edu/fwna/

Tools and Services for Today

- Correlating goals and expectations
- Addressing campus incident handling and preventative capabilities first
- Has two related components
  - Developing, with members and REN-ISAC, a set of community-wide security services and data exchanges
  - Bringing together campus senior incident handling personnel to design and implement a set of improvements in campus technical tools and capabilities
- Formed CSI2 WG

Improved data sharing and tools

- Two related agendas:
  - Identify and provide, with Indiana, the data services that would help campus incident response offices: central, inter-sector, national, multilateral exchange; develop associated tools to process data and improve human handling
  - Bring campus incident handling leads together to exchange information and build an agenda for tool development for prevention, detection and remediation
- Customer focus groups organized summer 05
  - Results helping to drive current work

Tools for today - cautions

- Expectation correlation and then management is needed to ensure that the agendas from CIOs, campus security officers, network managers, etc. are integrated
- Much of the technical development will have a policy component aspect. These will typically be framed and then “outsourced” to other groups for further work
- The tools activity needs to work closely with Effective Practices efforts and benefits greatly from common representation in both efforts

CSI2 Working Group

- Charter
  - How to consistently identify security incidents
  - How information about the incidents can be shared
    - To improve the overall security of the network and the parties connected to the network.
  - Publish a report identifying tools, tool output and existing information sharing frameworks
    Preparation and background for future systems and tools.

CSI2: Three primary activity areas

- Tools
  - Shared darknets
  - Distributed IDS
- Data
  - retention, anonymization, related policies
- Sharing
  - formats such as IODEF and tools to implement
  - Inter-institutional “trouble tickets”
  - Augment REN-ISAC services

Big Picture Security Work: RTP

- Charter: consider the overall ecology and how the pieces interact, rethink the problem of networking with security in mind.
- Lead person: Deke Kassabian, UPenn
- Key folks:
  - Good thinkers: Terry Gray, Jim Pepin,
  - Good practitioners: David Richardson, Andy Palms, Dave Vernon, Tom Zeller, Dane Skow, etc.

- http://security.internet2.edu/rtp/

“Reconnections” workshop

- “Towards a needs assessment for R&E networking cyberinfrastructure”
  - Bring together strategic thinkers and key practitioners from higher ed, prominent vendors, and large corporate networks to identify the basic services and capabilities that network layer
- Process & Focus
  - Working through identification of problems, and long term design approaches to deal with them
  - Focus on “Manageability” in Enterprise Networks
  - Consider policy and experience with trust fabric in future designs

Opportunities to improve infrastructure

- DNSSec
  - Advisory group formed
  - Pilot cross-signing deployment
    - UPenn, UMass, Others
  - Continue to work closely with Educause
- Advanced network management group
  - http://security.internet2.edu/docs/internet2-salsa-topics-advanced-network-management-200511.html

Working with others and outreach

- Security sessions at Internet2 Member meetings
  - Integration of security with apps as well as net sec
- Educause
  - Outsourcing key policy issues to STF
  - Close coordination with Effective Practices Group
  - Visible participation in security lists and conferences
- Indiana
  - As Abilene NOC
  - As REN-ISAC for information sharing
  - As tool developer

www.internet2.edu