Security BoF:
What Are The Community's Open Questions?

Joe St Sauver, Ph.D. (joe@internet2.edu or joe@uoregon.edu)
Manager, Internet2 Nationwide Security Programs and
InCommon Certificate & Multifactor Authentication Programs

Techs in Paradise, Tuesday, January 15th, 2013

http://pages.uoregon.edu/joe/jt-what-remains/

A Little About This Session

- This is meant to be a discussion among colleagues
- So, to begin, let's go around and briefly introduce ourselves.
- If there are open security issues you'd like to have us talk about today, please feel free to mention them as part of that
- Our primary question today:

  "What are the pressing open problems in the security area for our community, and what should we, the community, be doing about them?"
- Secondary question:

  "How can Internet2 help move security forward?"
- I've outlined a few topics to prime the pump on the next slide, but I suspect that I've just scratched the surface of security issues that are out there

Some Potential I2 Security Topics Moving Forward

- Network security architectures at 100Gbps (ScienceDMZ, etc.)
- Instrumenting 100Gbps networks (Netflow, etc.)
- Circuit-oriented architectures and security implications thereof
- OpenFlow/SDN security
- Security for Net+ services
- InCommon Trust Services (federation, certificates, assurance, multifactor, etc.)
- Operational security trust communities (such as the REN-ISAC)
- IPv6 security impacts
- DDoS mitigation and BCP 38 filtering
- DNSSEC; DNS security (e.g., query rate limiting, RPZ, passive DNS, etc)
- BGP security (route monitoring, RPKI, etc.)
- Community security expectations for Internet2-connected sites
- Disaster recovery and business continuity
- Malware/phishing/spam
- Mobile device security (security *for* smart phones, tablets, etc.)
- Academic security research

These Are NOT the DHS "11 Hard Problems"

- "A Roadmap for Cybersecurity Research,"
  November 2009,
  www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

1. Scalable Trustworthy Systems
2. Enterprise-Level Metrics (ELMs)
3. System Evaluation Life Cycle
4. Combatting Insider Threats
5. **Combatting Malware and Botnets ← exception**
6. Global-Scale Identity Management
7. Survivability of Time-Critical Systems
8. Situational Understanding and Attack Attribution
9. Provenance
10. Privacy-Aware Security
11. Usable Security

Related Questions

- What's the right time horizon for Internet2's security work? Immediate operational issues? 1 year out? 3 years out? 5 years out?
- What should the role between Internet2 and other entities, such as Educause and the REN-ISAC, look like when it comes to the security work space?
- How can we help the academic security research community? (c.f., NDSS)
- What should our engagement with vendors look like? Does the community want more (or different) sorts of engagement with security vendors?
- What about government agencies? Obviously the NSF has been very supportive of network research, but there are many, many federal agencies that are interested in network security research and operations today.
- If there are privacy implications, how do we manage those?
- Should security be a routine track area for Joint Techs or the Member Meetings?
- How do we make sure that we capture the security insights that the community generates, and leverage them effectively in the future? That is, "How do we leave tracks" and make sure that security-related work can easily be found?
- What level of formal funding is appropriate?