Network Security Breakout

Participants

- Matt Crawford, FNAL
- Phil Dykstra, DREN
- Chris Greer, NCO
- Karl Levitt, NSF
- Paul Love, NCO
- Grant Miller, NCO
- Thomas Ndousse, DOE
- Joe St Sauver, Internet2 and U. Oregon

Time Horizon/Scope

- Immediate term vs. longer term
- If we don't do the short term items, we may not be able to do the longer time items

- We limited our discussion to unclassified networks.

Vision Of the Future

- Everything is way too fast
- Everything is encrypted
- Multilayer: not just all layer three any longer

Immediate Term

- Research on how to deploy existing and developmental capabilities
- How do we provide incentives to encourage folks to use security capabilities
- Testbed creation to test and deploy capabilities and to see how folks respond to them

Moving perimeter into the host

- Chokepoints can't keep up at 10Gbps, 100G coming
- To scale border protection, move the perimeter "two inches into the host" -- put network security policy onto a trusted network interface card/chip.
- Deals with the issue of the firewalls not being able to keep up at increasingly high rates
- R&D direction
  - The NIC would be site-configurable, not host-configurable, and auditable. It would report events as required by configured security policy.
  - Verifying host & OS integrity is probably out of scope.

Any New Network Architecture

- ALL new network architectures must include a security model from the ground up
- Require this to be part of proposals!

Security Test Bed As Part of GENI

- DETER has limits on acceptable research (e.g., no malware testing)
- GENI would offer potentially large scale environment
- Cyber Range isn't accessible/is classified
- Applications to run on GENI or other experimental test bed networks should include security metrics

Security vs. Usability

- Completely secure if unplugged and locked up in a vault… but that's not what it is for
- Need to balance security vs. usability, and that will likely require research to understand and get right
- Who pays: some security mandates may be unfunded
- **Research area:** tradeoffs between usability vs. security.

Threat Assessment

- [we'll be discussing tomorrow]

Closer Coordination Between Security and Networking Folks, and Security and Apps Folks

- Currently those are silo'd communities
- Recommendation: develop mechanisms to foster sharing and cross fertilization.

Physical Layer (L1) Security

- OTDR checking on a reserved lambda while in-service to detect taps/cuts

Layer 2 Security

- Context: ethernet VPNs seem to be ubiquitous in the near future, therefore layer two security issues are of growing concern.
- Specifically, we know of ARP spoofing MITM attacks, MAC admission control manageability issues

Understanding Circuit-Based Risks

- Two sites:
  -- one with a circuit connected host (host A) that also has Internet connectivity
  -- other with a circuit connected host (host B) that also has sensitive internal network connectivity
- Risk is that path will bridge Internet --> host A --> circuit based connection --> host B --> sensitive internal network
- Doesn't have to occur at the same time

Optical Networks

- Opportunity for strong authentication prior to circuit establishment
- Critical to protect the control plane -- currently often inband

Virtualization

- Promise and peril
- Folks like the idea of being able to give people a virtual machine, then blow it away when it is done being used
- Issues associated with potentially saving state and then restoring a now-insecure VM
- Additional machines and complexity to administer
- Risk of hypervisor breakout attacks

Immunocomputing

- Things to be learned from nature which may be applicable to security
- Can the machine be introspective with respect to its own security?
- Possibility: third level of security -- user, kernel, security
- Possibility: other systems on the subnet paying attention to what's going on
- Diversity

Correlating Diverse Inputs

- Having a broad picture of network activity has security value -- for example, Einstein sees more than an individual IDS might
- Slow scan issues
- Asymmetric multihoming
- Bad routing
- Traceback
- Additional alarm possibilities
- Security implications of network architectures

Security Policies in the Face of Ubiquitous Encryption

- Assume all traffic is opportunistically encrypted host-to-host.
- What can "network security" still do if all it can see is (src,dst)?
- **Research area:** incorporate traffic analytic methods into security tools

Want IPSEC Support for IP Multicast Key Exchange

- May be able to build on an existing proprietary secure IP multicast solution
- 100% of DREN traffic is IPSEC encrypted -- except for IP multicast, and DREN would like to fix that.
- IETF MSEC group is working on it (drafts from 2007

Performance Measurement and Monitoring

- Tradeoff in sharing of information privacy of sensitive information vs. generalized access and timely alerts

Intrusion Prevention Systems Handling Asymmetric Traffic Flows

- Very hard problem, no one currently commercially addressing this
- Should be a topic for research

Longer Term

- May not be dealing with packets, might be circuits, flows, streams, …

Economics of Security

- Understanding the financial incentives of attackers
- Economic motivators for security solutions

If You Remember One Thing

- The security problem is distributed
- Therefore the solution needs to be distributed as well

- Topic
- Finding
- Recommendations