

GENI and Security



Deborah Frincke, PNNL, co-chair

Matt Bishop, UCD, co-chair

Chen-Nee Chuah, UCD, community collaborator

Karl Levitt, NSF, NSF co-ordinator

Mike Reiter, CMU, GENI security leader and
provider of early materials

Terry Benzel, USC/ISI, GENI resource

Introduction and Charge



- ✓ Our Focus:
 - ✓ Potential Uses: Security-related experiments to run on GENI
 - ✓ Necessary Components: Required instrumentation for GENI
 - ✓ Designing Security In: Security of GENI itself
- ✓ Our challenge for you:
 - ✓ Input, lots of input!
 - ✓ Your ideas for how to maximize GENI's usefulness to the security community
 - ✓ Access, architecture, guarantees, etc.

GENI Architecture



QuickTime™ and a
TIFF (LZW) decompressor
are needed to see this picture.

— from Tom Anderson's talk

What It Means



- ✓ GENI *manages* resources
 - ✓ Slices
 - ✓ Other objects (files, firewalls, monitors, ports)
- ✓ Manager *has* APIs
 - ✓ Users
 - ✓ Resources
 - ✓ Other networks such as ORBIT, DETER/EMIST, CENS, ESNET
- ✓ Manager *does* access control
 - ✓ Access determined by policy

Threats to GENI



- ✓ Exploitation of a slice
 - ✓ Runaway experiments
 - ✓ Unwanted Internet traffic, exhausting disk space
 - ✓ Misuse of experimental service by end users
 - ✓ eg, to traffic in illegal content
 - ✓ Corruption of a slice
 - ✓ Via theft of experimenter's credentials or compromise of slice software
- ✓ Exploitation of GENI itself
 - ✓ Compromise of host system
 - ✓ DoS or compromise of GENI management infrastructure

Build Security In From the Start



... critical for good security!

Experiments (Discussed)



- ✓ Threats to the core
 - ✓ Bad/malicious routers (black holes, etc.)
 - ✓ Worms propagating through routers
 - ✓ “Captured” routers
 - ✓ Lifecycle attacks on routers
- ✓ Threats to the end points
 - ✓ DDoS attacks

Instrumentation (Discussed)

- ✓ Extraction of data
- ✓ VM with ability to capture all traffic
- ✓ Hooks for digital forensics (traceback, etc.)
- ✓ Tools for experiment-specific monitors
- ✓ Controls over who can view data
- ✓ Ability to monitor any resource—CPU usage, memory usage, slices, etc.
- ✓ Highly instrumented, controllable testbed

GENI Security (Discussed)

- ✓ Access control
 - ✓ A decentralized framework based on credentials and formal logic
 - ✓ Focused on implementing least privilege with a small, assured TCB
 - ✓ Will be sufficiently flexible to regulate access to wide range of resources; have not identified the full list yet (but don't need to)
 - ✓ Will be available to GENI and applications alike
 - ✓ Can be used to implement slice "kill switch" and audit trail
 - ✓ Eventually incorporating attestation ala TCG
- ✓ Key management
 - ✓ Public key certification encompassed by access control framework
 - ✓ GENI will have a PKI
 - ✓ Private key protection optionally supported via capture-resilience protocols or hardware tokens

Experiment Ideas and Issues



- ✓ How do we scale experiments to reflect the larger networks?
- ✓ How fast could a worm really spread in the face of infrastructure and/or end host controls?
 - ✓ How do homogeneity and/or diversity affect this?
 - ✓ Create libraries of worms for use on GENI
- ✓ What protocols for protecting infrastructure are or can be made practical by augmenting infrastructure?
 - ✓ WATCHERS (routers monitor each other), others
- ✓ How do we use the infrastructure to help handle DDoS attacks?

More Experiments



- ✓ Use GENI to test Internet voting
- ✓ Test software, run time monitoring security
- ✓ Evaluate Internet threats to SCADA, power grid, other critical functions
 - ✓ Running a backup demo for power grid
- ✓ Disaster management and survivability
 - ✓ Graceful degradation
 - ✓ Containing the failures or attacks
 - ✓ Collaborative sensors to provide early warning
 - ✓ Priority of jobs, traffic to properly allocate scarce resources
 - ✓ How many failed nodes can be tolerated?

Instrumentation Ideas and Issues

✓ Monitoring

- ✓ What layer(s) of network
- ✓ What aspects of hosts
- ✓ What attributes (routing, performance, etc.)
- ✓ How much data to collect
- ✓ Where to collect it
- ✓ Where to store it

✓ Dissemination

- ✓ Privacy issues leading to data sanitization
- ✓ Access control

More Instrumentation



- ✓ How to demonstrate GENI results can be applied to Internet
 - ✓ How do you compare networks
 - ✓ What attributes are important
 - ✓ Is experiment repeatable
- ✓ Forensics
- ✓ Deceptive technologies
- ✓ Performance issues

GENI Management Support



- ✓ View GENI as resource manager
 - ✓ Slices, systems, routers, etc. all objects
 - ✓ API for experimenters to access GENI
- ✓ Access control
 - ✓ Formal logic to prove what accesses allowed
 - ✓ Combine it with certificates for identity management
- ✓ Privacy
 - ✓ Protect privacy of experiments, data used and derived

More GENI Management Support



- ✓ GENI's insider problem...how do we solve it?
 - ✓ Attacker masquerades as experimenter, uses that to compromise GENI, other experiments
- ✓ Vulnerabilities in the GMC
 - ✓ How do we find, mitigate them?
- ✓ Interaction with edge networks (eg, wireless)
 - ✓ Define the interface between GENI and other testbeds (ORBIT, DETER/EMULAB, CENS)
 - ✓ Determine what guarantees (if any) they provide when combined with access controls in GENI

Other Security Ideas and Issues

- ✓ *Critical and key problem:*

Build security into GENI

... this **includes assurance**

- ✓ Risks to GENI
- ✓ COTS, not COTS systems
- ✓ Heterogeneity vs. homogeneity
- ✓ PKI management
- ✓ Virtualization of resources
- ✓ Availability issues
- ✓ Legal issues
- ✓ Generally: advance the state of the art and science of security

See you in the breakout
session!



Remember:
***Build security into the GENI
architecture***