

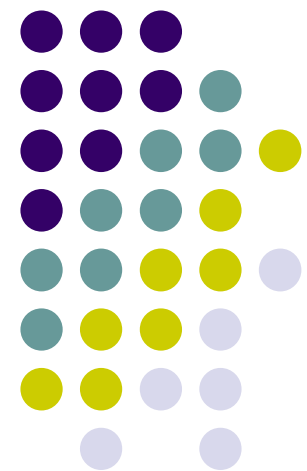
# Securing GENI, and Security Experiments on GENI

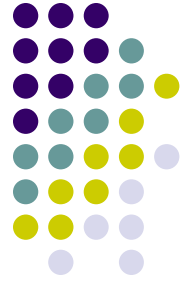
---

Karl Levitt, National Science Foundation

Sonia Fahmy, Purdue University

Planning Group: Mike Reiter, CMU





# Scope

- Security includes availability, robustness (“self-healing” functions), QoS (DoS is defined as unacceptably low QoS), as well as integrity, confidentiality, authentication, authorization, accounting, ...
- If GENI morphes into a new Internet, GENI security and security protocols to be tested on GENI become unified

# GENI Experimental Interface



- A security experiment includes: *attack/fault model*, plus typical experimental parameters: topologies/services/resources/legitimate or cross traffic, instrumentation tools, and the *architecture/service under test*
  - Network/device/implementation *diversity* and *autonomy*
    - Diversity/autonomy introduces vulnerabilities and management challenges to GENI
    - Sensitivity of results to particular hardware/software/settings problematic with some attacks (reproducibility vs. flexible resource assignment)
    - Built-in GENI intrusion detection/tolerance – understanding whether your results are due to the experiment versus platform is tricky when platform is complex
  - Ease of conducting very large-scale experiments, e.g., worm propagation (time to upload, finding large numbers of available nodes, ... etc)
  - Conducting an experiment with multiple administrative domains<sup>3</sup>?



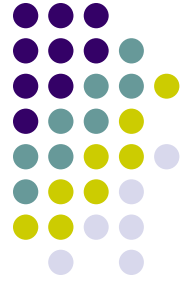
# Experiment (cont'd)

- Whether experiment is open to users/attacks
  - How to *attract* real users (especially if slice may be attacked) and attract red teams, and when?
  - What is an acceptable level of risk and when?
  - GENI services are first experimental, and then open to attack, then becoming operational services
- The real user expectations of *privacy* versus keeping/sharing logs: need to have reasons and timelines for accessing logs (IRBs), use of anonymization is acceptable in some cases but not others; GENI-specific IRB
- *Collaboration versus isolation levels* across users/experiments/with the Internet
  - How to ensure the *safety/availability* of a new network opting to *federate* with GENI, or a new slice connecting to another? Configuring firewalls, rate limiters, ...etc.



# Experiment (cont'd)

- A *key advantage* of GENI versus DETER is the interaction with real traffic
  - How to provide many levels of controlled interaction with real user and with attackers? This increases credibility of security solutions
- Capability to provide controlled replay: using GENI for forensic analysis and repeating on “shadow” network
- Isolated slice versus different types of shared slices
- Need to be as simple as flipping a switch for isolated versus open for collaboration experiment



## Experiment (cont'd)

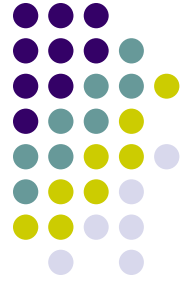
- Instrumentation tools need to be sophisticated and easy to understand: clocks synchronized, usable tools, tools to help with filtering and interpreting logs
- Security of GENI itself can utilize sophisticated access control, and proof-carrying code mechanisms
- However, GENI will not be 100% secure at all times
- From experience, many vulnerabilities/security problems are not malicious; rather inexperienced users or system administrators maintaining a part of GENI making mistakes or panicing too soon



# Attack/Fault Models

- Does having a distributed testbed, shared nodes, and “real” users limit the fault/attack models used in experiments?
  - Real vs. simulated/emulated attacks: live malware, attacks on VMM, node/link failures, DDoS floods causing receive (interrupt) livelock, wireless link jamming, attacks causing energy (battery) depletion?
  - GENI to emulate some of these attacks/faults; instrumentation tools must consider this!
  - Exclusive access to be granted to “regions” of the GENI facility at specific times for more “risky” tests? Multiple levels of isolation
  - Functions to recover from experimental effects are needed
- Defining attack models targeting new architectures is critical and using others as attackers is key

# Secure Designs to be Tested on GENI



- What is the scope of novel security ideas to be tested on GENI?
  - Some examples of network security solutions: randomization, redundancy, provably safe protocols, pervasive use of virtualization (GENI morphing into the new Internet), multi-level security, monitors (routers watching each other), disallowing any to any communications without prior consent
- Authentication, authorization, and accounting mechanisms
- Can GENI itself have an open platform for policy specification and access control?
  - How general should the GENI access control be?
- Security economics and market experiments on GENI (versus privacy concerns)
- Wired/wireless interaction and cross-layer security mechanisms
- Experiments to define *role* of security elements



## Secure Designs (cont'd)

- Experimenting with comprehensive DDoS solutions involving multiple mechanisms
- Incentives to deploy security mechanisms when new vulnerabilities are discovered
- Large-scale cyber-war simulation
- Incentives for users to think of security and use solutions such as secure e-mail
- Solutions for rootkits, spam, phishing, .....