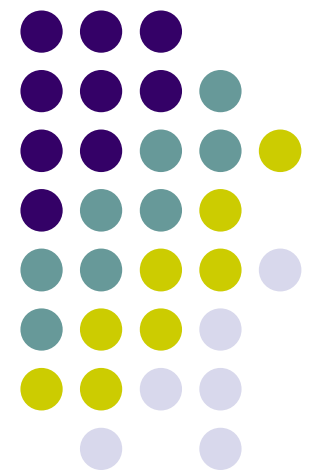


Securing GENI, and Security Experiments on GENI

Karl Levitt, National Science Foundation

Sonia Fahmy, Purdue University

Planning Group: Mike Reiter, CMU



What functionality can first phase GENI provide and still be reasonably secure?



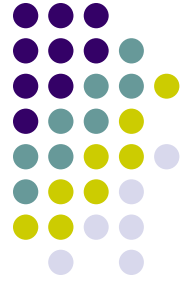
- What is an acceptable level of GENI security/availability/... for phase 1?
 - Tradeoff between flexibility/usability and security
- What are the GENI specifications to ensure that we achieve that level of security?
 - Architecture
 - Management and administration
 - Identity and access control
 - Experimental interface
 - Federation with GENI
 - Connection to other operational networks (the Internet...)

Isolation versus Collaboration



- Isolation at the level:
 - Time
 - Nodes/links
 - Resources on a single node/link – virtualization and rate limiters
 - Use of simulated/emulated attacks
- Tradeoff between having real users and real attacks
- Slicing has to be extremely robust if experiments are very damaging
- Traffic on GENI versus traffic on the Internet and other operational networks
 - Opting to direct your traffic on GENI
 - Having real user traffic on GENI is very important
 - Legal implications are problematic
 - What agreement can a GENI user sign to understand: GENI-wide IRB
 - Firewalls and rate limiters

Who can access GENI and how?



- How to define the GENI community? Can companies host their services on GENI? Akamai to GENI would be ideal for many experiments? Policy decisions to allow people access
 - Some only interested in bandwidth (anonymized headers are okay; even packet counts) but others need more
 - Small businesses? What are their security and confidentiality requirements? Is NSF interested in this?
- Policies to ensure organized crime, terrorists, business competitors can be traced back
- Naming in GENI – global namespace that is certified? Does that inherently limit new ideas? Will the GENI namespace by default become the new Internet namespace? Web of trust models for identity management.

GENI Security and Management



- Any legacy system has vulnerabilities and so GENI will have vulnerabilities since it employs some legacy components
- Who is ultimately in control of GENI? The participants contributing GENI.
- How centralized or distributed is GENI management?
- Networks federating with GENI have no control over GENI – they are not first-order citizens
- Misbehaving entities have to be detected – trust management and accounting required
- A typical user does not want to be subjected to a security experiment
 - Incentive to participate in an experiment must be very strong to offset that risk at certain times
 - Users (proposing new ideas) will benefit from knowing they have a vulnerability

GENI Security/Management (cont'd)

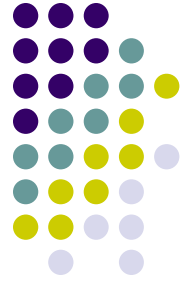


- Federating with GENI with trust and accountability: at a PI level or organizational level? Policies and agreements?
 - Your traffic can either go on the Internet, Internet2, or GENI. Set routing policies enforced at the edge: under what conditions do you chose to route/tunnel over GENI or the Internet?
- Transparency of the GENI design itself
 - What kind of GENI network management information can be released to researchers?
 - Some information is private and sensitive – e.g., BGP information
 - What about international parts of GENI?
 - Can we expose limits amounts of information – not everything!
 - Software, e.g., voting machines
 - Is GENI management software open? Free? GPL?



The Experimental Interface

- There is both an entry (access control) problem and scheduling problem; policies are needed to ensure both security and usability (a very limited slice is not very useful)
- Measurement without affecting experiment is important
- Interaction between experiments: network management and virtualization interacting in different ways – how to design an API that allows this?
 - Example: transport layer experiment versus other layer experiment; another experiment with attack 1, attack 2
 - Specifying characteristics of slices so you can choose the slice capabilities you want
 - You want guest OS to be compromised but VMM not be compromised in your worm experiments



Assessing GENI Security

- Difference between GENI and enterprise security (firewalls, rate limiters, ...)
 - The GENI facility has less control and more autonomy
 - Resources on GENI are not completely owned by GENI
- Security requirements
 - Phase 1: virtualization limiting and inaccurate
 - Worry more about GENI security versus features provided by GENI
 - Phase 2 more features since we learn more about security from GENI security experiments
- Assessment of GENI security: vulnerability models and checklists
- Dynamic process: attackers will come up with new attacks over time