

Security – Overall Facility Design

GENI Town Meeting

Security

- Overall security of the GENI facility
 - The major focus of this breakout session
- Security research in the GENI facility
 - A minor focus of this breakout session

Risks to Security of the Facility

What risks are tolerable and which are intolerable?

- Risk to the testbed
 - Inaccessibility (denial of outside access)
 - Malfunction (facility is down)
 - Contamination (facility integrity corrupted)
 - Subversion (facility functions overrun)
- Risk to the experimenter
 - Delay of test
 - Contamination (object under test corrupted)
 - Exposure (sensitive data about object under test released)
 - False results (test data corrupted)
- Risk to the world
 - Use as attack platform
 - Inability to test designs

Essential Functions

What functions are so desirable that they should be provided, despite the risk?

- Functions for the Experimenter
 - Access from external sites
 - Shared access (Experimenter permits others to access)
 - Simultaneous testing
 - Total isolation/ Controlled interconnection/ Globally available services
 - Extraction of data
 - Repeatability of experiment
 - Clean slate (security to what level? layer 3? layer 2? BIOS?)
- Functions for the Testbed
 - Programmability
 - Virtualization
 - Over-the-network management
 - External test monitoring and control

Threat Sources

Who do we want to consider a threat?

- Outsiders
 - Unknown to GENI
 - A GENI participant but not a participant in this experiment
- Insiders
 - Faulty equipment/processes
 - trojaned (deliberate faults) or accidents
 - Faulty experiments
 - Misconfigured experiments
 - Subverted experiments
 - GENI participants

Issues

- Identity
 - Representation, granularity (experiment? PI? Experimenter? Etc.), uniqueness...
- Authentication
- Authorization
 - To run an experiment
 - on GENI
 - on GENI on day X
 - that talks to another experiment
 - To access an experiment
 - As a researcher
 - As a “real user”

Security Research in the GENI Facility

- Wild ideas:
 - Authorization prior to transmit
 - Abandon global reachability
 - New mechanisms of identity
- Relationship of security experiments to security of experiments

What Else?

- Legal issues
 - Law enforcement intercept – especially wrt foreign network
 - Issues with privacy, etc. wrt serving “real users”
- OS question – need support for virtualization in downloaded OS (auditing, etc.) or do virtualization at hypervisor
 - What about using commercial OS’s/products to capture realism
 - Need VM with ability to capture all traffic
- Core should be intrusion and fault tolerant
- Preventative measures are fine; we need intrusion detection as well
- Challenges of wireless nets – computation/power/etc – security architecture must be aware of those challenges
- Identity – who is the authorized entity – university? Project team? PI? PI and all students? Etc.
- Authentication – need two factor to protect against credential loss
- Delegation of authority
 - Passing your authorization to other experiments, other experimenters, etc
 - What about federation with other networks – if they allow an experiment
- Should have levels of security

Dreams

- Log anonymization and sharing
- An Internet that allows ubiquitous access worldwide to global data – w/o unauthorized use and support for legal investigation
- Complete clean room w/o contamination but building on previous experiments and authorized interaction allowed
- Hooks for digital forensics (traceback, etc.)
- Support for peer discovery and collaboration
- Being able to do: attack, defense, host based things, accountability, anonymity, predicting behavior,
- Interaction bew sensor nets and GENI – how can we define security for a network when we don't know what the network will be
- How can GENI can be used to be building blocks for the future Internet – from service provider point of view, how provide new services for the users

Dreams

- Support end-end resource reservation for real-time applications with no way to attack the reservation
- How the GENI infrastructure can be securely managed
- Architecture that can secure last hop – accept less than absolute security
- Periods processing – sometimes highly secure, sometimes weakly secure
- GENI should defend itself from attack – prevention, detection, alerts, etc.
- Allow experiments of mechanisms that prevent unwanted traffic (determination of unwanted being more of the social context) – so must allow all sorts of traffic
- Allow experiments to identify themselves as open to attack
- Allow experiments of location management – attach user to domain to location when you are mobile
- Control of amount of information publicized about each slice
- Highly instrumented test bed – what is going on in testbed and what is going on in experiment

Tools for Experimentation

- Tools for experiment specific monitors/instrumentation and controls over who can view data – but need to anonymize or obfuscate logs – data retention beyond slice lifetime
- GENI specific authorization – I&A, authorization mechanisms, etc
- Tools for experiment specific authorization – I&A, authorization mechanisms, etc.
- Sufficient “virtual” end hosts for realistic scale experiments
- “Red Team” the GENI Infrastructure
- Control over the security between the real world and the GENI projection into the real world
- Library of common analysis tools, detection tools, etc
- Ability to monitor any resource – CPU usage, memory usage, etc