GENI Security Plan Update

21 July 2010

www.geni.net

Sponsored by the National Science Foundation

Outline

- Organizational Structure of GENI
- Process for developing the GENI security plan
- Spirals 2 & 3 security plan

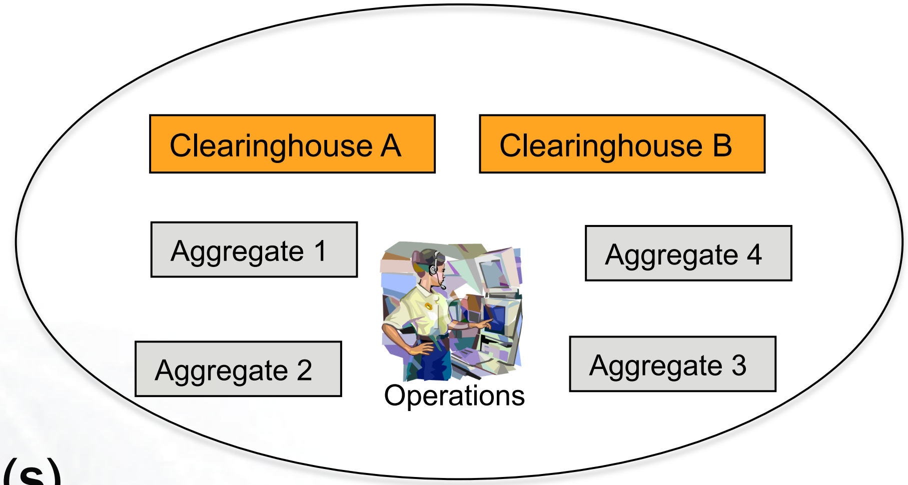
The Organizational Structure of GENI

- Organizational structure of GENI shapes
  - Operations plans
  - Security plans
  - Agreements signed by entities (organizations and individuals) that make up or use GENI
  - Roles and responsibilities of entities involved with GENI
  - Information exchanged among entities
  - Technical protocols for information exchange
- GENI is organized as a Federation

What is a Federation?

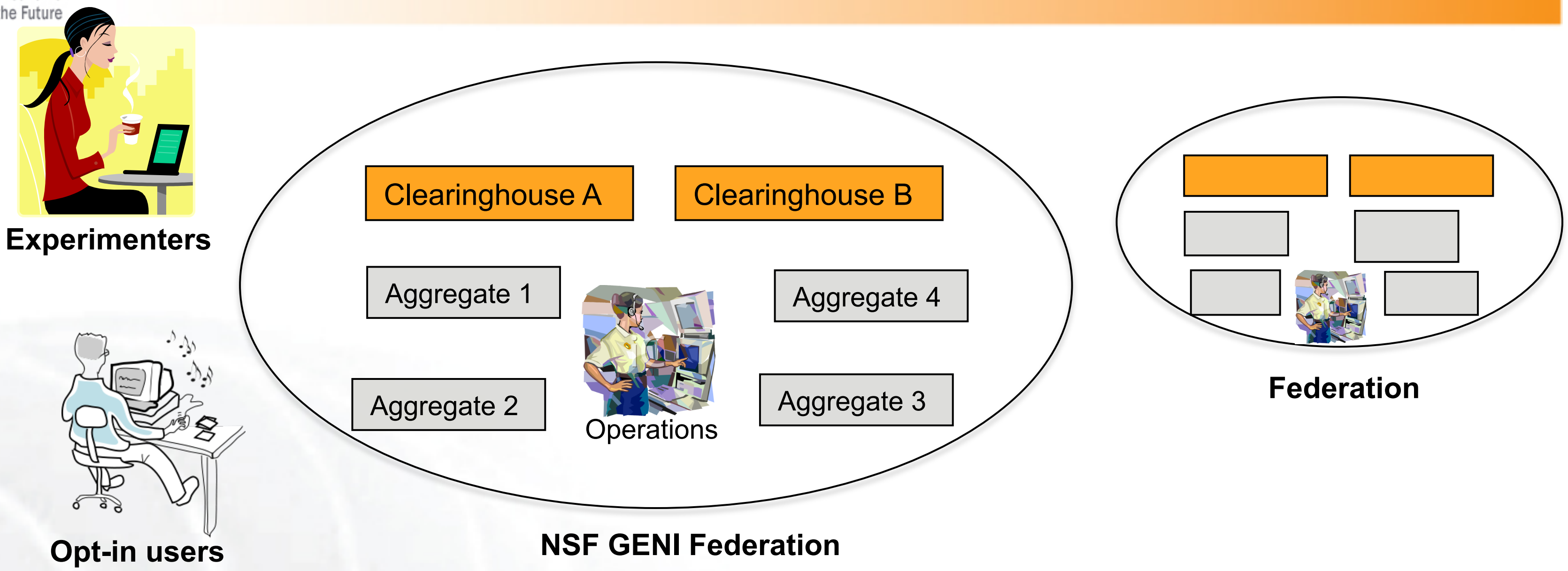
- “A federation is an association of organizations that use a common set of attributes, practices and policies to exchange information about their users and resources in order to enable collaborations and transactions.” - InCommon FAQ
- Information exchange is governed and facilitated by
  - Practices and policies
  - Agreed upon protocols
    - Shibboleth in the case of the InCommon federation

Potential Organization of the GENI Federation



- Clearinghouse(s)
  - Grant experimenters credentials to use resources
- Aggregates
  - Make resources available to experimenters with appropriate credentials
- Operations
  - Ensure federation goals for security and availability are met
- GPO led tasks
  - Draft practices and polices for federation
  - Define protocols for exchanging information within the federation
  - Get federation up and running

Other Associated Entities



- The GENI federation practices and policies must cover sharing of information and resources with these other entities
- The GENI security plan must consider threats to and from these entities

Outline

- Organizational Structure of GENI
- Process for developing the GENI security plan
  - Process illustrated by developing a security plan for aggregates
- Spiral 2 & 3 security plan

Process

- List security related responsibilities of federation entities
- Identify security threats to entities
  - And hence to the federation
- Develop threat mitigation strategies
  - Technical and non-technical
- Derive Spiral 2 & 3 tasks from mitigation strategies

Outline

- Organizational Structure of GENI
- Process for developing the GENI security plan
  - Process as applied to aggregates
- Spiral 2 & 3 security plan

Aggregate Provider Security Related Responsibilities

- Verify credentials of experimenters
- Protect resources from attackers
- Provide slice isolation
- Protect production resources
- Track and log resource allocations
- Provide status information to ops
- Participate in federation operations

Aggregate Security Threats

- Attacker gains access using stolen or forged credentials
- Aggregate manager compromised
- Experiment disrupts production hosts and networks
- Experiment accesses information in production hosts and network
- Insufficient slice isolation exploited to launch/grow attack
- Illegal/unacceptable use of aggregate resources

Aggregate Security Threat Mitigation

- AM follows best practices for a web service
- Best practices for isolating contributed resources from production resources
- Best practices for controlling information flow between contributed resources and production resources
- Best practices for isolating slivers
- Logging: Who held what resource and when
- Experimenter’s Recommended Use Policy prohibits illicit or unacceptable activity

Spirals 2 & 3 Security Plan for Aggregates

- Spiral 2
  - Security best practices for aggregates
  - Aggregate provider's agreement (draft)
  - GENI API includes software to verify experimenter credentials
  - Start requiring experimenters to agree to RUP
- Spiral 3
  - GENI SOWs will require aggregates to start implementing best practices

Outline

- Organizational Structure of GENI
- Process for developing the GENI security plan
- Spiral 2 & 3 security plan
  - Developed by applying process to all federation and associated entities
  - Details in backup slides

Spiral 2 Plans

- In progress
  - Document the entities, roles and responsibilities of the GENI federation (GPO)
  - Security best practices for wired & wireless aggregates (Sparta)
  - Aggregate provider's agreement (NCSA)
  - GENI API includes software to verify experimenter credentials (GPO)
  - Emergency stop procedures
- Planned
  - MOUs with CH operators (GPO)
    - E.g. CH will grant GENI credentials to experimenters approved by the GPO
  - MOUs with aggregates (GPO)
    - E.g. Aggregate will make resources available to experimenters with GENI credentials
  - Start requiring experimenters to agree to RUP (GPO)
  - Early draft of plan for responding to threats of legal action (NCSA)
  - Preliminary Ops security plan for OpenFlow and WiMax deployments (NCSA)
  - Some aggregates start providing health data to GMOC

Spiral 3 Plans

- Clearinghouse operator agreement
- Best security practices for CH operators
- GENI SOWs will require aggregates to start implementing best practices
- Ops related requirements in SOWs for aggregate providers before aggregate is “operational”
  - Monitoring and reporting to GMOC
  - Participation in ops team
- Draft of a “GENI Operations Security Plan”
- Draft plan for responding to threats of legal action
- Best practices for experimenters
- Libraries/tools experimenters can use to protect private data
- Review opt-in user protections in RUP and strengthen if necessary
- Draft of “Guidelines for Experimenters Working with Private Data”

Backup Slides

Clearinghouses: Security Related Responsibilities

- Authenticate experimenters
  - May make arrangements with identity providers to authenticate experimenters
- Issue GENI credentials to qualified experimenters
  - Qualified experimenters defined by federation
- Provide AMs with information about experimenters (e.g. experimenter attributes)
- Provide CH status information to Ops
- Participate in federation operations
- Track resource held by slices (TBD)

Clearinghouse Security Threats

- CH compromised by attacker(s)
- CH process for authenticating user fails
  - Incorrect information from identity provider
  - Forged identity documents
- CH implementation of federation policy is incorrect

In all these cases legitimate experimenters may be denied access or credentials may be granted when normally they would not be.

Clearinghouse Security Threat Mitigation

- Implement best practices for a web service
  - Firewalls, keep private data behind firewalls, insider controls, secure connections while exchanging private data (passwords, certs), up-to-date software, intrusion detectors
- Federation policies on who gets GENI credentials are clearly specified
- CH processes for authenticating users must meet federation guidelines
  - Are there industry standards?
- CH provider must periodically audit the policies it is using to grant credentials
- Whenever possible CH software that checks policy and grants credentials must be vetted by the GENI community

Aggregate Provider Security Related Responsibilities

- Verify credentials of experimenters before granting resources
- Protect resources from being compromised by attackers
- Provide slice isolation (and document the degree of isolation provided)
- Protect production resources (hosts, networks, etc) from malicious or accidental disruptions by experiments
- Track and log resources allocated to experimenters
- Provide status information to Ops
- Participate in federation operations team

Aggregate Security Threats

- Attacker gains access to aggregate resources using stolen or forged credentials
- Aggregate manager compromised
- Experiment using aggregate resource disrupts production hosts and networks
- Insufficient slice isolation exploited to launch/grow attack
- Experiment gets access to information in production hosts and network
  - Access that isn’t explicitly granted
- Illegal/unacceptable use of aggregate resources by experimenter

Aggregate Security Threat Mitigation

- AM follows best practices for a web service
- Best practices for isolating contributed resources from organization’s production resources and the Internet
- Best practices for blocking/controlling information flow between contributed resources and production resources
- Best practices for isolating slivers
- Logging: Who held what resource and when
- Experimenter’s Recommended Use Policy should prohibit use of resources for illicit or unacceptable activity

Spirals 2 & 3 Security Plan

- Spiral 2
  - Security best practices for wired aggregates
  - Aggregate provider's agreement (draft)
  - GENI API includes software to verify experimenter credentials
  - Start requiring experimenters to agree to RUP
- Spiral 3
  - GENI SOWs will require aggregates to start implementing best practices

GENI Operations Team Security Responsibilities

- Collect status information from CHs and AMs
- Monitor for security and operational events that threaten GENI
  - Including regular meetings of personnel from meta-ops, CH ops and aggregate ops
- Respond to security and operational event
- Audit security mechanisms put in place by CH and aggregate providers
- Make status information available to experimenters

GENI Operations Team Security Threats

- Attacker infiltrates team
  - Distributed team that spans organizations
- Operations team member(s) not reachable/ not responsive during a security event
- Insufficient monitoring or reporting by CH or aggregate operators

GENI Operations Team Threat Mitigation

- Mechanism for authenticating team members and team communications
- Event response procedure must account for team members not being reachable or responsive
- CH and aggregate provider agreements must specify and mandate minimum monitoring and reporting requirements

Spiral 2 & 3 Security Plan

- Spiral 2
  - Emergency stop procedure
  - Early draft of plan for responding to threats of legal action
  - Preliminary Ops security plan for OpenFlow and WiMax deployments
  - Some aggregates provide health data to GMOC
- Spiral 3
  - Ops related requirements in SOWs for aggregate providers before aggregate is "operational"
    - Monitoring and reporting to GMOC
    - Participation in ops team
  - Draft of a "GENI Operations Security Plan"
  - Draft plan for responding to threats of legal action

Notional Experimenter Responsibilities

- Use resources responsibly
  - Hold least number of resources required for least amount of time
- Abide by local laws and GENI policies
- Handle private data from opt-in users (or other sources) appropriately
  - Comply with local laws, IRB and funding agency requirements
- Ensure resources used by experiment cannot be hijacked
- Inform operations in advance is experiment might set of monitors/intrusion detectors (e.g. security)

Experimenter Security Threats

- Experimenter's credentials are stolen
- Attacker hijacks experimenter's resources
- Interference between experiments / leakage of information across slivers
  - Slice isolation insufficient / incorrect

Experimenter Security Threat Mitigation

- Best practices for experimenters
  - Protecting certs
  - Understanding level of slice isolation provided by aggregates and picking aggregates that provide isolation required by experiment
  - Encrypting data when slice isolation is not sufficient (e.g. when using wireless links)
- Best practices for aggregates

Spiral 2 & 3 Security Plan

- Spiral 2
  - Best practices for wired aggregates (draft)
  - Best practices for wireless aggregates
- Spiral 3
  - Best practices for experimenters
  - Provide libraries/tools experimenters can use to protect private data

Opt-In Users Security Responsibilities

- Read and understand opt-in user agreement from experimenter

Opt-In User Security Threats

- Experiment fails to protect private data
  - Insufficient/improper protections put in by the experimenter or the aggregate provider
  - Human error

Opt-In User Security Threat Mitigation

- Experimenter RUP must require GENI experimenters to do due diligence to protect opt-in users private information
  - Require experimenters to disclose to users what data will be collected, how it will be handled, who will have access to the data, how long it will be stored, etc.
- GENI published “Guidelines for Experimenters working with User Private Data”
  - Protection of data during processing, transmission, storage, etc.