



GENI

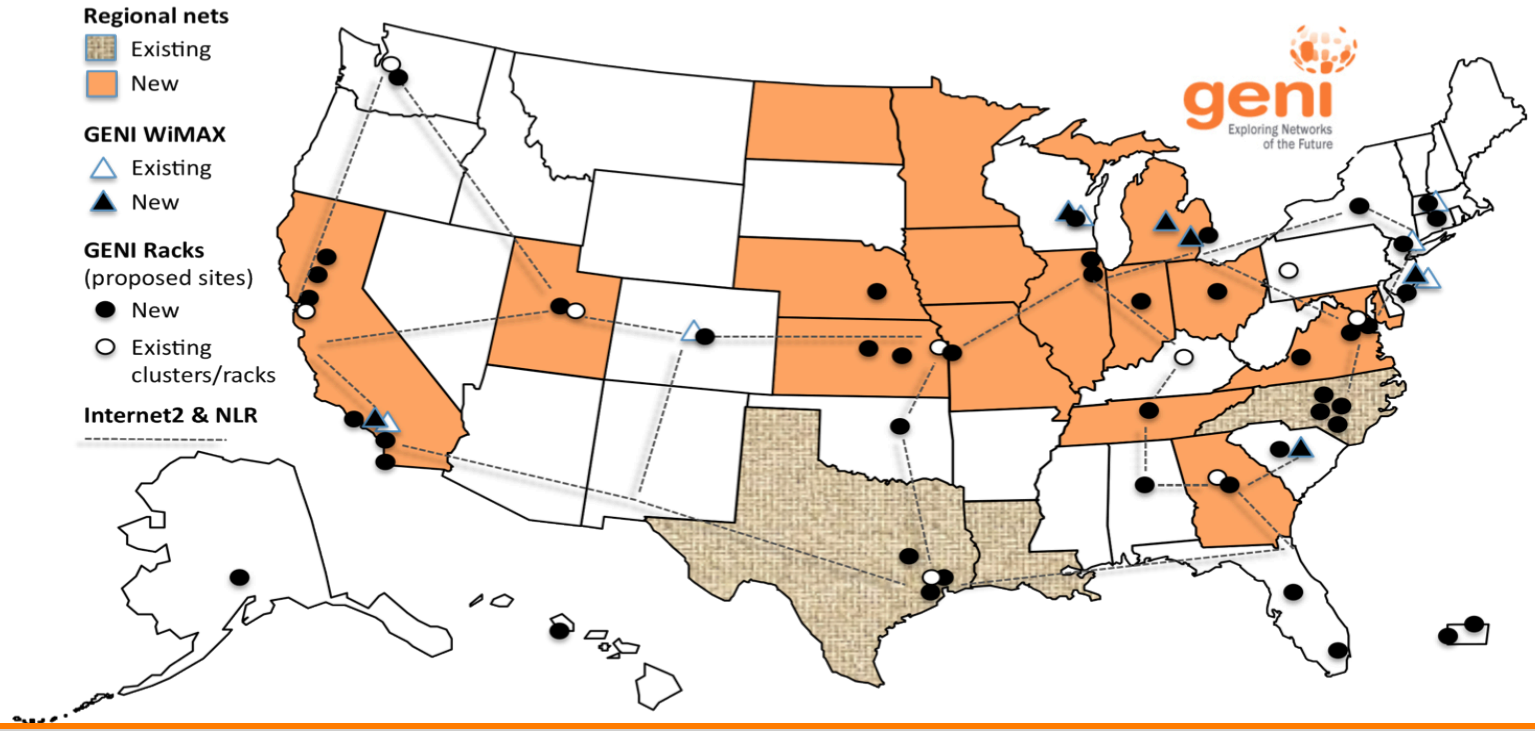
Security Mechanisms, Policies and Procedures

Vicraj "Vic" Thomas
www.geni.net

Sponsored by the National Science Foundation

Global Environment for Network Innovations

Infrastructure for Experimentation



GENI provides compute resources that can be connected in experimenter specified, programmable Layer 2 topologies.

geni
Exploring Networks of the Future

Compute Resources

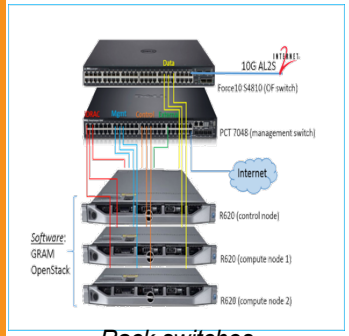
GENI Racks: small clouds
Virtual machines
Bare metal machines

Android Phones

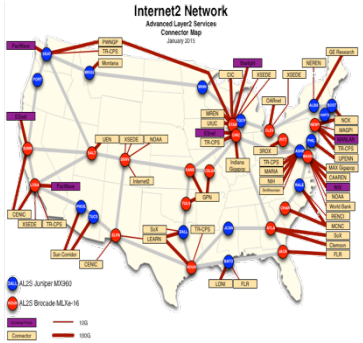
Existing Testbeds

Network Resources

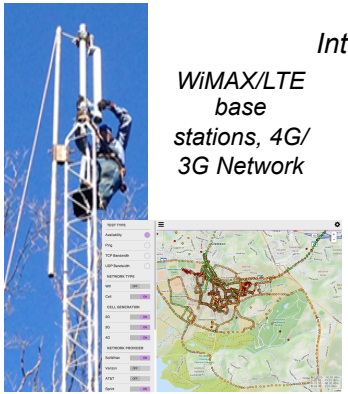
Layer 2 VLANS and Access to Programmable Switches



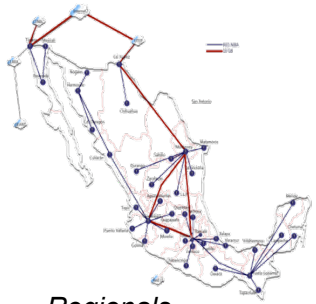
Rack switches



Internet2: US Research Backbone



WiMAX/LTE base stations, 4G/ 3G Network



Regionals

Key Concepts

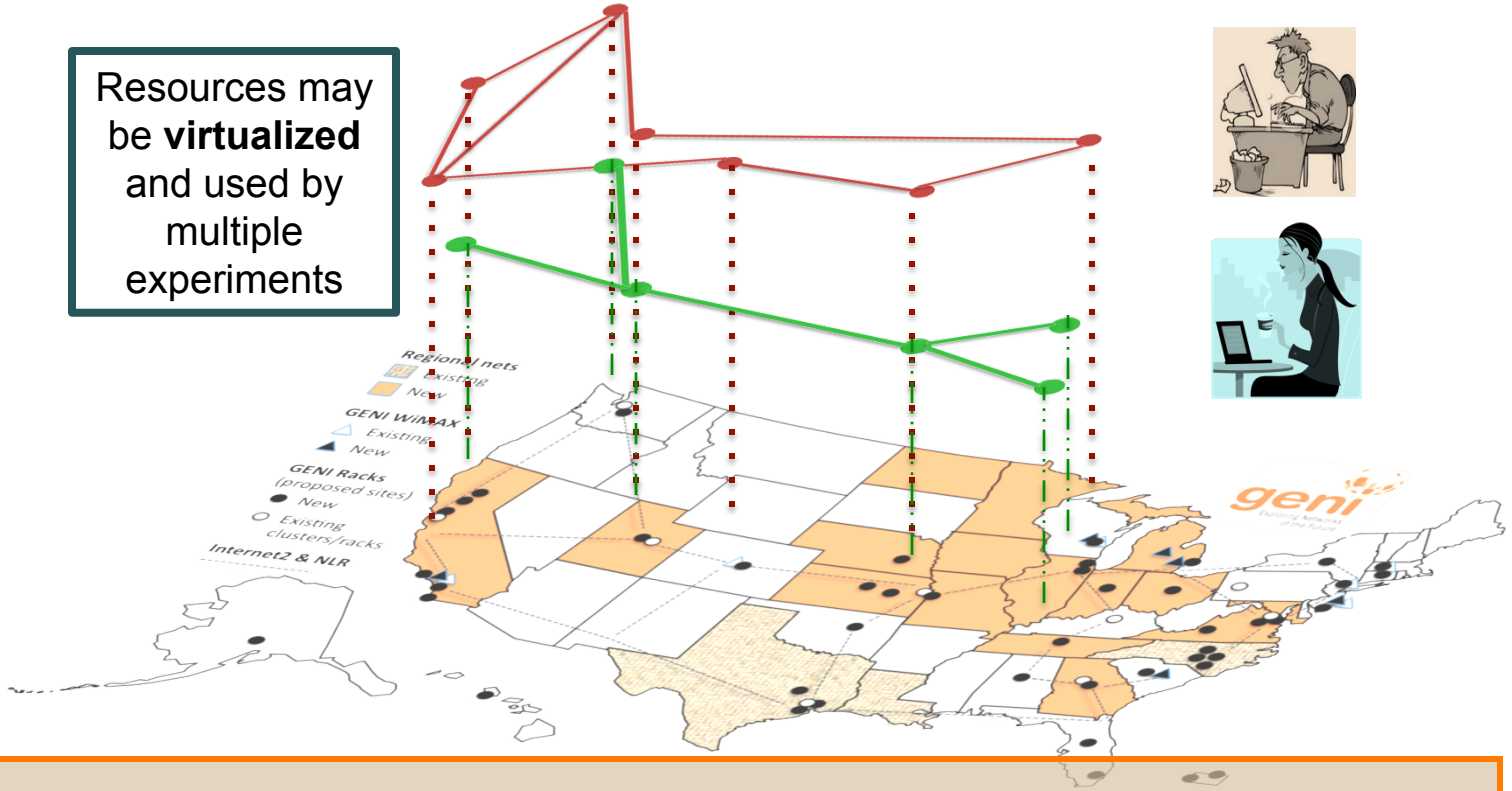
Sliceable
supports concurrent experiments

Deeply programmable
program everything, control forwarding

Federation
scalability, evolvability, common APIs

GENI Slices

Resources may be **virtualized** and used by multiple experiments



Experiments live in **isolated** “slices”

Key Concepts

Sliceable

supports concurrent experiments

Deeply programmable

program everything, control forwarding

Federation

scalability, evolvability, common APIs

GENI is “Deeply Programmable”

I install software I want throughout my network slice (into routers, switches, …) or control switches using OpenFlow

Experimenters can set up custom topologies, protocols and switching of flows

Key Concepts

Sliceable

supports concurrent experiments

Deeply programmable

program everything, control forwarding

Federation

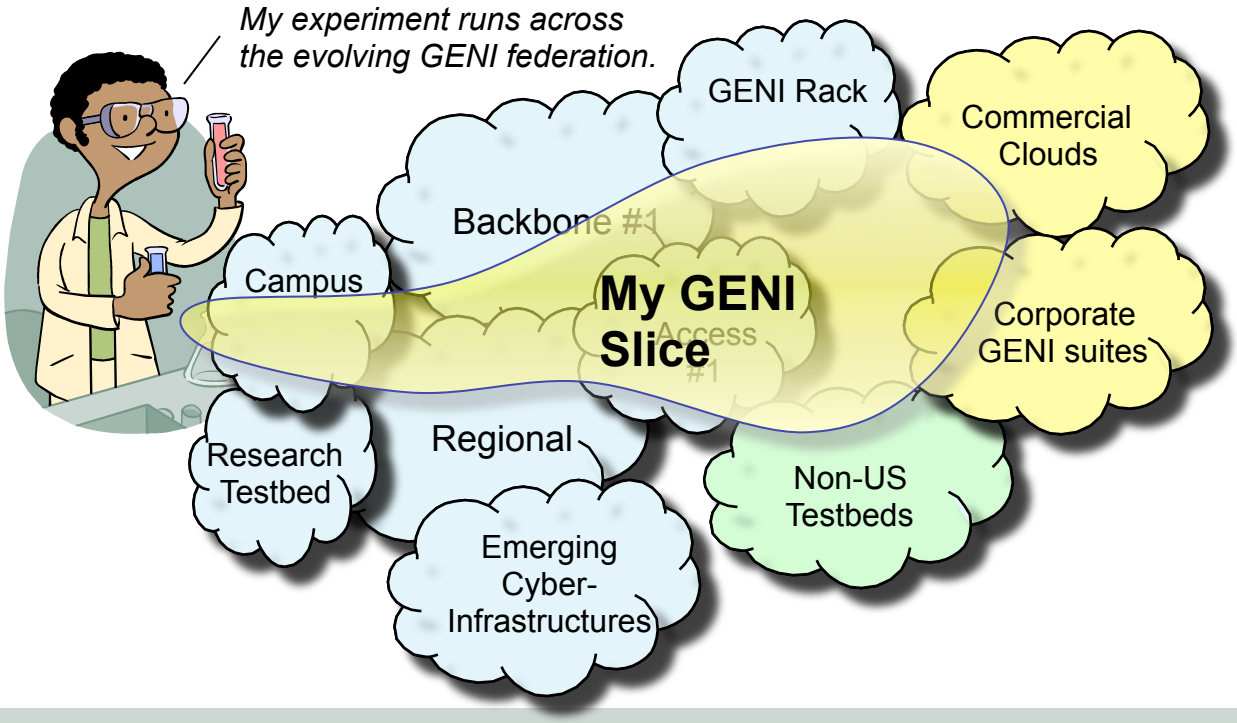
scalability, evolvability, common APIs

Federation

- Resources owned and operated by different organizations (aggregates)
  - Managed by local IT of that organization
- Aggregates provide resources to experimenters with GENI issued user and slice credentials
  - May implement local policy on who can get how many resources from that site

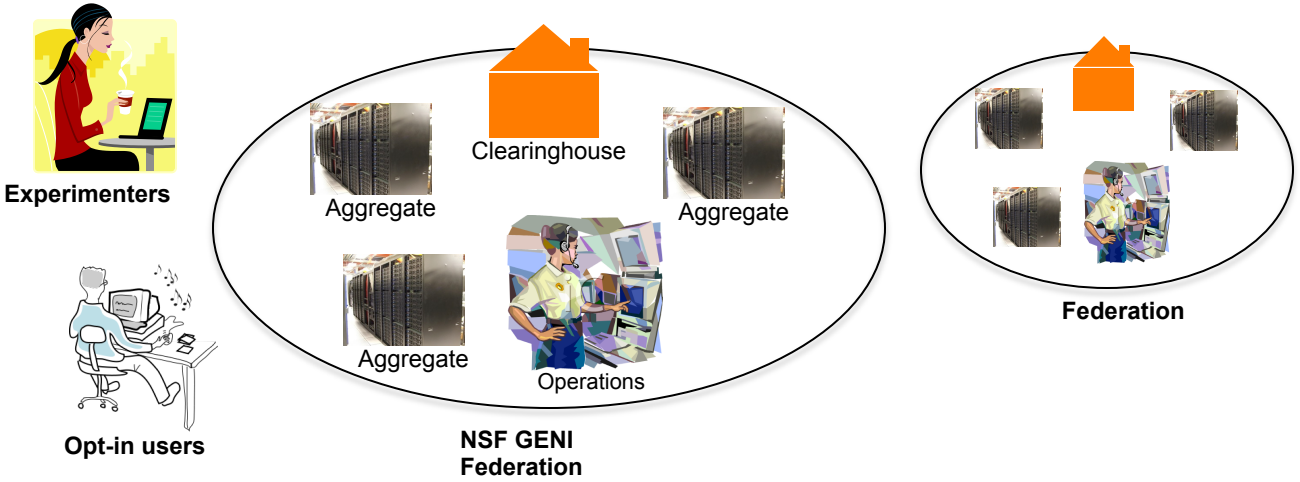
Federation

A GENI experiment may include resources from multiple aggregates (resource providers)



Resource owners do not authenticate individual users

GENI Security



- Security responsibilities shared among members of the GENI federation
- Federation agreements spell out responsibilities
  - Aggregate Provider's Agreement, Clearinghouse Provider's agreement, Acceptable Use Policy…

GENI Clearinghouse: Federation Trust Root

- Issues slice and user credentials
- Issues credentials
- Tracks project and slice membership

The NSF/GENI Federation has three Clearinghouses

Giving Experimenters the Resources they Want

Experimenter

Resource Owner

Who is this guy?
What should I allow him to have?
What happens if something goes wrong?

Expanding Resource Owner's Concerns

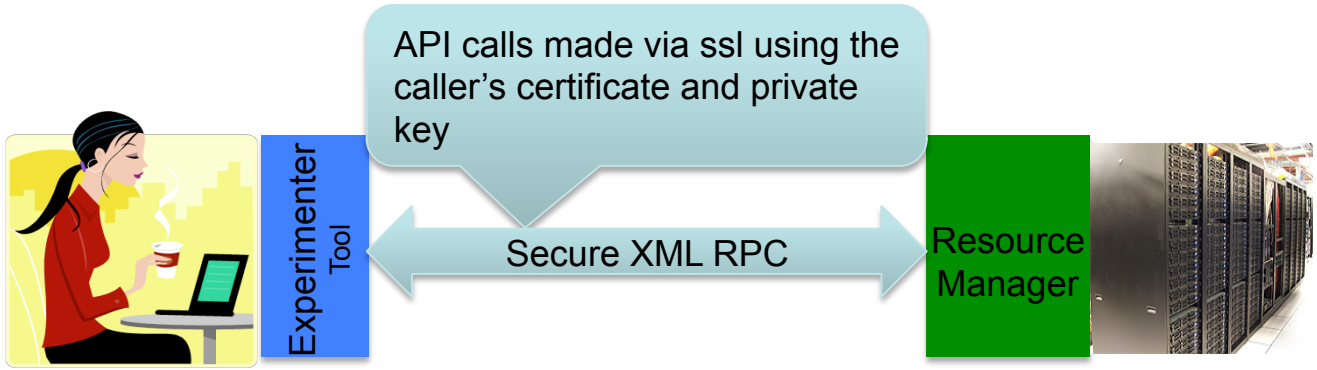
- "Who is this guy?": ***Authentication***
  - We need to know that the person asking for resources is who they claim to be.
- "What should I allow him to have?": ***Authorization***
  - We need to be able to determine which users are entitled to which resources in which context.
- "What happens if something goes wrong?": ***Accountability***
  - We need to be able to tell when an experiment is behaving in a way that risks my resources, and if so, shut it down and keep it from happening it again.

Providing experimenters with authenticated, authorized, accountable access to resources is the foundation of the GENI architecture.

Authentication

A ***credential*** is a signed statement.
In GENI, we have many different kinds of credentials that are used in different ways

- A ***Certificate*** is an *identity* credential:
  - "The person bearing the private key associated with this public key has these attributes: UUID, URN, email…"
  - In GENI, these are in X509 format, signed by a Federation Member Authority.
- Certificates are the basis of ***Authentication*** in GENI.



GENI User Authentication

The GENI Portal leverages InCommon
for single sign-on authentication

InCommon®

Experimenters from 304 educational and research institutions have InCommon accounts

For many experimenters:

- no new passwords
- familiar login screens

About **70% of our 7700 users** come from InCommon institutions.

GENI Project Office runs a federated IdP to **provide accounts** for non-federated organizations.

Authorization: Slice and User Credentials

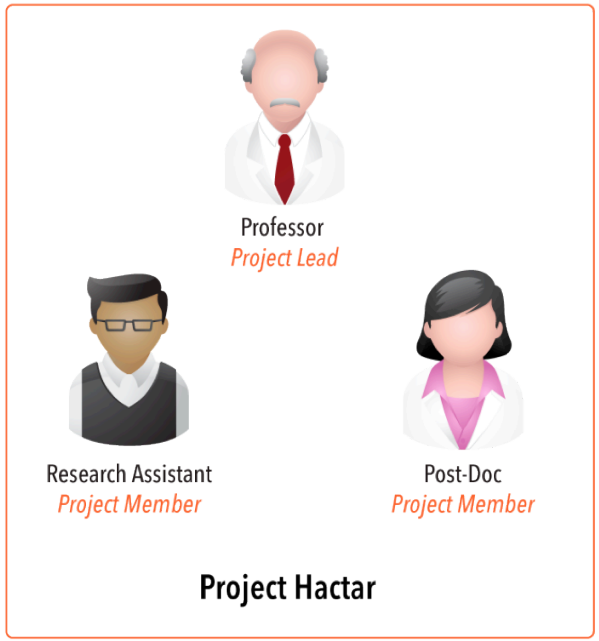
- Slice credentials are statements regarding rights and roles of a user with respect to a given slice
- User credentials are statements regarding rights and roles of a user independent of a slice
- The aggregate uses these to inform its own ***authorization*** decisions

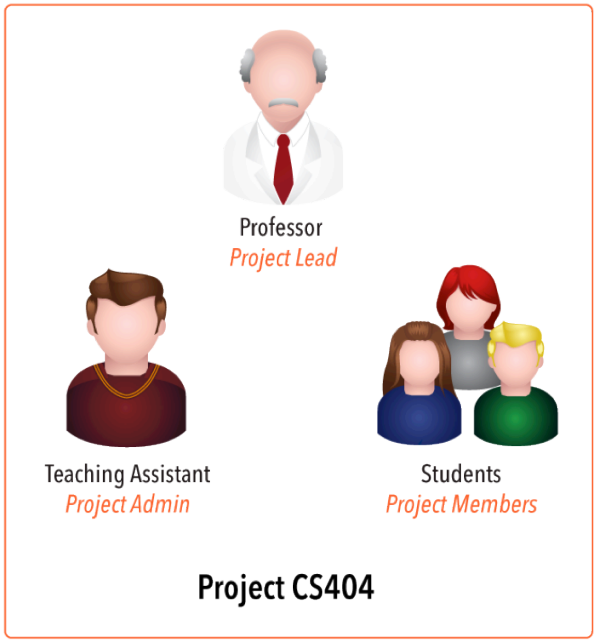
Authorization [2]

- Speaks-for Credentials
  - Agent: “I grant this tool (or user) to speak on my behalf.”
  - Actor: “I am acting on your behalf”
    - And YOU are accountable
- Delegation Credentials
  - Agent: “I grant a particular right/privilege of mine to this other user”
  - Actor: “I am acting with your blessing”
    - And I am accountable

Accountability

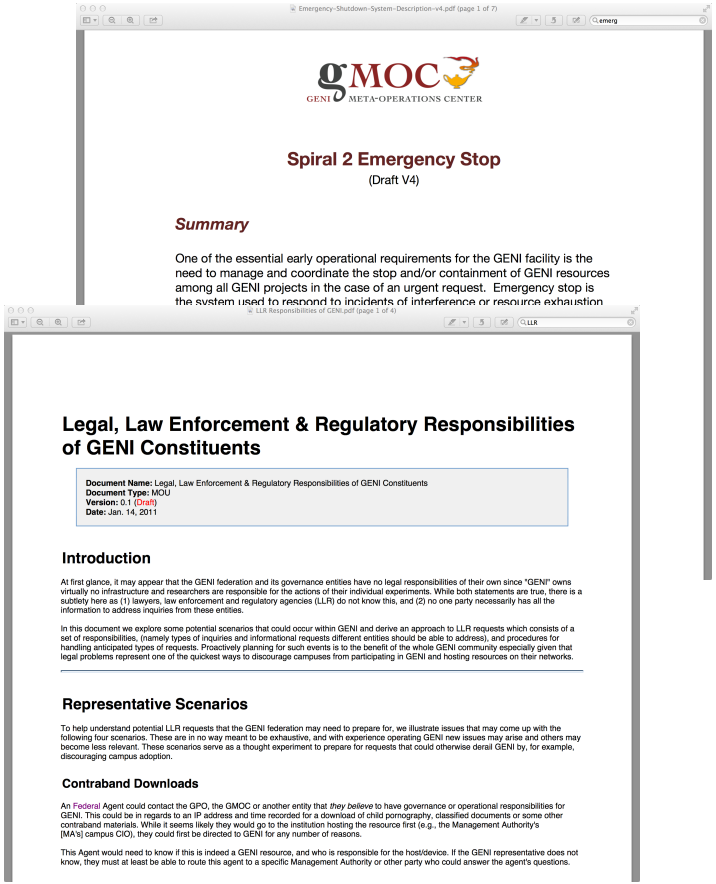
- GENI slices (experiments) are created in the context of a “project”
- Project lead must be a faculty member or senior staff member
- Project lead responsible for actions of project members





Accountability

- GENI Meta-Operations Center (GMOC) at IU coordinates operations
  - Emergency stop procedure
  - Coordination of investigation
- GENI Legal, Law Enforcement & Regulatory Representative



GENI META-OPERATIONS CENTER

Spiral 2 Emergency Stop
(Draft V4)

Summary

One of the essential early operational requirements for the GENI facility is the need to manage and coordinate the stop and/or containment of GENI resources among all GENI projects in the case of an urgent request. Emergency stop is

Legal, Law Enforcement & Regulatory Responsibilities of GENI Constituents

Document Name: Legal, Law Enforcement & Regulatory Responsibilities of GENI Constituents
Document Type: MOU
Version: 0.1 (Draft)
Date: Jan. 14, 2011

Introduction

At first glance, it may appear that the GENI federation and its governance entities have no legal responsibilities of their own since "GENI" owns virtually no infrastructure and researchers are responsible for the actions of their individual experiments. While both statements are true, there is a subtlety here as (1) lawyers, law enforcement and regulatory agencies (LLR) do not know this, and (2) no one party necessarily has all the information to address inquiries from these entities.

In this document we explore some potential scenarios that could occur within GENI and derive an approach to LLR requests which consists of a set of responsibilities, (namely types of inquiries and informational requests different entities should be able to address), and procedures for handling anticipated types of requests. Proactively planning for such events is to the benefit of the whole GENI community especially given that legal problems represent one of the quickest ways to discourage campuses from participating in GENI and hosting resources on their networks.

Representative Scenarios

To help understand potential LLR requests that the GENI federation may need to prepare for, we illustrate issues that may come up with the following four scenarios. These are in no way meant to be exhaustive, and with experience operating GENI new issues may arise and others may become less relevant. These scenarios serve as a thought experiment to prepare for requests that could otherwise derail GENI by, for example, discouraging campus adoption.

Contraband Downloads

An Federal Agent could contact the GPO, the GMOC or another entity that *they believe* to have governance or operational responsibilities for GENI. This could be in regards to an IP address and time recorded for a download of child pornography, classified documents or some other contraband materials. While it seems likely they would go to the institution hosting the resource first (e.g., the Management Authority's [MA's] campus CIO), they could first be directed to GENI for any number of reasons.

This Agent would need to know if this is indeed a GENI resource, and who is responsible for the host/device. If the GENI representative does not know, they must at least be able to route this agent to a specific Management Authority or other party who could answer the agent's questions.

Security Audits

- The NSF has funded outside teams to assess GENI security
- Steve Schwab of ISI currently has contract to do so

Common Security Incidents

- Experimenters using unpatched kernel versions
- DDoS amplification attacks on experimenter VMs
  - Portmapper
  - NTP

GENI for Cybersecurity Research and Education

- DDoS mitigation using SDN
- OpenFlow based firewalls and NATs
- Man-in-the-middle attacks
- ToR networks

Every semester GENI is used in over a dozen computer networking, distributed systems and security classes

Summary

- GENI seeks to build a trusted environment in which experimenters and resource owners can participate in resource allocation
  - These trust relationships reflect human/inter-organizational relationships, nothing more.
- Authorization, Authentication, Accountability are the pillars of that trust
- Credentials and Policies are critical enablers

ADDITIONAL INFO

GENI's footprint