

Reasoning for Security Architecture

March, 2011

Darwin Witt

While GENI allows for the development of a clean-slate network in which we can devise and construct all necessary authentication, authorization and security protocols to allow for secure Internet-style communication; a control framework that relies heavily on existing Internet protocols supports the GENI system. Therefore, consideration must be made to make sure this control framework is secure while prototypes are being constructed.

Another major concern is that pre-existing secure protocols, such as corporate and government PKI and authenticated identities, would be far too difficult to maintain due to GENI's proposed size.

GENI's method for growth via federation is also a cause for concern, because different authorities that have different authorization schemas typically manage such separate systems.

Due to the evolution of network protocols within GENI, there has been a move away from individual identities to attribute based identities and access control, meaning that the aspects of the principal's attributes may change as the principal interacts with the system. This is in stark contrast to the existing client-server based Internet where the client and server system must be explicitly identified and both have a common understanding of the expected identities or attributes that are important.

This also threatens the usage of old security protocols that rely on a well-defined notion of end-system address as a pre-requisite for negotiating and establishing an authenticated communication channel. Concerns related to keeping such well-defined addresses are due to the fact that in the current Internet, identities and addresses are linked, while GENI proposes flexible identities and addresses that may be unrelated.

There are three broad classes of attacks that must be addressed by the GENI Security Architecture and its operational procedures: external attacks launched by outsiders on the GENI infrastructure, accidentally or maliciously misbehaving GENI experiments, and finally a level of isolation between experimental slices.

The following are security threats that are liable to either be frequent occurrences or have serious effects on the GENI project during the prototyping phase. It has been suggested that the GENI Security Architecture be developed with these in mind.

- Containing runaway experiments causing unwanted traffic.
- Isolating runaway experiments that disrupt the execution environment for other experiments within GENI, e.g., by exhausting computation resources.
- Containing the misuse of an experimental service by an end user.

- Preventing and detecting theft or corruption of an experimenter's credentials to use GENI.
- Denial of service attacks against the GENI infrastructure.
- Direct attacks against vulnerabilities in the GENI management software.
- Privacy of experimental data and the privacy of management policy.

The nature of the GENI Security Architecture will assume that common security practices, such as updating mission-critical software on hardware components, will be in place. In addition, the researcher should not have to assume trust of the nodes, network environments, and other end-users of the GENI network, nor should it be necessary for the components or component managers to trust the rest of the GENI control framework it is connected to. This is due to the fact that the GENI architecture grants the component manager the authority to start and manage slices locally.