ExptsSec: S2.a. Experiment Design Document

Xiaoyan Hong, Fei Hu, Yang Xiao
University of Alabama
February 09, 2010

The goal of the project is to help define GENI security requirements. It will perform experiments and investigate selected security issues through ProtoGENI. This document describes the guidelines for initial preliminary experiments exploring security vulnerabilities in GENI/ProtoGENI. ProtoGENI is an implementation of GENI. Our first experiments will be performed using Emulab aggregate. At this time, we anticipate the possibilities that a few experiment findings may pertain to ProtoGENI (rather than GENI in general), due to the fact that a few related functions in ProtoGENI are in their initial statuses. This document is based on documents of GENI, ProtoGENI, and our trail experiments in Emulab and ProtoGENI.

An experimenter's interactions with GENI/ProtoGENI include initial authentications and later (maybe repeatedly) use for experiments. The security concerns relate to the GENI architectural building blocks, and the active experiment environment. This document describes potential security weaknesses and hence the experiments exploring them for the above two aspects. It organizes in the following three issues, namely, the authentication, the execution-time interaction with control frame, and the aggregate components in the virtualization that are involved in experiments. Experiments we plan to perform are listed for each issue. Some experiments may be performed at a later time. The experiments will be performed with careful supervisions, with notifications to related personals and will only perform against own testing PCs and slices.

This document reflects the feedback from ProtoGENI Utah team.

1. Authentication

   ProtoGENI authentication process 's first step is to acquire SSL certificate. The users use the Emulab webpage to generate a certificate from their Emulab passwords and a PassPhase, and then they can download their certificates to the local machine before using ProtoGENI.

   The potential vulnerability could be: attackers possibly steal the certificates of the authentication if they can inject malicious code, such as torjan horses to users' local machines. Our experiment could try to compromise the local host. Further experiments can use the certificates to manipulate the victim slices and users.

2. Experiment run-time interaction with ProtoGENI

   To perform experiments, users will interact with ProtoGENI control framework (clearinghouse, slice authority, component manager) to create a slice (including registering slice, requesting and redeeming tickets), then to use/renew the slivers, also to delete/unregister the slice. Exploring these steps, one could potentially pose threats to GENI

experimental services to other experimenters. The threats could impact the accessibility and availability of GENI. Our planned experiments include:

1) We could try DoS attacks through mixed steps of registering, creating , renewing, deleting and unregistering.
2) We could try to perform stress tests to see if the recourse usage is confined to its specification, to see if other sliver creations could be affected. In this aspect, Emulab experiments may demonstrate differently from ProtoGENI nodes.
3) We could try to test whether a sliver can receive from (or send to) another slice, or outside network.

3. Aggregate components and management

ProtoGENI slice authority will assign certain nodes and links to the ProtoGENI users using VLAN. The involved system components show three types: one is experiment host related system software, such as the OS and software set in the local host and in the virtual machines, the second one is GENI/ProtoGENI services such as aggregate manager and component manager, the third type is the virtual network components such as routers/switchers/gateways and links connecting them. All will potentially render vulnerability to DoS (Deny of Service) or DDoS (Distributed Deny of Service) attacks. The experiments will mimic attacking behavior to attack the components. We plan to perform the experiments:

1) We may run some codes (experiments) to automatically or manually scan the nodes for vulnerabilities, to break into them, and then install attack codes. The scan could be tested from nodes inside the current slice to outside, and vice versa. A small ProtoGENI test environment should be requested for this test.
2) We can also try to exploit different weaknesses, and then use this to consume excess amount of Components Manager's resources.
3) It is always common to see IP spoofing attack, we can also test the source address validity through the AC and CM. This issue relates to how the firewall is configured at the control frame.
4) We could try to compromise the third type component and to alter network topology. An issue to consider is that the control VLAN is not public known to experimenters.