ExptsSecurity – Additional Project Report

Summary Experimentation Findings and Suggestions

Period: Fourth quarter 2010

Title: GENI Experiments for Traffic Capture Capabilities and Security Requirement Analysis

Here to summarize our findings and suggestions reported in the technical document "Explore ProtoGENI Security Problems From Experimentation". More summary items will be added soon.

Summary part I relates to wireless testbed at Utah. Some experiments are performed using Emulab.

(a) In wireless testbed, sniffing is possible.

(b) We successfully launched a DOS attack from one (launching) experiment to another (victim) experiment. Using the addresses sniffed by the launching experiment, we sent wrong ARP data to disrupt the ARP table at the victim node. That caused the victim node to send frames to bogus receiving node.

(c) We found that DOS attack through TCP SYN flooding cannot successfully attack the TCP connections in wireless testbed using a similar two-experiments approach.

(d) We found that TCP SYN flooding attack can still decrease the throughput of another experiment in wireless network. Even when the attacker uses a different channel, throughput degradation still occurs.

(e) We found that current web interface for wireless resource allocation (by the users) leaves a time gap between node selection and real allocation. This can lead to “resource scramble”, i.e., a selected node can not be allocated. A suggestion is to provide a real time resource reservation interface.

Summary part II relates to control framework's resource allocation.

(a) A bug (cross-slice communications) in the development phase was discovered and fixed. The particular case sent traffic to another slice (relating to the isolation of slices in virtualization). The issue is fixed and validated through experiments.

(b) Extra large delay (hence large delay variance) was discovered in multi-hop topology experiments. This special case may be due to the shared use of Vnode (relating to resources in virtualization).

(c) Stress tests showed stable use of ProtoGENI resource by the experimenters as it is declared in the resource requests. This shows the property of separation in resource allocation.

Summary part III relates to experimenter's authentication and test scripts and interfaces.

(a) At the local machine of an experimenter, locations of SSL certificates and SSH keys are easy to find and thus are subject to stolen.
(b) "test-common.py" is the core of all the experimenter's scripts, it can be tampered to prompt an experimenter of "system available". The code can be more seriously changed.
(c) Flash interface could expose an authenticated experimenting environment to any people who happens to have an access of this web browser, or to a Trojan horse planted in the location machine.