Milestone ExptsSec: S3.d Experiment Design Document 3

Sept 17, 2011

Jason Bowman, Jincheng Gao, Xiaoyan Hong, Mohammad Hoque, Fei Hu, Dawei Li, Darwin Witt, Yang Xiao

University of Alabama

A. Summary

For the Milestone S3.d, we performed several analysis and experiments to explore vulnerability of ProtoGENI/GENI:

(1) Analyzed the security architecture and authorization mechanism in GENI.
(2) Performed experiments to explore potential deny of service (DoS) when multiple ProtoGENI aggregates are used.
(3) Performed experiments to validate the security concerns with ProtoGENI OS images.
(4) Performed primary experiments for analyzing security of GENI web access.
(5) Performed ProtoGENI DoS/DDoS Attacks

B. Experiment Description and Results

(1) Analysis of GENI Security Architecture

GENI relies heavily on existing authentication, authorization and security protocols to allow for secure Internet-scale management, operation and communication. One mechanism GENI uses is to implement a hierarchy of authorization of individuals and experiments through PKI. Such a mechanism is well developed through Clearing House and its interactions between Component Manager and Slice Authority (SA). Credentials will be used and passed around when an experimenter requests and uses slices and slivers. Then, GENI architecture grants the component manager the authority to start and manage slices locally. 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. Further, GENI control framework itself uses existing Internet protocols for managements and operations. Therefore, considerations are made to make sure this control framework is securely constructed.

Due to GENI's proposed size and its method for growth via federation, the pre-existing secure protocols, such as corporate and government PKI and authenticated identities, would be far too difficult to maintain, because different authorities that have different authorization schemas typically manage such separate systems. Currently, it is also under investigation for the GENI to use attribute based identities and access control. With this latter scheme, the aspects of the principal’s attributes may change as the principal interacts with a federated system.

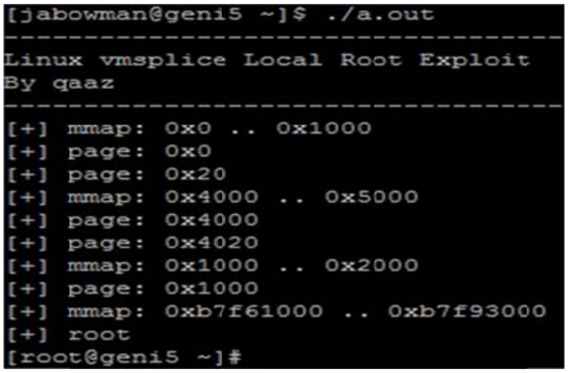
(2) Deny of service (DoS) experiments with multiple ProtoGENI aggregates

ProtoGENI allows users to request experimental nodes from different Component Managers (resource providers). The experimental nodes from different CMs are connected using GRE tunnels. We used an ARP cache poisoning attack to launch a DoS attack from one slide to another active slice. We observed different consequences in associated with different traffic patterns generated by the active experiment. We found that the ARP attack can cause a busy link, i.e., a link with traffic, to loss packets, but the link connection sustained under the attack. While on the hand, an idle link is subject to ARP attack. The attack will lead to a “connection closed” error when the user tried to ssh to the victim node in the active slice.

<u>Suggestions:</u> There is a need to consider tools to protect ProtoGENI experiments. Common tools may apply. We also plan to perform more experiments in this direction.

(3) Analysis of the security concerns with OS images

ProtoGENI is a collection of many components. At present, experimenters are unable to utilize custom machine images and must use those provided by ProtoGENI. According to the ProtoGENI wiki, only the FEDORA8-STD image fully supports all available nodes. With the limited availability of machine images to experimenters it is important to ensure their security. The level to which the provided image is patched may be unknown to an experimenter and his experiment may be at risk of compromise.



```
[jabowman@geni5 ~]$ ./a.out
-----------------------------------
Linux vmsplice Local Root Exploit
By qaaz
-----------------------------------
[+] mmap: 0x0 .. 0x1000
[+] page: 0x0
[+] page: 0x20
[+] mmap: 0x4000 .. 0x5000
[+] page: 0x4000
[+] page: 0x4020
[+] mmap: 0x1000 .. 0x2000
[+] page: 0x1000
[+] mmap: 0xb7f61000 .. 0xb7f93000
[+] root
[root@geni5 ~]#
```

Our experiment efforts focus on identifying vulnerabilities related to elevation of privilege once an attacker or user has gained access to a machine. We attempted to gain elevated privilege on several machine images. We were able to gain elevated root privileges on the FC6-STD image by exploiting a published vmsplice kernel vulnerability. Figure 1 is the screen shot of our experiment result. This particular exploit was not effective against the provided RHL-STD image, but that does not ensure other attacks wouldn't be equally effective. We were also able to gain root access to FBS72-STD image using another published vulnerability. Our approach was not exhaustive and other vulnerabilities may also exist, the intentions behind our efforts are to underline the importance of ensuring that system images are up to date.

Suggestions: Possible countermeasures to these kinds of vulnerabilities include ensuring the availability of recent and up to date system images and aggressive patching of known vulnerabilities in existing images.

(4) GENI Web access security analysis

Current GENI development is moving towards user convenience by using thin-client side web portal like "Emulab" and "Flack". The convenience is coming along with new security challenges caused by web-based attacks. We have conducted preliminary network experiments through Flack. But we haven't conducted experiments to explore potential risks. We'd like to continue in this direction.

(5) ProtoGENI DoS/DDoS Attacks, Jincheng Gao and Yang Xiao

Various DoS attacks have applied to the ProtoGENI nodes.

Classic DoS Attack: ICMP flood attack worked on the ProtoGENI node. After flooding the Victim's Node using ICMP flood for about 20minutes, the Victim's node rebooted itself. Also we conducted UDP flood attack on the ProtoGENI node; through the packets sniffed by the "victim" node we can conclude that given enough flood traffic flow, DoS is possible.

Advanced DoS Attack: we conducted source spoof attack and SYN spoof attack. Both spoof attack make the victim's SSH connection not open anymore. Even after we checked that sliverstatus.py showed the node was "started" and "ready", we could not use ssh command line to connect the victim anymore.

DDoS Attack: Our DDoS attack experiment showed that it is possible to exploit ProtoGENI nodes to launch DDoS attacks and succeed. After hacking the victim for about half an hour, the scan application of the victim's stopped working, and we tried to use ssh login victim's node was refused.

Even further, we could not access all the sliver nodes in that victim's slice. We failed in delete either that slice or that sliver, due to "the resource was busy". We also could not create new slice to do other experiment until the victim's slice will time out after 7200 minutes (5 days). Therefore, to this extent, the DDoS hacking successfully damaged the whole ProtoGENI user's credential for a while in the Slicing Authority.

However, since most of the ProtoGENI nodes are linux-based nodes, it is a lot of effort for the attacker to install the hacking tools on a large number of workstations or PCs even though the hacker gains the access to them and makes them to either zombie handlers or zombie agents to attack the actual victim. This means DDoS attack on ProtoGENI nodes is possible but effort-taking, but when we hacked the victim's node, the damage is much more than previous hacking experiment.

C. Future work

We are interested in a few directions for further investigations.

(1) Analysis of authentication, access control in GENI, ProtoGENI or other clusters.
(2) More experiments considering multiple aggregations and federation.
(3) Following common web-based security attacks to investigate the potential risks of GENI web access.
(4) Investigating issues listed for Year 3 milestones.