1783 Milestone ExptsSec: S4.b Report for GEC 13

University of Alabama
Dawei Li, Jingcheng Gao, Lei Zhao, Xiaoyan Hong, Fei Hu, and Yang Xiao
March 7, 2012

(1) ProtoGENI access control

We analyzed the public-address-based ProtoGENI architecture and a VPN-based Emulab environment. ProtoGENI architecture uses public accessible IP addresses for users to operate and control their experiment nodes through SSH. This will leave chances for external attackers to attack the experiment nodes. We have tried a port scan tool to find open ports. On the other hand, an Emulab testbed can be built to require VPN access before connecting to experimental nodes through SSH. Comparing these two access methods, the public-address-based ProtoGENI's access security is weaker.

Suggestions: potential solutions can be to enforce more strict firewall rules; or, for some ProtoGENI sites, to place the whole system behind a VPN.

(2) Follow-up early experiments

We have repeated the ARP based experiments per the results we reported at GEC12. And we found that we could not succeed this time. This validates that some kind of defense strategies have been deployed in ProtoGENI after GEC 12.

(3) Selection over a few clouds in GENI.

We analyzed the current available information on a few clouds in GENI. We were looking for information on system architectures and usage information. We analyzed the VICCI Cloud, GENICloud and DiCloud. The VICCI Cloud is based on PlanetLab but currently only users from the four hosting universities can use them. We didn't find enough usage information for GENICloud. The most feasible cloud to work on is DiCloud which is in conjunction with ORCA and can be used through Gush. DiCloud allows user to experiment with Amazon Web Service cloud resources including EC2, S3, EBS. Since it is budge limited project, the security to resources usage is important though the per user usage can be monitored.

(4) DoS/DDoS Security Tests

We continuously conducted some DoS/DDoS security experiments, which will be partially reported in First GENI Research and Educational Experiment Workshop (GREE12), in conjunction with GENI GEC 13. We conducted multiple sets of DoS/ DDoS attacks in the current ProtoGENI testbed, Spiral 3 [1]. These attacks show that it is very possible that ProtoGENI nodes may render vulnerabilities to such attacks [1], including Classic DoS Attacks (ICMP Flood Attack, UDP Flood Attack), Spoofing

DoS Attacks (Source Address Spoofing, SYN Spoofing), and Advance DoS Attacks (DDoS Attacks) [1].

[1] J. Gao and Y. Xiao, "ProtoGENI DoS/DDoS Security Tests and Experiments," Proceedings of First GENI Research and Educational Experiment Workshop (GREE12), in conjunction with GENI GEC 13.