ExptsSecurityAnalysis:

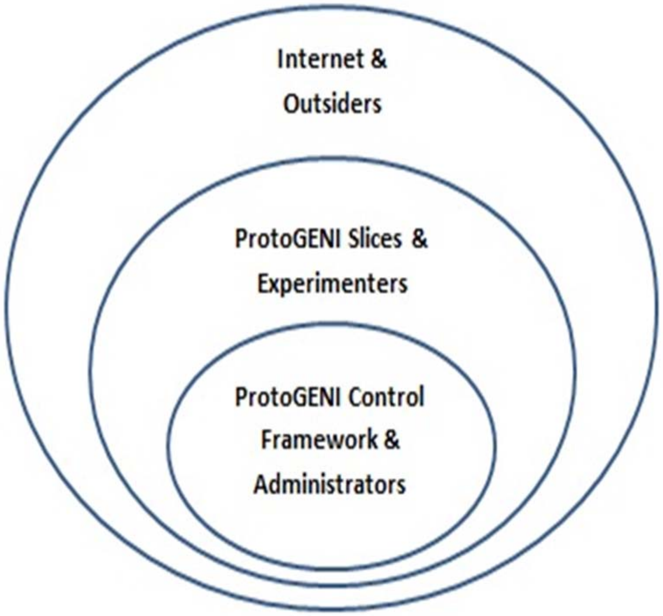
GENI Experiments for Traffic Capture Capabilities and Security Requirement Analysis

Xiaoyan Hong, Fei Hu, Yang Xiao
Jincheng Gao, Dawei Li, Fnu Shalini
Darwin Witt, Jason Bowman
University of Alabama

Project Introduction

- Project Goal:
  - To find vulnerabilities through ProtoGENI experiments
    - As an insider!
  - To suggest prevention approach
- GENI Security Goals:
  - To avoid being abused to conduct illegal activities or as a launchpad for attacks, and to ensure the availability of services not being compromised by attacks
- Year 2 findings and suggestions

THREAT MODEL



- Experimenter as an insider
  - Data Plane to Control Plane
    - Compromise the availability of ProtoGENI resources to other users
  - Data Plane to Data Plane
    - Compromise the correctness and confidentiality of other running experiments
  - Data plane to Internet
- Experimenter as a victim from an outsider

Network DoS experiments

Findings	Suggestions

An SSH connection from local PC to a sliver node can be disconnected.	(Performed using ARP Cache Poisoning)
	Tune ARP frequency;
	Software: ARPOn, ARPWatch;
	Hardware ARP Defender, VLANs;
	OS: Static ARP entry;
	Free node sleep;

A free node (as resource) can be prevented from being allocated to a requesting slice.	
A tunnel connection between Utah and Kentucky can be disrupted to loss 95% ping packets.	
Distributed flooding attack to Internet hosts from different sites, only warned by Utah site	Automated anomaly traffic detection; Install warning system at all CMs; emergency stop;
Flooding Control Framework	
A follow-up issue: the free node status was not correct for a few days after the ARP attack.	

Network DoS experiments (cont’d)

Findings	Suggestions
Classic ICMP flood, UDP flood, possible	Automated anomaly traffic detection; Install warning system at all CMs; Emergency stop
Advanced source spoof and SYN spoof possible, victim’s SSH connection not open anymore	
DDoS attack to a ProtoGENI node is possible, SSH connection close. Other nodes are not accessible too. The user can not create new slice.	
A follow-up issue: the user lost credential (can not delete or create new slice) until the victim slice expires .	

System issues

Findings	Suggestions

Dated Operating System.
E.g., Fedora 8 known issues:
Gain elevated privilege;
Unauthorized remote access;
Initial DoS attack;
	Update OS image as soon as possible;
	Using automated system updates;

Exposed Open Ports --though filtered by firewall, still has port open to Internet:
with known vulnerabilities like port 32769;
ports of well known services (5001 of Iperf);
GENI software;
	Refined filter;
	Leverage the scope of open ports;
	Service specific monitoring;
	VPN connection;

Spread malware using current file transfer method	Transfer encrypted data

- Thank you!
-
- Welcome to our demo!

- Questions and suggestions highly welcomed!