1783: GENI Experiments for Traffic Capture Capabilities and Security Requirement Analysis

Initial Experimentation

Xiaoyan Hong, Fei Hu, Yang Xiao
Students:
Jingcheng Gao, Dawei Li, Dong Zhang
The University of Alabama

Introduction

- Goal:
  - help define GENI security requirements based on investigations through ProtoGENI experiments
- Approach:
  - Select functions of ProtoGENI control framework
  - Experiments on aggregates (EMULAB first)
    - Experiment design, run, identify/exploit/validate potential vulnerabilities
    - Delivered experiment design documents
- Initial Experiments
  - Authentication, experiment run-time interaction, Aggregate components and management

Initial Experiments: Authentication

- Port scan is possible from outside
  - IP addresses are visible
    - Trace route or netstat -r , from local machine
  - Using free scan tools
- Results:
  - Port 22 is open (SSH)
  - Others are closed - mean safe at this moment

Conti'd

- Stealing SSL is possible (given a tragon horse)
  - other user account can use the stolen SSL certificate and PASSPHASE to perform all steps (of creating slice, start sliver, deleting etc)
  - Can manipulate the victim's active experiments
  - Can maliciously occupy resources in victim's name.
  - More to test.

Initial Experiments: Interaction

- Mixed steps of registering, creating , renewing, deleting and unregistering, etc.
- Purpose is to find the weakness in handshake procedure (like TCP SYN attack)
  - Test-common.py
    - leading to XMLRPC
    - Possible ways to modify the code for other purposes.
  - Create Sliver
    - If getticket.py and redeemticket.py are performed separately, we tested for possible TCP SYN flood -- in short time period.
    - Results: system does not allow multiple getticket from one slice
    - Possible way of creating many slices each performing getticket.py is still possible.
  - Others analyzed

Initial Experiments: VM

- Aggregate components and management
  – Installed FreeBSD
  – Port scan #23 (telnet) to identify FreeBSD by “%...”
  – Tried port 23 vulnerability
- Multihop topology