GENI Experiments for Traffic Capture Capabilities and Security Requirement Analysis

University of Alabama
PI: Xiaoyan Hong, Fei Hu, Yang Xiao
Participated students: Dawei Li, Fnu Shalini, Dong Zhang

GEC9, Nov 2, 2010

Sponsored by the National Science Foundation

Project 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
    - Deliver experiment design documents, experiment reports
- Experiments are in three directions
  - Authentication
  - Experiment run-time interaction
  - Aggregate components and management

Summary of Findings for Year 1:

- Findings and suggestions are summarized in the table.

Findings	Suggestions
Account certificate and credentials at local machines are subject to be stolen if compromised. With those, register slices and create slivers are possible.	strictly check user's access behaviors.
Security parameters used in the run-time are subject to be stolen if local machine is compromised. With those, experiment nodes can be accessed.	Audit experiment traffic pattern.
Port scan be done from inside and outside of slices. Most ports are closed.	Add anti-scan function.
Identity and credential for flash interface are subject to the compromise of the local machine.	Additional user identity check before one can create a slice using the interface.
Test scripts do not generate blocking points for potential exploitation.	
ProtoGENI (residual) resources are subject to DoS attack. Tools can help attacker be more efficient and harder to detect.	Audit each slice's creation and destroy operations. Good traffic analysis tools.

(continue on next page. Notes: the findings are based on the recent release of CM and test scripts. July 10, 2010)

Summary of Findings for Year 1 (cont'd):

Findings	Suggestions
Slice isolation of bandwidth.	Performance is satisfactory under stress test
Delays between vnodes show large variance in RTTs.	Further ProtoGENI debug needed
Slices using shared vnodes could cross communicate under a particular condition.	Further ProtoGENI debug needed Repeated.

Activities Since Last GEC Meeting:

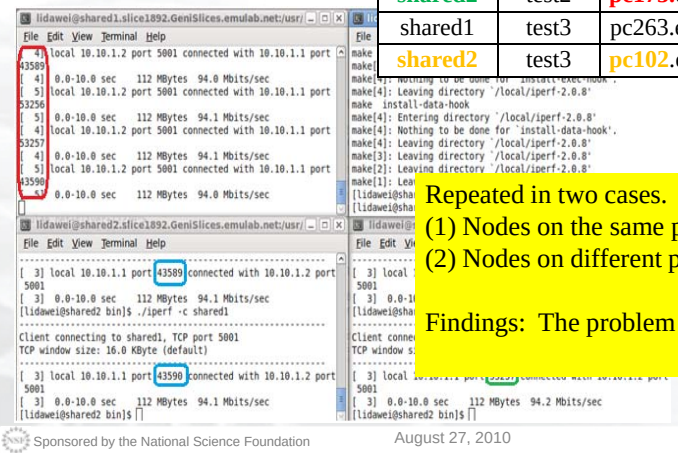
- Extend the scope to a wireless aggregate
  - Wireless nodes at Utah site
  - Initial experiments
  - Experiments going
- Experiments need to repeat to catch the new development

- Delivered Milestone#4 of year1;
- Planned SOW for Year 2;
- Next Milestone will due in the end of Nov.

Repeat of isolation issue

Node Name	Slice Name	Hostname	Port Number
shared1	test1	pc175.emulab.net	32058
shared2	test1	pc172.emulab.net	32058
shared1	test2	pc172.emulab.net	32570
shared2	test2	pc175.emulab.net	32570
shared1	test3	pc263.emulab.net	33850
shared2	test3	pc102.emulab.net	33850

43589, **53256, 53257**, 43590



Repeated in two cases.
(1) Nodes on the same physical nodes
(2) Nodes on different physical nodes

Findings: The problem didn't show.

Experiments with Wireless Nodes

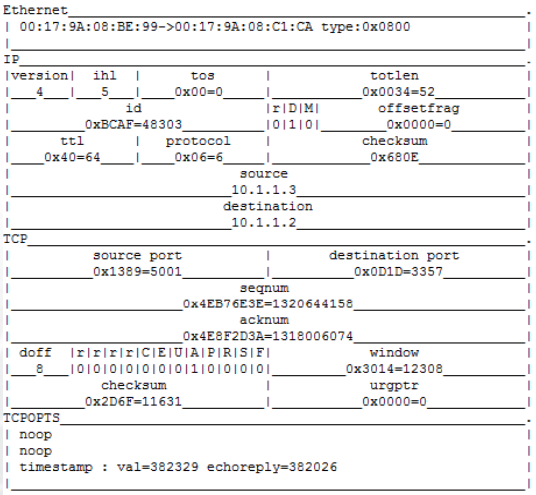
- The open wireless media makes it easier for one experimenter to intervene others' experiments
  - inherited physical deployment limitations for Emulab wireless nodes
  - Security and privacy policies are clearly given to the experimenters
- Our goal: reveal the potential threats that come from the wireless link and wireless networks
  - Eavesdropping capability
  - Selected protocols
- Do wireless nodes open protocol stack for exploitations?
- Is it possible to impact on resources and experiments in ProtoGENI and go beyond GENI?

Initial Investigations

- Test the configured parameters and the achieved metrics.
  - bandwidth, delay, packet loss, Lan mode (ad hoc vs Lan), protocol (b/g).
  - Ping, Rude and Crude, Iperf.
  - Observations: expected reduced achieved throughputs, can not add latency; ad hoc mode has extra loss.
- Test the channel interferences with two simultaneous experiments.
  - Capture observed
- Test multihop configuration in Emulab.
  - Resource allocation difficulty
- Test the capability of wireless traffic capture in Emulab/ProtoGENI.

Initial Test of Eavesdropping

- Installation of packet sniffers is possible.
- Two experiments.
  - Eavesdropping from another experiment, from the same channel.



SYN Flooding

>> netstat –na

```
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     9810   /dev/gpmctl
unix  2      [ ACC ]     STREAM     LISTENING     9894   /var/run/dbus/system_bu
s_socket
unix  13     [ ]         DGRAM                    9318   /dev/log
unix  2      [ ]         DGRAM                    8422   @udevd
unix  2      [ ACC ]     STREAM     LISTENING     8410   @kudzu_config_socket
unix  2      [ ACC ]     STREAM     LISTENING     9849   /tmp/.font-unix/fs7100
unix  3      [ ]         STREAM     CONNECTED     11348
unix  3      [ ]         STREAM     CONNECTED     11347
unix  2      [ ]         DGRAM                    10050
unix  3      [ ]         STREAM     CONNECTED     9897
unix  3      [ ]         STREAM     CONNECTED     9896
unix  2      [ ]         DGRAM                    9872
unix  2      [ ]         DGRAM                    9
unix  2      [ ]         DGRAM                    9
unix  2      [ ]         DGRAM                    9
unix  2      [ ]         DGRAM                    9
unix  2      [ ]         DGRAM                    9
unix  2      [ ]         DGRAM                    9
unix  2      [ ]         DGRAM                    9
unix  2      [ ]         DGRAM                    9335
unix  2      [ ]         DGRAM                    9322
[lidawei@nodew2 ~]$
```

Performed SYN flooding attack.
TCP connection status did not change.
Linux has protection mechanism.
The server being attacked slowed down.

- Potential issues:
  - Availability of resource for real multihop network.
  - Resource map has a lag indicating the availability.
  - How easy to ping in control network?

  e.g, at pc24.emulab.net

  >> ping pc25.emulab.net

  “ping xxx (155.98.36.25) 56 (84) bytes of data.

  ….
-