First Experiences with DETER Testbed

Dr. Xiao Su
Computer Engineering
San Jose State University
http://www.sjsu.edu/people/xiao.su

NSF TRUST WISE 2012
Agenda

- Prior experience with PlanetLab
  - Setup
  - Challenges in using PlanetLab in security research/education

- DETER Testbed
  - Overview
  - Setting up DETER experiments
  - Running DETER experiments

- Demo
Our Network Security Class

- How attackers think and work?
  - Attack phases

- What are the tools and algorithms to counter such attacks?
  - Crypto tools
  - Authentication
  - Access control
  - Key distribution

NSF TRUST WISE 2012
Experimental Setups

- Personal computer

- Local testbed
  - Isolated from campus networks

- Internet scale testbed
Challenges in Teaching Network Attacks

- Many tools need admin privilege
  - Sniffing, spoofing, MIM,…

- Attacking experiments hard to set up
  - Not interfering with normal network operations
  - Contained in a closed network
  - Some experiments heavily depend on compiler, OS types (e.g., buffer overflow)

- Hard to conduct security experiments in the Internet scale?
  - Evaluate how effective anti-DDoS schemes are?

- Need to use Internet scale testbed!!
Internet Scale Testbed - PlanetLab

1127 nodes at 544 sites (as of June 18, 2012)

Picture taken from http://www.planet-lab.org

NSF TRUST WISE 2012
Running Services in PlanetLab

- **First, create a slice (by PI only)**
  - UNIX shell access to a set of PlanetLab nodes
  - virtual machines
  - Faults or misbehaviors can be isolated and traced back to virtual machines

- **Create public/private key pair (by users)**
- **Upload public key to PlanetLab (by users)**
- **Remote access machines using ssh with slice name as the user name**
- **Install packages, deploy and run services**
Why Not PlanetLab in Security Experiments

- PlanetLab nodes are part of the Internet
  - Traffic impact the Internet: what happens when you experiment DoS on PlanetLab?
  - The testbed is closely monitored by a team of professionals, for network attacks, worm propagation, copyright infringement, and other malicious traffic.

- PlanetLab nodes run uniform Linux-based OS
  - Not possible if experiments require different types of OS
  - OS and network configurations on PlanetLab nodes are not customizable

- Operational concerns
  - Nodes in the same experiment (slices) don’t share home directories: lots of ssh copies
  - A good percentage of nodes not accessible by ssh, due to different ssh policies and versions
Here We Have DETER

DETER is a public testbed to run repeatable security experiments

- Based on Univ. of Utah’s Emulab
- Specially enhanced for security research/education
- Jointly run by USC’s ISI and UC Berkeley

Types of DETER Projects

---

NSF TRUST WISE 2012
# PlanetLab vs. DETER

<table>
<thead>
<tr>
<th>Feature</th>
<th>PlanetLab</th>
<th>DETER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Isolated or Open Network</td>
<td>Part of the Open Internet</td>
<td>Isolated Testbed</td>
</tr>
<tr>
<td>OS Uniformity</td>
<td>Only runs Linux OS (FC based)</td>
<td>Supports a large list of OS types</td>
</tr>
<tr>
<td>OS Customization</td>
<td>Not possible</td>
<td>Supports customized OS images</td>
</tr>
<tr>
<td>Network Configuration</td>
<td>Static, part of the Internet</td>
<td>Supports configuration of network, defined by NS scripts</td>
</tr>
<tr>
<td>Home directory</td>
<td>Different nodes have different home directories</td>
<td>Same home directory for all nodes</td>
</tr>
<tr>
<td>User Management</td>
<td>Site PI’s task</td>
<td>DETER support</td>
</tr>
</tbody>
</table>

**NSF TRUST WISE 2012**
Accessing DETER Testbed

- Login to https://www.isi.deterlab.net/login.php3

---

NSF TRUST WISE 2012
DETER Experiments

---

**News:**
- DETER Chat (IRC) no longer official support medium (2011-04-14)
- Web Login by email address is no longer supported. (2011-03-23)
- CSET'11 Call for Papers (2011-02-07)

**Scheduled downtime:** Wednesdays: 5PM-7PM, Saturdays: 10AM-1PM Pacific Time.

---

**Current Experiments**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SJSUCMPE209 BufferOverflow1004</td>
<td>swapped</td>
<td>1</td>
<td></td>
<td></td>
<td>Single node buffer overflow experiments on Ubuntu 10.04</td>
</tr>
<tr>
<td>SJSUCMPE209 SampleExp</td>
<td>swapped</td>
<td>3</td>
<td></td>
<td></td>
<td>To experiment with buffer overflow on Ubuntu 8.04</td>
</tr>
<tr>
<td>SJSUCMPE209 switchf2009</td>
<td>swapped</td>
<td>4</td>
<td></td>
<td></td>
<td>Experimenting with Active Snifing</td>
</tr>
<tr>
<td>SJSUCMPE209 synflood</td>
<td>swapped</td>
<td>5</td>
<td></td>
<td></td>
<td>TCP SYN flooding attack</td>
</tr>
</tbody>
</table>

1. Node counts in green show a rough estimate of the minimum number of nodes required to swap in. They account for delay nodes, but not for node types, etc.
2. A ? indicates that the data is stale, and at least one node in the experiment has not reported on its proper schedule.

---

NSF TRUST WISE 2012
Parameters to fill in

- Name of your experiment
- Description of your experiment
- Your NS file to specify a network topology
  - Don’t know NS? Use the GUI editor!

NSF TRUST WISE 2012
Beginning a New DETER Experiment

- Beginning experiment page
- This is how a GUI editor looks like

NSF TRUST WISE 2012
Configuring OS and Network Settings

- Configuring OS
- List of supported OS

NSF TRUST WISE 2012
Next Step: Swap Your Experiment In

- Be patient, may take sometime

NSF TRUST WISE 2012
Accessing Nodes in Your Experiment

- **First log into the gateway node**
  - ssh users.isi.deterlab.net

- **On gateway, accessing your nodes by**
  - ssh node0.homework2Test.SJSUCMPE209.isi.deterlab.net
Cleaning Up

- Swapping out your experiment
- Terminating an experiment
How Did We Use DETER in Our Class

- We used DETER
  - In-class demos
  - Assignments
    - Buffer overflow (Ubuntu 8.04LTS, gcc 3.x) – This combination of gcc compiler and OS version is hard to find now
    - TCP SYN flooding – Not possible on regular lab environments
    - Man-in-the-middle attack

NSF TRUST WISE 2012
Network configuration

- 4 nodes interconnected using a switch
- 3 nodes running Ubuntu 8.04LTS, and 1 node running Ubuntu 10.04
Can Node0 Sniff Other Nodes’ Packets?

- Logging into Node0 in the experiment

Macintosh-6:~ xsu$ ssh -l xiaosu users.isi.deterlab.net
Password:
Last login: Fri Apr 29 14:29:50 2011 from x130-65-152-108
> ssh node0.switchf2009.sjsucmpe209
Linux node0.switchf2009.sjsucmpe209.isi.deterlab.net 2.6.24-23-deter #4 SMP
Wed Jan 21 23:15:52 MST 2009 i686
node0:~>
Can Node0 Sniff Other Nodes’ Packets?

- Starting ettercap

Macintosh-6:~ xsu$ sudo ettercap -C

![Screenshot of ettercap interface]

Network interface: eth13

NSF TRUST WISE 2012
Can Node0 Sniff Other Nodes’ Packets?

- Scan for hosts
Can Node0 Sniff Other Nodes’ Packets?

- Start sniffing
- Generate packets from node1 to node2

node1:~> nc node2 54321
1st try: can you see me?

node2:~> nc -l -p 54321
1st try: can you see me?

NSF TRUST WISE 2012
Now Enabling ARP Poisoning
What Will Happen Next?

- Sending something from node1 to node2

node1:~> nc node2 54321
1st try: can you see me?
2nd try: can you see me?

node2:~> nc -l -p 54321
1st try: can you see me?
2nd try: can you see me?
Modifying Packet

- **Step 1: defining a filter**
  - What does the filter do?

  ```
  node2:~> cat ASniffing/ch.filter
  # change TCP payload
  if (tcp.dst == 54321 && search(DATA.data, "install")) {
    replace("install", "upgrade");
  }
  ```

- **Step 2: compiling the filter**

  ```
  node2:~/ASniffing> etterfilter -o ch.ef ch.filter
  ```
Modifying the Packet

- Step 3: load the filter
Will Packets Be Modified?

- Packets sent and received, after loading the filter

```
node1:~> nc node2 54321
1st try: can you see me?
2nd try: can you see me?
apt-get install gcc4
```

```
node2:~> nc -l -p 54321
1st try: can you see me?
2nd try: can you see me?
apt-get upgrade gcc4
```
Video capturing the above experiments

- Sniffing without arp spoofing
- Sniffing with arp spoofing enabled
- Sniffing with arp spoofing enabled and filter loaded to modify packet
Questions?