Teaching Security with Network Testbeds

Jelena Mirkovic, Mike Ryan, John Hickey (USC/ISI), Keith Sklower (UC Berkeley), Peter Reiher and Peter A. H. Peterson (UCLA), B. Hoon Kang (GMU), Mooi Choo Chuah (Lehigh University), Daniel Massey (Colorado State University), Gisele Ragusa (USC)
Education with DETERLab

- DETERLab: security experimentation testbed at USC/ISI and UC Berkeley
  - Built on Emulab software
  - Customized for security experimentation (tools, environments)

- Primarily built for research, increasing interest in education use
  - Lessons learned are relevant to all public testbeds
  - Research use requires collaboration, education use requires flexible isolation

- Testbed modifications to support use in classes
  - DETERLab Ops team (Mirkovic, Ryan, Hickey, Sklower)

- NSF CCLI grant to develop class exercises on DETERLab
  - Mirkovic, Chuah, Kang, Massey, Reiher, Peterson, Ragusa
Testbed Usage Per Semester

CCLI grant

Class support

Thousands of node hours

Semester

S'06  F'06  S'07  F'07  S'08  F'08  S'09  F'09  S'10  F'10  S'11

Class

Research
How Emulab Testbeds Work

- PIs create projects, approve members. Exclusive machine access.
  - Storage: user-private and project-private
  - All project files and experiments accessible to all members
  - Project files and member directories mounted to every experimental node within a project – users are roots there!
- Collaboration: ideal for research, not so much for classes
  - Some classes may require collaboration within a group
- FIFO service model
  - But class projects have deadlines
- Classes need specific support
  - Many short-lived accounts use up namespace
  - Teachers need to verify student claims
  - Too many naïve users for Ops to handle
Education-specific Testbed Support

- **Flexible isolation**
  - Special mechanisms prevent students accessing others' work
  - Collaborative work possible by belonging to the same group

- **Teacher: More than a PI, less than an Ops member**
  - Teachers/TAs can be root on experiments, no file mounts
  - Teachers/TAs can log in as students (Web or shell)
  - Teachers can freeze, thaw student accounts, edit them, add new accounts, see usage reports for their class

- **Automation**
  - Class accounts are automatically created and recyclable.

- **Offloading**
  - Students can't file tickets, must go through teacher/TA

- **Resource reservations and limits**
  - Fairness between classes and balance class/research use
Education-specific Materials

- Moodle server
  - Any teacher can use it for classes
- Teacher-only class for sharing materials
  - Student materials and teacher manuals
  - Seeded by us through our CCLI grant
  - Highly popular with teachers

<table>
<thead>
<tr>
<th>Topic</th>
<th>Posted/planned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intro to Linux and DETER</td>
<td>posted</td>
</tr>
<tr>
<td>Denial of service</td>
<td>posted</td>
</tr>
<tr>
<td>Buffer overflows, pathname</td>
<td>1 posted, 4 planned</td>
</tr>
<tr>
<td>attacks and SQL injection</td>
<td>posted</td>
</tr>
<tr>
<td>Man in the middle attack</td>
<td>posted</td>
</tr>
<tr>
<td>Firewalls and file system</td>
<td>posted</td>
</tr>
<tr>
<td>permissions</td>
<td>posted</td>
</tr>
<tr>
<td>Computer forensics</td>
<td>posted</td>
</tr>
<tr>
<td>NIDS</td>
<td>posted</td>
</tr>
<tr>
<td>OS hardening</td>
<td>posted</td>
</tr>
<tr>
<td>Worm modeling</td>
<td>posted</td>
</tr>
<tr>
<td>DNS prefix hijacking</td>
<td>1 posted, 3 planned</td>
</tr>
</tbody>
</table>
Human-Centric Support

- **Teacher-only mailing list**
  - Good for broad announcements
  - Archived
  - Opt-out period at the end of each semester

- **Class planning**
  - Teachers send us the initial timeline for their class assignments (deadlines and estimated number of machines)
  - This is entered into an online schedule
  - **Class limit = 1/4 weekly max; total class limit = 2/3 testbed**
  - Shared document, teachers have write access
  - We arbitrate if we note a potential for overload

- **1-1 support for each teacher**
  - I spend a lot of time bridging teacher-ops gap
Lessons Learned

- Education-specific support is crucial to make testbeds good fit for education
- Shared materials are key for drawing teachers in
  - Many start with those and then develop their own
- Predicting resource usage is hard
  - Big classes overestimate, small underestimate
  - Teachers move deadlines / prepare materials but don't tell us
  - Automated reservations = heavy rewriting of Emulab code
- Bridging teacher-ops gap is tough
  - Teachers are in tight spot between students and ops
  - Teachers are also very resilient
- Students generally LOVE hands-on exercises
  - They do learn more but that is hard to quantify
Not Oversubscribed But Busy

A line graph showing node usage over time, with different lines indicating total usage, class usage, and class limit. The x-axis represents dates from July 2010 to September 2011, and the y-axis represents node usage values ranging from 0 to 400,000,000.