Goal of This Talk

• Familiarize security professionals with DETER testbed
  • Recruit new users
  • Collect proposals of novel features to implement in DETER

• What you’ll hear
  • Short overview of DETER testbed and community
  • Why use DETER
  • Short demo
  • New directions: federation and risky experiment support
  • Q & A: how can DETER fit your needs?
What Is DETER?

- **Security testbed located at USC/ISI and UC Berkeley**
  - Funded by NSF and DHS, started in 2004.
  - Joint project of USC/ISI, UC Berkeley and SPARTA
  - 204 Nodes at ISI, 96 Nodes at UC Berkeley, constantly adding more
  - Many tools for experimenters: GUIs, traffic generators, simulators, …
  - Based on Emulab software, with focus on security experimentation

- **What DETER offers**
  - Exclusive access to multiple PCs and specialized hardware, running OS of your choice, for as long as needed
  - Tools for security experimentation
  - Large user community
Why Use DETER?

- **Accuracy: real-world experiments, not simulations**
  - Current network simulators do not correctly simulate security events
  - Difficult to convince reviewers about fidelity of custom simulators

- **Ease: Reuse real software for traffic and security**
  - Instead of writing novel traffic generators or simulators, use real client/server applications and real malicious code
  - Use/test existing security software and hardware and improve it

- **Learning: Understand novel phenomena/ test hypotheses**
  - Observe behavior of malicious code, security software, or hosts under attacks
DETER Vs. Other Testbeds

- Emulab, WAIL and DETER are based on the same software
  - DETER has focus on security experimentation, tools to support it and staff willing to accommodate risky experiments
  - We are in the process of automating risky experiment containment
- Synergy not competition
  - Emulab users migrate to DETER when Emulab runs out of nodes
  - We ran federation experiments spanning all three testbeds
- Easy transfer
  - Experiments can be easily transferred between testbeds, but some DETER-specific tools may not run on other testbeds
DETER Howto

- You only need Web and SSH access to work on DETER
- Open a user account and apply for a project (www.deterlab.net)
  - You can approve other users (e.g., your students) to join your projects
- When you need to run experiments:
  - Log on to www.deterlab.net
  - Draw a topology using the GUI on the page, or write it in NS
  - Start a new experiment with a given topology - nodes are assigned to you (approx. 10 min activation time)
  - Load software you need on nodes and run experiments
  - Existing experiments can be swapped in and out, and terminated when no longer needed
DETER Community

- Many users in academia, industry and government
- Many tools for security experimentation
  - Continually contributed by users
- Great project diversity
  - Opportunity to collaborate with other groups in your area of interest
  - Stand on shoulders of other users, reuse their wisdom
- Mailing lists for users
- Monthly teleconference calls with user participation
- Yearly community workshop
DETER Community

2119 Experiment days (~6 per day)
2933 Swap-ins

251 Users
70 Projects

Government
Industry
Academic

Users
Projects
DETER Projects

- DoS
- Worms and malware
- Overlays, routing, replic.
- Hw, sw and netw. test
- Traceback and attribution
- Models, policies
- Classes
- Diagnosis and recovery
- Multicast, group comm.
- Collaborative security
- Scanning
- Authentication
- DNS
- Spam
- Spoofing
- Botnets
- Wireless
**DETER Tools**

**All-In-One Experiment Development and Control Kits**
- SEER
- ESVT

**Experiment Automation/Visualization Utilities**
- Purdue Tool Suite

**Legitimate Traffic Generators**
- SEER
- Tcpexplay
- Performance Testing Tools
- Webstone
- NTGC
- TCP Opera
- Harpoon

**Attack Traffic Generators**
- DoS and DDoS Traffic
  - SEER
  - Trinoo
  - TFN2K
  - Stacheldraht
  - Mstream
- Custom Traffic
  - Packit
- Worm Traffic Simulators
  - KMSim
  - PAWS

**Traffic Forensic Tools**
- NTD

**Topology Generators and Converters**
- Rocketfuel-to-ns (lots AS topologies!)
- Inet
- Brite
- GT-ITM

**Benchmarks**
- DDoS Defense Benchmarks
DETER Demo

- **Create a simple DoS experiment**
  - One Web client, one Web server, one attacker
  - Server has a bottleneck link
  - UDP flood attack with randomly sized packets (100 - 1,200B) targeting port 80 - pulsing shape (10 sec on, 20 sec off)

- **Start experiment using DETER Web page**

- **Populate traffic generators and visualize traffic using SEER**
The DETER testbed is a public facility for security. Built using Utah's Emulab software, the DETER testbed has been configured and equipped for computer security experiments, including defense against attacks such as DDoS, with the routing infrastructure.

Once registered, a security experiment can manipulate collections of nodes and links with nearly-arbitrary network topologies. The box contains simultaneous experiments, isolated from each other. The node pool currently contains not more than managed as a single testbed. Supported operating systems include Linux, FreeBSD.

From this page you can reach extensive and immediate information or experience operational problems with DETER, please contact DETERlab.net.

DETER is currently supporting 10 active projects.

Links to help you get started:

- Authorization Scheme, Policy, and
- Overview of Installed Software
- Hardware Overview, "Emulab Class"
- Security Issues
- Administrative Policies and Disclaimers
Your automatically generated NS file has been uploaded. To finish creating your experiment, please fill out the following information.

<table>
<thead>
<tr>
<th>Select Project:</th>
<th>FloodWatch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group:</td>
<td>Default Group  (Must be default or correspond to selected project)</td>
</tr>
<tr>
<td>Name:</td>
<td>ACSAC</td>
</tr>
<tr>
<td>Description:</td>
<td>Demo of DETER for ACSAC</td>
</tr>
<tr>
<td>Your auto-generated NS file:</td>
<td>View NS File</td>
</tr>
</tbody>
</table>

**Swapping:**

- **Idle-Swap:** Swap out this experiment after 4 hours idle. If not, why not?
- **Max. Duration:** Swap out after 16 hours, even if not idle.

**Linktest Option:**

- Skip Linktest  *(What is this?)*

- **Batch Mode Experiment** *(See Tutorial for more information)*

- **Do Not Swap In**

[Submit]
More Complex Experiments
More Complex Experiments
More Complex Experiments
New Developments

- **Federation with other testbeds**
  - Current experiments run with minimal changes
  - Ran 210-node experiment on 3 testbeds: DETER (80), Emulab(70), WAIL (60)

- **Support for risky experiments**
  - Experiments will be able to run self-propagating code (e.g., Slammer) AND preserve outside connectivity
  - Experiments will be able to interact with the outside directly
  - Containment techniques to guarantee security of testbed and security to the Internet
  - Building a library of malicious code via Metasploit
For More Information

- **DETERlab Page**
  - [http://www.deterlab.net](http://www.deterlab.net)
  - Log on to testbed, documentation and tutorials

- **DETER Project Page**
  - [http://www.isi.edu/deter](http://www.isi.edu/deter)
  - Information about DETER project and its results

- **My email**
  - Ted Faber (faber@isi.edu)