

# Security Testing with **DETER**

The DETER testbed provides experimental infrastructure to support the development and demonstration of next-generation information security technologies. The DETER testbed offers researchers a safe, flexible, and scalable platform for conducting experiments to evaluate and thwart various cyber threats - some examples include worms, malware, distributed denial of service (DDoS) attacks, and viruses.

DETER provides a medium-scale facility for safe, repeatable security-related experimentation to validate theory and simulation. DETER Researchers can emulate real systems in a controlled environment, having access to a testbed of 400 physical machines. The DETER testbed is comprised of hardware - high-end PCs as experimental nodes - and extensive control software.

## What's New

**Join us for the 2nd Workshop on Cyber Security Experimentation and Test in Montreal, Canada on August 10th, 2009.** CSET '09 aims to bring together researchers and testbed developers to share their experiences and find a forward-looking agenda for the development of scientific, realistic evaluation approaches for security threats and defenses. More information and the call for papers can be found at the CSET '09 website:

<http://www.usenix.org/event/cset09>.

**New Users:** DETER is an open facility used by academic, industrial, and government organizations for researching, testing, and evaluating computer security. Within the last six months, DETER has added:

- 200 new users
- 11 new research programs
- over 370 experiments

**Hardware Upgrades:** In order to expand in a space constrained environment, the University of California, Berkeley site has recently installed a Sun Modular Datacenter — a full datacenter squeezed into a standard cargo container. This new space has allowed Berkeley to add 64 more quad core Dell Poweredge 860 nodes to the DETER testbed with more room to grow.

For more news, please visit <http://www.isi.edu/deter>.

## Using DETER

Faculty members and senior researchers can become Principal Investigators (PIs) on DETER (based on Emulab). PIs can register and create new projects for research on the DETER testbed. A project has a research objective and usually consists of multiple experiments. Furthermore, an experiment consists of a specific physical node topology and configuration. Once research projects are created and approved by DETER, PIs may add and approve other users who may wish to join their projects. Users can be members of multiple projects, and their privileges are set per project by the PI.

Users interact with DETER through a remote interface, making the testbed accessible from anywhere on the Internet, enabling students, researchers, and faculty to collaborate and interact from different locations.

Once created, experiments are saved and can be easily retrieved. They are said to be "swapped in" when physical machines are assigned to them and "swapped out" otherwise.

## Useful Links

DETER Web page: <http://www.deterlab.net/>

To become a user click [Request Account](#) on the DETER Web page

User Support: [testbed-ops@isi.deterlab.net](mailto:testbed-ops@isi.deterlab.net)

## Where Is DETER Used?



### INSIDE

- Using DETER to Power Your Experiments **Page 1**
- Federation: Harness the Power of Multiple Testbeds **Page 2**
- Managing Risk **Page 2**



### Profile of a DETER User: Prof. Dawn Song

Research Area: **Detection of malware applications that infect browsers**  
Institution: **UC Berkeley**

Dr Dawn Song is one of the first to take advantage of DETER's risky experiment management tools (see page 2 for additional details). Dr Song performs research in computer security, in particular detection of malware applications that infect browsers via their behavior profiles.

The DETER testbed is a perfect environment for Dr Song's experimentation as it allows her to run tests in a safe, controlled environment. Her new research pushes the envelope on DETER's experiment support as it requires interaction and communication with malicious applications outside DETER, without contaminating and endangering the rest of the Internet. Dr Song was able "to do meaningful experimentation and to analyze and study the malicious code phenomenon on the Internet" by using DETER's risky experimentation management tools.

## Easy-to-Use Tools to Get Started

Security experimentation on a testbed usually requires a user to generate some traffic and events, such as attacks of a given kind. DETER comes equipped with many traffic generation, visualization and experiment monitoring tools. These tools facilitate easy, point-and-click experimentation via a Java GUI, and also support scripting for sophisticated sequencing and large-scale experiments. Tools are integrated with our open-source experiment control and development platform, called SEER (<http://seer.isi.deterlab.net>). Advanced users can also access physical machines directly via SSH and manually setup traffic generation and monitoring.

The DETER Web user's interface is flexible enough for new users to create their own topologies with an intuitive drag and drop architecture. The SEER tool further allows users to set up traffic generation, simulate attacks and monitor progress in a Java-based interface.



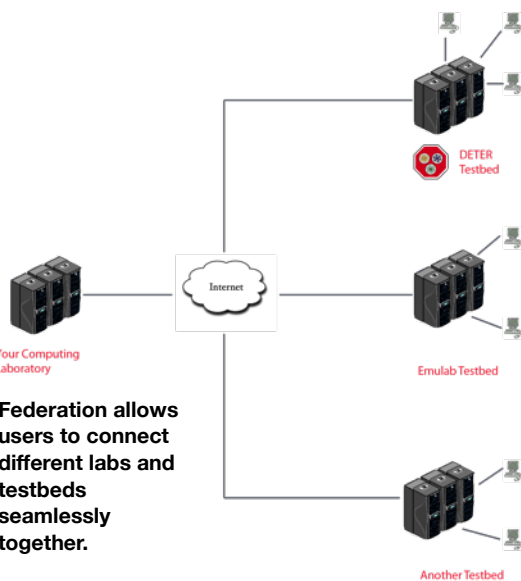
## DETER Offers Support When You Need It

The operations of DETER's testbed are supported by a dedicated full-time team of administrators and user coordinators, that are reachable via email and chat. Technical support response is usually within a matter of hours. For technical assistance, please email [testbed-ops@isi.deterlab.net](mailto:testbed-ops@isi.deterlab.net) or join the chat session as described at <http://www.isi.deterlab.net/deterchat.php3>.

## DETER Research: Expanding Testbed Capabilities

### Risky Experiment Management

Security experimentation is inherently risky, because it must replicate realistic security threats. The challenge for testbed operators lies in managing this risk while supporting research goals. DETER is now migrating from its strict containment policy to flexible management of risky experiments. We manage three risk dimensions: risk to shared testbed infrastructure, risk to other experiments, and risk to the Internet. Risk to the shared infrastructure is managed by carefully controlling conversations between experiments and control nodes. Inter-experiment risk is handled by strict isolation so nodes in different experiments cannot talk to each other. The most complex risk - to the Internet - is managed by a two-constraint approach called "T1/T2". Within this framework, experimenters define their research goals and the constraints they have put on the experiment behavior. For example a user may want to run a bot code in DETER, connect to the outside botmaster, and study command and control traffic (research goal). The researcher knows the botmaster's IP address and only needs the bot to talk to this one master (T1 constraint). The testbed parses goals and T1 constraints and develops T2 constraints to achieve safety. In the previous example, T2 constraint would filter all traffic between the experiment and the Internet, and only allow traffic to/from the botmaster's IP. Examples of T1 constraints are: asking for communication with specific IPs and ports, marking malicious traffic, specifying malware signature and defanging malware. Examples of T2 constraints are: setting up a firewall to the Internet with holes for specific ports and IPs, filtering marked traffic to the outside, and dropping traffic with known signatures. The beta version of our T1/T2 framework will be released soon to DETER users. Please contact [sunshine@isi.edu](mailto:sunshine@isi.edu) if you would like more information and/or are interested in being a beta tester.



### Federation: Harnessing the Power of Multiple Testbeds

The DETER Federation architecture enables DETER experimenters to make use of resources from other cooperating labs and testbeds seamlessly. Using federation, experimenters can gain access to more nodes as well as to hardware and software capabilities directly available from DETER. The initial deployment of this service is in place supporting Emulab-style testbeds, and future updates will support a richer authorization model and access to wide-area network connectivity with performance guarantees. More information is available from <http://fedd.isi.deterlab.net/trac>.

