Join Us at **CSET ’09**

The 2nd Workshop on Cyber Security Experimentation and Test (CSET ’09) is co-located with the USENIX Security Symposium in Montreal, Canada on August 10th, 2009. CSET ’09 will bring together researchers and testbed developers to share their experiences and define a forward-looking agenda for the development of scientific, realistic evaluation approaches for security threats and defenses.

A strong workshop is planned this year, with 27 papers submitted and 9 accepted. Find more information about the DETER project at: [http://www.isi.edu/deter](http://www.isi.edu/deter)

---

**Types of DETER Projects**

- Worms, malware, intrusions
- Performance testing
- Comprehensive security
- DDoS
- Building testbeds
- Security classes
- Routing, DNS, infrastructure
- Botnets
- Overlays
- Wireless security
- Traceback
- Privacy
- Spoofing
- Spam
- Multicast
- Watermarking
- Trust
- Metrics
- Forensics

---

**Where Is DETER Used?**

---

**Profile of a DETER User: Dr. David Nicol**

**Research Area:** Power Systems Simulation and Emulation

**Institution:** University of Illinois, Urbana-Champaign

Systems that connect cyber and physical worlds, such as power infrastructure, are an appealing target for attackers. Successful attacks on these systems could have devastating consequences to our national economy, and may even lead to loss of lives. Dr. David Nicol and his team are working on developing simulation and emulation tools for power systems, by integrating large scale features of parallel simulators with high-fidelity of hardware and software used for actual power-system control.

Prof. Nicol along with his colleague Prof. Carl Gunter and their students have used the DETER infrastructure to simulate power-systems’ operation and explore their security posture. They have also developed a stand-alone Virtual Power System Testbed (VPST) at the University of Illinois, which provides detailed SCADA-specific protocols. VPST is being extended to federate with testbeds, such as DETER to leverage additional resources and collaborator expertise.
SEER: Making the most of DETER
Text contributed by Alefiya Hussain and Brett Wilson of Cobham, Inc.

Security Experimentation Environmment (SEER) is a powerful experiment management tool that provides an easy to use GUI and a Python backend. SEER GUI runs on a user’s desktop and is highly portable due to its implementation in Java. Users can:

- create an experiment, swap it in or out and configure nodes
- visualize the topology and experiment statistics
- set up, start and stop traffic and event generators

SEER also provides a large number of tools for traffic generation and tools for traffic collection and analysis. The top Figure shows the setup dialog for the FTP traffic generator.

A popular use of SEER is in testing. Users have reported that SEER’s visualization capability allows them to rapidly spot configuration errors or node failures and rectify them on the fly. The Figure on the bottom shows the visualization of legitimate and attack traffic on several network interfaces in an experiment.

SEER experiments are repeatable and support complete automation with a python-based scripting language. An experimenter can define a whole battery of agent configurations to explore the research space. SEER is also extensible. Current agents can be extended to support functions specific to the needs of an experimenter and new agents can be developed to support new tools. Check out SEER code, tutorials and instructions at: http://seer.isi.deterlab.net

---

SLINGbot: A System for Live Investigation of Future Botnets
Text contributed by Alden Jackson and W. Timothy Strayer of BBN.

Scientists at BBN have developed System for Live Investigation of Next Generation bots (SLINGbot) to aid researchers in studying botnet communication patterns, which is now available on DETER. SLINGbot is a composable botnet framework, which enables researchers to construct benign botnets with varying command and control (C&C) structures. Researchers can thus study current and potential future botnet C&C structures, which facilitates proactive development of botnet defenses.

SLINGbot creates and controls live, benign bots that have realistic C&C infrastructure and generate real traffic. No attack or auto-propagation functionality is included, so researchers can study botnet threats in a controlled and safe manner. SLINGbot is extensible and new C&C infrastructures can be easily added.

SLINGbot, written in Python, is composed of the Scenario Driver and the Composable Bot Framework modules. The Scenario Driver is a control mechanism that drives botnet actions and behavior via an “out-of-band” channel that effectively separates botnet C&C traffic and scenario control traffic. Custom scenarios encapsulated within simple XML files facilitate reproducible and rapid experimentation by describing botnet setup, execution, and cleanup. The Composable Bot Framework enables the creation of live, but benign, bots that are customizable from a library of components. The components encapsulate bot instructions and C&C feature functionalities, e.g., topology, rally mechanism, communication, control mechanism and command authentication. The SLINGbot architecture is shown in the figure on the right. Several Bot variants including IRC bot, TinyP2P bot, Kademlia bot (used in the Storm/Peacomm botnet), and Hierarchical Kademlia bot have been tested on the DETER testbed and are available to the researchers. More information about SLINGbot can be found at: http://www.ir.bbn.com/documents/articles/catch-slingbot-09.pdf

Information about the DETER project at: http://www.isi.edu/deter