Announcement and Call for Papers USENIX

DETER Community Workshop on Cyber Security Experimentation and Test 2007

http://www.usenix.org/deter07

August 6–7, 2007 **Boston, MA, USA**

The workshop will will be co-located with the 16th USENIX Security Symposium (Security '07), which will take place August 6–10, 2007.

Important Dates

Position paper submissions due: *June 3, 2007, 11:59 p.m. PDT*
Notification of acceptance: *July 2, 2007*
Final files due: *July 16, 2007*

Workshop Organizers

Program Chairs

Terry V. Benzel, *University of Southern California Information Sciences Institute (ISI)*
George Kesidis, *Pennsylvania State University*

Program Committee

Bob Braden, *University of Southern California Information Sciences Institute (ISI)*
Sonia Fahmy, *Purdue University*
Anthony Joseph, *University of California, Berkeley*
Peng Liu, *Pennsylvania State University*
Jelena Mirkovic, *University of Delaware*
Clifford Neuman, *University of Southern California Information Sciences Institute (ISI)*
Steve Schwab, *Sparta, Inc.*
Felix Wu, *University of California, Davis*

Overview

This workshop will address issues in the design and use of moderate-to-large scale network testbeds to conduct experiments on security topics such as worm propagation, infrastructure defense (e.g., defending the DNS and BGP routing), and denial of service defense. Such experiments are challenging because of complexity, scale, and possible risk. This workshop will examine questions around research requirements for security testbeds and provide an opportunity to share experiences, results, problems, and approaches to experimentation. The workshop will also accept papers on the design of general-purpose testbeds with adequate containment for safe experimentation with malware.

The Community Workshop on Cyber Security Experimentation and Test will be held on August 6–7, 2007, in Boston, MA, USA, in conjunction with the 16th USENIX Security Symposium.

Researchers are encouraged to submit 5–8 page papers on secure testbed technologies or testbed-based security experiments.

This workshop is being organized by the DETER testbed project, a joint testbed operated by the University of Southern California's Information Sciences Institute and the University of California, Berkeley. The DETER testbed uses the Emulab technology created at the University of Utah and has been funded by the National Science Foundation and the Department of Homeland Security. More information on the DETER testbed can be found at http://www.isi.edu/deter and http://www.isi.deterlab.net. The upcoming workshop follows on previous workshops held within the DETER community of security researchers and testbed builders, but participation from those outside the DETER community is encouraged. Specifically, the workshop will accept papers on distributed network security results, including work in:

- Security experimentation
  - Internet infrastructure protection (e.g., DNS, BGP)
  - Defenses against distributed denial of service (DDoS) attacks
  - Analysis of or defenses against malicious code
  - Other testbed-based security experimentation
- Testbed and methodologies
  - Traffic model generation or validation
  - Using virtualization to scale experiments
  - Experience designing or deploying secure testbeds
  - Instrumentation and automation of security experiments
  - Archiving or preservation of experiments

- Visualization of security experiments
- Diagnosis of and methodologies for dealing with experimental artifacts
- Sharing secure testbed resources and federation

Submission Instructions

Submissions must be 5–8 pages—including tables and figures—in 2 columns, single-spaced, in 10 point Times Roman font. Text outside a 6.5" by 9" block will be ignored. Submit your paper in PDF format via the Web submission form, which will be available soon on the DETER 2007 Call for Papers Web site, http://www.usenix.org/deter07/cfp. We encourage authors to follow the U.S. National Science Foundation's guidelines for preparing PDF grant submissions:

https://www.fastlane.nsf.gov/documents/pdf_create/pdfcreate_01.jsp

Each submission should have a contact author who should provide full contact information (email, phone, fax, mailing address). One author of each accepted paper will be required to present the work at the workshop.

Simultaneous submission of the same work to multiple venues, submission of previously published work, and plagiarism constitute dishonesty or fraud. USENIX, like other scientific and technical conferences and journals, prohibits these practices and may, on the recommendation of a program chair, take action against authors who have committed them. In some cases, program committees may share information about submitted papers with other conference chairs and journal editors to ensure the integrity of papers under consideration. If a violation of these principles is found, sanctions may include, but are not limited to, barring the authors from submitting to or participating in USENIX conferences for a set period, contacting the authors' institutions, and publicizing the details of the case.

Authors uncertain whether their submission meets USENIX's guidelines should contact the workshop organizers at deter07chairs@usenix.org or the USENIX office, submissionspolicy@usenix.org.