Announcement and Call for Papers USENIX

Workshop on Cyber Security Experimentation and Test (CSET '08)

Sponsored by USENIX, the Advanced Computing Systems Association

http://www.usenix.org/cset08

July 28, 2008 **San Jose, CA**

CSET '08 will be co-located with the 17th USENIX Security Symposium (USENIX Security '08), which will take place July 28–August 1, 2008.

Important Dates

Paper submissions due: *May 31, 2008*
Notification of acceptance: *June 30, 2008*
Electronic files due: *July 15, 2008*

Workshop Organizers

General Chair
Terry Benzel, *USC Information Sciences Institute*

Program Chairs
Sonia Fahmy, *Purdue University*
Jelena Mirkovic, *USC Information Sciences Institute*

Program Committee
Andy Bavier, *Princeton University*
Bob Braden, *USC Information Sciences Institute*
Tom Daniels, *Iowa State University*
Alefiya Hussain, *SPARTA*
Anthony Joseph, *University of California, Berkeley*
Sean Peisert, *University of California, Davis*
Peter Reiher, *University of California, Los Angeles*
Robb Ricci, *University of Utah*
Stephen Schwab, *SPARTA*
Mark Stamp, *San Jose State University*
Angelos Stavrou, *George Mason University*
Nick Weaver, *ICSI*
Vinod Yegneswaran, *SRI International*

Overview

Security challenges constantly grow in complexity and scale. To meet these challenges, security professionals need safe experiment environments, tools, and methodologies to:

- capture new threats,
- study threats through interactive experimentation,
- dissect and reassemble malware,
- pit new attacks against proposed defenses, and
- test defensive technologies in a large-scale, realistic setting.

This workshop aims to gather both researchers who use testbeds for security experimentation and testbed developers to share their ideas and results and to discuss open problems in this area. While we particularly invite papers that deal with security experimentation, we are also interested in papers that address general testbed/experiment issues that have implications on security experimentation such as traffic and topology generation, large-scale experiment support, experiment automation, etc.

Topics

Topics of interest include but are not limited to:

- Security experimentation
  - Experiments for Internet infrastructure protection (e.g., DNS, BGP)
  - Experiments with distributed denial-of-service attacks
  - Experiments with botnets and malware
  - Experiments that evaluate existing or novel defenses
  - Other testbed-based security experiments
- Testbeds and methodologies
  - Tools, methodologies, and infrastructure that support risky and/or realistic experimentation
  - Supporting experimentation at a large scale through virtualization or federation, or by scaling down problems while preserving realism and experiment fidelity
  - Experience in designing or deploying secure testbeds
  - Tools for realistic traffic generation
  - Instrumentation and automation of experiments; their archiving, preservation, and visualization
  - Diagnosis of and methodologies for dealing with experimental artifacts

    - Fair sharing of testbed resources and experiment federation
- Hands-on security classes
    - Experiences teaching security classes that use testbeds for homework, in-class demonstrations, or class projects
    - Organizing red team/blue team exercises in classes

Submission Instructions

Submissions must be no longer than 6 pages—including tables, figures and references—in 2-column format, using 10 point fonts. Text outside a 6.5" by 9" block will be ignored. Submit your paper in PDF via the Web submission form on the CSET '08 Call for Papers Web site, http://www.usenix.org/cset08/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 cset08chairs@usenix.org or the USENIX office, submissionspolicy@usenix.org.

Papers accompanied by nondisclosure agreement forms will not be considered. All submissions will be treated as confidential prior to publication in the Proceedings.