Announcement and Call for Papers **USENIX**

2nd Workshop on Cyber Security Experimentation and Test (CSET ’09)

Sponsored by USENIX, the Advanced Computing Systems Association

http://www.usenix.org/cset09

August 10, 2009 **Montreal, Canada**

CSET ’09 will be co-located with the 18th USENIX Security Symposium (USENIX Security ’09), which will take place August 10–14, 2009.

Important Dates

Submissions due: *June 1, 2009, 11:59 p.m. PDT*
Notification to authors: *June 30, 2009*
Electronic files due: *July 15, 2009*

Workshop Organizers

General Chair

Terry V. Benzel, *USC Information Sciences Institute (ISI)*

Program Co-Chairs

Jelena Mirkovic, *USC Information Sciences Institute (ISI)*
Angelos Stavrou, *George Mason University*

Program Committee

Paul Barford, *University of Wisconsin*
Andy Bavier, *Princeton University*
Matt Bishop, *University of California, Davis*
Thomas Daniels, *Iowa State University*
Sonia Fahmy, *Purdue University*
Carrie Gates, *Computer Associates*
Alefiya Hussain, *SPARTA Inc.*
Brent Kang, *The University of North Carolina at Charlotte*
Vern Paxson, *ICSI*
Sean Peisert, *University of California, Davis*
Peter Reiher, *University of California, Los Angeles*
Rob Ricci, *University of Utah*
Mark Stamp, *San Jose State University*
Kashi Vishwanath, *Microsoft Research*
Vinod Yegneswaran, *SRI International*

Overview

Effective cyber security and network experimentation is challenging for today’s network testbeds for a number of reasons. Among these are:

- *Scale:* Experiments that involve complicated composite behaviors, rare event detection, or emergent effects may need to be quite large and complex to be accurate or indicative.
- *Multi-party nature:* Most interesting cyber security experiments involve more than one logical or physical party, due to the adversarial nature of the problem as well as the distributed, decentralized nature of the networked systems environment.
- *Risk:* Cyber security experiments by their fundamental nature may involve significant risk if not properly contained and controlled. At the same time, these experiments may well require some degree of interaction with the larger world to be useful.

Meeting these challenges requires both transformational advance in capability and transformational advance in usability of the underlying research infrastructure. The second annual Workshop on Cyber Security Experimentation and Test (CSET ’09) invites submissions on the design, architecture, construction, operation, and use of cyber security experiments in network testbeds and infrastructures. While we are particularly interested in works that relate to emulation testbeds, we invite all works relevant to cyber security experimentation and evaluation (e.g., simulation, deployment, traffic models).

Topics of interest include but are not limited to:

- Security experimentation
    - Positive or negative experiences from past experiments
    - Novel experimentation approaches
- Testbeds and methodologies
    - Tools, methodologies, and infrastructure that support risky and/or realistic experimentation
    - Supporting experimentation at a large scale (virtualization, federation, high-fidelity scale down)
    - Experience in designing or deploying secure testbeds
    - Realistic traffic and topology generators
    - Instrumentation and automation of experiments; their archiving, preservation, and visualization
    - Diagnosis of and methodologies for dealing with experimental artifacts
    - Fair sharing of testbed resources
- Hands-on security education
    - Experiences teaching security classes that use hands-on security experiments for homework, in-class demonstrations, or class projects
    - Experiences from red team/blue team exercises

Submissions

Submissions must be no longer than six 8.5” x 11” pages—including tables, figures, and references—in two-column format in 10-point type on 12-point (single-spaced) leading, with the text block being 6.5” wide by 9” deep. Text outside the 6.5” x 9” block will be ignored. Submit your paper in PDF format via the Web submission form on the CSET ’09 Call for Papers Web site, http://www.usenix.org/cset09/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.

All papers will be available online to registered attendees prior to the workshop and will be available online to everyone starting on August 10, 2009. If your accepted paper should not be published prior to the event, please notify production@usenix.org.

Simultaneous submission of the same work to multiple venues, submission of previously published work, or plagiarism constitute dishonesty or fraud. See http://www.usenix.org/cset09/cfp for the complete USENIX policy. Authors uncertain whether their submission meets USENIX’s guidelines should contact the program chairs, cset09chairs@usenix.org, or the USENIX office, submissionspolicy@usenix.org.

Papers accompanied by nondisclosure agreement forms will not be considered. Accepted submissions will be treated as confidential prior to publication on the USENIX CSET ’09 Web site; rejected submissions will be permanently treated as confidential.

Rev. 5/8/09