Announcement and Call for Papers USENIX

3rd Workshop on Cyber Security Experimentation and Test (CSET '10)

Sponsored by USENIX, the Advanced Computing Systems Association

http://www.usenix.org/cset10

August 9, 2010 **Washington, DC**

CSET '10 will co-located with the 19th USENIX Security Symposium (USENIX Security '10), which will take place August 11–13, 2010.

Important Dates

Submissions due: *May 28, 2010, 11:59 p.m. PDT*
Notification to authors: *June 30, 2010*
Final paper files due: *July 15, 2010*

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

Mark Allman, *International Computer Science Institute*
Andy Bavier, *Princeton University*
Jose M. Fernandez, *Polytechnique Montréal*
Efstratios Gavas, *United States Merchant Marine Academy*
Celeste Matarazzo, *Lawrence Livermore National Laboratory*
Roy Maxion, *Carnegie Mellon University*
Sean Peisert, *University of California, Davis, and Lawrence Berkeley National Laboratory*
Golden G. Richard III, *University of New Orleans*
Stephen Schwab, *Cobham, Inc.*
Anil Somayaji, *Carleton University*
Mark Stamp, *San Jose State University*
Kashi Viswanath, *Microsoft Research*
Charles Wright, *MIT Lincoln Laboratory*
Vinod Yegneswaran, *SRI International*

Overview

Effective cyber security experimentation on network testbeds is challenging for a number of reasons:

- *Scale*: Experiments may need to be quite large and complex to accurately portray the phenomenon being investigated.
- *Multi-party nature*: Interesting experiments include humans, drawn from several logical or physical parties, who either collaborate or compete with each other.
- *Risk*: Cyber security experiments naturally carry 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.
- *Realism*: Experiments must faithfully recreate the relevant features of the phenomena they investigate in order to obtain correct results, yet data about threats and the Internet landscape is sparse and often must undergo transformations to reduce scale and sensitivity before being ported to testbeds. Hence careful reasoning about "realism" is required.
- *Rigor*: Repeatability and correctness must be ensured in any scientific experimentation. These are extremely hard to achieve on distributed network testbeds, due to testbed dynamics, sharing and unpredictability, and experimentation scale and complexity that overwhelm humans.
- *Setup/scenario complexity*: Testbed experiments are very complex and evolve over time. Time investment needed for setup and manipulation of experiments that are realistic, correct, and repeatable is too large for a single user and requires community involvement. Tools and practices for sharing experiments and their components are lacking.

Meeting these challenges requires both transformational advance in capability and transformational advance in usability of the underlying research infrastructure. The 3rd Workshop on Cyber Security Experimentation and Test (CSET '10) invites submissions on the science, 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 work relevant to cyber security experimentation and evaluation (e.g., simulation, deployment, traffic models).

Topics

Topics of interest include but are not limited to:

- Science of security/testbed experimentation
  - Data and tools to achieve realistic experiment setup/scenarios
  - Diagnosis of and methodologies for dealing with experimental artifacts
  - Support for experimentation on a large scale (virtualization, federation, high fidelity scale-down)
  - Tools and methodologies to achieve, and metrics to measure, correctness, repeatability, and sharing of experiments
- Testbeds and methodologies
  - Tools, methodologies, and infrastructure that support risky experimentation
  - Support for experimentation in emerging security topics (cyber-physical systems, wireless, botnets, etc.)
  - Novel experimentation approaches (e.g., coupling of emulation and simulation)
  - Experience in designing or deploying secure testbeds
  - Instrumentation and automation of experiments; their archiving, preservation, and visualization
  - 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

Research submissions must have a separate section labeled "Methodology" in which they clearly identify their research hypothesis and tests designed to prove/disprove it. Submissions that recount experiences (e.g., from education or testbed deployment) must have a separate section labeled "Lessons Learned" where they draw conclusions from their experience and generalize it to other environments.

Submissions must be 6–8 pages long including tables, figures, and references. Text should be formatted in two columns on 8.5" x 11" paper using 10 point type on 12 point leading ("single-spaced"), with the text block being no more than 6.5" wide by 9" deep. Text outside the 6.5" x 9" block will be ignored.

Submissions must be in PDF and must be submitted via the Web submission form on the CSET '10 Call for Papers Web site, http://www.usenix.org/cset10/cfp.

All papers will be available online to registered attendees before the workshop. If your accepted paper should not be published prior to the event, please notify production@usenix.org. The papers will be available online to everyone beginning on the day of the workshop, August 9, 2010.

Simultaneous submission of the same work to multiple venues, submission of previously published work, or plagiarism constitutes dishonesty or fraud. USENIX, like other scientific and technical conferences and journals, prohibits these practices and may take action against authors who have committed them. See the USENIX Conference Submissions Policy at http://www.usenix.org/submissionspolicy. Questions? Contact your program co-chairs, cset10chairs@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 '10 Web site; rejected submissions will be permanently treated as confidential.