Announcement and Call for Papers USENIX

4th Workshop on Cyber Security Experimentation and Test (CSET '11)

Sponsored by USENIX, the Advanced Computing Systems Association

http://www.usenix.org/cset11

August 8, 2011 **San Francisco, CA**

CSET '11 will co-located with the 20th USENIX Security Symposium (USENIX Security '11), which will take place August 8–12, 2011.

Important Dates

Submissions due: *April 25, 2011, 11:59 p.m. PDT*
Notification to authors: *June 1, 2011*
Final paper files due: *June 30, 2011*

Workshop Organizers

Program Co-Chairs

Sean Peisert, *University of California, Davis, and Lawrence Berkeley National Laboratory*
Stephen Schwab, *USC Information Sciences Institute (ISI)*

Program Committee

Matt Bishop, *University of California, Davis*
Elie Bursztein, *Stanford University*
Ron Dodge, *U.S. Military Academy*
Sonia Fahmy, *Purdue University*
Deborah Frincke, *Pacific Northwest National Laboratory*
Cynthia Irvine, *Naval Postgraduate School*
Angelos Keromytis, *Columbia University*
Christian Kreibich, *International Computer Science Institute*
Patrick Lardieri, *Lockheed Martin ATL*
Ulf Lindqvist, *SRI International*
Mark Matties, *Johns Hopkins Applied Physics Laboratory*
Sean Smith, *Dartmouth University*
Jessica Staddon, *Google, Inc.*
Ed Talbot, *Sandia National Laboratory*
Robert Watson, *University of Cambridge Computing Laboratory*

Steering Committee

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

Overview

The focus of CSET is on the science of cyber security evaluation, as well as experimentation, measurement, metrics, data, and simulations as those subjects relate to computer and network security. The science of cyber security is challenging for a number of reasons:

- Data: There is an absence of data usable by the community. Moreover, there is no clear understanding of what good data would look like if it was obtained, and how the value of data changes over time.
- 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, modeling humans is hard, and issues of scaling (up or down) are not well understood. Hence careful reasoning about "realism" is required.
- Rigor: Repeatability and correctness must be ensured in any scientific experimentation. These can be extremely hard to achieve.
- 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.

Meeting these challenges requires transformational advance in understanding of the relationship between scientific method and cyber security evaluation, as well as transformational advance in capability of the underlying resources and infrastructure and usability of the data. The 4th Workshop on Cyber Security Experimentation and Test (CSET '11) invites submissions on the science, design, architecture, construction, operation, and use of cyber security data and experiments.

Topics

Topics of interest include but are not limited to:

- Science of cyber security, e.g., experiences with and discussions of experimental methodologies
- Measurement and metrics, e.g., what are useful or valid metrics? how do we know? how does measurement interact with (or interfere with) evaluation?
- Data sets, e.g., what makes good data sets? how do we know? how do we compare data sets? how do we generate new ones? how do they hold up over time? how well do teaming or capture-the-flag exercises generate data sets?
- Simulations and emulations, e.g., what makes good ones? how do they scale (up or down)?
- Testbeds and experimental infrastructure, e.g., usage techniques, support for experimentation in emerging security topics (cyber-physical systems and wireless)
- Experiences with cyber security education, e.g., capture-the-flag exercises, novel experimentation techniques used in education, novel ways to teach hands-on cyber security

Workshop Format

Because of the complex and open nature of the subject matter, CSET '11 is designed to be a workshop in the traditional sense. Presentations are expected to be interactive, 45 minutes long, with the expectation that a substantial amount of this time may be given to questions and audience discussion. Similarly themed papers and extended abstracts may be grouped together for discussion. Papers and presentations should be conducive to discussion, and the audience is encouraged to participate. To ensure a productive workshop environment, attendance will be limited to 80 participants.

Submissions

Position papers, research papers, and extended abstracts are welcome as submissions.

Position papers, particularly those that are critiques of past work, should make certain to also include detailed, proposed solutions.

Research papers should have a separate section labeled "Methodology" in which the paper clearly identifies the research hypothesis and experiments designed to be proven or disproven. Submissions that recount experiences (e.g., from experiments or teaching) should have a section labeled "Lessons Learned" that discusses conclusions drawn from experience and generalized to other environments.

In addition to full-length position and research papers, the program committee also solicits extended abstracts focused on espousing positions or presenting critiques that challenge currently accepted consensus. Authors of abstracts may be invited to participate as presenters and/or champions of a viewpoint in interactive, moderated, topic-focused discussions.

Full position and research submissions must be 6–8 pages long including tables, figures, and references. Extended abstracts must be 2–4 pages long. 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.

All submissions must be anonymized.

Submissions must be in PDF and must be submitted via the Web submission form on the CSET '11 Call for Papers Web site, http://www.usenix.org/cset11/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 8, 2011.

At least one author from every accepted paper must plan to attend the workshop and present.

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, cset11chairs@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 '11 Web site; rejected submissions will be permanently treated as confidential.