Announcement and Call for Papers

usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

6th Workshop on Cyber Security Experimentation and Test (CSET '13)

Sponsored by USENIX, the Advanced Computing Systems Association

www.usenix.org/conference/cset13

August 12, 2013 **Washington, DC**

CSET '13 will be co-located with the 22nd USENIX Security Symposium (USENIX Security '13) and will take place on Monday, August 12, 2013.

Important Dates

Submissions due: *Thursday, May 2, 2013, 11:59 p.m. EDT*
Notification to authors: *May 30, 2013*
Final paper files due: *June 27, 2013*

Workshop Organizers

Program Co-Chairs

Chris Kanich, *University of Illinois at Chicago*
Micah Sherr, *Georgetown University*

Program Committee

Adam Aviv, *Swarthmore College*
Michael Bailey, *University of Michigan*
Kevin Bauer, *MIT Lincoln Laboratory*
Matt Blaze, *University of Pennsylvania*
Kevin Butler, *University of Oregon*
Stephen Checkoway, *Johns Hopkins University*
Eric Cronin, *Laboratory for Telecommunications Sciences*
Sonia Fahmy, *Purdue University*
Deb Frincke, *U.S. National Security Agency*
Rob Jansen, *U.S. Naval Research Laboratory*
Kirill Levchenko, *University of California, San Diego*
Celeste M. Matarazzo, *Lawrence Livermore National Laboratory*
Damon McCoy, *George Mason University*
Tyler Moore, *Southern Methodist University*
Angelos Stavrou, *George Mason University*

Steering Committee

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

Overview

CSET invites submissions 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 and privacy.

The science of cyber security is challenging for a number of reasons. For example, very little data is available for research use, and little is understood about what good data would look like if it were obtained. Experiments must recreate relevant, realistic features—including human behavior—in order to be meaningful, yet identifying those features and modeling them is hard. Repeatability and measurement accuracy are essential in any scientific experiment yet hard to achieve in practice. Cyber security experiments carry significant legal and ethical risks if not properly contained and controlled, yet often require some degree of interaction with the larger world in order to be useful.

Meeting these challenges requires transformational advances, including understanding the relationship between scientific method and cyber security evaluation, advancing capabilities of underlying experimental infrastructure, and improving data usability.

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, particularly when human behavior and perception (such as privacy) are considered? how do we know? how does measurement interact with (or interfere with) evaluation?
- Ethics of cyber security research, e.g., experiences balancing stakeholder considerations, frameworks for evaluating the ethics of cyber security experiments
- Alternative approaches to cyber security research, e.g., the application of methodologies from the social sciences (where observational experiments involving human behaviors are often used) to advance our understanding of cyber security phenomena
- Data sets, e.g., what makes good data sets? how do we know? how do we compare data sets? how do we collect new ones or generate derived ones? how do they hold up over time? how well do red 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., tools, usage techniques, support for experimentation in emerging security topics (cyber-physical systems, wireless, etc.)
- 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 '13 is designed to be a workshop in the traditional sense. Presentations are expected to be interactive with the expectation that a substantial amount of this time may be given to questions and audience discussion. Some papers will be given their own time slot of about 45 minutes, while similarly themed papers 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 and research papers are welcome as submissions. Submissions that recount experiences (e.g., from experimentation or teaching) are especially desired; these submissions should focus on take-aways and lessons learned which might be helpful to other researchers conducting similar research. For all submissions, the program committee will give greater weight to papers that lend themselves to interactive discussion among attendees.

Research papers should have a clearly stated methodology including a hypothesis and experiments designed to prove or disprove this hypothesis.

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

Position and research 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.

All submissions must be anonymized. Blind reviewing of papers will be conducted by the program committee. Authors must make a good faith effort to completely anonymize their submissions. Submissions violating the detailed formatting and anonymization rules will not be considered for the workshop.

Submissions must be in PDF format and must be submitted via the Web submission form on the CSET '13 Call for Papers Web site, www.usenix.org/conference/cset13/call-for-papers.

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.

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

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 www.usenix.org/conferences/submissions-policy for details. Questions? Contact your program co-chairs, cset13chairs@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 '13 Web site; rejected submissions will be permanently treated as confidential.