Announcement and Call for Papers

www.usenix.org/cset15/cfp

usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

8th Workshop on Cyber Security Experimentation and Test (CSET ’15)

Sponsored by USENIX

August 10, 2015, Washington, D.C.

CSET ’15 will be co-located with the 24th USENIX Security Symposium (USENIX Security ’15) and take place on Monday, August 10, 2015.

Important Dates

- Submissions due: *Tuesday, May 5, 2015, 8:59 p.m. PDT*
- Notification to participants: *Monday, June 8, 2015*
- Final papers due: *Tuesday, June 23, 2015*

Workshop Organizers

Program Co-Chairs

Adam Aviv, *U.S. Naval Academy*
Iulian Neamtiu, *University of California, Riverside*

Program Committee

Lujo Bauer, *Carnegie Mellon Univeristy*
Kevin Bauer, *MIT Lincoln Labs*
Matt Bishop, *University of California, Davis*
Nikita Borisov, *Univeristy of Illinois at Urbana-Champaign*
Kevin Butler, *University of Florida*
L. Jean Camp, *Indiana University*
Tudor Dumitras, *University of Maryland, College Park*
Sonia Fahmy, *Purdue University*
Mark Gondree, *Naval Postgraduate School*
Cynthia Irvine, *Naval Postgraduate School*
Daniel Marino, *Symantec Research Labs*
Michelle Mazurek, *University of Maryland, College Park*
Daniela Oliveria, *University of Florida*
Zachary Peterson, *California State Polytechnic University*
Zhiyun Qian, *University of California, Riverside*
John Sonchack, *University of Pennsylvania*
Robert Walls, *The Pennsylvania State University*
Andrew West, *Verisign Labs*

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 poses significant challenges—very little data are 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—experiences with and discussions of experimental methodologies, as well as topics in the broader area of science of security including holistic approaches to evaluating the security of systems, such as scalability and reusability of security systems, policy of security systems, predictive security metrics, and human factors of security.
- Measurement and metrics—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—experiences balancing stakeholder considerations, frameworks for evaluating the ethics of cyber security experiments.
- Data sets—both methodology (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?) and experimental results/analyses of interesting security data sets.
- Simulations and emulations—what makes good ones? How do they scale (up or down)?
- Testbeds and experimental infrastructure—supporting interconnected non-IT system such as telecommunications or industrial control, tools for improving speed and fidelity of testbed configuration, sensors for robust data collection with minimal testbed artifacts.
- Experiences with cyber security education—capture-the-flag exercises, novel experimentation techniques used in education, novel ways to teach hands-on cyber security.
- Panel Focus Area—Evaluation and Testing of Smartphone Security, including smartphone testbeds, system security, large scale usability studies, and new security metrics, will be the focus of a panel discussion. See below for details of submissions in this focus area.

Workshop Format

Because of the complex and open nature of the subject matter, CSET '15 is designed to be a workshop in the traditional sense. Presentations are expected to stimulate and facilitate audience discussion of the author's work with substantial time for questions and discussion. Each presentation will be formatted to include an abbreviated list of high-level results and time for initial questions or discussion with the audience, as well as time to follow up the initial presentation with additional details. Papers on similar topics may be grouped into a theme with other papers. To ensure a productive workshop environment, attendance will be limited to 80 participants.

Submission Instructions

Position papers and research papers are welcome as submissions. Submissions that recount experiences (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.

New this year: Authors may also choose to submit short position papers (3–4 pages) in the area of Evaluation and Testing of Smartphone Security, including smartphone testbeds, system security, large scale usability studies, and new security metrics. These papers will be evaluated for inclusion in a panel session on the topic. Short position paper titles should start with "Panel Submission:".

Full 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" x 9" deep. Text outside the 6.5" x 9" block will be ignored. Panel submissions should conform to the same format requirements except must be 3–4 pages including tables, figures, and references.

All full (6-8 page) research and position paper submissions must be anonymized. Blind reviewing of full 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.

Panel submissions are non-anonymous; they should include a list of authors on the first page and identify, via underlining, which author(s) wishes to participate in the panel discussion. All papers must be submitted via the Web submission form linked from the Call for Papers Web site: www.usenix.org/cset15/cfp.

Program committee members are allowed and encouraged to submit papers to the workshop in both full and short forms.

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 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. Please see the USENIX Conference Submissions Policy at www.usenix.org/conferences/submissions-policy for details. Questions? Contact your program co-chairs, cset15chairs@usenix.org, or the USENIX office, submissions-policy@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 '15 Web site; rejected submissions will be permanently treated as confidential.

Rev. 4/17/15