CSET '17: 10th USENIX Workshop on Cyber Security Experimentation and Test

August 14, 2016 • Vancouver, BC, Canada

Sponsored by USENIX, the Advanced Computing Systems Association

CSET '17 will be co-located with the 26th USENIX Security Symposium (USENIX Security '17) and take place August 14, 2017.

Important Dates

- Submissions due: **Tuesday, May 2, 2017, 11:59 p.m. PDT (no extensions)**
- Notification to authors: **Tuesday, June 13, 2017**
- Final papers due: **Tuesday, July 11, 2017**

Workshop Organizers

Program Co-Chairs

José M. Fernandez, *École Polytechnique de Montréal*
Mathias Payer, *Purdue University*

Program Committee

John Aycock, *University of Calgary*
Saurabh Bagchi, *Purdue University*
Kevin Borgolte, *University of California, Santa Barbara*
Sergey Bratus, *Dartmouth College*
Lucas Davi, *University of Duisburg-Essen*
Sven Dietrich, *CUNY John Jay College & The Graduate Center*
Brendan Dolan-Gavitt, *New York University*
Simon Edwards, *SE Labs*
Sonia Fahmy, *Purdue University*
Ryan Gerdes, *Virginia Tech University*
Fanny Lalonde-Lévesque, *École Polytechnique de Montréal*
Antoine Lemay, *École Polytechnique de Montréal*
Dave Levin, *University of Maryland*
Stefan Mangard, *TU Graz*
Jelena Mirkovic, *USC Information Sciences Institute (ISI)*
Cristina Nita-Rotaru, *Northeastern University*
Aravind Prakash, *Binghamton University*
Anil Somayaji, *Carleton University*
Peter Stelzhammer, *AV-Comparatives*
Gianluca Stringhini, *University College London*
Laura S. Tinnel, *SRI International*
Erik van der Kouwe, *Vrije Universiteit Amsterdam*
Chao Zhang, *Tsinghua 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

The CSET workshop invites submissions on cyber security evaluation, experimentation, measurement, metrics, data, simulations, and testbeds for software, hardware, or malware.

The science of cyber security poses significant challenges. For example, experiments must recreate relevant, realistic features in order to be meaningful, yet identifying those features and modeling them is very difficult. Repeatability and measurement accuracy are essential in any scientific experiment yet hard to achieve in practice. Few security-relevant datasets are publicly available for research use and little is understood about what "good datasets" look like. Finally, cyber security experiments and performance evaluations carry significant risks if not properly contained and controlled yet often require some degree of interaction with the larger world in order to be useful.

Addressing all these challenges is fundamental not only for scientific advancement in the field of Computer Security but also in order to enable evidence-based decision making on security products and policies by industry, government and individual users. 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:

- **Benchmarks for security:** e.g., development and evaluation of benchmark suites that evaluate certain security metrics
- **Research methods for cyber security experiments:** e.g., experiences with and discussions of experimental methodologies; experiment design and conduct addressing cybersecurity challenges for software, hardware, and malware
- **Measurement and metrics:** e.g., what are useful or valid metrics, test cases, and benchmarks? 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 collect new ones or generate derived ones? How do they hold up over time?
- **Security product evaluation methodologies:** e.g. what product evaluation methodologies provide more accurate prediction of real-world performance? How should user-related characteristics (behaviour, demographics) be modeled for in security product performance evaluation?
- **Simulations and emulations:** e.g., what makes good ones? How do they scale (up or down)?
- **Design and planning of cyber security studies:** e.g., hypothesis and research question, study design, data (collection, analysis, and interpretation), accuracy (validity, precision)
- **Ethics of cyber security research:** e.g., experiences balancing stakeholder considerations; frameworks for evaluating the ethics of cyber security experiments
- **Testbeds and experimental infrastructure:** e.g., tools for improving speed and fidelity of testbed configuration; sensors for robust data collection with minimal testbed artifacts; support for interconnected non-IT systems such as telecommunications or industrial control

Special note: Papers that primarily focus on computer security education are likely a better fit for the 2017 USENIX Workshop on Advances in Security Education (ASE '17), also co-located with the USENIX Security Symposium. Authors of education-centered papers should strongly consider submitting their work to ASE.

Workshop Format

Because of the complex and open nature of the subject matter, CSET '17 is designed to be a workshop in the traditional sense. Presentations are expected to be interactive, and presenters should ensure that sufficient time is reserved for questions and audience discussion. Audience participation is encouraged. To ensure a productive workshop environment, attendance will be limited to 80 participants.

Submission Instructions

Research papers and position papers are welcome as submissions. Research papers should have a clearly stated methodology including a hypothesis and experiments designed to prove or disprove the hypothesis. Position papers, particularly those that critique past work, should present detailed solutions, either proposed or implemented. Submissions that recount experiences (e.g., from experiments or deployments) are especially desired; these should highlight takeaways and lessons learned that might help researchers in the future. For all submissions, the program committee will give greater weight to papers that lend themselves to interactive discussion among attendees.

Submissions must be no longer than eight pages including all tables, figures, and references. Text should be formatted in two columns on 8.5"x11" paper using 10-point type on 12-point leading ("single-spaced"), with the text block being no more than 6.5"x9". Text outside the 6.5"x9" block will be ignored. Authors are encouraged to use the LaTeX and Word guides from the USENIX paper templates page at www.usenix.org/conferences/author-resources/paper-templates. The review process will be single-blind; submissions do not need to be anonymized.

All papers must be submitted in PDF format via the Web submission form on the CSET '17 Web site, www.usenix.org/cset17/cfp. Please do not email submissions.

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 the paper.

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, cset17chairs@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 '17 Web site; rejected submissions will be permanently treated as confidential.