CSET '18: 11th USENIX Workshop on Cyber Security Experimentation and Test

August 13, 2018, Baltimore, MD, USA

Sponsored by USENIX, the Advanced Computing Systems Association

The 11th USENIX Workshop on Cyber Security Experimentation and Test (CSET '18) will be co-located with the 27th USENIX Security Symposium (USENIX Security '18) and take place on August 14, 2018.

Important Dates

- Submissions due: **Thursday, May 10, 2018, (no extensions)**
- Notification to authors: **Tuesday, June 19, 2018**
- Final papers due: **Thursday, July 19, 2018**

Conference Organizers

Program Co-Chairs

Christian Collberg, *University of Arizona*
Peter A. H. Peterson, *University of Minnesota Duluth*

Program Committee

David Balenson, *SRI International*
Kevin Bauer, *MIT Lincoln Labs*
Matt Blaze, *University of Pennsylvania*
Sven Dietrich, *City University of New York*
Brendan Dolan-Gavitt, *New York University*
Eric Eide, *University of Utah*
Fanny Lalonde-Levesque, *École Polytechnique de Montréal*
Micah Sherr, *Georgetown University*
Peter Stelzhammer, *AV Comparatives*
Gianluca Stringhini, *University College London*
Laura S. Tinnel, *SRI International*
Brian Trammell, *ETH Zurich*
Robert Walls, *Worcester Polytechnic Institute*
Tim Yardley, *University of Illinois at Urbana-Champaign*
Chao Zhang, *Tsinghua University*

Steering Committee

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

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, emulations, and virtualizations: e.g., what makes good ones? How do they scale (up or down)? Are there fidelity problems that could affect results?
- 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 2018 USENIX Workshop on Advances in Security Education (ASE '18), 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 '18 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.

If the research presented in a paper produced research artifacts (code and data), authors should include in the paper an artifact sharing statement describing whether some or all of the artifacts will be made available to the community and, if so, how they will be shared (for example, the statement could include a URL to an artifact repository or an email address to a corresponding author). This statement should be present during both submission and in the final version of the paper. Authors are strongly encouraged to share artifacts whenever possible in order to enable analysis or validation, or to facilitate future investigations by the community. However, while sharing may be taken into account by reviewers, it is not a requirement for acceptance.

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" x 9". Text outside the 6.5" x 9" block will be ignored. Authors are encouraged to use the LaTeX and Word guides from the USENIX paper templates page (https://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 submission form linked from the CSET '18 website. 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 (https://www.usenix.org/conferences/author-resources/submissions-policy) for details. Questions? Contact your program co-chairs, cset18chairs@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 '18 website; rejected submissions will be permanently treated as confidential.