CSET '19: 12th USENIX Workshop on Cyber Security Experimentation and Test

August 12, 2019 • Santa Clara, CA, USA

Sponsored by USENIX, the Advanced Computing Systems Association

The 12th USENIX Workshop on Cyber Security Experimentation and Test (CSET '19) will be co-located with the 28th USENIX Security Symposium and will take place August 12 at the Hyatt Regency Santa Clara in Santa Clara, CA, USA.

Important Dates

- Paper submissions due: **Tuesday, May 21, 2019 (no extensions)**
- Notification to authors: **Tuesday, June 18, 2019**
- Final paper files due: **Tuesday, July 16, 2019**

Workshop Organizers

Program Co-Chairs

Rob Jansen, *U.S. Naval Research Laboratory*
Peter A. H. Peterson, *University of Minnesota Duluth*

Program Committee

Gunes Acar, *Princeton University*
Sadia Afroz, *University of California, Berkeley*
David Balenson, *SRI International*
Genevieve Bartlett, *USC Information Sciences Institute (ISI)*
Lujo Bauer, *Carnegie Mellon University*
Matt Bishop, *University of California, Davis*
Cecylia Bocovich, *University of Waterloo*
Nikita Borisov, *University of Illinois at Urbana–Champaign*
Kevin Butler, *University of Florida*
L. Jean Camp, *Indiana University*
Stephen Checkoway, *Oberlin College*
Heather Crawford, *Florida Institute of Technology*
Tamara Denning, *University of Utah*
Sven Dietrich, *The City University of New York*
Brendan Dolan-Gavitt, *New York University*
Adam Doupe, *Arizona State University*
Josiah Dykstra, *National Security Agency*
Eric Eide, *University of Utah*
Tariq Elahi, *University of Edinburgh*
William Enck, *North Carolina State University*
Jennifer Fernick, *NCC Group*
Deb Frincke, *National Security Agency*
Simson Garfinkel, *US Census Bureau*
Ian Goldberg, *University of Waterloo*
Julie Haney, *National Institute of Standards and Technology (NIST)*
Erik Kline, *USC Information Sciences Institute (ISI)*
Fanny Lalonde Levesque, *Element AI*
Ada Lerner, *Wellesley College*
Dave Levin, *University of Maryland, College Park*
Damon McCoy, *New York University*
Catherine Meadows, *U.S. Naval Research Laboratory*
Alyssa Milburn, *Vrije Universiteit Amsterdam*
Ariana Mirian, *University of California, San Diego*
Tyler Moore, *University of Tulsa*
Elissa Redmiles, *University of Maryland, College Park*
Stefanie Roos, *TU Delft*
Stephen Schwab, *USC Information Sciences Institute (ISI)*
Mahmood Sharif, *Carnegie Mellon University*
Jessica Staddon, *Google*
Laura S. Tinnel, *SRI International*
Carmela Tronosco, *École Polytechnique Fédérale de Lausanne (EPFL)*
Michael Carl Tschantz, *International Computer Science Institute (ICSI)*
Ingrid Verbauwhede, *Katholieke Universiteit Leuven*
Daniel Votipka, *University of Maryland, College Park*
Robert Walls, *Worcester Polytechnic Institute*
Daphne Yao, *Virginia Polytechnic Institute and State 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 of 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.

We highlight that **new changes for CSET '19 include:**

- A call for **preliminary work papers** describing works-in-progress and results (e.g., papers that could eventually be extended as full papers for publication at a conference).
- A call for **extended work papers** that expand upon a CSET-related component of previously published work (e.g., papers that provide more details about a previously developed approach, method, tool, measurement, benchmark, data set, simulation/emulation, experiment, or other experimental component).
- A preference for papers from a **more diverse** set of topic areas than those that have traditionally appeared at the workshop.

We also note that for CSET '19 we will feature new extended abstract and short paper submission options to facilitate these changes.

Topics

For CSET '19, we will prefer exciting work across a broad range of security-relevant areas, and we will endeavor to build a program with a diverse set of topics. Topic areas not traditionally found at CSET are especially encouraged and welcomed!

Topics of interest include but are not limited to the following (this list should be generously and broadly interpreted):

- **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

What to Submit

We welcome the submission of papers containing the following type of content:

- **Research Papers:** Research papers should have a clearly stated methodology including a hypothesis and experiments designed to prove or disprove the hypothesis.
- **Position Papers:** Position papers, particularly those that critique past work, should present detailed solutions, either proposed or implemented.
- **Experience Papers:** Experience papers should recount experiences (e.g., from experiments or deployments) and should highlight takeaways and lessons learned that might help researchers in the future.
- **Preliminary Work Papers:** Preliminary work papers should describe interesting and new ideas and early results, and we expect that such works-in-progress papers may eventually be extended as full papers for publication at a conference.
- **Extended Work Papers:** Extended work papers should expand upon a CSET-related component of previously published work (e.g., an extended set of experimental results or measurements that did not make it into a previous paper, or a presentation/evaluation of a tool or framework used in the published work) and should carefully explain the novel contribution compared to the original work.

For all submissions, the program committee will give greater weight to papers that lend themselves to interactive discussion among workshop attendees.

Submission Instructions

Page length limits vary by the type of submission:

- **Extended Abstract:** Submissions must be no longer than **two** pages. Extended abstracts should convince the reader that the author would give an exciting presentation at the workshop. We envision that extended abstracts will be position or experience papers, but this is not a hard requirement.
- **Short Paper:** Submissions must be no longer than **four** pages. Short papers should provide enough context and background for the reader to understand the contribution. We envision that short papers will be preliminary work or extended work papers, but this is not a hard requirement.
- **Long Paper:** Submissions must be no longer than **eight** pages. We envision that long papers will be the more traditional type of CSET research paper, but this is not a hard requirement.

The page length limits for all submissions include the space allowed for all tables, figures, references, and any appendices. 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 7" x 9". Text outside the 7" x 9" 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.

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). 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.

The review process will be double-blind; all submissions should be anonymized so as not to reveal the authors names or affiliations during the review process. All anonymized papers must be submitted in PDF format via the submission form linked from the Call for Papers website, www.usenix.org/cset19/cfp. Please do not email submissions.

All accepted 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/author-resources/submissions-policy for details. Note, however, that we expect that many preliminary work papers accepted for CSET '19 will eventually be extended as full papers suitable for formal academic publication and presentation at future conferences, and many extended work papers will expand upon previously published work; such papers are eligible for submission to CSET.

Papers accompanied by nondisclosure agreement forms will not be considered. Accepted submissions will be treated as confidential prior to publication on the USENIX CSET '19 website; rejected submissions will be permanently treated as confidential.

Questions? Contact your program co-chairs, cset19chairs@usenix.org, or the USENIX office, submissions-policy@usenix.org.