CSET '20: 13th USENIX Workshop on Cyber Security Experimentation and Test

August 10, 2020, Boston, MA, USA

Sponsored by USENIX, the Advanced Computing Systems Association.

The 13th USENIX Workshop on Cyber Security Experimentation and Test (CSET '20) will be co-located with the 29th USENIX Security Symposium and will take place August 10, 2020, at the Boston Marriott Copley Place in Boston, MA, USA.

Important Dates

- Paper submissions due: Tuesday, May 26, 2020, 8:59 pm PDT, (no extensions)
- Notification to authors: Thursday, July 2, 2020
- Final paper files due: Tuesday, July 21, 2020

Conference Organizers

Program Co-Chairs

Tamara Denning, *University of Utah*
Tyler Moore, *University of Tulsa*

Program Committee

AbdelRahman Abdou, *Carleton University*
Hussain Almohri, *Kuwait University*
David Balenson, *SRI International*
David Barrera, *Carleton University*
Genevieve Bartlett, *USC Information Sciences Institute (ISI)*
Kevin Bauer, *MIT Lincoln Laboratory*
Leyla Bilge, *NortonLifeLock Research Group*
Cecylia Bocovich, *The Tor Project*
Stephen Checkoway, *Oberlin College*
Heather Crawford, *Florida Institute of Technology*
Adam Doupé, *Arizona State University*
Josiah Dykstra, *National Security Agency*
Eric Eide, *University of Utah*
Tariq Elahi, *University of Edinburgh*
Sonia Fahmy, *Purdue University*
Simson Garfinkel, *US Census Bureau*
Mark Gondree, *Sonoma State University*
Julie Haney, *National Institute of Standards and Technology (NIST)*
Cormac Herley, *Microsoft*
Alice Hutchings, *University of Cambridge*
Cynthia Irvine, *Naval Postgraduate School*
Chris Kanich, *University of Illinois at Chicago*
Erin Kenneally, *Elchemy*
Doowon Kim, *University of Maryland, College Park*
Fanny Lalonde Lévesque, *Element AI*
Nektarios Leontiadis, *Facebook*
Ada Lerner, *Wellesley College*
Michelle Mazurek, *University of Maryland, College Park*
Catherine Meadows, *US Naval Research Laboratory*
Alyssa Milburn, *Vrije Universiteit Amsterdam*
Ariana Mirian, *University of California, San Diego*
Adwait Nadkarni, *College of William & Mary*
TJ OConnor, *Florida Institute of Technology*
Sean Peisert, *Berkeley Lab and University of California, Davis*
Zachary Peterson, *California Polytechnic State University*
Stefan Savage, *University of California, San Diego*
Micah Sherr, *Georgetown University*
Jonathan Spring, *CERT, SEI, Carnegie Mellon University*
Jessica Staddon, *Google*
Gianluca Stringhini, *Boston University*
Blair Taylor, *Towson University*
Laura S. Tinnel, *SRI International*
Tavish Vaidya, *Google*
Michel van Eeten, *Delft University of Technology*
Marie Vasek, *University College London*
Ingrid Verbauwhede, *Katholieke Universiteit Leuven*
Geoff Voelker, *University of California, San Diego*

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

What is CSET all about? For 12 years, the USENIX Workshop on Cyber Security Experimentation and Test (CSET) has been an important and lively space for presenting research and discussing "meta" topics related to reliability, validity, reproducibility, and scalability in cybersecurity and cybersecurity research, including: cybersecurity evaluation and measurement, experiment design, benchmarks, datasets, tools, simulations, testbeds, and education.

Submissions that model a scientific approach to cybersecurity are especially encouraged, as well as those that advance the "infrastructure" of cyber security science. Significant challenges abound. For example, experiments should operate in realistic environments, yet identifying salient features and modeling them in testbeds is hard. Repeatability is a worthy goal, but not always feasible. Few security-relevant datasets are publicly available for research use and little is understood about what "good datasets" look like. Cybersecurity 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; hence, ethical issues often arise. Finally, evidence-driven education practices and practices that leverage datasets are often absent in traditional computer science curricula.

Tackling these challenges helps promote evidence-based decision-making involving cybersecurity products and policies by industry, government and individual users.

We highlight for CSET '20:

- An explicit addition of cybersecurity education to the list of invited topics.
- The continuation from CSET '19 of multiple submission lengths (4-page short papers, 8-page long papers) and an invitation for papers from a more diverse set of topic areas than those that have traditionally appeared at the workshop.

Invited Topics

For CSET '20, we solicit exciting work across a broad range of security-relevant areas. Topics of interest include the following, broadly interpreted:

- **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?
- **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
- **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?
- **Benchmarks for security:** e.g., development and evaluation of benchmark suites that evaluate certain security metrics
- **Education:** e.g., evaluating and/or presenting educational approaches to cybersecurity, particularly (but not exclusively) approaches that leverage datasets, utilize testbeds, or promote awareness of research methods and sound measurement approaches.
- **Research methods for cybersecurity experiments:** e.g., experiences with and discussions of methods (including qualitative methods); experiment design and conduct addressing cybersecurity challenges for software, hardware, and malware
- **Design and planning of cybersecurity studies:** e.g., how to improve hypotheses and research questions, study designs, data (collection, analysis, and interpretation), and accuracy (validity, precision)
- **Ethics of cybersecurity research:** e.g., experiences balancing stakeholder considerations; frameworks for evaluating the ethics of cybersecurity experiments
- **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 in security product performance evaluation?

Submission Instructions

Types of Submissions (Lengths)

Page length limits vary by the type of submission:

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.

Page Limits and Formatting

The page length limits for all submissions include the space allowed for all tables, figures and any appendices. **New this year: References are excluded from page limits.** 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 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.

Additional Submission Categorization

During the submission process, authors will be asked to categorize their submission as either a research paper, position paper, experience paper, preliminary work paper, or extended work paper. While reviewers can see this categorization, the review process for all submission types will be identical. For all submissions, the program committee will give greater weight to papers that lend themselves to interactive discussion among workshop attendees.

- **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 previously published work and carefully explain the novel contribution compared to prior work. We welcome papers that provide more details about a previously developed approach, method, tool, measurement, benchmark, data set, simulation/emulation, experiment, or other experimental component. Extended work papers could also describe an extended set of experimental results or measurements that did not make it into a previous paper. We would also welcome presentation or evaluation of a tool or framework used in the published work. Note that the previous work could have been published in any venue, not just CSET. Scholars can also extend the work of other authors (e.g., using a previously published tool in a new way).

Sharing Research Artifacts

CSET is strongly focused on advancing the state-of-the-art and the state-of-the-practice in cybersecurity measurement, experimentation, research, and education. Authors are strongly encouraged to share artifacts whenever possible in order to enable transparency (including analysis or validation) and to facilitate building resources and tools for the cybersecurity community. Sharing will be taken into account by reviewers; however, it is not a requirement for acceptance.

If the research presented in a paper produced research artifacts (code or 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.

Anonymization and the Review Process

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.

Submitting

All anonymized papers must be submitted in PDF format via the submission form linked from the CSET '20 Call for Papers web page. Please do not email submissions.

Further Notes

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 constitute 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 '20 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 '20 website; rejected submissions will be permanently treated as confidential.

Questions? Contact your program co-chairs, cset20chairs@usenix.org, or the USENIX office, submissions-policy@usenix.org.