CSET 2021 – Call For Papers

CSET 2021 is organized in cooperation with USENIX, and is sponsored by USC Information Sciences Institute. We plan to hold the workshop virtually at the time when it would originally have been held—on Monday, August 9, preceding USENIX Security Symposium 2021. Proceedings will be published through ACM Digital Library.

Important Dates

- Paper submissions due: May 11, 2021 (no extensions)
- Notification to authors: July 1, 2021
- Final paper files due: July 12, 2021
- Workshop: August 9, 2021 - **virtual participation**

Overview

What is CSET all about? For 13 years, the Workshop on Cyber Security Experimentation and Test (CSET) has been an important and lively space for presenting research on and discussing **"meta" cybersecurity topics** related to reliability, validity, reproducibility, transferability, ethics, and scalability—in practice, in research, and in education. Submissions are particularly encouraged to **employ a scientific approach to cybersecurity** and/or **demonstrably grow community resources.**

Invited Topics

For CSET '21, we solicit exciting work across a broad range of areas relevant to security and privacy. A list of topics of interest (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?
- **Experimental infrastructure:** Testbeds, simulations, emulations, and virtualizations. e.g.,: tools for improving speed and fidelity of testbed configuration; sensors for robust data collection with minimal testbed artifacts
- **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. Submissions in this category are encouraged to bolster broader educational efforts, for example by enabling adoption by other educators.
- **Cybersecurity research methods:** e.g., designing and conducting evaluations in the context of cybersecurity challenges, experiences with and discussions of methods (including qualitative methods); data (collection, analysis, and interpretation)
- **Ethics of cybersecurity research:** e.g., experiences balancing stakeholder considerations; frameworks for evaluating the ethics of cybersecurity experiments
- **Evaluating real-world security controls:** e.g., what evaluation methodologies provide more accurate evaluation of real-world security performance? How should user-related characteristics (behavior, demographics) be modeled in security product performance evaluation?

Committees

Program Chairs

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

Publication Chair

- Giorgio Giacinto, University of Cagliari, Italy

Program Committee

- AbdelRahman Abdou, Carleton University
- Hussain Almohri, Department of Computer Science, Kuwait University
- David Balenson, SRI International
- David Barrera, Carleton University
- Kevin Bauer, MIT Lincoln Laboratory
- Josiah Dykstra, National Security Agency
- Eric Eide, University of Utah
- Sonia Fahmy, Purdue University
- Simson Garfinkel, George Washington University
- Mark Gondree, Sonoma State University
- Cynthia Irvine, Naval Postgraduate School
- Erin Kenneally, Elchemy
- Doowon Kim, University of Tennessee, Knoxville
- Inna Kouper, Indiana University
- Fanny Lalonde, None
- Nektarios Leontiadis, Facebook
- Ada Lerner, Wellesley College
- Catherine Meadows, US Naval Research Laboratory
- Alyssa Milburn, Vrije Universiteit Amsterdam
- Ariana Mirian, University of California, San Diego
- TJ O'Connor, Florida Institute of Technology
- Sean Peisert, Berkeley Lab and UC Davis
- Stefan Savage, UC San Diego
- Jono Spring, CERT/CC, SEI, Carnegie Mellon University
- Jessica Staddon, Google
- Laura Tinnel, SRI International
- Michel van Eeten, Delft University of Technology
- Ingrid Verbauwhede, KU Leuven
- Geoff Voelker, UC 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)

Submission Instructions

Proceedings
CSET 2021 proceedings will be published through ACM Digital Library.

Sharing Research Artifacts
CSET is focused on advancing the state-of-the-art and the state-of-the-practice in cybersecurity in practice, research, and education. Authors are **strongly** encouraged to share artifacts whenever possible in order to enable transparency (e.g., analysis or validation) and to facilitate the accumulation of resources 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 (e.g., code, 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 (e.g., web site). This statement should be present during both submission and in the final version of the paper.

Submission Length Options
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.

Submissions should use (2-column) ACM proceedings templates. The page length limits include the space allowed for all tables and figures. References and appendices are excluded from page limits, however reviewers are not required to view the appendices when evaluating submissions.

Submission Types
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 make a novel contribution in line with one of the topics of interest.
- **Position Papers:** Position papers discuss new or provocative ideas of interest to the CSET community.
- **Experience Papers:** Experience papers should describe activities and recount lessons learned (e.g., from experiments or deployments) that might help researchers in the future.
- **Preliminary Work Papers:** Preliminary work papers should describe early results from interesting and new ideas. We anticipate that such works-in-progress papers may eventually be extended as full papers for publication at a conference.
- **Extended Work Papers:** Extended work papers can expand upon unpublished aspects of a previous work (published in any venue). We welcome papers that provide a compelling addition to a previously developed approach, method, tool, measurement, benchmark, data set, simulation/emulation, evaluation results, etc. Notes that submissions in this category can extend the work of others (e.g., using a previously published tool in a new way). Submissions in this category should clearly explain which sections are novel compared to prior work.

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.

Ethics & Human Subjects
Submissions that have potential ethical implications must include a section on ethics. Any submission that introduces research or results related to human subjects (including their data) must include a statement on its review by the appropriate institutional review boards.

Respectful and Inclusive Terminology
Please refer to the ACM's list of charged terminology and use alternatives in your submissions.

Submitting
All anonymized papers must be submitted in PDF format via the submission system at https://cset21.hotcrp.com/. Please do not email submissions.

Further Notes
(*) At least one author from every accepted paper must register for the workshop and present the paper. (*) Fraud and dishonesty are prohibited, including: simultaneous submission of the same work to multiple venues, submission of previously published work, and plagiarism. (*) Papers accompanied by nondisclosure agreement forms will not be considered.

Questions? Contact your program co-chairs: cset21chairs@gmail.com.