The Proceedings of
CSET 2022

15th Workshop on

Cyber Security Experimentation and Test

Hosted virtually

August 8th 2022

https://cset22.isi.edu

The Association for Computing Machinery
1601 Broadway, 10th Floor
New York, New York 10019, USA

ACM ISBN: 978-1-4503-968 4-4

Organizing Committee

Program Chairs

Alefiya Hussain, USC Information Sciences Institute
Thomas Tarman, Sandia National Laboratories

Technical Program Committee

Aydin Aysu, North Carolina State University
David Balenson, SRI International
Matt Bishop, University of California at Davis
Claudiu Danilov, The Boeing Company
Katherine Davis, Texas A&M University
Eric Eide, University of Utah
Michael Clifford, Toyota InfoTech Labs
Karl Levitt, University of California at Davis
David Manz, Pacific Northwest National Laboratory
Tyler Moore, University of Tulsa
Sean Oesch, Oak Ridge National Laboratory
Jeremiah Onaolapo, University of Vermont
Onyema Osuagwu, Morgan State University
Luke Rostowfske, United States Air Force
Meghan Sahakian, Sandia National Labs
Elizabeth Stobert, Carleton University
Laura Tinnel, SRI International
Arun Viswanathan, Jet Propulsion Laboratory
Eric Vugrin, Sandia National Laboratories
Mythili Vutukuru, Indian Institute of Technology, Bombay
Katsunari Yoshioka, Yokohama National University

External Reviewers

Alexander Outkin, Sandia National Laboratories
Brian Kocoloski, USC Information Sciences Institute (ISI)
Christophe Hauser, USC Information Sciences Institute (ISI)
Luis Garcia, USC Information Sciences Institute (ISI)
Michelle Leger, Sandia National Laboratories
Novak Boskov, Boston University
Thamme Gowda, USC Information Sciences Institute (ISI)
Vasanta Chaganti, Swarthmore College

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)

Preface

This volume contains the papers presented at the 15th Workshop on Cyber Security Experimentation and Test (CSET), held virtually on August 8th 2022. We received a strong collection of papers on a diverse set of topics and accepted 18 out of 36 submissions for publication and presentation at the workshop. The technical program committee of 23 people and 8 external reviewers helped reach this decision. All papers received at least 3 reviews and several papers were debated heavily at the technical program committee meeting.

We thank the program committee for their expertise in carefully selecting papers for a vibrant program. They selected 12 long papers and 6 short papers to cover topics in (i) **experimental infrastructure** on specialized testbeds and emulations and virtualizations studies, (ii) **data sets** including collection, analysis, and interpretation of data, (iii) **education** with tools and techniques for cyber security education and training (iv) **cybersecurity research methods** including designing and conducting large and complex system evaluations, traffic generation, binary analysis and vulnerability propagation, and (v) **measurement and metrics** for malicious attacks and cybersecurity systems.

The huge advantage of a virtual workshop is that it reduces the barrier for global participation. The workshop had several international submissions, and the final program has three papers from Europe, one from South Korea, one from India, and one from Canada. All authors have been encouraged to publish artifacts and datasets if feasible so that others in the research community can build upon their work. Several papers in the dataset session have committed to providing open access to their data.

Until two years ago, CSET was held in conjunction with the USENIX Security Symposium. USENIX made the difficult decision to not hold workshops alongside the symposium to reduce COVID-related infections in 2022. CSET will continue to explore partnership with the USENIX Security symposium again next year.

The proceedings for the CSET 2022 program are being published by the ACM International Conference Proceeding Series (ICPS). All CSET papers will appear in the ACM Digital Library (DL) and will be assigned DOIs, enhancing discovery, enabling persistent reference linking and archiving in digital preservation repositories, and ensuring perpetual access. Publication in the ACM DL ensures high visibility. The ACM DL averages over 4 million unique users from 195 countries every month. On average, users generate 4.4 million page views and 1.75 million downloads each month, thereby increasing the visibility of the CSET workshop within the international computing community.

Finally, we thank the authors who submitted papers to CSET, as well as the participants in the workshop for providing the kind of stimulating discussions and feedback that make CSET so enjoyable and productive.

Thank you and sincerely,
Alefiya Hussain
Thomas Tarman