THE LASER WORKSHOP

Learning from Authoritative Security Experiment Results

Co-located with the
2025 Annual Computer Security Applications Conference (ACSAC)

December 9, 2025

LASER Workshop Series

Focuses on learning from and improving cybersecurity experiment results

The workshop strives to provide a highly interactive, collegial environment for discussing and learning from experimental methodologies, execution, and results

Ultimately, the workshop seeks to foster a dramatic change in the experimental paradigm for cybersecurity research, improving the overall quality and reporting of practiced science

https://www.laser-workshop.org/

Accelerating Cybersecurity Research

While safety and security challenges brought on by new technological advances are mounting, the overall progress in cybersecurity research to meet these challenges has historically been slow

The lack of scientific progress in cyber security is due, in part, to issues in three areas, on which past LASER workshops have focused:

- Learning from and reporting of unsuccessful or unanticipated results, leading to a reduction in the repetition of past failures
- Adequate reporting of experiments, leading to an ability to understand the approach taken and reproduce results
- Solid experiment methodologies and execution, leading to reliable, conclusive results

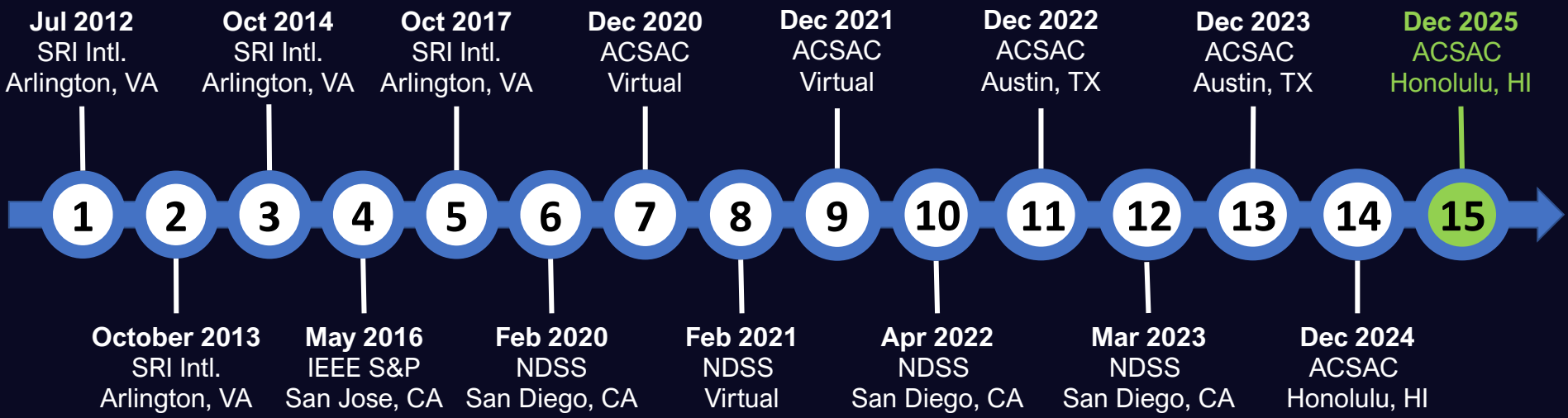
LASER 2020-2025 Workshops

Authors of accepted ACSAC (and NDSS) papers are invited to present the experimental aspects of their work

Authors lead a focused discussion on the experimental approaches and methodologies used to obtain their results



LASER Timeline – Our 15th Workshop!



https://laser-workshop.org/workshops.html

Some Related Work

NSF-funded Cybersecurity Experimentation of the Future (CEF) Study. https://cyberexperimentation.org/

National Academies of Sciences, Engineering, and Medicine 2019. Reproducibility and Replicability in Science. Washington, DC: The National Academies Press. https://doi.org/10.17226/25303

Cybersecurity Experimentation Workshop, 2022. https://bit.ly/CyberExperWkshp2022

Workshop on Improving the Quality and Reuse of Cybersecurity Datasets, Software, and Other Research Artifacts, March 2023. https://bit.ly/CyberArtifactsWkshp2022

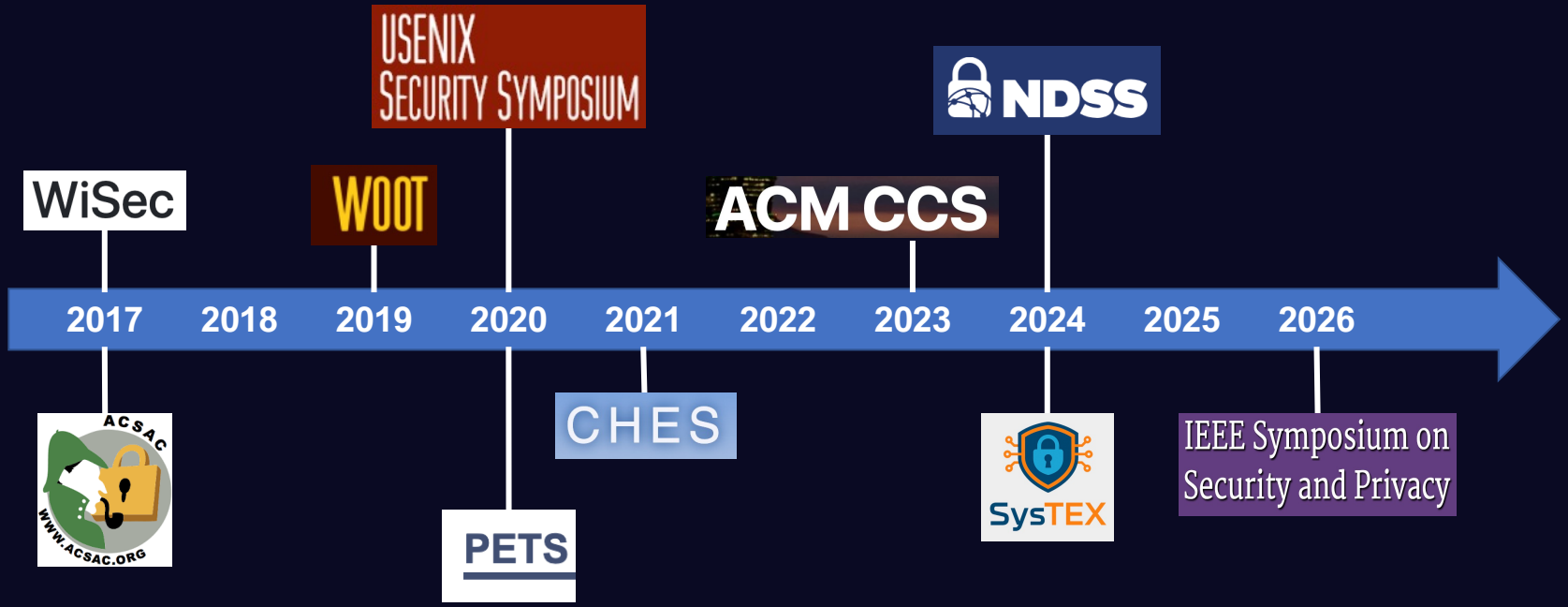
Workshop on Cybersecurity Experimentation and Test (CSET). https://cset25.isi.edu/past.html

Sharing Expertise and Artifacts for Reuse Through Cybersecurity Community Hub (SEARCCH). https://searcch.cyberexperimentation.org/

Community Understanding of Network Datasets (CLASSNET). https://comunda.isi.edu/

Security and Privacy Heterogeneous Environment for Reproducible Experimentation (SPHERE). https://sphere-project.net

Security Conferences w/ Artifact Initiatives



Security Research Artifacts. https://secartifacts.github.io/

LASER@ACSAC 2025 Organizers



David Balenson
(USC-ISI)

“The LASER Workshop” Social Media



- The LASER Workshop
- @LASER_Workshop



- The LASER Workshop
- @TheLASERWorkshop



- Learning from Authoritative Security Experiment Results
- https://www.linkedin.com/groups/8116696/

Hashtag
#LASER2025

Workshop Format

The workshop will be structured as a true “workshop” in the sense that it will focus on discussion and interaction around the topic of

Experimental methodologies, execution, and results

Authors will lead the group in a discussion of the experimental aspects of their work

Ultimate goal is to share and learn from each other and encourage improvements in experimental science in cybersecurity research

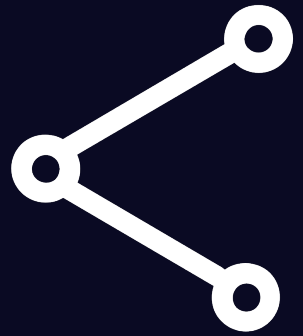
Additional information, abstracts, bios, and links to papers are available in the LASER Workshop program on the ACSAC website at https://www.openconf.org/acsac2025/modules/request.php?module=oc_program&action=page.php&id=17

Areas of Interest



- Research questions and/or hypotheses
- Experimental methodologies and design
- Simulation, emulation, virtualization, and/or physical testbeds
- Specialized hardware (e.g., CPS, IoT)
- Modeling human behavior
- Tools used/developed for experimentation
- Validation, monitoring, and data collection
- Datasets used/developed
- Measurements, metrics, and analysis techniques

Interesting Meta-Questions



- Did you use artifacts borrowed from the community?
- Did you attempt to replicate or reproduce prior results?
- What can others learn from your methodology and experience?
- What approaches failed before the results you presented?
- Did you generate intermediate or negative results?

Session Format

Time	Topic
5 mins	Introduce the main topic of your work (e.g., EM control flow verification or automotive CAN bus)
10 mins	Discuss the experiments or evaluations performed, including the areas of interest (as applicable)
10 mins	Lead the group in a discussion of the meta-questions
5 mins	Wrap up discussion (next steps)
30 mins	**TOTAL**

Agenda (1)

WELCOME AND INTRODUCTION

SESSION 1: Experiment Design and Reproducibility Foundations

- Taming the Chaos: Managing Reproducibility in Experiments and Results, Sebastian Neef (TU-Berlin)
- TS;DR (too spammy; didn't read) - Challenges when disclosing vulnerabilities to small- and medium-sized businesses, Anne Hennig (KIT)
- EM-Flow: Advanced Electromagnetic Control Flow Verification for Embedded Systems, Carson Stillman (U. Florida)

BREAK

SESSION 2: Session 2: System-Level Experimentation and Validation

- Zeus-IoT: Experimental Evaluation of Integrity Enforcement on OpenWrt, Alireza Roshandel (Boston University)
- CarDS – Controller Area Network and Automotive Ethernet Realistic Data Set: How to record a Comprehensive and Multimodal Automotive Dataset, Jannis Hamborg (Darmstadt University of Applied Sciences)

Agenda (2)

LUNCH

INVITED TALKS

- Supporting Artifact Evaluation – LLMs to the Rescue?, Jan Pennekamp (RWTH Aachen U)
- The SPHERE Research Infrastructure and its Support for Artifact Evaluation, David Balenson (USC-ISI)

BREAK

SESSION 3: Experimental Frameworks for AI and Security Tools

- Securing LLM-Generated Code: Experimental Insights from APILOT, Weiheng Bai (University of Minnesota)
- Siren: A Learning-Based Multi-Turn Attack Framework for Simulating Real-World Human Jailbreak Behaviors, Yi Zhao (The Hong Kong Polytechnic University)
- Domain-specific Qualitative Evaluation of LLMs for End-users, Vijay Prakash (NYU)

WRAP-UP

LASER “Experiment”

H1: ACSAC authors are excited about sharing their experimental methodologies, execution, and results

H2: ACSAC authors and LASER participants are interested in learning about other researchers’ experimental methodologies, execution, and results

H3: ACSAC authors and LASER can work collaboratively to improve experimental science in cybersecurity research

