THE LASER WORKSHOP

Learning from Authoritative Security Experiment Results

Co-located with the
2024 Annual Computer Security Applications Conference (ACSAC)

December 10, 2024

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 2020-2024 Workshops

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

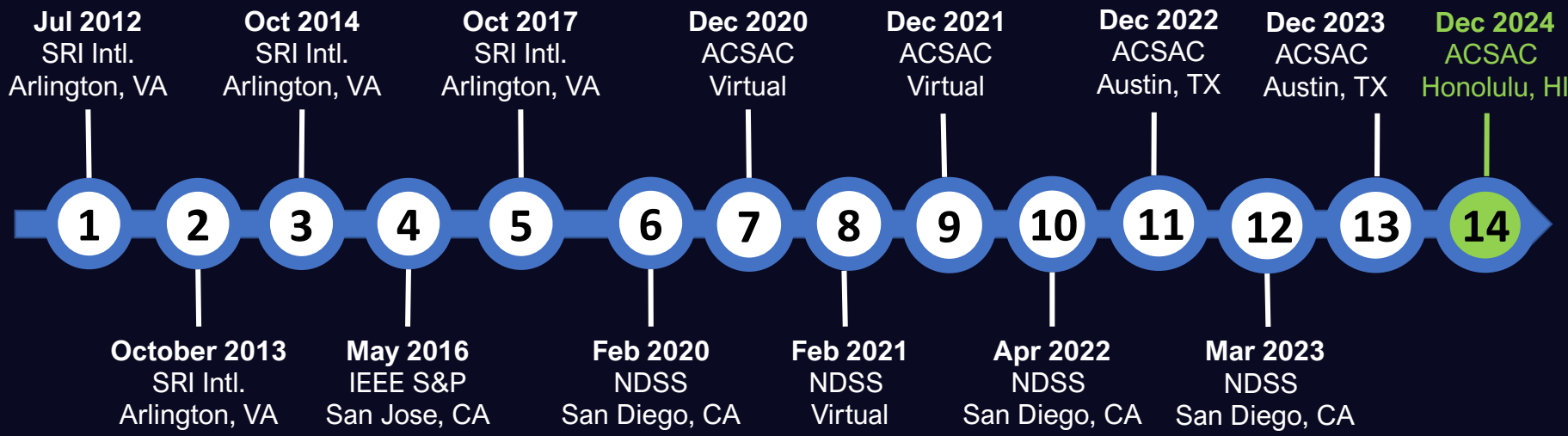
Authors lead a focused discussion on the experimental approaches and methodologies used to obtain their results

Authors are invited to write new papers focused on their experimental work

- Published in post-workshop proceedings
- Could be guided, in part, by the discussions and interactions at the workshop



LASER Timeline – Our 14th 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 Cybersecurity Experimentation and Test (CSET). https://cset24.isi.edu/past.html

ACSAC Artifacts Submission. https://www.acsac.org/2024/submissions/papers/artifacts/

USENIX Security Artifacts Submission. https://www.usenix.org/conference/usenixsecurity25/call-for-artifacts

ACM CCS Artifacts Submission. https://www.sigsac.org/ccs/CCS2024/call-for/call-for-artifacts.html

NDSS Artifacts Submission. https://www.ndss-symposium.org/ndss2025/submissions/call-for-artifacts/

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

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

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

LASER@ACSAC 2024 Organizers



David Balenson
(USC-ISI)

“The LASER Workshop” Social Media



- The LASER Workshop
- @LASER_Workshop

Hashtag
#LASER2024



- The LASER Workshop
- @TheLASERWorkshop



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

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

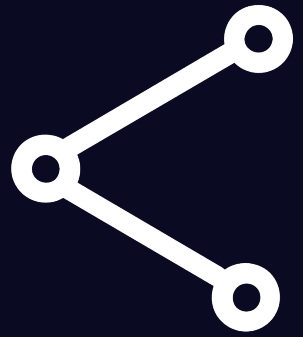
Additional information, abstracts, bios, and links to papers are available in the LASER Workshop program on the ACSAC website at https://www.openconf.org/acsac2024/modules/request.php?module=oc_program&action=page.php&id=19

Areas of Interest



- Research questions and/or hypothesis
- Experimental methodologies used and/or developed
- Experiment design
- Use of simulation, emulation, virtualization, and/or physical testbeds
- Use of specialized hardware including CPS and IoT devices
- Modeling of human-behavior characteristics
- Software tools used and/or developed to perform experimentation
- Approaches to experiment validation, monitoring, and data collection
- Datasets used and/or developed to perform experimentation
- Measurements and metrics
- Analytical techniques used and/or developed to evaluate experimental results

Interesting Meta-Questions



- Did you use experimentation artifacts borrowed from the community?
- Did you attempt to replicate or reproduce results of earlier research as part of your work?
- What can be learned from your methodology and your experience using your methodology?
- What did you try that did not succeed before getting to the results you presented?
- Did you produce any intermediate results including possible unsuccessful tests or experiments?

Session Format

Time	Topic
~~10~~ 5 mins	Introduce the main topic of your work (e.g., federate learning or honeypots)
~~20~~ 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, post-workshop paper)
~~45~~ 30 mins	**TOTAL**

Agenda (1)

WELCOME, GOALS, AND AGENDA

SESSION 1

- VaktBLE: Evaluating a Wireless Man-in-the-Middle Bridge against Malevolent BLE Connections
- Experimental Approaches for Robust Authentification Based on Hardware Impairments
- Electromagnetic Interference Experiments - Design and Best Practices

BREAK

SESSION 2

- Evaluating Machine Learning-Based Binary Vulnerability Detectors: Lessons From the Trenches
- Evaluating Approaches for Identifying Cryptographic Functions in Binaries
- Cybersecurity Research in 3D Bioprinting: Experiments and Evaluation Challenges and Future Directions

Agenda (2)

LUNCH

SESSION 3

- KEYNOTE: Well, It Worked on My Computer: Reproducibility in Computer Security Research

BREAK

SESSION 4

- From Groundhog Day to Ground Truth Data: We Need Curated Datasets to Spur Innovation
- Benchmarking Large Language Models: From General Purpose to Cybersecurity Applications
- Experimental Aspects of Investigating the Failures and Shortcomings of Security Countermeasures

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

