The LASER Workshop

Learning from Authoritative Security Experiment Results

Co-located with the
2022 Annual Computer Security Applications Conference (ACSAC)

December 6, 2022

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/

THE LASER WORKSHOP

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 2020-2022 Workshops

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

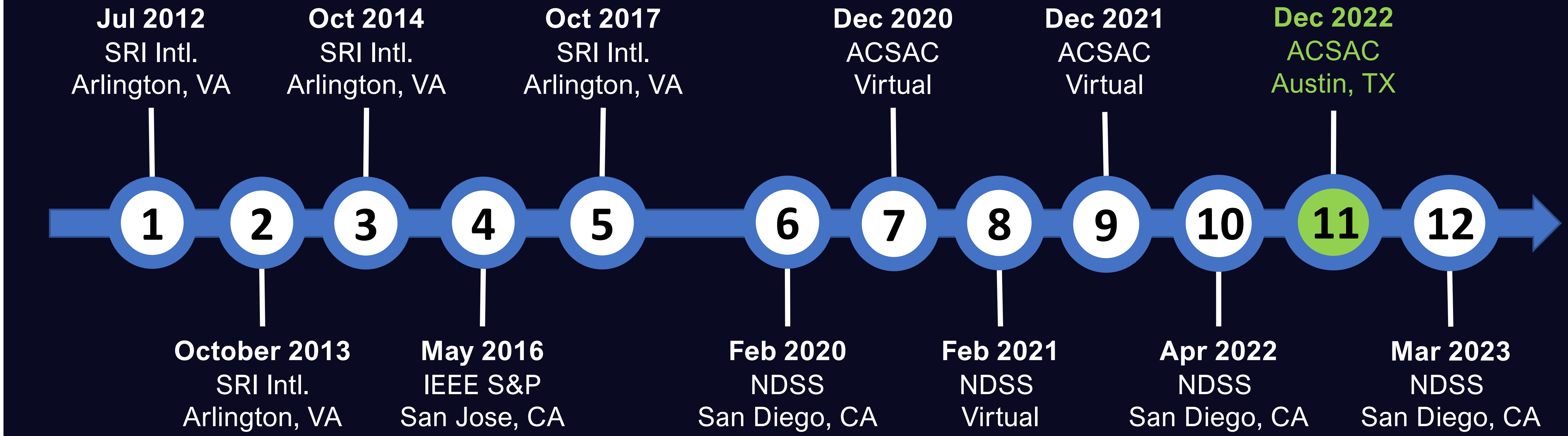
Authors lead a focused discussion on the experimental approaches and methodologies used to obtain their results

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

THE LASER WORKSHOP

LASER Timeline – Our 11th Workshop!



Jul 2012
SRI Intl.
Arlington, VA

October 2013
SRI Intl.
Arlington, VA

Oct 2014
SRI Intl.
Arlington, VA

May 2016
IEEE S&P
San Jose, CA

Oct 2017
SRI Intl.
Arlington, VA

Feb 2020
NDSS
San Diego, CA

Dec 2020
ACSAC
Virtual

Feb 2021
NDSS
Virtual

Dec 2021
ACSAC
Virtual

Apr 2022
NDSS
San Diego, CA

Dec 2022
ACSAC
Austin, TX

Mar 2023
NDSS
San Diego, CA

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

Some Related Work

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

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

USENIX Workshop on Cybersecurity Experimentation and Test (CSET). https://www.usenix.org/conferences/byname/135

ACSAC Artifacts Submission. https://www.acsac.org/2022/program/artifacts/

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

LASER@ACSAC 2022 Organizers

David Balenson
(USC-ISI)

Laura Tinnel
(SRI International)

“The LASER Workshop” Social Media

Twitter

- The LASER Workshop
- @LASER_Workshop

Facebook

- The LASER Workshop
- @TheLASERWorkshop

LinkedIn

- Learning from Authoritative Security Experiment Results
- groups/8226696

Hashtag
#LASER2022

THE LASER WORKSHOP

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/acsac2022/modules/request.php?module=oc_program&action=page.php&id=15

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 mins	Introduce the main topic of your work (e.g., federate learning or honeypots)
20 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 mins	**TOTAL**

Agenda (1)

Workshop Welcome, Goals, and Agenda

Session 1

- Threats in Crowdsourcing Threat Intelligence for Practical Threat Triaging, Afsaf Anwar, Northeastern University
- Exploring Backdoors in Federated Graph Neural Networks, Stjepan Picek, TU Delft

Session 2

- Simulation of Differentially Private Federated Meta-learning Systems, Ning Wang, Virginia Tech
- Torches on Pitchfork: Multi-feature Evaluation of a Security-oriented Programming Toolchain, Nik Sultana, Illinois Institute of Technology

Agenda (2)

Keynote Talk

- Towards True Reproducibility of Findings in Cybersecurity Research, Emma Tosch, Researcher, Northeastern University

Session 3

- Performance Analysis: Robust Combiners vs. Secret Sharing, Reza Samavi, Toronto Metropolitan University

Session 4

- Design and Methodology of a Longitudinal Honeypot Study, Shreyas Srinivasa, Aalborg University

Wrap-up

THE LASER WORKSHOP

LASER 2020-2022 “Experiment”

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

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

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