THE LASER WORKSHOP

Learning from Authoritative Security Experiment Results

Co-located with the
Annual Computer Security Applications Conference (ACSAC 2021)

December 7, 2021

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

Authors can write new papers focused on their experimental work

- Published in post-workshop proceedings
- Guided, in part, by the discussions and interactions at the workshop

Applied Computer Security Associates

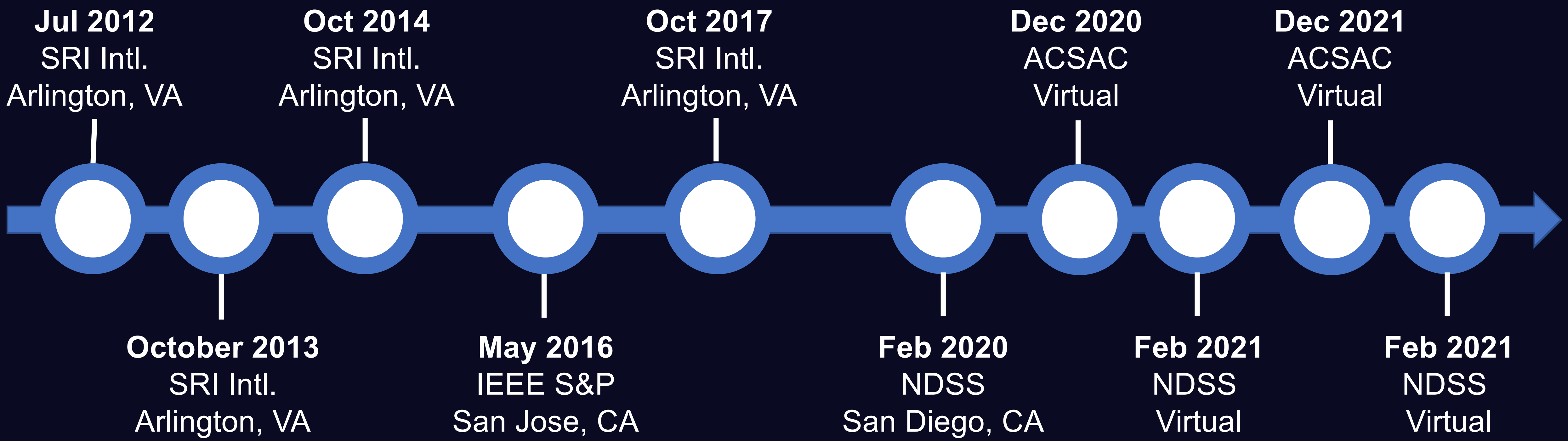
ACSA is a non-profit association of computer security professionals who have a common goal of improving the understanding, theory, and practice of computer security

To this end, ACSA supports a number of activities, all of which serve the goal of improving the computer security field:

- ACSAC - Annual Computer Security Applications Conference
- NSPW - New Security Paradigms Workshop
- LASER - Learning from Authoritative Security Experiment Results

https://www.acsac.org/acsa/

LASER Timeline



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

Feb 2021
NDSS
Virtual

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/2021/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 2021 Organizers

Organizing Committee

- David Balenson (SRI International)
- Laura S. Tinnel (SRI International)
- Terry Benzel (USC-ISI)

“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
#LASER2021

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 on the NDSS website at https://www.openconf.org/acsac2021/modules/request.php?module=oc_program&action=page.php&id=43

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
5 mins	Introduce the main topic of your work (e.g., Screen Gleaning or Binary-level symbolic analyzers)
15 mins	Discuss the experiments or evaluations performed, including the areas of interest (as applicable)
15 mins	Lead the group in a discussion of the meta-questions
10 mins	Wrap up discussion (next steps, post-workshop paper)
45 mins	**TOTAL**

Agenda (1)

Workshop Welcome, Goals, and Agenda

Session 1

- Under the Hood of MARVEL
  Antonio Ruggia (U. Genoa)

- Methodological Challenges In Investigating the User Experience of Cyber Threat Intelligence Data Sharing Platforms
  Gabriele Lenzini, Borce Stojkovski (U. Luxembourg)

Session 2

- Keynote: Using Co-Simulation for Model Reuse and Experiment Reproducibility
  Thomas Roth (NIST)

Agenda (2)

Session 3

- Dissecting ARID: Implementing and Evaluating Security Solutions on Open-Source Drones
Pietro Tedeschi (HBKU), Savio Sciancalepore (TU/e), Roberto Di Pietro (HBKU)

- Evaluating Fast Speech Based Adversarial Audio Attack
Edwin Yang (U. Oklahoma)

Session 4

- A Proof of Concept for Usability and Efficacy Evaluations as a Component of IETF Standards Using MUD
Vafa Andalibi and Jayati DevWorkshop (Indiana U. Bloomington)

- An Experimental Approach to Evaluate the Security of Mobile Autofill Frameworks on iOS and Android
Sean Oesch (ORNL)

Wrap-up

LASER 2020-2021 “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

Workshop Papers

Participants in the LASER Workshop are invited to write new papers on their experimental work

The papers will be published in post-workshop proceedings

The new papers will be driven and guided, in part, by the discussions and interactions, and possibly even new collaborations, forged at the workshop

Notional Schedule

- Draft papers due approximately two (2) months after workshop
- Program committee will review papers and provide notifications and feedback one (1) month later
- Final camera-ready papers will be due approximately one (1) month later

Tentative Dates

Draft Papers Submitted: February 7, 2022
Notifications and feedback: March 7, 2022
Final Papers Submitted: April 7, 2022
Papers Published: May 7, 2022

Workshop Papers Additional Guidance

Focus on and expand the experimental aspects of your work

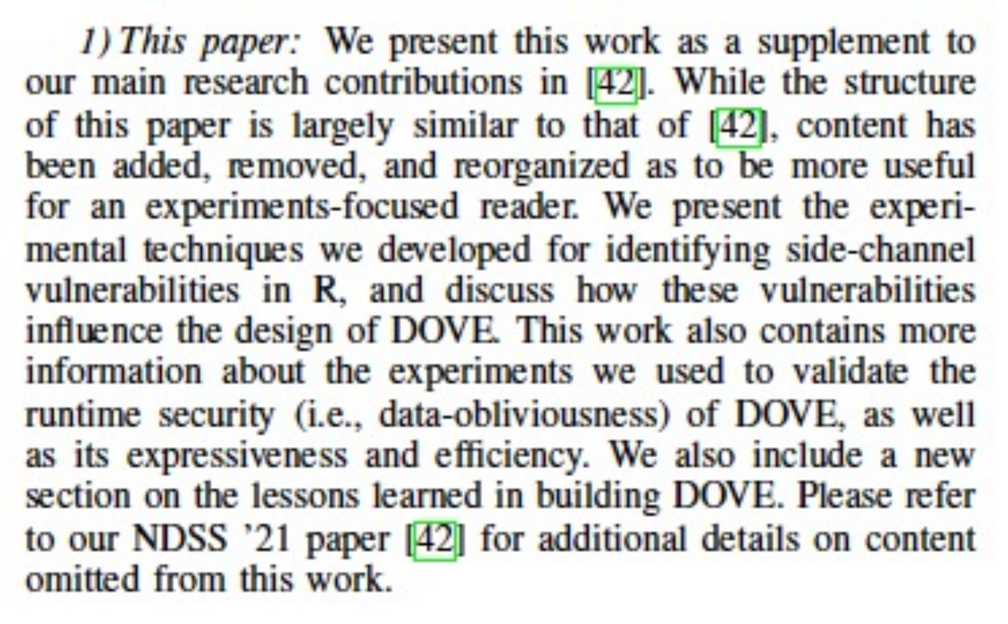
Cite the original paper and briefly summarize the content as background

Touch on relevant areas of interest and meta-questions discussed earlier

Include lessons learned

At least 30% new content, but percentage should be higher if you follow the guidance

Paper should be no more than 12 pages



1) This paper: We present this work as a supplement to our main research contributions in [42]. While the structure of this paper is largely similar to that of [42], content has been added, removed, and reorganized as to be more useful for an experiments-focused reader. We present the experimental techniques we developed for identifying side-channel vulnerabilities in R, and discuss how these vulnerabilities influence the design of DOVE. This work also contains more information about the experiments we used to validate the runtime security (i.e., data-obliviousness) of DOVE, as well as its expressiveness and efficiency. We also include a new section on the lessons learned in building DOVE. Please refer to our NDSS '21 paper [42] for additional details on content omitted from this work.

Tushar M. Jois , Hyun Bin Leey, Christopher W. Fletchery, and Carl A. Gunter, On Building the Data-Oblivious Virtual Environment, LASER (NDSS) 2021, February 25, 2021, https://dx.doi.org/10.14722/laser.2021.23056.

Use the LASER Workshop paper formatting instructions and templates on the NDSS website set (currently https://www.ndss-symposium.org/ndss2021/templates/)