THE LASER WORKSHOP

Learning from Authoritative Security Experiment Results

Co-located with Annual Computer Security Applications Conference (ACSAC 2020)

Virtual Zoom Land

December 8, 2020

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/

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/

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 Timeline

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/2019/program/artifacts/

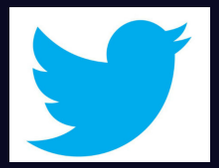
National Academies of Sciences, Engineering, and Medicine 2019. Reproducibility and Replicability in Science. Washington, DC: The National Academies Press. https://doi.org/10.17226/25303

LASER 2020 Organizers

Organizing Committee

- David Balenson (SRI International)
- Terry Benzel (USC-ISI)
- Laura S. 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
#LASER2020

LASER 2020 ACSAC “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

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

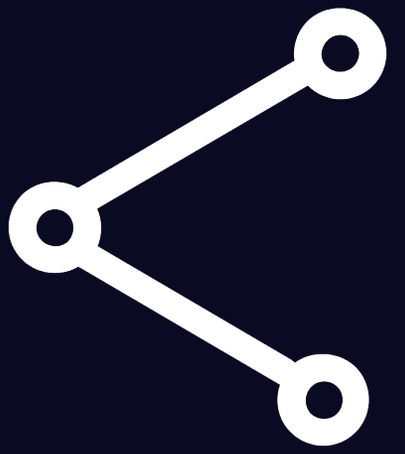
Ultimate goal is to share and learn from each other and encourage improvements in experimental science in cybersecurity research

Additional information, abstracts, bios, and links to papers are available on the ACSAC website at https://www.acsac.org/2020/workshops/laser/

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., assisted ROP exploit generation or automated stock manipulation)
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 Organization

Session 1

- Guide Me to Exploit: Assisted ROP Exploit Generation for ActionScript Virtual Machine
  Fadi Yilmaz; Meera Sridhar; Wontae Choi
- A Process Cycle View on Utilizing Security and Privacy Research to Realize Novel Forms of Industrial Applications and Collaboration
  Jan Pennekamp; Erik Buchholz; Yannik Lockner; Markus Dahlmanns; Tiandong Xi; Marcel Fey; Christian Brecher; Christian Hopmann; Klaus Wehrle

Session 2

- Invited Talk: Experiments, Methods, Measurements, Instruments -- A Few Details
  Roy Maxion, Research Professor, Carnegie Mellon University

Agenda (2)

Session 3

- On the Feasibility of Automating Stock Market Manipulation
  Carter Yagemann; Simon P. Chung; Erkam Uzun; Sai Ragam; Brendan Saltaformaggio; Wenke Lee
- Analyzing IoT Malware
  Emanuele Cozzi; Pierre-Antoine Vervier; Matteo Dell'Amico; Yun Shen; Leyla Bilge; Davide Balzarotti

Session 4

- Session Key Distribution Made Practical for CAN and CAN-FD Message Authentication
  Yang Xiao; Shanghao Shi; Ning Zhang; Wenjing Lou; Y. Thomas Hou

Workshop Wrap-up

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 8, 2021
Notifications and feedback: March 8, 2021
Final Papers Submitted: April 8, 2021
Papers Published: May 8, 2021