

# LASER 2017

Learning from Authoritative Security Experiment Results

# CALL FOR PAPERS

**OCTOBER 18-19, 2017**

**1100 WILSON BLVD, SUITE 2800, ARLINGTON, VIRGINIA**

**Full Papers Due:** July 15, 2017

**Decisions to Authors:** September 1, 2017

**Workshop:** October 18-19, 2017

**Pre-Workshop Papers Due:** Sept. 29, 2017

**Final Papers Due:** November 22, 2017

## THE LASER WORKSHOP

The *Learning from Authoritative Security Experiment Results (LASER)* workshop series focuses on learning from and improving cyber security experiment results. The workshop explores both positive and negative experimental results, the latter of which are not often published.

LASER strives to provide a highly interactive, collegial environment for discussing and learning from experiment design, issues, and outcomes. Ultimately, the workshop seeks to foster a dramatic change in the paradigm of cyber security research and experimentation, improving the overall quality and reporting of practiced science.

## SPONSORS

The LASER workshop is funded in part by NSF Grant (#1446407) and by the Applied Computer Security Associates (ACSA). LASER is additionally sponsored by SRI International and by USENIX Association.



# SRI International

## 2017 WORKSHOP GOALS AND FOCUS

The LASER Workshop invites papers that seek to improve experimental methods in the field of cybersecurity. The goal of this workshop is to improve the rigor and quality of security experimentation by providing a venue where cybersecurity researchers can discuss experimental methods and present research that exemplifies sound scientific practice.

This year we particularly encourage papers in three areas:

- Well-designed security experiments, with positive or negative results.
- Experimental techniques that help address common sources of error.
- Replications (successful or failed) of previously published experiments.

Well-done security experiments, aside from the immediate value provided by the result of the experiment, can serve as methodological examples for future work. We therefore invite submissions reporting on the results of carefully designed and executed studies. Reviewers will be advised to judge the quality of the design and how well that design was carried out rather than whether the result validates the original hypothesis. In other words, both positive and negative results will be accepted, provided the methodology is sound.

LASER also solicits papers that give new insights into common sources of error in security experiments. Awareness of common pitfalls allows researchers to avoid them, and to notice them in others' work during peer review. In machine learning, for example, it is well known that testing an algorithm on the same data that was used for training will result in overfitting and give an inflated view of the algorithm's performance. What sorts of mistakes in cybersecurity experimentation can lead us astray?

Finally, replications of prior work are an essential part of the scientific process: all experimentation has some natural level of error, and replication helps validate the soundness of existing work and provide a deeper understanding of the conditions under which published results hold. Replications of important security results are therefore a natural fit for LASER. In order to ensure fairness, we ask that submissions that fail to replicate prior work include a discussion of the authors' efforts to contact the authors of the original study and reconcile the differences.

Papers that include an analysis of a data set are encouraged to make said data available, as well as any analysis code. This helps ensure that work presented at LASER will can be meaningfully checked and reproduced by other researchers.

Well-written papers on these topics, as well as any others consistent with the workshop's goals of advancing the state of the art in cybersecurity experimentation, will be presented at the workshop and included in the proceedings.

## PAPER FORMAT AND SUBMISSIONS

Submissions may be 6-10 pages long including tables, figures, and references. Short papers of up 3-6 pages long are also welcome.

Submissions must be in PDF format using USENIX conference paper formatting guidelines. <https://www.usenix.org/conferences/author-resources/paper-templates>

Papers must be submitted via HotCRP: <https://laser2017.hotcrp.com/>

Reviewing will be double-blind, so authors should anonymize their papers and remove obvious self-references.

Authors are encouraged to use the “structured abstract” format. Structured abstracts help make different submissions comparable, and allow readers to quickly understand the overall structure, methods, and conclusions of a study. A structured abstract should contain concise statements, presented in a consistent structure to help quickly facilitate an understanding of the study. Essential elements of structured abstracts are:

**Background.** State the background and context of the work described in the paper.

**Aim.** State the research question, objective, or purpose of the work in the paper.

**Method.** Briefly summarize the method used to conduct the research, including subjects, procedures, data, and analytical methods.

**Results.** State the outcome of the research using measures appropriate for the study conducted.

**Conclusions.** State the surprises, lessons learned as a result of the study, and recommendations for future work.

Additional relevant sections may be included as the author deems relevant to capturing the whole of the paper. See [LASER 2014](#) or [LASER 2013](#) for example structured abstracts. LASER recognizes that some studies may not reasonably fit this format. In such cases, authors should modify the format as needed to capture their own paper contents.

## WORKSHOP FORMAT

Because of the complex and open nature of the experimental methods, LASER is designed to be a workshop in the traditional sense. Presentations are expected to be interactive with the expectation that a substantial amount of this time may be given to questions and audience discussion, rather than pure presentation. Papers and presentations should be conducive to discussion, and the audience is encouraged to participate. To promote a high level of interaction, attendance is limited. First

# LASER 2017

Learning from Authoritative Security Experiment Results

## CALL FOR PAPERS

preference is given to participating authors. Additional seats are available on a first-come first-served basis.

Additionally, a pre-workshop version of the paper will be distributed to attendees. However, authors are encouraged to incorporate comments from the discussions at the workshop into final, camera-ready versions of their paper, to be published publicly by USENIX. Camera-ready paper versions are due November 22, 2017.

### STUDENT SCHOLARSHIPS

LASER seeks to foster learning in experimental methods for the next generation of computer security researchers. As such, LASER offers a limited number of student scholarships for participation.

### PROGRAM COMMITTEE

**Brendan Dolan-Gavitt** (NYU), Chair  
**Christian Collberg** (University of Arizona)  
**Kovila Coopamootoo** (Newcastle Univ.)  
**Eric Eide** (Utah)  
**Lori Flynn** (SEI/CMU)  
**Thomas Gross** (Newcastle University)  
**Bart Knijnenburg** (Clemson)  
**Jelena Mirkovic** (USC Information Sciences Institute (ISI))  
**Pradeep Murukannaiah** (RIT)  
**Daniela Oliveira** (University of Florida)  
**Konrad Rieck** (TU Braunschweig)  
**John Seymour** (UMBC)  
**Xinyu Xing** (Penn State)  
**Michael Zhivich** (MIT LL)

### ORGANIZING COMMITTEE

**Terry Benzel** (USC ISI), General Chair  
**Brendan Dolan-Gavitt** (NYU), Program Chair  
**David Balenson** (SRI), Funding/Local Arrangements/Scholarships  
**Laura S. Tinnel** (SRI), Publicity/Web/IT Services  
**Fanny Lalonde Levesque** (Ecole Polytechnique de Montreal), Publications  
**Carrie Gates** (Consultant), Advisor  
**Greg Shannon** (CMU/CERT), Advisor

### QUESTIONS

Please send questions to [info@laser-workshop.org](mailto:info@laser-workshop.org).