LASER 2012—Learning from Authoritative Security Experiment Results

The goal of this workshop is to provide an outlet for publication of unexpected research results in security—to encourage people to share not only what works, but also what doesn't. This doesn't mean bad research—it means research that had a valid hypothesis and methods, but the result was negative. Given the increased importance of computer security, the security community needs to quickly identify and learn from both success and failure.

`Journal papers and conferences typically contain papers that report successful experiments that extend our knowledge of the science of security, or assess whether an engineering project has performed as anticipated. Some of these results have high impact; others do not. Unfortunately, papers reporting on experiments with unanticipated results that the experimenters cannot explain, or experiments that are not statistically significant, or engineering efforts that fail to produce the expected results, are frequently not considered publishable, because they do not appear to extend our knowledge. Yet, some of these "failures" may actually provide clues to even more significant results than the original experimenter had intended. The research is useful, even though the results are unexpected.

Useful research includes a well-reasoned hypothesis, a well-defined method for testing that hypothesis, and results that either disprove or fail to prove the hypothesis. It also includes a methodology documented sufficiently so that others can follow the same path. When framed in this way, "unsuccessful" research furthers our knowledge of a hypothesis and testing method. Others can reproduce the experiment itself, vary the methods, and change the hypothesis; the original result provides a place to begin.

As an example, consider an experiment assessing a protocol utilizing biometric authentication as part of the process to provide access to a computer system. The null hypothesis might be that the biometric technology does not distinguish between two different people; in other words, that the biometric element of the protocol makes the approach vulnerable to a masquerade attack. Suppose the null hypothesis is not rejected. It would still be worth publishing this result. First, it might prevent others from trying the same biometric method. Second, it might lead them to further develop the technology—to determine whether a different style of biometrics would improve matters, or if the environment in which authentication is being attempted makes a difference. For example, a retinal scan may be a failure in recognizing people in a crowd, but successful where the users present themselves one at a time to an admission device with controlled lighting, or when multiple "tries" are included. Third, it might lead to modifying the encompassing protocol so as to make masquerading more difficult for some other reason.

Equally important is research designed to reproduce the results of earlier work. Reproducibility is key to science, to validate or uncover errors or problems in earlier work. Failure to reproduce the results leads to a deeper understanding of the phenomena that the earlier work uncovers.

The workshop focuses on research that has a valid hypothesis and reproducible experimental methodology, but where the results were unexpected or did not validate the hypotheses, where the methodology addressed difficult and/or unexpected issues, or that identified previously unsuspected confounding issues.

We solicit research and position papers addressing these issues, especially (but not exclusively) on the following topics:

- Unsuccessful research in experimental security
- Methods, statistical analyses, and designs for security experiments
- Experimental confounds, mistakes, mitigations
- Successes and failures in reproducing the experimental techniques and/or results of earlier work

Extended abstracts, full position papers, and research submissions should be 6–10 pages long including tables, figures, and references. Please use the ACM Proceedings Format at http://www.acm.org/sigs/publications/proceedings-templates (Option 1, if using LaTeX).

At least one author from every accepted paper must plan to attend the workshop and present.

	Schedule:	**Location:**
Mar 26	submissions deadline	SRI International
May 7	decisions to authors	1100 Wilson Boulevard, Suite 2800
Jun 15	final papers	Arlington, VA 22209
Jul 18 & 19	workshop	

For further information: http://www.laser-workshop.org

Funded in part by a grant from NSF

Program Committee:
Matt Bishop (UC Davis), PC Co-Chair
Greg Shannon (CMU/CERT), PC Co-Chair
Alessandro Acquisti (CMU)
Ross Anderson (Cambridge)
Terry Benzel (USC/ISI)
George Cybenko (Dartmouth)
Jeremy Epstein (SRI International)
Carrie Gates (CA Labs)
Dan Geer (In-Q-Tel)
Kevin Killourhy (CMU)
John Knight (University of Virginia)
Tom Longstaff (JHU/APL)
Brad Martin (ODNI)
Roy Maxion (CMU)
John McHugh (University of North Carolina)
Vern Paxson (ICSI & UC Berkeley)
Shari Pfleeger (Dartmouth/I3P)
Angela Sasse (University College London)
Christoph Schuba (Oracle)
Gene Spafford (Purdue)
Ed Talbot (Consultant)
Steve Taylor (Dartmouth)
Charles Wright (MIT/LL)

Organizing Committee:
Carrie Gates (CA Labs), General Chair
Matt Bishop (UC Davis), PC Co-Chair
Greg Shannon (CMU/CERT), PC Co-Chair
Jeremy Epstein (SRI International)
Deb Frincke (NSA)
Christoph Schuba (Oracle), Publications Chair
Ed Talbot (Consultant)