Call for Papers (extended due dates): New Security Paradigms Workshop

Schloss Dagstuhl, Germany
September 18-21, 2006
http://www.nspw.org

NSPW is a unique workshop that is devoted to the critical examination of new paradigms in security. Each year, since 1995, we examine proposals for new principles upon which information security can be rebuilt from the ground up. We conduct extensive, highly interactive discussions of these proposals, from which we hope both the audience and the authors emerge with a better understanding of the strengths and weaknesses of what has been discussed.

In his seminal book *The Structure of Scientific Revolutions*, Thomas Kuhn describes the progress of science as “a series of peaceful interludes punctuated by intellectually violent revolutions.”These revolutions, which he called “paradigm shifts”, are periods during which “one conceptual world view is replaced by another.”

A paradigm shift is thus not an incremental contribution to an established branch of science; it is an attempt to replace the fundamental dogma of a branch of science with a different, and completely incompatible, set of core principles.

The New Security Paradigms workshop is dedicated to the proposition that what Kuhn called “anomalies” - signs that the prevailing paradigm can no longer explain phenomena observed in the real world - are already visible in the science of information security, and, indeed, that the anomalies are so obvious and so serious that the prevailing information security paradigm is or soon will be in crisis. NSPW aspires to be the philosophical and intellectual breeding ground from which a revolution in the science of information security will emerge.

We solicit and accept papers on any topic in information security subject to the following caveats:

1. Papers that present a significant shift in thinking about difficult security issues are welcome.

2. Papers that build on a recent shift are also welcome.
3. Contrarian papers that dispute or call into question accepted practice or policy in security are also welcome.
4. We solicit papers that are not technology-centric, including those that deal with public policy issues and those that deal with the psychology and sociology of security theory and practice.
5. We discourage papers that represent established or completed works as well as those that substantially overlap other submitted or published papers.
6. We discourage papers which extend well-established security models with incremental improvements.
7. We encourage a high level of scholarship on the part of contributors. Authors are expected to be aware of related prior work in their topic area, even if it predates Google. In the course of preparing an NSPW paper, it is far better to read an original source than to cite a text book interpretation of it.

Our program committee particularly looks for new paradigms, innovative approaches to older problems, early thinking on new topics, and controversial issues that might not make it into other conferences but deserve to have their try at shaking and breaking the mold.

Participation in the workshop is limited to authors of accepted papers and conference organizers. Each paper is typically the focus of 45 to 60 minutes of presentation and discussion. Prospective authors are encouraged to submit ideas that might be considered risky in some other forum, and all participants are charged with providing feedback in a constructive manner. The resulting intensive brainstorming has proved to be an excellent medium for furthering the development of these ideas. The proceedings, which are published after the workshop, have consistently benefited from the inclusion of workshop feedback.

We welcome three categories of submission:

1. Research papers. These should be of a length commensurate with the novelty of the paradigm and the amount of novel material that the reviewer must assimilate in order to evaluate it.
2. Position papers. These should be 5 - 10 pages in length and should espouse a well reasoned and carefully documented position on a security related topic that merits challenge and / or discussion.
3. Discussion topic proposals. Discussion topic proposals should include an in-depth description of the topic to be discussed, a convincing argument that the

topic will lead to a lively discussion, and supporting materials that can aid in the evaluation of the proposal. The later may include the credentials of the proposed discussants. Discussion topic proposers may want to consider involving conference organizers or previous attendees in their proposals.

Submissions must include the following:

1. The submission in PDF format, viewable by Adobe Acrobat reader.
2. A justification for inclusion in NSPW. Specify the category of your submission and describe, in one page or less, why your submission is appropriate for the New Security Paradigms Workshop. A good justification will describe the new paradigm being proposed, explain how it departs from existing theory or practice, and identify those aspects of the status quo it challenges or rejects. The justification is a major factor in determining acceptance.
3. An Attendance Statement specifying how many authors wish to attend the workshop. Accepted papers require the attendance of at least one author for the entire duration of the workshop. Attendance is limited, and we cannot guarantee space for more than one author.

No submission may have been published elsewhere nor may a similar submission be under consideration for publication or presentation in any other forum during the NSPW review process.

The submission deadline is Thursday, 20 April 2006. Notification of acceptance will be Sunday, 4 June 2006.

Workshop proceedings will be published by the ACM and put in the ACM digital library.

In order to ensure that all papers receive equally strong feedback, all attendees are expected to stay for the entire duration of the workshop.

We expect to offer a limited amount of financial aid to those who require it.

See *http://www.nspw.org* for details of the workshop policies and for submission procedures.