

2008 New Security Paradigms Workshop

Plumpjack Squaw Valley Inn, Olympic Valley, CA, USA — September 22-25, 2008

Call for Papers and Participation

The computers of the world are under siege. Denial of service attacks plague commercial sites, large and small. Major companies are hacked for consumer credit card numbers. Phishing attacks for personal information are commonplace, and million-machine botnets are a reality. Our tools for combating these threats—cryptography, firewalls, access controls, vulnerability scanners, malware and intrusion detectors—are insufficient. We need radical new solutions, but most security researchers propose only incremental improvements. Since 1992, the New Security Paradigm Workshop (NSPW) has been a home for research that addresses the fundamental limitations of current work in information security.

NSPW welcomes unconventional, promising solutions to important problems and critiques of standard security practice. To facilitate research interactions, NSPW features supportive paper presentations, extended discussions, group meals, and shared activities, all in attractive surroundings. By encouraging researchers to think “outside the box” and giving them an opportunity to communicate with open-minded peers, NSPW fosters paradigm shifts in the field of information security.

In 2008, NSPW will be held in Lake Tahoe (Olympic Valley, CA) at the Plumpjack Squaw Valley Inn, from September 22nd to 25th. We will accept about a dozen papers and invite the authors to attend the three-day workshop. One author of each accepted paper must attend NSPW; other authors may attend on a space-available basis. 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 absolutely require it.) Final proceedings are published after the workshop. Authors always revise their papers to include feedback received at NSPW.

Important Dates.

- The submission deadline is *April 11, 2008, 23:59 (GMT -12, or Y time)*.
- Notification of acceptance will be *June 3, 2008*.
- Camera-ready papers for pre-proceedings due *August 28, 2008*.
- Camera-ready papers for proceedings due *November 1, 2008*.

Submissions. NSPW welcomes papers that present a significant shift in thinking about difficult security issues, build on such a recent shift, offer a contrarian view of accepted practice or policy, or address non-technological aspects of security. Our program committee particularly looks for new approaches to information security, early thinking on new topics, innovative solutions to long-time problems, and controversial issues which might not be accepted at other conferences but merit a hearing. We discourage papers that represent completed or established works, or offer incremental improvements to well-established models. NSPW expects a high level of scholarship from contributors, including awareness of prior work produced before the World Wide Web.

We welcome three categories of submission:

1. *Research papers* should be of a length commensurate with the significance of the work and the amount of material that the reviewer must assimilate for evaluation.
2. *Position papers* 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 panel proposals* should include an in-depth description of the topic to be discussed, an argument for why the topic will lead to a lively discussion, and other optional supporting materials such as the credentials of the proposed panelists.

Submissions are accepted at www.nspw.org. Submissions should be accompanied by a justification statement and an attendance statement. A justification statement specifies the category of your submission and describes, in one page or less, why your submission is appropriate for NSPW. A good justification will describe the new approach being proposed, explain how it departs from existing theory or practice, and identify those aspects of the status quo it challenges or rejects. An attendance statement specifies 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. As attendance is limited, we cannot guarantee space for more than one author.

Submissions should be in PDF format, while justifications and attendance statements should be in plain text. All submissions are treated as confidential, both as a matter of policy and in accordance with the U.S. Copyright Act of 1976. Workshop proceedings will be published by the ACM and put in the ACM digital library. As such, prospective authors are encouraged (but not required) to submit their manuscripts in the format of ACM SIG proceedings, preferably using the corresponding template.

Submissions accompanied by nondisclosure agreement forms will not be considered. No submission to NSPW 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. NSPW, like other research and technical conferences and journals, prohibits these practices and may, on the recommendation of a program chair, take action against authors who have committed them. In some cases, program committees may discreetly share information about submitted papers with other conference chairs and journal editors to ensure the integrity of papers under consideration. If a violation of these principles is found, sanctions may include, but are not limited to, barring the authors from submitting to or participating in future NSPW meetings for a set period, contacting the authors' institutions, and publicizing the details of the case. Authors uncertain whether their submission meets the NSPW guidelines should contact the program chairs.

NSPW 2008 Organizers:

General Chair: **Matt Bishop** (bishop@cs.ucdavis.edu), *Univ. of California, Davis, USA*

Program Committee Co-Chairs: **Angelos Keromytis** (angelos@cs.columbia.edu), *Columbia Univ., USA*
Anil Somayaji (soma@scs.carleton.ca), *Carleton Univ., Canada*

Program Committee:

Matt Beaumont-Gay, *Univ. of Calif., Los Angeles, USA*

Kosta Beznosov, *Univ. of British Columbia, Canada*

Matt Bishop, *Univ. of California, Davis, USA*

Steve Borbash, *US Department of Defense*

Stanley Chow, *Alcatel-Lucent Bell Labs, Canada*

Keith Edwards, *Georgia Institute of Tech., USA*

Jan Feyereisl, *Univ. of Nottingham, UK*

Stephanie Forrest, *Univ. of New Mexico, USA*

Carrie Gates, *CA Labs, USA*

Steven J. Greenwald, *Independent Consultant, USA*

Jeffrey Hunker, *Carnegie Mellon Univ., USA*

Klaus Kursawe, *Philips Research, Netherlands*

Michael Locasto, *Columbia Univ., USA*

Carla Marceau, *Architecture Technology Corp., USA*

Christian Probst, *Technical Univ. of Denmark*

Vidyaraman Sankaranarayanan, *Univ. at Buffalo, USA*

M. Angela Sasse, *Univ. College London, UK*

Jon Solworth, *Univ. of Illinois at Chicago, USA*

Brian Snow, *Independent Security Advisor, USA*

Carol Taylor, *Eastern Washington Univ., USA*

Paul Van Oorschot, *Carleton Univ., Canada*