2009 New Security Paradigms Workshop

The Queen's College, University of Oxford, UK — September 8–11, 2009

Call for Papers and Participation

The New Security Paradigms Workshop (NSPW) is seeking papers that address the current limitations of information security. Today's security risks are diverse and plentiful—botnets, database breaches, phishing attacks, distributed denial-of-service attacks—and yet present tools for combatting them are insufficient. To address these limitations, NSPW welcomes unconventional, promising approaches to important security problems and innovative critiques of current security practice.

We are particularly interested in perspectives from outside computer security, both from other areas of computer science (such as operating systems, human-computer interaction, databases, programming languages, algorithms) and other sciences that study adversarial relationships such as biology and economics. We discourage papers that offer incremental improvements to security and mature work that is appropriate for standard information security venues.

To facilitate research interactions, NSPW features informal paper presentations, extended discussions in small and large groups, shared activities, and group meals, all in attractive surroundings. By encouraging researchers to think "outside the box" and giving them an opportunity to communicate with open-minded peers, NSPW seeks to foster paradigm shifts in the field of information security.

Submission deadline	*April 17, 2009, 23:59 (UTC -12, or Y time)* Please submit at **www.nspw.org** in PDF (ACM SIG formatting preferred).
Notification of acceptance	*May 29, 2009*
Camera-ready papers for pre-proceedings	*August 14, 2009*
Workshop	*September 8–11, 2009* in Oxford, UK (September 8th is the day after Labor Day.)
Camera-ready papers for proceedings	*October 24, 2009*

NSPW 2009 Organizers:

General Chair: **Christian Probst** (probst@imm.dtu.dk), *Technical University of Denmark*
Vice Chair: **Angelos Keromytis** (angelos@cs.columbia.edu), *Columbia University*

Program Committee Co-Chairs: **Anil Somayaji** (soma@scs.carleton.ca), *Carleton University*
Richard Ford (rford@se.fit.edu), *Florida Institute of Technology*

Program Committee:
Matt Bishop, *University of California, Davis*
Mark Burgess, *Oslo University College*
Rachna Dhamija, *Usable Security Systems*
Michael Franz, *University of California, Irvine*
Deborah Frincke, *Pacific Northwest National Laboratory*
Carrie Gates, *CA Labs*
Steven J. Greenwald, *Independent Consultant*
Markus Jakobsson, *PARC*
Christopher Kruegel, *University of California, Santa Barbara*
Ben Laurie, *Google*
Michael Locasto, *George Mason University*
Brian Snow, *Indepent Security Advisor*
Matt Williamson, *Sana Security*

NSPW welcomes three categories of submissions:

- research papers,
- position papers (10 pages maximum), and
- discussion panel proposals.

Submissions should include a cover page with justification and attendance statements. A justification statement specifies the category of your submission and briefly describes why your submission is appropriate for NSPW. An attendance statement specifies which of the authors wish to attend the workshop. Note that all accepted papers are shepherded to help authors incorporate the feedback provided throughout the process.

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 by the ACM after the workshop. All submissions are treated as confidential, both as a matter of policy and in accordance with the U.S. Copyright Act of 1976. 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.