NSPW 2021: Call for Papers

New Hampshire, USA
October, 2021
www.nspw.org

Submission deadline:	**May 21, 2021 23:59 (UTC -11)**
Format:	PDF file (ACM SIG formatting) via Easychair
Notification of acceptance:	July 9, 2021
Pre-proceedings deadline:	September 8, 2021
Invitations sent:	Depends on state of the pandemic
Workshop:	October 25 - 28, 2021
Final version:	November 24, 2021

The New Security Paradigms Workshop (NSPW) seeks embryonic, disruptive, and unconventional ideas on information and cyber security that benefit from early, in-depth, and constructive feedback. Submissions typically address current limitations of information security, directly challenge long-held beliefs or the very foundations of security, or discuss problems from an entirely novel angle, leading to new solutions. We welcome papers both from computer science and other disciplines that study adversarial relationships and other aspects of security, as well as from practice. The workshop is invitation-only; all accepted papers receive a 1 hour plenary time slot for presentation and discussion. In order to maximize diversity of perspectives, we particularly encourage submissions from new NSPW authors, from Ph.D. students, and from non-obvious disciplines and institutions.

The theme for NSPW 2021 is interdisciplinarity and translation zones in the context of emerging technologies. We welcome intersectional papers that bring information security into contact with multiple disciplines. Papers should offer new frameworks for bringing information security into contact, but also challenge principles of information security by way of the intersection. Emergent technologies and emergent uses of existing technologies challenge traditional positions in information security by calling into question what we need to secure and how we need to secure it. Working with different disciplines both enhances analysis and challenges traditional technological security responses. Theme papers should therefore also include some reflection on the type of interdisciplinary working that has been carried out to produce the paper and how interdisciplinarity was put into practice.

The following are provocations that require interdisciplinary responses. When developing ideas for Theme submissions, authors might consider such types of provocation in the context of security and emerging technologies:

- Technological accessibility is an extension of usable security and central to the principle of availability.
- Protection of data and technology must always be a public good.

- Informed consent is no longer possible in societies dependent on ubiquitous digital technologies.
- The security of an emerging technology is dependent on a common understanding of the benefits of that technology.
- Security for one party always results in insecurity for another party—whether at the policy, technology or societal level.

NSPW 2021 is scheduled to be held at the White Mountain Hotel and Resort in North Conway, NH USA. As in the past, this choice of venue is designed to facilitate interactions between the invited attendees throughout the workshop.

Submission Instructions

Submit through EasyChair: https://easychair.org/conferences/?conf=nspw2021
NSPW accepts three categories of submissions:

- **Regular Submissions** present a new approach (paradigm) to a security problem or critique existing approaches. While regular submissions may present research results (mathematical or experimental), unlike papers submitted to most computer security venues, these results should not be the focus of the submission; instead, the change in approach should be the focus.
- **Theme Submissions** are focused on "Interdisciplinarity and translation zones in the context of emerging technologies", and should explain the connection with the theme in the justification statement (see below). They follow the format of a regular submission.
- **Panel Proposals** describe a debatable topic of interest to the security community that merits significant discussion. Proposals should describe the major perspectives on the chosen topic. They should also present the background of the panelists, explaining how they are the right people to discuss the chosen topic at NSPW.

Submissions must be made in PDF format, 6-15 pages, ACM "sigconf" formatting, through EasyChair. Submissions should blind author identity where possible. The LaTeX document option `anonymous=true` provides a minimum level of protection; however, authors should also avoid referencing their own work in the first person or other obvious de-anonymization in the submission.

Submissions must include a cover page with authors' names, affiliation, and participation statement. To support double-blind reviewing, this cover page should not be part of the PDF submission, but will be submitted separately. Before or after the abstract, a submission must include a **justification statement** (which will not appear in the final publication). Papers not including both statements risk rejection without review. The justification statement briefly explains why the submission is appropriate for NSPW and the chosen submission category. The participation statement must specify which author(s) will attend upon acceptance/invitation, that all authors will engage in good faith with the feedback given in the review and revision periods, and that all authors will abide by the NSPW code of conduct. Organizers and PC members are allowed to submit, but will not be involved in the evaluation of their own papers. All submissions are treated as confidential as a matter of policy. NSPW does not accept previously published or concurrently submitted papers.

Acceptance to the workshop is conditional; all accepted papers are shepherded, with final proceedings published after the workshop.

The submission, review, and workshop phases of NSPW are all governed by the NSPW code of conduct, https://www.nspw.org/conduct.

Attendance

The workshop itself is invitation-only, with typically 30-35 participants consisting of authors of about 10-12 accepted papers, panelists, program committee members, and organizers. One author of each accepted paper must attend; additional authors may be invited if space permits. All participants must commit to a “social contract”: no one arrives late, no one leaves early, no electronic distractions (including laptops, tablets, and mobile devices), attend all sessions of the 2.5 day program, sharing meals in a group setting, and complying with the code of conduct. The workshop is preceded by an evening reception allowing attendees to meet each other beforehand.

COVID-19

The NSPW organizers are committed to holding a productive workshop in some form at the dates listed. Although worldwide conditions related to COVID-19 may force some changes, we will update the NSPW website with meeting and planning information as the situation continues to evolve. We had a successful virtual NSPW in 2020. Although we hope to have a successful in-person NSPW 2021, we may decide that a virtual event is in the best interests of authors and attendees. We expect to finalize this decision sometime in August.

Program Committee Co-chairs:

Jonathan Spring, *CERT/CC, SEI, Carnegie Mellon University*, jspring@sei.cmu.edu
Lizzie Coles-Kemp, Royal Holloway, Lizzie.Coles-Kemp@rhul.ac.uk

Program Committee:

Carrie Gates, Bank of America
Ceri Jones, Natwest Group
Christian Probst, Unitec Institute of Technology
Cormac Herley, Microsoft
Debi Ashenden, University of Portsmouth
Eirann Levrett, Concinnity Risks
Elizabeth Stobert, Carleton University
Jassim Happa, Royal Holloway University of London
Karen Renaud, University of Strathclyde
Laura Koksch, Ruhr University Bochum

Leonie Tanzcer, University College London
Lori Flynn, CERT
Matilda Rhode, Airbus
Matt Bishop, University of California, Davis
Reem Talhouk, Northumbria University
Richard Ford, Cyren LLC
Rikke Bjerg Jensen, Royal Holloway University of London
Shamal Faily, Bournemouth University
Simon Parkin, TU Delft
Tom Millar, CISA
Volker Roth, Freie Universitaet Berlin