NSPW 2020: Call for Papers

New Hampshire, USA
October 26-29, 2020
www.nspw.org

Submission deadline:	**May 22, 2020 23:59 (UTC -11)**
Format:	PDF file (ACM SIG formatting) via Easychair
Notification of acceptance:	July 10, 2020
Pre-proceedings deadline:	August 7, 2020
Invitations sent:	July 20, 2019
Workshop:	October 26 - 29, 2020
Final version:	December 5, 2020

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, 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.

In 2020, NSPW invites theme submissions relating to “Automated Reasoning for Security” in addition to regular submissions. Computers are making ever more decisions on behalf of humans. This recent growth in deployment of automated reasoning has also led to the development and application of technologies for automated reasoning in security. At NSPW 2020, we invite authors to consider how the cybersecurity community should deal with the rise of automation: how do we secure automated reasoning, and how should it be used for security of other systems?

NSPW is interested in methods of securing automated reasoning; applications of technology for automated reasoning (e.g., machine learning (ML)) to security; the implications of such applications; and how it might create or affect new security paradigms, including how we understand human reasoning before automating it. Any attack papers should follow guidelines for writing up case studies, and should clearly explain why understanding of this particular attack is transferable, trustworthy, and contributes to more general understanding of automated reasoning and security.

Possible topics include, but are not limited to:

- prevention (e.g., program verification to provide improved security)
- protection (e.g., anti-virus or intrusion detection systems containing ML)
- attacker use of automation
- adversarial ML (all the different ways that machine learning can be attacked and protected)
- the vulnerabilities in ML or automated reasoning systems, and how they are coordinated, disclosed, and remediated?
- understanding human reasoning

NSPW 2020 will 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

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 “Automated reasoning for Security”, 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 SIG formatting, through EasyChair. **Submissions must include a cover page with authors' names, affiliation, justification statement and participation statement.** Papers not including these 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. Submissions *should not* be blinded. 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.

Attendance

The workshop itself is invitation-only, with typically 30-35 participants consisting of authors of about 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), and all 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 on the website. Although worldwide conditions related to COVID-19 may force some changes, we will update the NSPW website with meeting and planning information over the next few months.

To demonstrate what a NSPW presentation and discussion is like, we conducted a virtual session. For those who have never attended NSPW, the video gives you a sense of how valuable NSPW can be for authors, and for those who have attended, the video is some evidence that, even virtually, we can keep up the high level of interactivity that defines NSPW. Watch the video here: https://youtu.be/wUOS8d3QSiw

Program Committee Co-chairs:

Elizabeth Stobert, *Carleton University*, elizabeth.stobert@carleton.ca
Jonathan Spring, *CERT/CC, SEI, Carnegie Mellon University*, jspring@sei.cmu.edu

Program Committee:

Alisa Frik, *ICSI UC Berkeley*
Anil Somayaji, *Carleton University*
Brian Lindauer, *Duo Security*
Carrie Gates, *Bank of America*
Hadi Asghari, *TU Delft*
Heather Crawford, *Florida Institute of Technology*
Joel Wilbanks, *McAfee*
John Bambenek, *University of Illinois at Urbana-Champaign*
Julie Thorpe, *Ontario Tech University*
Laura Kocksch, *Ruhr-University Bochum*
Lori Flynn, CERT/CC, SEI, *Carnegie Mellon University*
Mansoor Ahmed-Rengers, *University of Cambridge*
Mary Ellen Zurko, *MIT Lincoln Laboratory*

Olgierd Pieczul, *Oracle*
Simon Parkin, *University College London*
Trent Jaeger, *Pennsylvania State University*
Vera Rimmer, *KU Leuven*
Wolter Pieters, *TU Delft*