Call for Papers

8th Annual **HOT TOPICS** *in the* **SCIENCE OF SECURITY *(HoTSoS)***

APRIL 13-15, 2021 | *virtually hosted by* THE NATIONAL SECURITY AGENCY

https://hotsos.org

HOTSOS 2021

Overview

Submissions are solicited for the 8th Annual Hot Topics in the Science of Security (HoTSoS) Symposium, which will be virtually held April 13-15, 2021. The 8th Symposium continues the series' emphasis on cyber-security with a strong methodology and scientific rigor. This symposium solicits presentations of already published work in security and privacy, particularly that which examines the scientific foundations of trustworthy systems. In addition to these presentations, the symposium solicits work in progress papers for discussion, presentations of student research projects, and research posters. The program will also include invited talks and panels.

Authors may submit to one of four categories:

Already Published Research Presentation: Papers in this category will be reviewed by a selection of members of the Program Committee. These presentations will be based on already published work with a goal of presenting to HotSoS's unique attendees for awareness and collaboration.

Works in Progress (WiP): Papers in this category will receive feedback on a research direction, technology, or idea before it has been fully evaluated, or to discuss systems in an early, pre-prototyping phase. Accepted manuscripts will not be published at the symposium. Additional information on this special working session is below.

Student Research Project Presentations: Abstracts of student research projects can be submitted for consideration. Authors of accepted abstracts will be invited to present at the symposium. Appropriate research in this category would consist of capstone projects, master thesis research, REU work, and other similar types of research from students. The objective is to provide students with feedback on their work and provide an opportunity to gain experience presenting at conferences.

Posters: We invite submissions of poster abstracts for inclusion and presentation at HoTSoS. The poster session will be highlighted by a poster competition.

Vision & Scope

HoTSoS brings together researchers, practitioners, and thought leaders from government, industry, and academia. The National Security Agency (NSA) sponsorship of HoTSoS provides for a collaborative relationship with NSA researchers, practitioners and leaders and results in a unique attendee audience. The symposium is a forum for technical dialogue and exchange of experiences about the development and advancement of scientific foundations in cyber security and privacy. The technical emphasis of HoTSoS is on scientific methods, data gathering and analysis, development and evaluation of metrics and measurements, experimental approaches, mathematical models, and the interactions among those various techniques to build a foundational science of security. The HoTSoS vision is to engage and grow a community that includes researchers and skilled practitioners from diverse disciplines focused on the advancement of scientific methods. We invite submissions on any topic that aligns with the symposium scope and vision.

Themes

The symposium invites submissions on any topic related to the science of security as described above. The 2021 HoTSoS will highlight the following themes:

- Methodologies for analyzing and designing resilient system architectures
- Construction of scalable, composable, provably secure systems
- Designing, modeling, and analyzing systems with specified security properties by taking into account human behavior, including operators, users, and adversaries
- Security-Metrics-Driven Development and Evaluation for guiding choice-making assuring or predicting the security properties of cyber systems, Policy-based tools for secure, private collaboration across different domains of authority
- Policy enforcement that enables the collection, storage, and sharing of data in accordance with privacy requirements
- Trustworthy AI topics to include understanding theoretical limitations, explainability, design principles, verification and validation metrics.

These research themes can be applied to System Security, Cyber-Physical Systems Security including related to the Internet of Things, and in the application of privacy.

Important Dates

Already Published Research Presentations:	February 7, 2021
Works in Progress Manuscripts:	February 7, 2021
Student Presentations:	February 7, 2021
Poster Submissions:	February 7, 2021
Acceptance Decisions:	February 28, 2021
Videos of Presentations:	March 31, 2021
Symposium:	April 13-15, 2021

Please send any questions about topics or submission requirements to hotsos2021@cps-vo.org

NATIONAL SECURITY AGENCY ★ UNITED STATES OF AMERICA ★

Works in Progress (WiP) Session

In keeping with the goal of collaborative community engagement, this year's Symposium will again feature special working sessions for works in progress (WiP). WiP papers offer an opportunity for authors to get early feedback on a research direction, technology, or idea before it has been fully evaluated, or to discuss systems in an early, pre-prototyping phase. Authors who have a WiP paper accepted will attend a special session in which they appear on stage with a discussant for up to one hour of in-depth discussion of their submission. A session will include a 10min introduction of the research by the author. Authors are expected to incorporate session feedback into revisions of their manuscript prior to their next submission for publication. Attendees are expected to read the manuscript in advance and be prepared for discussing the topic. Manuscripts accepted for discussion will not be published at the symposium, and access to the submissions will remain confidential and be restricted to session attendees who have agreed to keep the material confidential. The authors and general description of accepted WiP papers will appear on the symposium website. After the manuscript is published, its inclusion as a WiP paper will be documented on the symposium website.

Submission & Eligibility

Submissions of WiP papers must be made by the deadline of February 7, 2021 AoE (Anywhere on Earth) through https://cps-vo.org/group/hotsos/submit and specifying the submission category to be as "WiP paper". Submissions may use the double-column ACM conference proceedings "Master" Template format provided at https://www.overleaf.com/latex/templates/acm-conference-proceedings-master-template/pnrfvrrdbfwt.

WiP papers should be at most 10 pages in the double-column ACM format including the bibliography or, alternatively, 9 pages not including the bibliography. Note that WiP papers are encouraged even if they are substantially shorter than the page limit. The paper may have optional appendices, but reviewers are not required to read them. Submissions must be in PDF format and the title should begin with "WiP: ".

Each author must assert that the manuscript is unpublished and revisions can be incorporated into the manuscript prior to their next submission for publication. Prior publication includes the appearance in a proceeding, online or in print, of any version of the work that received peer review, including short papers. Posters and online, pre-submission non-archival versions of non-peer reviewed papers will not be considered prior publication. Pre-submission non-archives include arXive.org and CiteSeerX. A short paper version of a submission may not immediately disqualify the submission, however, and the committee will consider the differences in the versions prior to making final decisions. Thus, authors are encouraged to briefly disclose in a cover page to their submission any prior submissions and/or publications related to the submission.

Selection Process

Shortly after the submission deadline, a small program committee will review WiP manuscripts for acceptance. Acceptance is determined by the following criteria: (1) is the manuscript topic appropriate for the Science of Security; (2) is the manuscript sufficiently clear about the problem, approach, evaluation and results to engage an audience in productive discussions; (3) has the manuscript been previously published in any format; and (4) does the manuscript complement the overall program. Manuscripts that are not accepted may be invited as posters for presentation in a separate poster session.

WiP Workshop Format

One month prior to the workshop session and symposium, registered attendees will be provided confidential access to accepted manuscripts. Because the manuscripts are unpublished, all attendees are instructed to keep the research results and discussions confidential. Registered attendees to the special session are expected to read the manuscripts prior to attendance and they are encouraged to participate in discussions. There are no formal presentations of the work.

Each manuscript will be assigned up to a one-hour, in which an author will present the manuscript for up to 10 minutes. The discussant will then identify the strengths and weaknesses along multiple dimensions:

- Is the problem framing clear, is this the right problem given the approach? Is the threat model described, the right model?
- Is the chosen analysis appropriate for the claims being made?
- Is there an alternative analysis better suited to the research questions or hypotheses? Do threats to internal validity exist, if so, how can those be appropriately acknowledged and/or mitigated?
- Are the results being presented clearly, what alternative presentations exist?
- Is the scope of impact consistent with the results, are connections to a broader impact missing or available for further research?

Following the discussant questions and author reactions, the remaining minutes will be used by the audience to raise their own questions and to engage in audience discussion. It is expected that audience members will prepare their own questions in advance, when reading the manuscript prior to attending the workshop. The discussant and author can moderate the discussion by choosing audience members to speak and by asking audience members follow-up questions. The ultimate goal for each session is to provide authors with detailed actionable feedback, which they will then use to improve their manuscripts prior to submission for publication at a different venue.

Already Published Research Papers

Submissions of research papers must be made by the deadline of February 7, 2021 AoE through https://cps-vo.org/group/hotsos/submit and specifying the submission category to be as "research paper". Submissions may use the format of the published venue.

Submissions must be in PDF format.

Student Research Presentations

Please upload a PDF submission of your abstract of your student research presentation by the deadline of February 7, 2021 AoE through https://cps-vo.org/group/hotsos/submit. Authors of accepted abstracts will be invited to present at the symposium. When preparing the abstract, please use the ACM template provided below. Your abstract submission should include the following information:

1 Title
2 Author names and their affiliations
3 Abstract no longer than 250 words.
4 Keywords
5 Citations and references (if needed)

Poster Submissions

Please upload a submission of your poster abstract by the deadline of February 7, 2021 AoE through https://cps-vo.org/hotsos21/poster-cfp. Accepted posters will be displayed on the symposium website. Each extended abstract should be at most 2 pages, including citations and references.

Nominations or proposals for government or industry talks can be sent directly to the program chairs via email at hotsos2021@cps-vo.org.

ACM Template: https://www.overleaf.com/gallery/tagged/acm-official#.WlayAktG3v0

General Chair

ADAM TAGERT is the technical director the National Security Agency Science of Security Initiative.

He sets the technical direction for research projects at 18 Science of Security (SoS) funded universities, leads the NSA Best Cybersecurity Paper Competition, guides the SoS awards at the International Science and Engineering Fair, and builds community with the SoS Virtual Organization. He received his Ph.D. from Carnegie Mellon University in Engineering and Public Policy where he researched national cybersecurity strategies of small developing nations, particularly Rwanda. He obtained a Computer Science degree from Princeton University

Program Co-Chairs

ÖZGÜR KAFALI is a Lecturer (Assistant Professor) and the Ethics Officer at the School of Computing at the University of Kent, UK. His research interests lie within the intersection of cybersecurity, multiagent systems, and requirements engineering. Kafali received a PhD in Computer Engineering from Bogazici University, Turkey. Previously he was a Postdoctoral researcher at the Department of Computer Science at North Carolina State University, working on the Science of Security Lablet project with Dr. Munindar Singh and Dr. Laurie Williams.

AHMAD RIDLEY is a Senior Researcher at the NSA in the Laboratory for Advanced Cybersecurity Research. He received a Ph. D in applied mathematics from the University of Maryland-College Park, with a concentration on stochastic optimization of queuing systems. At NSA, Dr. Ridley has focused his research interests on the application of machine learning methods to improve the human analysts' ability to defend networks from cyber-attacks while enhancing the cyber-resilience of services dependent on those networks. Currently, he is researching the use of reinforcement learning in developing autonomous cyber defenses to automate and adapt cyber responses at high-speeds and large-scales.