Hot Topics in the Science of Security (HotSoS) brings together researchers and practitioners from academia, industry, and government to advance the scientific foundations of Cybersecurity, Security of Superintelligence, and SI for Cybersecurity. Sponsored by the National Security Agency (NSA), HotSoS provides a unique forum for emerging research, cross-disciplinary discussion, mentorship, and collaboration.

HotSoS '27 will be held virtually in April 2027 and will feature research presentations, invited talks, panels, and posters.

We Invite Submissions in Two Categories

Workshop Papers

Short papers (up to 4 pages) presenting emerging or ongoing research, new ideas, implementations, theoretical results, follow-up studies, negative results, systematization of knowledge (SoK), or fresh perspectives on existing work.

Invited Talk Nominations

Nominations for talks addressing timely topics aligned with the HotSoS mission and research themes.

Topics of Interest

HotSoS seeks high-quality work advancing the science of cybersecurity, with particular interest in the following areas:

Security of Superintelligence

Evaluation and benchmarking of LLM and SI-agent safety and security

Attack mechanisms (e.g., prompt injection, jailbreaks, and tool misuse)

Defense mechanisms (e.g., guardrails, judge models, and alignment)

Control, oversight, and monitoring of SI and agentic systems

Security of agent memory, and persistent state
(e.g., poisoning and context manipulation)

Security of multimodal and multi-agent systems
(e.g., adversarial observations, compromised agents, and cascading failures)

Secure agent architectures
(e.g., isolation, sandboxing, least privilege, and secure tool interfaces)

Superintelligence for Cybersecurity

SI/ML and SI agents for cyber threat detection and response

Agentic software analysis, vulnerability discovery, and reverse engineering

Novel SI architectures and reasoning for cybersecurity

Defenses against SI-enabled adversaries and security-focused evaluation

Cybersecurity & Resilient Systems

Scientific methods in vulnerability discovery and reverse engineering
(human studies, analyses, and evaluation)

Securing software, cyber-physical, and embedded systems

Provably secure systems, composable security frameworks, and secure-by-design approaches

Secure operation in degraded, contested, or compromised environments

Scalable security architectures, continuous monitoring, and continuous authorization

Submission Requirements

All submissions should be made through **OpenReview**.
https://openreview.net/group?id=HotSoS.org/2027/Symposium#tab-your-consoles

All **invited talk nominations** should be submitted via the HotSoS website:
https://sos-vo.org/group/hotsos/invited-talks

A link to the Overleaf Submission Requirements for HoTSoS 2027 can be found as a downloadable zip file linked from the OpenReview website, and on the HotSoS 2027 Call for Papers page on the conference website.

Additional submission instructions and deadlines will be provided on the HotSoS 2027 website.

Workshop Papers

We invite **short papers of up to 4 pages,** excluding references and supplementary materials. Submissions may present ongoing or unpublished work, implementations of new ideas, modest theoretical results, follow-up experiments, negative results, systematization of knowledge (SoK), or fresh perspectives on existing work.

All accepted workshop papers will have the opportunity to be presented as posters. Outstanding workshop papers will also be selected for oral presentations with deep dive discussions.

Dual-Submission Policy

HotSoS 2027 will follow a non-archival policy. We welcome ongoing and unpublished work, as well as work that is under review or recently accepted at another venue, provided the submission does not violate the dual-submission, prior-publication, or anonymity policies of that venue.

We discourage submissions that substantially duplicate work already published at major conferences or journals.

Double-Blind Review

Workshop paper submissions must be **fully anonymized** for double-blind review. This requirement applies to the paper and any supplementary or linked materials, including code repositories. Submissions that reveal author identities may be desk-rejected.

Visibility

Accepted workshop papers will be made publicly available.
Rejected submissions and their reviews will remain private.

Best Paper Award

The workshop will recognize exceptional contributions with two awards, the Best Paper Award and the Best Paper Runner-Up Award.

Invited Talk Nominations

Nominations for invited talks are welcome on topics aligned with the scope and scientific mission of HotSoS. Submission instructions for nominations will be provided on the HotSoS website.

Important Dates

Submission Deadline: Jan 17, 2027
Notification to Authors: Feb 26, 2027
Virtual Symposium: April 13 - 15, 2027

Organization

General Chair
Adam Tagert (National Security Agency)

Program Co-Chairs
Benjamin Erichson (ICSI Berkeley)
Zion Basque (University of Georgia)

Please send any questions about topics or submission requirements to hotsos2027@sos-vo.org