September 17, 2026

Submission Deadline: 19th June, 2026 — 42 days remaining

CONFERENCE WEBSITE: https://hs3-workshop.github.io/2026.html

About the Conference

****

Call for Papers

HS3 2026: 2nd Workshop on Hardware-Supported Software Security
Monday, September 17 (To Be Confirmed) 2026, Rome (Italy)
https://hs3-workshop.github.io/2026.html

Co-located with ESORICS 2026: https://sites.google.com/di.uniroma1.it/esorics2026/

****

The HS3 workshop seeks to share experience, tools and methodology on hardware-assisted software security. We are looking forward to submissions that propose new architectures offering better resilience against software attacks. These architectures should rely on hardware-based security mechanisms to protect the software stack. One of

Important Dates

JUN 19 — PAPER SUBMISSION: **19th June, 2026** • 42 days left

JUL 20 — NOTIFICATION: **20th July, 2026**

AUG 28 — FINAL VERSION DUE: **28th August, 2026**

SEP 17 — CONFERENCE DATE: **September 17, 2026**

the challenges is to
formally specify and verify the security guarantees offered by such
architectures and to better assess the security guarantees provided by
existing hardware architectures against software attacks, especially
attacks against micro-architecture. This can be achieved by identifying new
vulnerabilities using reverse engineering, fuzzing or other attack
approaches. The goal of the HS3 workshop is to provide a forum for
researchers and practitioners from academia, industry and government that
work on hardware-assisted software security.

Special Theme: Hardware-Supported Software Security for AI Systems

As Artificial Intelligence (AI) systems become more deeply integrated
into critical sectors, including healthcare, education, manufacturing,
and mobility, these systems become high-value targets for cyber attacks.
At the same time, hardware vendors rise to the challenge and provide,
e.g., Trusted Execution and and Confidential Computing infrastructure on
GPUs or other AI-targeting hardware. For this year’s edition of the HS3
workshop, we want to encourage submissions that investigate questions
regarding hardware-supported security

approaches for AI systems and
low-level attacks against, and attack mitigations
for AI systems,
specifically if these involve (micro-)architectural
aspects of the
execution environment. HS3 will not accept
general papers on AI security
and we suggest that authors working on these
topics submit their work to
the RAISE or SecAI workshops instead.

==== Topics of interest include, but are not
limited to the following

* Hardware-based security mechanisms
* Hardware-assisted and secure system monitoring
* Hardware-assisted intrusion detection and
reaction
* Hardware-assisted privacy and anonymity
* Hardware enclaves and Trusted Execution
Environments
* Security co-processors
* Leveraging hardware features at the software
level (e.g. compiler, OS)
for security
* Hardware/software contracts for security
* Formal methods applied to the hardware-assisted
security
* Hardware trace mechanisms for security
* OS and VM introspection
* Secure Monitoring, Intrusion Detection, and
Incident Response
* Software side-channel attacks
* Software attacks against micro-architecture
* Software-activated fault attacks

==== Important Dates

* Submission: June 19, 2026 -- 11:59pm AoE
* Author Notification: July 20, 2026
* Camera Ready Version: August 28, 2026
* Workshop: September 17, 2026 (To be Confirmed)

==== Submission and Publication

There are two categories of submissions:

1. Regular papers describing fully developed work and complete results (20 pages, references included, LNCS format)
2. Short papers, position papers, industry experience reports, work-in-progress submissions and ideas (10 pages, references included, LNCS format; work-in-progress and idea submissions should clearly outline the research hypothesis, evaluation strategy and potential impact)

All papers must be written in English and describe original work that has not been published or submitted elsewhere. The submission category (regular paper, short paper) should be clearly indicated. Members of the Program Committee will fully review all submissions. Papers will be published by Springer in the Lecture Notes in Computer Science (LNCS) series as workshop post-proceedings of ESORICS 2026. Contact the Program Chairs if you *do not

want your short paper* to appear in the proceedings.

Papers must be typeset in LaTeX using the LNCS template:
https://www.springer.com/gp/computer-science/lncs/conference-proceedings-guidelines
Failure to adhere to the page limit and formatting requirements can be
grounds for rejection. Well-marked appendices do not count into the page
limit; PC members are also not required to consider material presented in
appendices when reviewing submissions. We will clarify the constraints for
including appendices in camera-ready papers closer to the camera-ready
deadline and after discussion with the workshop chairs and the publisher.
We follow the ESORICS Call for Papers regarding anonymity of submissions
and do not require papers to be anonymised. Anonymised submissions are,
however, welcome at HS3.

Papers must be submitted through the ESORICS EasyChair website; select the
"HS3" track to indicate that you are submitting to this workshop:
https://easychair.org/conferences/?conf=esorics2026

For accepted papers, authors must agree with Springer LNCS copyright and at
least one author must attend the workshop.

==== Program Chairs

- Yuko Hara, CNRS, Laboratoire Hubert Curien, Saint-Etienne, France.
- Jan Tobias Muehlberg, ULB/KU Leuven, Belgium.
- Thomas Rokicki, IRISA, CentraleSupelec/Inria, France.

* Iness Ben Guirat, Universite Libre de Bruxelles
* Pascal Cotret, ENSTA Bretagne
* Kevin Cheang, University of California, Berkeley
* Chris Dalton, HP Labs
* Lesly-Ann Daniel, KU Leuven
* Merve Gülmez, Ericsson Research/KU Leuven
* Karine Heydemann, Thales
* Guillaume Hiet, IRISA, CentraleSupelec/Inria, France
* Vianney Lapôtre, Univ. South Brittany
* Clémentine Maurice, CNRS
* Maria Méndez Real, Université Bretagne Sud
* Cristofaro Mune, Raelize B.V.
* Antonio Muñoz, University of Málaga
* Kaveh Razavi, ETH Zurich
* Simon Rokicki, ENS Rennes
* Volker Stolz, HVL
* Marcus Voelp, Uni Luxembourg
* Pierre Wilke, CentraleSupélec/Inria

* Contact email: hs3-workshop@inria.fr

TOPICS OF INTEREST 3 topics

Research papers are invited in, but not limited to, the following areas:

- cybersecurity
- security
- hardware security

Venue Information

Rome (Italy)

Special conference rates often available near the venue.