callforpaper.org

Italy June 30, 2025

CONFERENCE WEBSITE: https://acsw.unimore.it/

About the Conference

Dear Colleagues,

We would like to invite you to contribute a paper to the 2025 Automotive
Cyber Security Workshop (ACSW'25) co-located with the 10th IEEE European
Symposium on Security and Privacy (Venice, Italy, June 30, 2025).

Conference website https://acsw.unimore.it/
Submission link https://easychair.org/conferences/?conf=acsw25
Submission deadline February 3rd, 2025
Author Notification March 24th, 2025

The workshop will take place on June 30, 2025 (pre-conference workshop)
in Venice, Italy.

Call for Papers
The fourth edition of the Automotive Cyber Security Workshop aims to
bring together researchers and practitioners, interested in all aspects
of automotive systems security, to contribute with

Important Dates

JUN 30

CONFERENCE DATE
June 30, 2025

and discuss new
advances in the field of automotive cybersecurity.
The Automotive Cyber
Security Workshop aims to present recent
advances in the
state-of-the-art for cybersecurity of road vehicles,
bringing together
researchers and practitioners across all areas of
computer security
focusing on automotive systems.

All papers discussing security and privacy issues of
modern vehicles are
welcome for submission. ACSW particularly
welcomes papers focusing on
the security of communication networks found
inside and outside the
modern vehicles, on the privacy issues related to
modern infotainment
systems, and on the forensic analysis of modern
vehicle components.
Topics of interest include, but are not limited to:
- Hardware security and privacy in automotive
components
- Forensic analysis of automotive components
- Firmware analysis and vulnerability assessment
in automotive contexts
- Reverse engineering of automotive components
and proprietary protocols
- Privacy-preserving applications in modern
vehicles
- Secure and privacy-preserving communications
for in-vehicle
communication protocols
- Intrusion detection and prevention systems for
automotive systems

- Replication and Reproduction of security and privacy-preserving
solutions for automotive systems
- Secure and privacy-preserving communications for Vehicle-to-Vehicle
(V2V) and Vehicle-to-Everything (V2X) applications
- Secure and privacy-preserving applications in Cooperative
Intelligent Transportation Systems (C-ITS)
- Security and privacy for automotive-related infrastructures
- Security and privacy in automotive-related industries
- Vulnerability assessment and attack simulations of automotive systems

[new this year - Replication and Reproduction track] This year, we are
inviting studies that confirm, challenge, or clarify the findings of
previous research. These papers must include the prefix “R+R:” in their
title and select the dedicated track in the submission form. We strongly
encourage authors to adhere to the well-known guidelines on
reproducibility (same experimental setup, conducted by a different team,
utilizing original artifacts) and replicability (different experimental
setup, conducted by a different team, re-implementing original
artifacts). However, submissions must go beyond merely re-running the
original artifacts or re-implementing existing

methods. We are seeking
contributions that not only replicate previous studies but also
critically analyze, refine, and expand upon their findings and
limitations. This includes, but is not limited to:
- Verifying the validity and reliability of existing research results
across diverse contexts,
- Extracting lessons learned from applying research outcomes in
real-world or industrial settings, and
- Adapting artifacts to address modern cybersecurity challenges.

Reproducibility and replication submissions will be subject to the same
rigorous scientific standards as other technical paper submissions. They
will undergo full program committee review, be included in the
proceedings, and have to be presented during the technical program of
the conference. We particularly encourage authors of these papers to
provide the software and data artifacts used in their studies, making
them publicly available to the entire community.

Important Dates
- Submission deadline for papers: February 3rd, 2025
- Author notification: March 24th, 2025
- Workshop day: June 30th, 2025

Submission Instructions - Page Limit and Formatting

Instructions regarding page limits and formatting can be found on the workshop web page: https://acsw.unimore.it/submission.html. Papers must be submitted electronically, in PDF format, through EasyChair (https://easychair.org/conferences/?conf=acsw25).

Review Process
Submitted papers will undergo a double-blind reviewing process, so authors must make sure that initial submissions do not contain information that might reveal their identity (e.g., author names, affiliations, email addresses or obvious self references). It is the author’s responsibility to ensure that their anonymity is preserved when citing their own work. Failures to adhere to these requirements can be grounds for rejection.

Submission and Proceedings
Accepted articles in the regular and short paper tracks will be published through IEEE Xplore in a volume accompanying the main IEEE EuroS&P 2025 proceedings. Authors can choose to have their paper excluded from the proceedings. At least one

author for each accepted
paper is expected to register and participate in the workshop for
presentation.
All submissions considered for inclusion in the proceedings must contain
an original contribution and should not be concurrently submitted to
other workshops, conferences, or journals. These requirements are
relaxed for papers which will not be included in the proceedings.

Organizing Committee
- Pal-Stefan Murvay, Faculty of Automation and Computers, Politehnica
University of Timișoara, Romania
- Dario Stabili, Department of Engineering ¨Enzo Ferrari¨, University
of Modena and Reggio Emilia, Italy

Program committee
- Daniele Antonioli, EURECOM, France
- Alessandro Brighente, University of Padova, Italy
- Meryem Benyahya, Université de Genève, Switzerland
- Jeremy Bryans, Coventry University, UK
- Mauro Conti, University of Padova, Italy
- Denis Donadel, University of Verona, Italy
- Giovanni Gambigliani Zoccoli, University of Modena and Reggio
Emilia, Italy
- Bela Genge, Bitdefender, Romania
- Bogdan Groza, Politehnica University of Timișoara, Romania
- Niclas Ilg, Bosch Research, Germany

- Konstantinos Kalogiannis, KTH Royal Institute of Technology, Sweden
- Wenjuan Lu, Block Harbor Security, USA
- Francesco Marchiori, University of Padova, Italy
- Ryo Kurachi, Nagoya University, Japan
- Stefano Longari, Polytechnic University of Milan, Italy
- Mirco Marchetti, University of Modena and Reggio Emilia, Italy
- Ilaria Matteucci, CNR, Italy
- Mario Raciti, University of Catania, Italy
- Samuel Woo, Dankook University, Korea

Contacts
All questions about submissions should be emailed to:
- Pal-Stefan Murvay (pal-stefan.murvay@aut.upt.ro)
- Dario Stabili (dario.stabili@unimore.it)

TOPICS OF INTEREST 4 topics

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

- Networking & Cloud Computing
- Uncategorized
- Cybersecurity & Privacy
- Mechanical engineering