CyberICPS 2023 CALL FOR PAPERS

9th Workshop on the Security of Industrial Control Systems and of Cyber-Physical Systems

The Hague, The Netherlands, September 28, 2023 (in conjunction with ESORICS 2023)
https://conferences.ds.unipi.gr/cybericps2023/

Important Dates
Submission due: June 30, 2023 **Notification to authors:** July 25, 2023 **Camera-ready due:** September 18, 2023

Cyber-physical systems (CPS) are physical and engineered systems that interact with the physical environment, whose operations are monitored, coordinated, controlled and integrated by information and communication technologies. These systems exist everywhere around us, and range in size, complexity and criticality, from embedded systems used in smart vehicles, to SCADA systems in smart grids to control systems in water distribution systems, to smart transportation systems, to plant control systems, engineering workstations, substation equipment, programmable logic controllers (PLCs), and other Industrial Control Systems (ICS). These systems also include the emerging trend of Industrial Internet of Things (IIoT) that will be the central part of the fourth industrial revolution.

CyberICPS invites submissions that present innovative ideas, proof of concepts, use cases, and results from a variety of topics relevant to ICS and CPS security, including (but not limited to) the following ones:

- Security governance
  - Security policies
  - Risk analysis and management
  - Vulnerability assessment and metrics
  - Awareness, training and simulation
  - ICS/CPS security standards
  - Privacy and Anonymity in ICS/CPS
- System and network security
  - Threat modeling
  - Security architectures
  - Access control
  - Malware and cyber weapons
  - Intrusion detection and visualization
  - Defense in depth
  - Monitoring and real time supervision
  - Applied cryptography
  - Perimeter security
  - Safety-security interactions
  - Cyber security engineering
  - Secure communication protocols
  - Formal models for ICS/CPS security
  - Hardware Security
  - Resilient ICS/CPS
  - Application Security
  - Secure Firmware
- Incident Response and Digital Forensics for ICS/CPS
  - Forensics in ICS
  - Incident Response
  - Accountability
- Case Studies
  - Case studies in the energy, utility, chemical, transportation, manufacturing, and other industrial and critical infrastructure sectors.

General Chair(s)
Frédéric Cuppens (Polytechnique Montréal, Canada)
Sokratis Katsikas (Norwegian University of Science and Technology, Norway)

Program Chairs
Nora Boulahia-Cuppens (Polytechnique Montréal, Canada)
Costas Lambrinoudakis (University of Piraeus, Greece)

Publicity Chair
Nikolaos Pitropakis (Edinburgh Napier University)

Program Committee (TBC)

Habtamu Abie (Norsk Regnesentral, Norway)
Cristina Alcaraz (University of Malaga, Spain)
Marios Anagnostopoulos (Aalborg University, Denmark)
Samiha Ayed (Telecom Bretagne, France)
Mauro Conti (University of Padua, Italy)
David Espes (University of Brest, France)
Khan Ferdous Wahid (Airbus Group, France)
Joaquin Garcia-Alfaro (Telecom SudParis, France)
Vasileios Gkioulos (Norwegian University of Science and Technology, Norway)
Dieter Gollmann (Hamburg University of Technology, Germany)
Georgios Kavallieratos (Norwegian University of Science and Technology, Norway)
Stefano Longari (Politecnico di Milano, Italy)
Youssef Laarouchi (EDF R&D, France)
Michail Maniatakos (NYU-Abu Dhabi, UAE)
Sjouke Mauw (University of Luxembourg, Luxembourg)
Weizhi Meng (Technical University of Denmark, Denmark)
Pankaj Pandey (Norwegian University of Science and Technology, Norway)
Nikolaos Pitropakis (Edinburgh Napier University, UK)
Indrakshi Ray (Colorado State University, USA)
Rodrigo Roman (University of Malaga, Spain)
Andrea Saracino (Consiglio Nazionale delle Ricerche, Italy)
Georgios Spathoulas (University of Thessaly, Greece)
Nils Ole Tippenhauer (CISPA, Germany)
Stefano Zanero (Politecnico di Milano, Italy)
Jianying Zhou (SUTD, Singapore)

Submission Instructions

Submitted papers must not substantially overlap with papers that have been published or that have been simultaneously submitted to a journal or a conference with proceedings. Submissions should be at most 20 pages long, including the bibliography and well-marked appendices, and should follow the LNCS style. Submissions are to be made to the submission web site. Only pdf files will be accepted. Authors should consult Springer's authors' guidelines and use their proceedings templates, either for LaTeX or for Word, for the preparation of their papers. LaTeX templates for Springer's proceedings are also available in Overleaf. Like in all previous editions of CyberICPS, it is expected that the conference proceedings will be published in the LNCS series. Submissions not meeting these guidelines risk rejection without consideration of their merits. Papers must be received by the submission deadline listed below (11:59 p.m. American Samoa time). Authors of accepted papers must guarantee that their papers will be presented at the workshop.

For further inquiries, please contact one of the program committee chairs at:
nora.boulahia-cuppens@polymtl.ca or clam@unipi.gr

POLYTECHNIQUE MONTRÉAL University of Piraeus NTNU Norwegian University of Science and Technology NORCICS SFI Norwegian Centre for Cybersecurity in Critical Sectors