CALL FOR PAPERS

2nd Workshop on the Security of Industrial Control Systems and of Cyber-
Physical Systems
(CyberICPS 2016)
in conjunction with ESORICS 2016
Heraklion, Greece, September 26-30, 2016

The 2nd Workshop on the Security of Industrial Control Systems and of Cyber-
Physical Systems (CyberICPS 2016) will be held in Heraklion, Crete, Greece, in
conjunction with ESORICS 2016, in September 2016. CyberICPS is the result of
the merging of the CyberICS and WOS-CPS workshops that were held for the
first time in conjunction with ESORICS 2015.

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).

As ICS and CPS proliferate, and increasingly interact with us and affect our life,
their security becomes of paramount importance. CyberICPS intends to bring
together researchers, engineers and governmental actors with an interest in the
security of ICS and CPS in the context of their increasing exposure to cyber-
space, by offering a forum for discussion on all issues related to their cyber
security.

CyberICPS invites submissions that present innovative ideas, proof of concepts,
use cases, and results from a variety of topics relevant to ICS and CPS, 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 visualisation
• 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.

Submissions

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 16 pages long, including the bibliography and well-marked appendices, and should follow the LNCS style (http://www.springeronline.com/lncs). Submissions are to be made to the submission web site at https://easychair.org/conferences/?conf=cybericps2016. Only pdf files will be accepted. Submissions not meeting these guidelines risk rejection without consideration of their merits. Papers must be received by the deadline of July the 15th, 2016 (11:59 p.m. American Samoa time). Authors of accepted papers must guarantee that their papers will be presented at the workshop. Pre-proceedings will be made available at the workshop. It is planned to have post-proceedings published by Springer in the Lecture Notes in Computer Science (LNCS) series.

Important dates

Submission deadline: 26 June 2016
15 July 2016 (Extended)

Notification to authors: 25 July 2016
15 August 2016

Camera ready due: 42 August 2016
29 August 2016
Organization

General Chairs
• Frederic Cuppens, Telecom Bretagne, France
• Sokratis Katsikas, Norwegian University of Science and Technology, Norway

Program Chairs
• Nora Cuppens-Bulahia, Telecom Bretagne, France
• Costas Lambrinoudakis, University of Piraeus, Greece

Technical Program Committee
• Hervé Debar, Telecom Sudparis, France
• Jozef Vyskoc, VAF, Slovakia
• Juha Röning, University of Oulu, Finland
• Mauro Conti, University of Padua, Italy
• Stefano Zanero, Politecnico di Milano, Italy
• Stephen Wolthusen, Royal Holloway, UK
• Wael Kanoun, Alcatel-Lucent (Bell Labs), France
• Weizhi Meng, Institute for Infocomm Research, Singapore
• Yves Roudier, EURECOM, France
• Chris Mitchell, Royal Holloway, UK
• Cristina Alcaraz, University of Malaga, Spain
• David Espes, University of Brest, France
• Dieter Gollmann, Technical University of Hamburg, Germany
• Mourat Debbabi, Concordia University, Canada
• Sjouke Mauw, University of Luxembourg, Luxembourg
• Samiha Ayed, Telecom Bretagne, France
• Masahiro Mambo, Kanazawa University, Japan
• Khan Ferdous Wahid, Airbus Defence and Space GmbH, Germany


PC chairs email:
• Nora Cuppens-Bulahia, nora.cuppens@telecom-bretagne.eu
• Costas Lambrinoudakis, clam@unipi.gr