Security and Communication Networks

Special Issue on
Security of Cyberphysical Systems and Industrial Control Systems and Networks

WILEY | Hindawi

CALL FOR PAPERS

Cyberphysical systems (CPS) are large-scale, interconnected physical, and engineered systems made up from heterogeneous components that interact with the physical environment, whose operations are monitored, coordinated, controlled, and integrated by information and communication technologies (ICT). These systems exist everywhere around us and range in size, complexity, and criticality, from embedded systems used in smart vehicles, to Supervisory Control And Data Acquisition (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) connected through Industrial Control Networks (ICN).

As ICS, CPS, and ICN proliferate and increasingly interact with us and affect our life, their security becomes of paramount importance. CPSs have some special characteristics that distinguish them from other types of ICT systems, such as the need for real-time availability, that render the use of known security approaches prohibitive and create new security (and privacy) challenges. Examples of such challenges include, but are not limited to, identifying ways for motivating the industry to adopt best practices, standards and guidelines for preventing attacks against CPSs; developing risk assessment and management methodologies that will combine security, safety, and resilience requirements; developing efficient techniques for intrusion detection that will not only exploit network traffic data but will also take into account the nature and the dynamics of the physical process that is controlled by the CPS, in real or near real time; designing systems resilient to cyberattacks, that is, systems able to operate, perhaps at a lower operational capacity, even when they have been compromised.

With this special issue, we intend to bring together researchers, engineers, and governmental actors with an interest in the security of ICS, CPS, and ICN in the context of their increasing exposure to cyberspace. We seek novel submissions describing theoretical and practical security solutions to the security of CPS, ICS, and ICN. Papers that are pertinent to the security of embedded systems, SCADA, smart grid, and critical infrastructure networks are all welcome, especially in the domains of energy, manufacturing, autonomous systems, and transportation.

We invite submissions that present innovative ideas, proof of concepts, use cases, and results from a variety of topics relevant to ICS, CPS, and ICN.

Potential topics include but are not limited to the following:

- Security governance
  - Security policies
  - Risk analysis and management
  - Vulnerability assessment and metrics
  - Awareness, training, and simulation
  - ICS/CPS/ICN security standards
  - Privacy and anonymity in ICS/CPS/ICN
- System and network security
  - Threat modeling
  - Security architectures
  - Access control
  - Malware and cyberweapons
  - Intrusion detection and visualization
  - Defense in depth
  - Monitoring and real-time supervision
  - Applied cryptography
  - Perimeter security
  - Safety-security interactions
  - Cybersecurity engineering
  - Secure communication protocols
  - Formal models for ICS/CPS/ICN security
  - Hardware security
  - Resilient ICS/CPS/ICN
  - Application security
  - Secure firmware
- Incident response and digital forensics for ICS/CPS/ICN
  - Forensics in ICS/CPS/ICN
  - Incident response
  - Accountability
- Clinical Studies
  - Clinical studies in the energy, utility, chemical, transportation, manufacturing, and other industrial and critical infrastructure sectors

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/scn/spsi/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Sokratis Katsikas, Norwegian University of Science and Technology, Trondheim, Norway
sokratis.katsikas@ntnu.no

Guest Editors
Javier Lopez, University of Malaga, Malaga, Spain
jlm@lcc.uma.es

Jianying Zhou, Singapore University of Technology and Design, Singapore
zhou_jianying@yahoo.com

Indrakshi Ray, Colorado State University, Fort Collins, USA
indrakshi.ray@colostate.edu

Submission Deadline
Friday, 29 September 2017

Publication Date
February 2018