

CPS-SPC'18: Call for Papers

4th ACM Workshop on Cyber-Physical Systems Security and PrivaCy

In Conjunction with the ACM Conference on Computer and Communications Security

October 19 2018, Toronto, Canada

<https://www.cps-spc.org/>

1 Motivation and Scope

Cyber-Physical Systems (CPS) integrate computing and communication capabilities with monitoring and control of entities in the physical world. These systems are usually composed of a set of networked agents, including sensors, actuators, control processing units, and communication devices. While some forms of CPS are already in use, the widespread growth of wireless embedded sensors and actuators is creating several new applications in areas such as medical devices, autonomous vehicles, and smart infrastructure, and is increasing the role that the information infrastructure plays in existing control systems for areas such as manufacturing or power.

Many CPS applications are safety-critical: their failure can cause irreparable harm to the physical system under control, and to the people who depend, use or operate it. In particular, critical cyber-physical infrastructures such as electric power generation, transmission and distribution grids, oil and natural gas systems, water and waste-water treatment plants, and transportation networks play a fundamental and large-scale role in our society. Their disruption can have a significant impact on individuals, and nations at large. Securing these CPS infrastructures is, therefore, vitally important.

Similarly, because many CPS collect sensor data non-intrusively, users of these systems are often unaware of their exposure. Therefore, in addition to security, CPS systems must be designed with privacy considerations.

To address these issues, we invite original research papers on the security and privacy of Cyber-Physical Systems. We seek submissions from multiple interdisciplinary backgrounds tackling security and privacy issues in CPS, including but not limited to:

- mathematical foundations for secure CPS
- control-theoretic approaches to secure CPS
- high assurance security architectures for CPS
- security and resilience metrics for CPS
- metrics and risk assessment approaches for CPS
- privacy in CPS
- network security for CPS
- game theory applied to CPS security
- security of embedded systems, IoT and real-time systems in the context of CPS
- human factors and humans in the loop
- understanding dependencies among security, reliability and safety in CPS
- economics of security and privacy in CPS
- intrusion detection in CPS

- model-based security systems engineering
- experimental insights from real-world CPS or CPS testbeds

CPS domains of interest include but are not limited to:

- health care and medical devices
- manufacturing
- industrial control systems
- SCADA systems
- Robotics
- smart building environments
- unmanned aerial vehicles (UAVs)
- autonomous vehicles
- transportation systems and networks

Also of interest will be papers that can point the research community to new research directions, and those that can set research agendas and priorities in CPS security and privacy. **There will be a best paper award.**

2 Submission Instructions

Submitted papers can be up to 12 pages including appendices and references. Submissions must use the ACM SIG Proceedings Templates (see <https://www.acm.org/publications/proceedings-template>, with a simpler version here: <https://github.com/acmccs/format>). Only PDF files will be accepted. Submissions not meeting these guidelines risk rejection without consideration of their merits. Accepted papers will be published by the ACM Press and/or the ACM Digital Library.

Submissions must not substantially overlap with papers that have been published or that are simultaneously submitted to a journal or a conference with proceedings. Each accepted paper must be presented by one registered author. Submissions not meeting these guidelines risk immediate rejection. For questions about these policies, please contact the chairs.

Please submit your work at <https://easychair.org/conferences/?conf=cpsspc2018>

3 Important Dates

- Submission Deadline: July 1, 2018 (23:59 Anywhere on Earth time)
- Notification of Acceptance/Rejection: July 30, 2018
- Camera Ready Papers Due: August 19, 2018

4 Organization

4.1 Steering Committee

- Rakesh Bobba, Oregon State University
- Alvaro Cardenas, University of Texas at Dallas
- Roshan Thomas, MITRE Corporation

4.2 PC Chairs

- Awais Rashid, University of Bristol
- Nils Ole Tippenhauer, Singapore University of Technology and Design

4.3 TPC members

- Aditya Mathur, SUTD
- Alvaro Cardenas, UT Dallas
- Avishai Wool, Tel Aviv Univ.
- Ben Green, Lancaster
- Chris Poskitt , SUTD
- Claire Vishik, Intel
- Cristina Alcaraz, University of Malaga
- Daisuke Mashima, ADSC
- Emil Lupu, Imperial College
- Gerhard Hancke, City University of Hong Kong
- Jianying Zhou, SUTD
- Jose M. Such, King's College
- Katerina Mitrokotsa, Chalmers University of Technology
- Magnus Almgren, Chalmers Univ.
- Marina Krotofil, FireEye
- Martín Ochoa, Universidad del Rosario
- Michail (Mihalis) Maniatakos, NYU-Abu Dhabi
- Nora Cuppens, IMT Atlantique
- Pauline Anthonysamy, Google
- Quanyan Zhu, NYU
- Raheem Beyah, Georgia Tech.
- Rakesh Bobba, Oregon State Univ.
- Saman Zonouz, Rutgers Univ.
- Simon Foley, IMT-Atlantique
- Stefano Zanero, Politecnico di Milano
- Sylvain Frey, Google DeepMind