Call for Papers

Workshop on Security Issues in Cyber Physical Systems (SecCPS)

In conjunction with IEEE HASE 2017

January 14, 2017 – Singapore

Important Dates:

Submission Deadline:
Nov 14, 2016

Acceptance Notification:
Dec 12, 2016

Camera Ready:
Dec 26, 2016

Workshop Date:
Jan 14, 2016

Workshop Chairs:
Mauro Conti
University of Padua, Italy

Dieter Gollmann
TUHH, Germany

Lejla Batina
Radboud University, Netherlands

Publicity Chairs:
[TBC]

Web Chair:
[TBC]

Cyber Physical Systems (CPS) are embedded systems composed of computing elements and physical processes. In the past, CPS were proprietary and not connected to the cyber space; with the advent of networked control systems to enable better operations and monitoring of the physical processes, these systems are increasingly becoming part of cyberspace. Connection to the cyber space enables effective management of public infrastructures such as public transportation, smart grid and water treatment facilities. However, these advantages come with new security challenges.

Attacks on CPS may lead to performance degradation to complete shutdown, or even equipment damage depending on the knowledge, goals and resources of the attacker. Most work in area of CPS security focus on the cyber part and attempts to ensure secure exchange of information across controllers, sensors, and actuators. The nature of security threats and attacks in a CPS is different from those found in pure cyberspace. Threat models have evolved significantly and the fact that any successful attack could be fatal – as it is more than a computer being hacked and disturbs the physical process – may result in dangerous scenarios. It is not only about the consequences of attacks but the fact that besides cyber attacks, attacks on physical devices are also possible: An adversary may add, remove or replace some physical components which may result in severe consequences. Understanding the physical part, and how it can be compromised, is essential to ensure CPS security. Thus focus ought to be on both physical and cyber domains.

SecCPS seeks novel submissions describing practical and theoretical solutions to securing CPS. Submissions may represent any application area for CPS. Hence, papers that are pertinent to the security of embedded systems, Internet of Things, SCADA Systems, Water Systems, Smart-Grid Systems, Critical Infrastructure Networks, Transportation Systems, Medical Devices etc., are welcome.

Example topics of interest are given below, but are not limited to:

- Cyber Physical Systems (CPS) security
- Authentication mechanisms for CPS Hardware
- Embedded systems security
- Design for Security (DfS) of CPS Devices
- Security analysis and protection of Internet of Things (IoT)
- Forensics for CPS
- Intrusion detection for CPS
- Hardware Trojan attacks and detection techniques
- Hardware-based security primitives (PUFs, RNGs, Aging Sensors) for CPS
- Availability, recovery and auditing for CPS
- Security of biomedical systems, e-health, and medicine
- Threat models for CPS
- Physical layer security for CPS
- Hardware IP trust (watermarking, fingerprinting, trust verification)
- Secure and efficient hardware implementation of cryptographic algorithms
- Vulnerability analysis of CPS
- Hardware tampering attacks and protection
- Hardware obfuscation, encryption and metering
- Hardware techniques that ensure software, firmware and system security
- Security vs. Reliability, Security vs. Energy-efficiency Tradeoffs
- Automotive systems security
- Security of industrial control systems
- Security of IoT

For more information please visit: http://itrust.sutd.edu.sg/hase2017/workshop-2/

Submission Instructions: Submitted papers must represent original material that is not currently under review in any other conference or journal, and has not been previously published. All submissions must be written in English with a maximum paper length of 6 (six) pages (including text, figures, and references) and formatted according to the two column IEEE conference format. Accepted papers will be published in the IEEE Digital Library after the conference and included in the IEEE HASE proceedings. Papers must be submitted through EasyChair.

Technical Programme Committee Members

- Frederik Armlnecht, Uni-Mannheim, Germany
- Matthias R. Brust, University of Luxembourg
- Andrew Clark, Worcester Polytechnic Institute, USA
- Chhagan Doot, University of Padova, Italy
- Jean-Luc Danger, Telecon Paristech, France
- Tooska Dargahi, University of Rome Tor Vergata, Italy
- Earlence Fernandes, University Michigan, USA
- Ensuk Kang, UC Berkley, USA
- Riccardo Lazzeretti, University of Padova, Italy
- Qi Li, Tsinghua University, China
- Yilin Mo, Nanyang Technological University, Singapore
- Parthajit Mohatpatra, Indian Institute of Technology Kharagpur, India
- Veelasha Moonsamy, Radboud University, Netherlands
- Atul Prakash, Michigan University, USA
- Saman Aliari Zonouz, Rutgers University, USA