Call for Papers

Workshop on Security and Privacy in Cyber-Physical Systems (SPCPS) 2017

Website: http://spcps2017.sccs.surrey.ac.uk/

Co-Sponsored by

IEEE Technical Committee on Cyber-Physical Systems

IEEE SMC Society Technical Committee on CyberMatics

Surrey Centre for Cyber Security (SCCS), University of Surrey

Part of the 3rd IEEE International Conference on Cybernetics (CYBCONF 2017)

University of Exeter, UK, 21-23 June 2017

Website: http://cse.stfx.ca/~CybConf2017

Important Dates

Paper Submission:	**23 March 2017 (extended)**
Authors Notification:	22 April 2017
Camera-Ready Paper:	15 May 2017

Introduction

In the past several decades the rapid development of computer systems and networking technologies have made the physical world highly connected and digitized, thus moving many physical systems and processes into the cyber space. The more recent growth of new technologies such as mobile computing, wearable computing, cloud computing, Internet of Things (IoT), intelligent transport systems (ITS), autonomous and connected vehicles, and augmented/virtual reality have pushed the cyber space to the next level, where cyber and physical worlds become more intermingled and their boundary become more and more blurred.

In cyber-physical systems (CPSs), it is not sufficient to consider the cyber and physical worlds separately, and the dynamic interactions between the two worlds become more critical especially when security and user privacy are of concern, which call for more complicated monitoring, measurement, control, adaptation and protection mechanisms at all levels of the system and its different components. In addition to machines and physical objects (things) involved, humans also play a very most important role in CPSs since such systems are designed to serve humans either directly or indirectly. The involvement of human users in CPSs also lead to concerns on privacy protection as there are often much more avenues to leakage of private information ranging from unintended leakage to more attacking vectors.

When humans are involved, social interactions between human users form part of the complicated cyber-physical world interactions, so understanding the social elements

is also very important. One typical example is the concept of social IoT proposed recently, where social networks and IoT networks are connected via human users who cross over both networks thus forming a larger CPS with even more complicated dynamics. Another example is mobile crowdsensing where human users use their mobile devices and/or in-vehicle sensors to participate in collective sensing of the physical world, which often involve a high level of social interactions among human participants who share and consume such information.

Another unique issue around security of human-involved CPSs is that a security flaw or an attack can cause safety risks to human users and/or lead to high financial losses to industry and customers. This can be easily seen from CPSs in application domains such as e-health, transportation, civil engineering, smart grids, and industrial control systems (ICS).

The complexity of ensuring security and privacy in CPSs calls for more research in this area, especially on system-level, human-centric and adaptive techniques which can provide more intelligence and automation while providing human users with better experience, more effective control, and an increased level of situational awareness.

Topics of Interest

We welcome submissions addressing research problems in the following topics (not limited to):

- Security industrial control systems for CPSs
- Lightweight cryptography for CPSs
- Data security and privacy for CPS
- Authentication and access control for CPS
- Autonomous vehicle security
- Availability, recovery and auditing for CPS
- Supervisory control and data acquisition (SCADA) security
- Self-adaptive techniques for improving security and privacy in CPSs
- Intelligent systems for security and privacy in CPSs
- Optimization of security and privacy solutions for CPSs
- CPS system modelling and simulation for security and privacy purposes
- Cognitive modelling of human users in CPSs for security and privacy purposes
- Human behavioral studies around security and privacy issues of CPSs
- CPS user interfaces for security and privacy purposes
- Security protocols for CPSs
- Privacy enhancing technologies for CPSs
- New attacks to CPSs especially side channel attacks and countermeasures
- Security and privacy risk management of CPSs
- Security and privacy situational awareness in CPSs
- Security and privacy issues around interplay between CPSs and social media
- Security and privacy issues around sensor networks
- Security and privacy issues around participatory sensing
- Multimedia techniques for improving security and privacy protection of CPSs
- New architectures and platforms for designing more secure CPSs

- New frameworks for analyzing security and privacy issues in CPSs
- Connections between security, privacy, safety and reliability of CPSs
- Security and privacy problems and solutions in ITS
- Security and privacy problems and solutions in e-health and medical devices
- Security and privacy problems and solutions around robots
- Security and privacy in intelligent power and energy systems

Guidelines for Authors

All papers need to be submitted electronically through the CYBCONF 2017 workshops and special sessions' online submission website (https://easychair.org/conferences/?conf=cybconf2017wsss, select the **"Security and Privacy in Cyber-Physical Systems" track**) with PDF format. The materials presented in the papers should not be published or under submission elsewhere. Each paper is limited to 6 pages (or 8 pages with over length charge) including figures and references using the IEEE Proceedings Manuscripts style (two columns, single-spaced, 10pt). More guidelines for preparing final camera-ready papers can be found at http://www.ieee.org/conferences_events/conferences/publishing/cybconf17.html.

Presented papers will appear in the conference proceedings, available on IEEE Xplore and submitted to be indexed in CPCi (ISI conferences and part of Web of Science) and Engineering Index (EI).

Post-Workshop Journal Special Issues

After the workshop's program is fixed, the workshop organizers will apply for a special issue at a prestigious journal such as *ACM Transactions on Cyber-Physical Systems*, *IEEE Internet of Things Journal*, *IEEE Sensors Journal*, *IEEE Systems Journal*, *IET Cyber-Physical Systems: Theory & Applications*, *IET Information Security*, *International Journal of Information Security* (Springer), *Computer & Security* (Elsevier), *Journal of Information Security and Applications* (Elsevier), and *EURASIP Journal on Information Security*. Authors of selected best papers from the workshop will be invited to submit extended versions of their papers to the special issue with a post-workshop deadline.

In addition to the above planned journal special issue dedicated to the workshop, CYBCONF 2017 will also invite authors of selected papers (presented at the main conference and associated workshops including SPCPS 2017) to extend their papers for recommended submissions and publications in the following prestigious journals or their special issues: *IEEE Transactions on Cybernetics*, *IEEE Systems, Man, and Cybernetics Magazine*, *Evolving Systems* (Springer), and *Peer-to-Peer Networking and Applications* (Springer).

Organizers

General and Program Committee Co-Chairs

Shujun Li, University of Surrey, UK
Chunhua Su, Osaka University, Japan

Publicity Co-Chairs

Jiageng Chen, Central China Normal University, China
Flavia C. Delicato, Universidade Federal do Rio de Janeiro, Brazil
Kuo-Hui Yeh, National Dong Hwa University, Taiwan

Web Chair

Haiyue Yuan, University of Surrey, UK

Program Committee

- Shujun Li, University of Surrey, UK (Co-Chair)
- Chunhua Su, Osaka University, Japan (Co-Chair)
- Panagiotis Andriotis, University of West England, UK
- David Arroyo Guardeño, Universidad Autónoma de Madrid (UAM), Spain
- Hassan Jameel Asghar, Data61, CSIRO, Australia
- Joonsang Baek, Khalifa University of Science, Technology and Research, UAE
- Jiageng Chen, Central China Normal University, China
- Kim-Kwang Raymond Choo, The University of Texas at San Antonio, USA
- Mauro Conti, University of Padua, Italy
- Hervé Debar, Telecom SudParis, France
- Flavia C. Delicato, Universidade Federal do Rio de Janeiro, Brazil
- Chuan Heng Foh, University of Surrey, UK
- Athanasios Giannetsos, University of Surrey, UK
- Matt Henricksen, Institute for Infocomm Research, Singapore
- Xinyi Huang, Fujian Normal University, China
- Helge Janicke, De Montfort University, UK
- Shancang Li, University of West England, UK
- Wei Li, The University of Sydney, Australia
- Yingjiu Li, Singapore Management University, Singapore
- Kaitai Liang, Manchester Metropolitan University, UK
- Joseph Liu, Monash University, Australia
- Zhe Liu, University of Waterloo, Canada
- Grigorios Loukides, King's College London, UK
- Shinsaku Kiyomoto, KDDI R&D Laboratories Inc., Japan
- Di Ma, University of Michigan-Dearborn, USA
- Leandros Maglaras, De Montfort University, UK
- Weizhi Meng, Technical University of Denmark, Denmark
- Kazumasa Omote, Tsukuba University, Japan
- Guenther Pernul, University of Regensburg, Germany
- Zhongyuan Qin, Southeast University, China
- Isabel Wagner, De Montfort University, UK
- Edgar Weippl, SBA Research and TU Wien, Austria
- Xinyu Yang, Xi'an Jiaotong University, China
- Kuo-Hui Yeh, National Dong Hwa University, Taiwan
- Zonghua Zhang, Institut Mines-Télécom, France