CPS-SPC 2017: Third Workshop on Cyber-Physical Systems Security and PrivaCy

Rakesh B. Bobba
Oregon State University
Corvallis, Oregon, USA
rakesh.bobba@oregonstate.edu

Awais Rashid
Lancaster University
Lancaster, United Kingdom
a.rashid@lancaster.ac.uk

ABSTRACT

Cyber-Physical Systems (CPS) are becoming increasingly critical for the well-being of society (*e.g.,* electricity generation and distribution, water treatment, implantable medical devices *etc.*). While the convergence of computing, communications and physical control in such systems provides benefits in terms of efficiency and convenience, the attack surface resulting from this convergence poses unique security and privacy challenges. These systems represent the new frontier for cyber risk. CPS-SPC is an annual forum, in its 3rd edition this year, that aims to provide a focal point for the research community to begin addressing the security and privacy challenges of CPS in a comprehensive and multidisciplinary manner and, in tandem with other efforts, build a comprehensive research road map.

CCS CONCEPTS

• **General and reference → General literature**;

KEYWORDS

cyber-physical systems; security; privacy; workshop

1 INTRODUCTION

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 such as in the process control industry or the power grid.

Many CPS applications are safety-critical: their failure can cause irreparable harm to the physical system under control, and to the people who depend on it or use and 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 systems 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.

The challenges in securing CPS are many. But fundamentally, it is important to recognize that securing CPS differs from the traditional cyber security concerns of confidentiality, integrity and availability (CIA) that have dominated the security of information technology (IT) systems. At its core, CPS security must be approached and framed from the perspective of how attacks on CIA properties perturb control-theoretic properties such as controllability, observability and stability and consequently system safety. Like past editions, CPS-SPC 2017 aims to bring together a community around security and privacy challenges in CPS. It is held in conjunction with ACM Computer and Communications Security (CCS) conference, a flagship annual conference of ACM SIGSAC (Special Interest Group on Security, Audit and Control) and a premier security conference. The co-location of these two events brings advantages to both, as well as to the community itself.

2 SCOPE

CPS-SPC 2017 encourages participation from researchers and practitioners from diverse CPS domains and multiple disciplinary backgrounds representative of CPS, including but not limited to information security, control theory, embedded systems, and human factors. It provides a forum for researchers from these various CPS domains and backgrounds to share their ideas and results, to discuss emerging technologies and trends that impact CPS, to study differences and commonalities across different CPS domains, and to build a multidisciplinary body of knowledge in this sub-field that is still in its infancy.

This year's workshop builds on the foundations laid by the last two editions and invited submissions at the interface of control theory, information security, embedded and real-time systems, and human factors among others as applied to CPS. Specifically the topics of interest included but were 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

CCS'17, , October 30–November 3, 2017, Dallas, TX, USA
© 2017 Association for Computing Machinery.
ACM ISBN ISBN 978-1-4503-4946-8/17/10…$15.00
https://doi.org/10.1145/3133956.3137051

- 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 and 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 were 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.

3 PROGRAM

CPS-SPC 2017 is a one day workshop held on November 3rd 2017. The program comprises four technical sessions with talks on accepted short and regular length research papers. This year the workshop received 26 papers from 11 different countries and accepted 9 full and 4 short papers for presentation at the workshop.

4 WORKSHOP COMMITTEES

4.1 Program Committee

We are thankful to the members of our program committee without whose help and support this workshop wouldn't have been successful.

- Cristina Alcaraz, Universidad de Malaga, Spain
- Magnus Almgren, Chalmers University of Technology, Sweden
- Pauline Anthonysamy, Google
- Raheem Beyah, Georgia Institute of Technology, USA
- Alvaro Cardenas, University of Texas at Dallas, USA
- Gabriela Ciocarlie, SRI International, USA
- Simon Foley, IMT-Atlantique, France
- Sylvain Frey, University of Southampton, UK
- Benjamin Green, Fujistu/Lancaster University, UK
- Adam Hahn, Washington State University, USA
- Wouter Joosen, KU Leuven, Belgium
- Marina Krotofil, Honeywell Industrial Cyber Security Lab
- Michail Maniatakos, New York University Abu Dhabi, UAE
- Daisuke Mashima, Advanced Digital Sciences Center, Singapore
- Aditya Mathur, Singapore University of Technology and Design, Singapore
- Sibin Mohan, University of Illinois at Urbana-Champaign, USA
- Xinming Ou, University of South Florida, USA
- Jose M. Such, King's College London, UK
- Roshan Thomas, MITRE, USA
- Nils Ole Tippenhauer, Singapore University of Technology and Design, Singapore
- Claire Vishik, Intel Corporation, UK
- Avishai Wool, Tel Aviv University, Israel
- Quanyan Zhu, New York University, USA

4.2 PC Co-Chairs

Rakesh B. Bobba is an Assistant Professor in the School of Electrical Engineering and Computer Science (EECS) at Oregon State University (OSU). He obtained his Ph.D. and M.S. in Electrical and Computer Engineering from the University of Maryland at College Park. Prior to joining OSU, Dr. Bobba was a Research Assistant Professor at the Information Trust Institute, University of Illinois, Urbana-Champaign. His research interests are in the design of secure and trustworthy networked and distributed computer systems, with a current focus on cyber-physical critical infrastructures, shared computing infrastructures and real-time systems. Together with Roshan K. Thomas and Alvaro C. Cardenas he initiated CPS-SPC in 2015 and served as a PC member.

Awais Rashid is Director of the Security-Lancaster Institute, comprising 100 researchers focusing on human and technical aspects of security. He leads multiple research projects on CPS, including a project as part of the UK Research Institute on Trustworthy Industrial Control Systems and an EU project (with KU Leuven and University College Cork) on adaptive security for CPS under attack. He also co-leads the Security and Safety Stream within the UK Research Hub on Cyber Security of the Internet of Things. He also organized and chaired the first workshop on security and resilience of cyber-physical infrastructures at the International Symposium on Engineering Secure Software and Systems (ESSoS) in 2016 and has served on the PC of the first two CPS-CPC workshops at CCS. Rashid is also leading a major project on developing a cyber-security body of knowledge (CyBOK).

ACKNOWLEDGMENTS

The co-chairs would like to thank members of the Program Committee and the external reviewers for their support and service to CPS-SPC and the community. We would also like to thank the CPS-SPC Steering Committee for their support in organizing the workshop. Thanks to Taesoo Kim and Cliff Wang, ACM CCS Workshop Co-Chairs; Matthew Wright and Apu Kapadia, ACM CCS Proceedings co-chairs; and Bhavani Thuraisingham ACM CCS General Chair. Last, but not least, we would like to thank all the authors who submitted their work to CPS-SPC 2017 and all the participants of the event.