

# Preface

This book contains revised versions of the papers presented at the Third Workshop on Security of Industrial Control Systems and Cyber-Physical Systems (CyberICPS 2017) and the First International Workshop on Security and Privacy Requirements Engineering (SECPRE 2017). Both workshops were co-located with the 22nd European Symposium on Research in Computer Security (ESORICS 2017) and were held in Oslo, Norway, on September 15, 2017.

CyberICPS aims to bring together researchers, engineers, and governmental actors with an interest in the security of industrial control systems and cyber-physical systems in the context of their increasing exposure to cyber-space, by offering a forum for discussion on all issues related to cyber-security. Cyber-physical systems range in size, complexity, and criticality, from embedded systems used in smart vehicles, to SCADA and industrial control systems like energy and water distribution systems, smart transportation systems etc.

CyberICPS 2017 attracted 32 high-quality submissions, each of which was assigned to three referees for review; the review process resulted in ten full and two short papers being accepted to be presented and included in the proceedings. These cover topics related to threats, vulnerabilities, and risks that cyber-physical systems and industrial control systems face; cyber attacks that may be launched against such systems; and ways of detecting and responding to such attacks.

For many years, software engineers have focused on the development of new software thus considering security and privacy mainly during the development stage as an ad hoc process rather than an integrated one initiated during the system design stage. However, the data protection regulations, the complexity of modern environments such as IoT, IoE, cloud computing, big data, cyber-physical systems etc. and the increased level of users' awareness in IT have forced software engineers to identify security and privacy as fundamental design aspects leading to the implementation of more trusted software systems and services. Researchers have addressed the necessity and importance of implementing design methods for security and privacy requirements elicitation, modeling, and implementation in the past few decades. Today security by design (SbD) and privacy by design (PbD) are established research areas that focus on these directions. SECPRE aimed to provide researchers and professionals with the opportunity to present novel and cutting-edge research on these topics.

SECPRE 2017 attracted 14 high-quality submissions, each of which was assigned to three referees for review; the review process resulted in accepting five papers to be presented and included in the proceedings. These cover topics related to security and privacy requirements assurance and evaluation, and to security requirements elicitation and modeling.

We would like to express our thanks to all those who assisted us in organizing the events and putting together the programs. We are very grateful to the members of the Program Committees for their timely and rigorous reviews. Thanks are also due to the Organizing Committees for the events. Last, but by no means least, we would like to thank all the authors who submitted their work to the workshops and contributed to an interesting set of proceedings.

November 2017

Sokratis K. Katsikas  
Frédéric Cuppens  
Nora Cuppens  
Costas Lambrinoudakis  
Christos Kalloniatis  
John Mylopoulos  
Annie Antón  
Stefanos Gritzalis

Computer Security

ESORICS 2017 International Workshops, CyberICPS

2017 and SECPRE 2017, Oslo, Norway, September

14-15, 2017, Revised Selected Papers

Katsikas, S.K.; Cuppens, F.; Cuppens-Boulahia, N.;

Lambrinoudakis, C.; Kalloniatis, C.; Mylopoulos, J.; Antón,

A.; Gritzalis, S. (Eds.)

2018, XII, 281 p. 76 illus., Softcover

ISBN: 978-3-319-72816-2