

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen 

TU Dortmund University, Dortmund, Germany

Gerhard Woeginger 

RWTH Aachen, Aachen, Germany

Moti Yung

Columbia University, New York, NY, USA

More information about this subseries at <http://www.springer.com/series/7410>

Sokratis Katsikas · Frédéric Cuppens ·
Nora Cuppens · Costas Lambrinoudakis ·
Christos Kalloniatis · John Mylopoulos ·
Annie Antón · Stefanos Gritzalis ·
Weizhi Meng · Steven Furnell (Eds.)


Computer Security

ESORICS 2020 International Workshops,
CyberICPS, SECPRE, and ADIoT
Guildford, UK, September 14–18, 2020
Revised Selected Papers

Editors

Sokratis Katsikas 
Norwegian University of Science
and Technology
Gjøvik, Norway


Nora Cuppens
Polytechnique Montréal
Montréal, QC, Canada


Christos Kalloniatis 
University of the Aegean
Mytilene, Greece

Annie Antón
Georgia Institute of Technology
Atlanta, GA, USA

Weizhi Meng 
Technical University of Denmark
Lyngby, Denmark

Frédéric Cuppens
Polytechnique Montréal
Montréal, QC, Canada

Costas Lambrinoudakis 
University of Piraeus
Piraeus, Greece

John Mylopoulos 
Department of Computer Science
University of Toronto
Toronto, ON, Canada

Stefanos Gritzalis
University of Piraeus
Piraeus, Greece

Steven Furnell 
University of Nottingham
Nottingham, UK

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-030-64329-4

ISBN 978-3-030-64330-0 (eBook)

<https://doi.org/10.1007/978-3-030-64330-0>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2020

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

CyberICPS 2020 Preface

This book contains revised versions of the papers presented at the 6th Workshop on Security of Industrial Control Systems and Cyber-Physical Systems (CyberICPS 2020). The workshop was co-located with the 25th European Symposium on Research in Computer Security (ESORICS 2020) and was held online as a virtual event on September 17, 2020.

Cyber-physical systems (CPS) are physical and engineered systems that interact with the physical environment, whose operations are monitored, coordinated, controlled, and integrated by information and communication technologies. These systems exist everywhere around us, and range in size, complexity, and criticality, from embedded systems used in smart vehicles, to SCADA systems in smart grids, to control systems in water distribution systems, to smart transportation systems, to plant control systems, engineering workstations, substation equipment, programmable logic controllers (PLCs), and other Industrial Control Systems (ICS). These systems also include the emerging trend of Industrial Internet of Things (IIoT) that will be the central part of the fourth industrial revolution. As ICS and CPS proliferate, and increasingly interact with us and affect our lives, their security becomes of paramount importance. CyberICPS 2020 brought together researchers, engineers, and governmental actors with an interest in the security of ICS and CPS in the context of their increasing exposure to cyberspace, by offering a forum for discussion on all issues related to their cyber security.

CyberICPS 2020 attracted 21 high-quality submissions, each of which was assigned to 4 referees for review; the review process resulted in 8 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.

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

October 2020

Sokratis Katsikas
Frédéric Cuppens
Nora Cuppens
Costas Lambrinoudakis

CyberICPS 2020 Organization

General Chairs

Nora Cuppens
Costas Lambrinoudakis

Polytechnique Montréal, Canada
University of Piraeus, Greece

Program Chairs

Sokratis Katsikas

Norwegian University of Science and Technology,
Norway

Frédéric Cuppens

Polytechnique Montréal, Canada

Publicity Chair

Vasileios Gkioulos

Norwegian University of Science and Technology,
Norway

Program Committee

Cristina Alcaraz
Marios Anagnostopoulos

University of Malaga, Spain
Norwegian University of Science and Technology,
Norway

Alvaro Cardenas
Mauro Conti
David Espes
Khan Ferdous Wahid
Joaquin Garcia-Alfaro
Vasileios Gkioulos

University of California Santa Cruz, USA
University of Padua, Italy
University of Brest, France
Airbus Group, France
Telecom SudParis, France
Norwegian University of Science and Technology,
Norway

Dieter Gollmann
Youssef Laarouchi
Masahiro Mambo
Michail Maniatakos
Sjouke Mauw
Weizhi Meng
Pankaj Pandey

Hamburg University of Technology, Germany
EDF R&D, France
Kanazawa University, Japan
NYU Abu Dhabi, UAE
University of Luxembourg, Luxembourg
Technical University of Denmark, Denmark
Norwegian University of Science and Technology,
Norway

Nikos Pitropakis
Indrakshi Ray
Rodrigo Roman
Ayed Samiha
Andrea Saracino

Edinburgh Napier University, UK
Colorado State University, USA
University of Malaga, Spain
Telecom Bretagne, France
Consiglio Nazionale delle Ricerche, Italy

Houbing Song	Embry-Riddle Aeronautical University, USA
Georgios Spathoulas	Norwegian University of Science and Technology, Norway
Qiang Tang	LIST, Luxembourg
Nils Ole Tippenhauer	CISPA, Germany
Stefano Zanero	Politecnico di Milano, Italy
Jianying Zhou	Singapore University of Technology and Design, Singapore

SECPRE 2020 Preface

This volume contains revised versions of the papers presented at the 4th International Workshop on SEcURITY and Privacy Requirements Engineering (SECPRE 2020), which was co-located with the 25th European Symposium on Research in Computer Security (ESORICS 2020), and held virtually in Surrey, UK on September 17, 2020.

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 last decades in various innovative research domains. Today Security by Design (SbD) and Privacy by Design (PbD) are established research areas that focus on these directions. The new GDPR regulation sets even stricter requirements for organizations regarding its applicability. SbD and PbD play a very critical and important role in assisting stakeholders in understanding their needs, complying with the new legal, organizational, and technical requirements, and finally selecting the appropriate measures for fulfilling these requirements. SECPRE aimed to provide researchers and professionals with the opportunity to present novel and cutting-edge research on these topics.

SECPRE 2020 attracted seven high-quality submissions, each of which was assigned to four referees for review; the review process resulted in four papers being selected for presentation and inclusion in these proceedings. The topics covered include: security and privacy requirements and GDPR compliance issues, security and privacy verification on Cyber-Physical Systems, security and privacy in ITS domain, as well as vulnerability analysis though goal 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 Committee for their timely and rigorous reviews. Thanks are also due to the Organizing Committee of the events. Last, but by no means least, we would like to thank all the authors who submitted their work to the workshop and contributed to an interesting set of proceedings.

October 2020

John Mylopoulos
Christos Kalloniatis
Annie Anton
Stefanos Gritzalis

SECPRE 2020 Organization

General Chairs

Annie Antón
Stefanos Gritzalis

Georgia Institute of Technology, USA
University of Piraeus, Greece

Program Chairs

John Mylopoulos
Christos Kalloniatis

University of Toronto, Canada
University of the Aegean, Greece

Program Committee

Frederic Cuppens
Sabrina De Capitani
di Vimercati
Vasiliki Diamantopoulou
Eric Dubois

Telecom Bretagne, France
Università degli Studi di Milano, Italy
University of the Aegean, Greece
Luxembourg Institute of Science and Technology,
Luxembourg

Carmen Fernandez-Gago
Eduardo Fernandez-Medina
Mohamad Gharib
Paolo Giorgini
Maritta Heisel
Jan Juerjens
Maria Karyda
Costas Lambrinoudakis
Tong Li
Fabio Martinelli
Aaron Massey
Haralambos Mouratidis
Liliana Pasquale
Michalis Pavlidis
David Garcia Rosado
Pierangela Samarati
Aggeliki Tsohou
Nicola Zannone

University of Malaga, Spain
University of Castilla-La Mancha, Spain
University of Florence, Italy
University of Trento, Italy
University of Duisburg-Essen, Germany
University of Koblenz-Landau, Germany
University of the Aegean, Greece
University of Piraeus, Greece
Beijing University of Technology, China
CNR, Italy
University of Maryland, USA
University of Brighton, UK
University College Dublin, Ireland
University of Brighton, UK
University of Castilla-La Manca, Spain
Università degli Studi di Milano, Italy
Ionian University, Greece
Eindhoven University of Technology, The Netherlands

ADIoT 2020 Preface

This volume contains the papers that were selected for presentation and publication at the Third International Workshop on Attacks and Defenses for Internet-of-Things (ADIoT 2020), which was held virtually online on September 18, 2020. The Internet of Things (IoT) technology is widely adopted by the vast majority of businesses and is impacting every aspect of the world. However, the nature of the Internet, communication, embedded OS, and backend recourses make IoT objects vulnerable to cyber attacks. In addition, most standard security solutions designed for enterprise systems are not applicable to IoT devices. As a result, we are facing a big IoT security and protection challenge, and it is urgent to analyze IoT-specific cyber attacks to design novel and efficient security mechanisms. This workshop focused on IoT attacks and defenses, and sought original submissions that discuss either practical or theoretical solutions to identify IoT vulnerabilities and IoT security mechanisms.

This year, 2 full papers and 2 short papers (extended abstract) out of 12 submissions were selected with an acceptance rate of 33.3%. All papers were reviewed by at least three members of the Program Committee. We would like to extend our thanks to the Program Committee members as well as the additional reviewers who contributed their precious time and expertise to provide professional reviews and feedback to authors in a timely manner. We would also like to express our thanks to all the authors who submitted papers to ADIoT 2020.

October 2020

Weizhi Meng
Steven Furnell

ADIoT 2020 Organization

Steering Committee

Steven Furnell	University of Nottingham, UK
Anthony T. S. Ho	University of Surrey, UK
Sokratis Katsikas	Norwegian University of Science and Technology, Norway
Weizhi Meng (Chair)	Technical University of Denmark, Denmark
Shouhuai Xu	The University of Texas at San Antonio, USA

General Chairs

Anthony T. S. Ho	University of Surrey, UK
Kuan-Ching Li	Providence University, China

Program Co-chairs

Weizhi Meng	Technical University of Denmark, Denmark
Steven Furnell	University of Nottingham, UK

Technical Program Committee

Claudio Ardagna	Università degli Studi di Milano, Italy
Ali Ismail Awad	Luleå University of Technology, Sweden
Alessandro Bruni	IT University of Copenhagen, Denmark
Chao Chen	Swinburne University of Technology, Australia
Nathan Clarke	University of Plymouth, UK
Georgios Kambourakis	University of the Aegean, Greece
Jianming Fu	Wuhan University, China
Linzhi Jiang	University of Surrey, UK
Javier Parra-Arnau	Universitat Rovira i Virgili, Spain
Wenjuan Li	Hong Kong Polytechnic University, China
Jiqiang Lu	Beihang University, China
Xiaobo Ma	Xi'an Jiaotong University, China
Reza Malekian	Malmö University, Sweden
Jianbing Ni	Queen's University, Canada
Meng Shen	Beijing Institute of Technology, China
Kar-Ann Toh	Yonsei University, South Korea
Ding Wang	Peking University, China
Lam Kwok Yan	Nanyang Technological University, Singapore
Xuyun Zhang	Macquarie University, Australia
Peng Zhou	Shanghai University, China

Contents

CyberICPS Workshop

Integrated Analysis of Safety and Security Hazards in Automotive Systems	3
<i>Rhea C. Rinaldo and Dieter Hutter</i>	
Attack Path Analysis for Cyber Physical Systems	19
<i>Georgios Kavallieratos and Sokratis Katsikas</i>	
Identifying and Analyzing Implicit Interactions in a Wastewater Dechlorination System	34
<i>Jason Jaskolka</i>	
A Survey of Cryptography-Based Authentication for Smart Grid Communication	52
<i>Nabin Chowdhury</i>	
Cybersecurity Awareness Platform with Virtual Coach and Automated Challenge Assessment	67
<i>Tiago Gasiba, Ulrike Lechner, Maria Pinto-Albuquerque, and Anmoal Porwal</i>	
IoT Vulnerability Scanning: A State of the Art	84
<i>Ahmed Amro</i>	
Learning from Vulnerabilities - Categorising, Understanding and Detecting Weaknesses in Industrial Control Systems	100
<i>Richard J. Thomas and Tom Chothia</i>	
Self Adaptive Privacy in Cloud Computing Environments: Identifying the Major Socio-Technical Concepts	117
<i>Angeliki Kitsiou, Eleni Tzortzaki, Christos Kalloniatis, and Stefanos Gritzalis</i>	

SECPRE Workshop

Definition and Verification of Security Configurations of Cyber-Physical Systems	135
<i>Ángel Jesús Varela-Vaca, David G. Rosado, Luis Enrique Sánchez, María Teresa Gómez-López, Rafael M. Gasca, and Eduardo Fernández-Medina</i>	

GDPR Compliance: Proposed Guidelines for Cloud-Based Health Organizations	156
<i>Dimitra Georgiou and Costas Lambrinoudakis</i>	
Aligning the Concepts of Risk, Security and Privacy Towards the Design of Secure Intelligent Transport Systems	170
<i>Vasiliki Diamantopoulou, Christos Kalloniatis, Christos Lyvas, Konstantinos Maliatsos, Matthieu Gay, Athanasios Kanatas, and Costas Lambrinoudakis</i>	
Identifying Implicit Vulnerabilities Through Personas as Goal Models	185
<i>Shamal Faily, Claudia Iacob, Raian Ali, and Duncan Ki-Aries</i>	
ADIoT Workshop	
Cooperative Speed Estimation of an RF Jammer in Wireless Vehicular Networks	205
<i>Dimitrios Kosmanos, Savvas Chatzisavvas, Antonios Argyriou, and Leandros Maglaras</i>	
Extended Abstract: Towards Physical-Layer Authentication for Backscatter Devices	224
<i>Thiemo Voigt, Carlos Pérez-Penichet, and Christian Rohner</i>	
P2Onto: Making Privacy Policies Transparent.	235
<i>Evgenia Novikova, Elena Doynikova, and Igor Kotenko</i>	
Extended Abstract - Transformers: Intrusion Detection Data in Disguise	253
<i>James Boorman, Benjamin Green, and Daniel Prince</i>	
Author Index	265