

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zurich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology Madras, Chennai, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

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

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

Computer Security

ESORICS 2018 International Workshops,
CyberICPS 2018 and SECPRE 2018
Barcelona, Spain, September 6–7, 2018
Revised Selected Papers

Editors

Sokratis K. Katsikas 
Norwegian University of Science and
Technology
Gjøvik, Norway

Frédéric Cuppens
IMT Atlantique
Cesson-Sévigné, France

Nora Cuppens
IMT Atlantique
Cesson-Sévigné, France

Costas Lambrinouidakis
University of Piraeus
Piraeus, Greece

Annie Antón
Georgia Institute of Technology
Atlanta, GA, USA

Stefanos Gritzalis
University of the Aegean
Karlovasi, Greece

John Mylopoulos
University of Toronto
Toronto, ON, Canada

Christos Kalloniatis 
University of the Aegean
Mytilene, Greece

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-12785-5 ISBN 978-3-030-12786-2 (eBook)
<https://doi.org/10.1007/978-3-030-12786-2>

Library of Congress Control Number: 2019930854

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2019

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, express 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

Preface

This book contains revised versions of the papers presented at the Fourth Workshop on the Security of Industrial Control Systems and Cyber-Physical Systems (CyberICPS 2018), and the Second International Workshop on Security and Privacy Requirements Engineering (SECPRE 2018). Both workshops were co-located with the 23rd European Symposium on Research in Computer Security (ESORICS 2018) and were held in Barcelona, Spain, during September 6–7, 2018.

CyberICPS aims to bring together researchers, engineers, and government 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 their cyber-security. Cyber-physical systems range in size, complexity, and criticality, from embedded systems used in smart vehicles, to SCADA and industrial control systems such as energy and water distribution systems, smart transportation systems, etc.

CyberICPS 2018 attracted 15 high-quality submissions, each of which was assigned to three referees for review; the review process resulted in accepting eight full papers 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 adhoc 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 in various innovative research domains. 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 2018 attracted 11 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 of 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 2018

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

Organization

Fourth Workshop on the Security of Industrial Control Systems and of Cyber-Physical Systems (CyberICPS 2018)

General Chairs

Sokratis K. Katsikas	Center for Cyber and Information Security, Norwegian University of Science and Technology, Norway and Open University of Cyprus, Cyprus
Frédéric Cuppens	IMT Atlantique, Cybersecurity and Digital Law, France

Program Committee Co-chairs

Nora Cuppens	IMT Atlantique, Cybersecurity and Digital Law, France
Costas Lambrinoudakis	University of Piraeus, Greece

International Program Committee

Alcaraz Cristina	University of Malaga, Spain
Ayed Samiha	IMT-Telecom Bretagne, France
Conti Mauro	University of Padua, Italy
Espes David	University of Brest, France
Garcia-Alfaro Joaquin	Telecom SudParis, France
Gkioulos Vasileios	Norwegian University of Science and Technology, Norway
Gollmann Dieter	Hamburg University of Technology, Germany
Laarouchi Youssef	EDF R&D, France
Mambo Masahiro	Kanazawa University, Japan
Mauw Sjouke	University of Luxembourg, Luxembourg
Meng Weizhi	Institute for Infocomm Research, Singapore
Mitchell Chris	Royal Holloway, University of London, UK
Pandey Pankaj	Norwegian University of Science and Technology, Norway
Roudier Yves	EURECOM, France
Song Houbling	Embry-Riddle Aeronautical University, USA
Spathoulas Georgios	University of Thessaly, Greece
State Radu	University of Luxembourg, Luxembourg
Wahid Khan Ferdous	Airbus Defence and Space GmbH, Germany
Yaich Reda	IRT SystemX, France
Zanero Stefano	Politecnico di Milano, Italy

Second International Workshop on Security and Privacy Requirements Engineering (SECPRE 2018)

General Chairs

Annie Antón	Georgia Institute of Technology, College of Computing, School of Interactive Computing, USA
Stefanos Gritzalis	University of the Aegean, School of Engineering, Greece

Program Committee Co-chairs

John Mylopoulos	University of Toronto, Department of Computer Science, Canada
Christos Kalloniatis	University of the Aegean, School of Social Sciences, Greece

International Program Committee

Cuppens Frederic	Telecom Bretagne, France
De Capitani di Vimercati Sabrina	Università degli Studi di Milano, Italy
Dimitrakos Theo	University of Kent, UK
Dubois Eric	Luxembourg Institute of Science and Technology, Luxembourg
Fernandez-Gago Carmen	University of Malaga, Spain
Fernandez-Medina Eduardo	University of Castilla-La Mancha, Spain
Gharib Mohamad	University of Florence, Italy
Giorgini Paolo	University of Trento, Italy
Heisel Maritta	University of Duisburg-Essen, Germany
Juerjens Jan	University of Koblenz-Landau, Germany
Lambrinoudakis Costas	University of Pireus, Greece
Li Tong	Beijing University of Technology, China
Martinelli Fabio	National Research Council, CNR, Italy
Massey Aaron	University of Maryland, USA
Mouratidis Haralambos	University of Brighton, UK
Pavlidis Michalis	University of Brighton, UK
Rosado David Garcia	University of Castilla-La Manca, Spain
Salnitri Mattia	University of Trento, Italy
Samarati Pierangela	Università degli Studi di Milano, Italy
Staddon Jessica	North Carolina State University, USA
Zannone Nicola	Eindhoven University of Technology, The Netherlands

Contents

Security of Industrial Control Systems and Cyber-Physical Systems (CyberICPS 2018)

Improving SIEM for Critical SCADA Water Infrastructures Using Machine Learning	3
<i>Hanan Hindy, David Brosset, Ethan Bayne, Amar Seeam, and Xavier Bellekens</i>	
Cyber-Attacks Against the Autonomous Ship	20
<i>Georgios Kavallieratos, Sokratis Katsikas, and Vasileios Gkioulos</i>	
EPIC: An Electric Power Testbed for Research and Training in Cyber Physical Systems Security	37
<i>Sridhar Adepu, Nandha Kumar Kandasamy, and Aditya Mathur</i>	
A Hardware Based Solution for Freshness of Secure Onboard Communication in Vehicles	53
<i>Sigrid Gürgens and Daniel Zelle</i>	
Enhancing Usage Control for Performance: An Architecture for Systems of Systems	69
<i>Vasileios Gkioulos, Athanasios Rizos, Christina Michailidou, Paolo Mori, and Andrea Saracino</i>	
Comparative Study of Machine Learning Methods for In-Vehicle Intrusion Detection	85
<i>Ivo Berger, Roland Rieke, Maxim Kolomeets, Andrey Chechulin, and Igor Kotenko</i>	
SDN-Enabled Virtual Data Diode	102
<i>Miguel Borges de Freitas, Luis Rosa, Tiago Cruz, and Paulo Simões</i>	
Realistic Data Generation for Anomaly Detection in Industrial Settings Using Simulations	119
<i>Peter Schneider and Alexander Giehl</i>	

Security and Privacy Requirements Engineering (SECPRE 2018)

Sealed Computation: Abstract Requirements for Mechanisms to Support Trustworthy Cloud Computing	137
<i>Lamya Abdullah, Felix Freiling, Juan Quintero, and Zinaida Benenson</i>	

Understanding Challenges to Adoption of the Protection Poker Software Security Game	153
<i>Inger Anne Tøndel, Martin Gilje Jaatun, Daniela Cruzes, and Tosin Daniel Oyetoyan</i>	
An Experimental Evaluation of Bow-Tie Analysis for Cybersecurity Requirements	173
<i>Per Håkon Meland, Karin Bernsmed, Christian Frøystad, Jingyue Li, and Guttorm Sindre</i>	
Towards General Scheme for Data Sharing Agreements Empowering Privacy-Preserving Data Analysis of Structured CTI	192
<i>Fabio Martinelli, Oleksii Osliak, and Andrea Saracino</i>	
Run-Time Monitoring of Data-Handling Violations	213
<i>Jassim Happa, Nick Moffat, Michael Goldsmith, and Sadie Creese</i>	
Author Index	233