

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, 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

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

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

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

Computer Security

ESORICS 2017 International Workshops
CyberICPS 2017 and SECPRE 2017
Oslo, Norway, September 14–15, 2017
Revised Selected Papers


Editors

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

Frédéric Cuppens
IMT Atlantique
Brest
France

Nora Cuppens
IMT Atlantique
Brest
France

Costas Lambrinouidakis
University of Piraeus
Piraeus
Greece

Christos Kalloniatis 
University of the Aegean
Mytilene
Greece

John Mylopoulos
University of Toronto
Toronto, ON
Canada

Annie Antón
Georgia Institute of Technology
Atlanta, GA
USA

Stefanos Gritzalis
University of the Aegean
Karlovassi
Greece

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-72816-2 ISBN 978-3-319-72817-9 (eBook)
<https://doi.org/10.1007/978-3-319-72817-9>

Library of Congress Control Number: 2017962874

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 2018, corrected publication 2018

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.

Printed on acid-free paper

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



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

Organization

CyberICPS 2017 General Chairs

Nora Cuppens	IMT Atlantique, France
Costas Lambrinoudakis	University of Piraeus, Greece

CyberICPS 2017 Program Committee Chairs

Sokratis K. Katsikas	Norwegian University of Science and Technology - NTNU, Norway; and University of Piraeus, Greece
Frédéric Cuppens	IMT Atlantique, France

CyberICPS 2017 Technical Program Committee

Cristina Alcaraz	University of Malaga, Spain
Samiha Ayed	Devoteam, France
Mauro Conti	University of Padua, Italy
Mourad Debbabi	Concordia University, Canada
Hervé Debar	Telecom SudParis, France
David Espes	University of Brest, France
Joaquin Garcia-Alfaro	Telecom SudParis, France
Dieter Gollmann	Technical University of Hamburg, Germany
Wael Kanoun	Nokia, France
Jean Leneutre	Telecom ParisTech, France
Javier Lopez	University of Malaga, Spain
Masahiro Mambo	Kanazawa University, Japan
Sjouke Mauw	University of Luxembourg, Luxembourg
Weizhi Meng	Institute for Infocomm Research, Singapore
Chris Mitchell	Royal Holloway, UK
Jonathan Petit	Security Innovation, USA
Juha Rönning	University of Oulu, Finland
Yves Roudier	EURECOM, France
Pierangela Samarati	Università degli Studi di Milano, Italy
Radu State	University of Luxembourg, Luxembourg
Houbling Song	West Virginia University, USA
Craig Valli	Edith Cowan University, Australia
Jozef Vyskoc	VAF, Slovakia
Khan Ferdous Wahid	Airbus Defence and Space GmbH, Germany
Stephen Wolthusen	Royal Holloway, UK
Stefano Zanero	Politecnico di Milano, Italy

CyberICPS 2017 Additional Reviewers

Abbas Acar
 Saed Alrabae
 Nathan Clarke
 Pallavi Kaliyar
 Marcello Pogliani
 Mario Polino
 Sarada Prasad
 Davide Quarta
 Paria Shirani

SECPRE 2017 General Chairs

Annie Antón	Georgia Institute of Technology, USA
Stefanos Gritzalis	University of the Aegean, Greece

SECPRE 2017 Program Committee Chairs

John Mylopoulos	University of Toronto, Canada
Christos Kalloniatis	University of the Aegean, Greece

SECPRE 2017 Technical Program Committee

Travis Breaux	Carnegie Mellon University, USA
Frédéric Cuppens	Telecom Bretagne, France
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Theo Dimitrakos	University of Kent, UK
Mohamad Gharib	University of Florence, Italy
Paolo Giorgini	University of Trento, Italy
Maritta Heisel	University of Duisburg-Essen, Germany
Jan Juerjens	University of Koblenz-Landau, Germany
Costas Lambrinoudakis	University of Piraeus, Greece
Tong Li	Beijing University of Technology, China
Javier Lopez	University of Malaga, Spain
Fabio Martinelli	National Research Council, C.N.R., Italy
Aaron Massey	University of Maryland, USA
Haralambos Mouratidis	University of Brighton, UK
Liliana Pasquale	University College Dublin, Ireland
Michalis Pavlidis	University of Brighton, UK
David Garcia Rosado	University of Castilla-La Mancha, Spain
Mattia Salnitri	University of Trento, Italy
Pierangela Samarati	Università degli Studi di Milano, Italy
Nicola Zannone	Eindhoven University of Technology, The Netherlands

SECPRE 2017 Additional Reviewers

Francesco Mercaldo
Mina Sheikhalishahi

Contents

Protecting Industrial Control and Cyber-Physical Systems

Towards End-to-End Data Protection in Low-Power Networks	3
<i>Vasily Mikhalev, Laurent Gomez, Frederik Armknecht, and José Márquez</i>	
Development of an Embedded Platform for Secure CPS Services	19
<i>Vincent Raes, Jan Vossaert, and Vincent Naessens</i>	
Introducing Usage Control in MQTT.	35
<i>Antonio La Marra, Fabio Martinelli, Paolo Mori, Athanasios Rizos, and Andrea Saracino</i>	

Threats, Vulnerabilities and Risks

Towards Security Threats that Matter	47
<i>Katja Tuma, Riccardo Scandariato, Mathias Widman, and Christian Sandberg</i>	
A Methodology to Assess Vulnerabilities and Countermeasures Impact on the Missions of a Naval System.	63
<i>Bastien Sultan, Fabien Dagnat, and Caroline Fontaine</i>	
STRIDE to a Secure Smart Grid in a Hybrid Cloud	77
<i>Bojan Jelacic, Daniela Rosic, Imre Lendak, Marina Stanojevic, and Sebastijan Stoja</i>	

Cyber Attacks in Industrial Control and Cyber-Physical Systems

Stealthy Deception Attacks Against SCADA Systems	93
<i>Amit Kleinmann, Ori Amichay, Avishai Wool, David Tenenbaum, Ofer Bar, and Leonid Lev</i>	
On Ladder Logic Bombs in Industrial Control Systems	110
<i>Naman Govil, Anand Agrawal, and Nils Ole Tippenhauer</i>	
Enforcing Memory Safety in Cyber-Physical Systems	127
<i>Eyasu Getahun Chekole, John Henry Castellanos, Martín Ochoa, and David K. Y. Yau</i>	

Detecting Attacks in Industrial Control and Cyber-Physical Systems

Supporting the Human in Cyber Defence	147
<i>Kirsi Helkala, Benjamin J. Knox, Øyvind Jøsok, Ricardo G. Lugo, Stefan Sütterlin, Geir Olav Dyrkolbotn, and Nils Kalstad Svendsen</i>	
CRBP-OpType: A Constrained Approximate Search Algorithm for Detecting Similar Attack Patterns	163
<i>Ambika Shrestha Chitrakar and Slobodan Petrović</i>	
Multistage Downstream Attack Detection in a Cyber Physical System	177
<i>Rizwan Qadeer, Carlos Murguia, Chuadhry Mujeeb Ahmed, and Justin Ruths</i>	

Security and Privacy Requirements Assurance and Evaluation

A UML Profile for Privacy-Aware Data Lifecycle Models	189
<i>Majed Alshammari and Andrew Simpson</i>	
Evaluation of a Security and Privacy Requirements Methodology Using the Physics of Notation	210
<i>Vasiliki Diamantopoulou, Michalis Pavlidis, and Haralambos Mouratidis</i>	

Security Requirements Elicitation and Modelling

What Users Want: Adapting Qualitative Research Methods to Security Policy Elicitation.	229
<i>Vivien M. Rooney and Simon N. Foley</i>	
An Anti-pattern for Misuse Cases	250
<i>Mohammad Torabi Dashti and Saša Radomirović</i>	
Decision-Making in Security Requirements Engineering with Constrained Goal Models.	262
<i>Nikolaos Argyropoulos, Konstantinos Angelopoulos, Haralambos Mouratidis, and Andrew Fish</i>	
Erratum to: Enforcing Memory Safety in Cyber-Physical Systems.	E1
<i>Eyasu Getahun Chekole, John Henry Castellanos, Martín Ochoa, and David K. Y. Yau</i>	

Author Index	281
-------------------------------	-----