

Advanced Sciences and Technologies for Security Applications

Cristina Alcaraz *Editor*

Security and Privacy Trends in the Industrial Internet of Things

 Springer

Advanced Sciences and Technologies for Security Applications

Series editor

Anthony J. Masys, Associate Professor, Director of Global Disaster Management, Humanitarian Assistance and Homeland Security, University of South Florida, Tampa, USA

Advisory Board

Gisela Bichler, California State University, San Bernardino, CA, USA

Thirimachos Bourlai, WVU - Statler College of Engineering and Mineral Resources, Morgantown, WV, USA

Chris Johnson, University of Glasgow, UK

Panagiotis Karampelas, Hellenic Air Force Academy, Attica, Greece

Christian Leuprecht, Royal Military College of Canada, Kingston, ON, Canada

Edward C. Morse, University of California, Berkeley, CA, USA

David Skillicorn, Queen's University, Kingston, ON, Canada

Yoshiki Yamagata, National Institute for Environmental Studies, Tsukuba, Japan

The series *Advanced Sciences and Technologies for Security Applications* comprises interdisciplinary research covering the theory, foundations and domain-specific topics pertaining to security. Publications within the series are peer-reviewed monographs and edited works in the areas of:

- biological and chemical threat recognition and detection (e.g., biosensors, aerosols, forensics)
- crisis and disaster management
- terrorism
- cyber security and secure information systems (e.g., encryption, optical and photonic systems)
- traditional and non-traditional security
- energy, food and resource security
- economic security and securitization (including associated infrastructures)
- transnational crime
- human security and health security
- social, political and psychological aspects of security
- recognition and identification (e.g., optical imaging, biometrics, authentication and verification)
- smart surveillance systems
- applications of theoretical frameworks and methodologies (e.g., grounded theory, complexity, network sciences, modelling and simulation)

Together, the high-quality contributions to this series provide a cross-disciplinary overview of forefront research endeavours aiming to make the world a safer place.

The editors encourage prospective authors to correspond with them in advance of submitting a manuscript. Submission of manuscripts should be made to the Editor-in-Chief or one of the Editors.

More information about this series at <http://www.springer.com/series/5540>

Cristina Alcaraz
Editor

Security and Privacy Trends in the Industrial Internet of Things



 Springer

Editor

Cristina Alcaraz
Computer Science Department
University of Malaga
Malaga, Spain

ISSN 1613-5113

ISSN 2363-9466 (electronic)

Advanced Sciences and Technologies for Security Applications

ISBN 978-3-030-12329-1

ISBN 978-3-030-12330-7 (eBook)

<https://doi.org/10.1007/978-3-030-12330-7>

© 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

We are increasingly witnessing how the industry in general is modernizing its underlying critical systems to move toward the fourth industrial revolution, commonly known as Industry 4.0. This new industrial paradigm encompasses, among others, the Industrial Internet of Things (IIoT) as one of the most relevant technologies of the today's industry. Through IIoT, it is possible to open the industrial connections to address effective and more extensive controls, allowing monitoring from anywhere, at any time, and in anyhow, and in this way to increase the effectiveness and reliability of production states, reduce operational costs, and improve the overall market economy.

Although there exist already consortiums and bodies working on the deployment of this technology, there are also diverse entities (academy, governments, international organizations, and industries) working on many aspects related to security and privacy. Particularly, certain interest issues deserve to be considered in their own right. For example, the hardware and software limitations of the vast majority of the IIoT devices do not help provide complex and robust security approaches; and the current predominance to lead advanced persistent attacks in the diverse industrial sectors brings about numerous security risks. There exists a special attraction to track and exploit zero-day vulnerabilities in order to proceed with potential attacks related to information exfiltration, data manipulation, false data injection, or end users' privacy violation. In addition to this, the incorporation of IIoT-related technologies in Industry 4.0 does not help avoid these types of risks. Cyber-physical systems, cloud/fog computing, big data, digital twins, and the diverse emergent technologies that need to collaborate each other for the convergence IT (information technologies) – OT (operational technologies) certainly add new security and privacy risks that should widely be considered from the security point of view.

Therefore, the present volume highlights all these issues from the beginning, showing the current research challenges and ongoing work lines, with an eye toward keeping the operability of the underlying critical systems and their monitoring infrastructures. Diverse standpoints are addressed, capturing a theoretical analysis of the current situation and the benefits and drawbacks that the IIoT technology

itself can bring to the operational processes. Part of these analyses likewise involves the provision of lightweight approaches based on cryptographic algorithms, access control, anomaly detection, intrusion detection methodologies, or remote attestation algorithms. But beyond this, privacy techniques are also addressed in this book to evaluate the impact of the problem and its occurrence in determined critical environments such as smart health ecosystems. In counterpart to the theoretical procedures, practical researches in the IIoT security field are equally keys to demonstrate the validity of the approaches and their applications in critical scenarios. In this case, the design of IIoT-based testbeds and their influence on research procedures undoubtedly constitute a fundamental part to consolidate the new security and privacy trends on IIoT and its real application.

This book can therefore serve as a timely introduction to the state of the art of the technology of IIoT, trying to aid researchers to gain an overview of a field that is still largely unexplored, industries interested in modernizing their infrastructures from a secure perspective, and lecturers wishing to prepare future Industry 4.0 experts with solid criterion and contents.

Malaga, Spain
December 2018

Cristina Alcaraz

Contents

Part I Security Analysis and Advanced Threats

Securing Industrial Control Systems	3
Marina Krotofil, Klaus Kursawe, and Dieter Gollmann	
Towards a Secure Industrial Internet of Things	29
Georgios Spathoulas and Sokratis Katsikas	
Advanced Persistent Threats and Zero-Day Exploits in Industrial Internet of Things	47
Ioannis Stelios, Panayiotis Kotzanikolaou, and Mihalis Psarakis	

Part II Secure Interconnection Mechanisms

A Survey on Lightweight Authenticated Encryption and Challenges for Securing Industrial IoT	71
Megha Agrawal, Jianying Zhou, and Donghoon Chang	
Access Control in the Industrial Internet of Things	95
Stavros Salonikias, Antonios Gouglidis, Ioannis Mavridis, and Dimitris Gritzalis	
A Distributed Usage Control Framework for Industrial Internet of Things	115
Antonio La Marra, Fabio Martinelli, Paolo Mori, and Andrea Saracino	

Part III Advanced Protection Techniques

Profiling Communications in Industrial IP Networks: Model Complexity and Anomaly Detection	139
Mustafa Amir Faisal, Alvaro A. Cardenas, and Avishai Wool	
Improving Security in Industrial Internet of Things: A Distributed Intrusion Detection Methodology	161
Giuseppe Bernieri and Federica Pascucci	

Who's There? Evaluating Data Source Integrity and Veracity in IIoT Using Multivariate Statistical Process Control	181
Iñaki Garitano, Mikel Iturbe, Enaitz Ezpeleta, and Urko Zurutuza	
Secure Machine to Machine Communication in Industrial Internet of Things	199
Mauro Conti, Pallavi Kaliyar, and Chhagan Lal	
Part IV Privacy Issues in Industrial Connected Networks	
Modelling the Privacy Impact of External Knowledge for Sensor Data in the Industrial Internet of Things	223
Salaheddin Darwish, Ilia Nouretdinov, and Stephen Wolthusen	
Security and Privacy Techniques for the Industrial Internet of Things....	245
Yuexin Zhang and Xinyi Huang	
Part V Application Scenarios	
IIoT in the Hospital Scenario: Hospital 4.0, Blockchain and Robust Data Management	271
Luca Faramondi, Gabriele Oliva, Roberto Setola, and Luca Vollero	
Design and Realization of Testbeds for Security Research in the Industrial Internet of Things	287
Nils Ole Tippenhauer	

Advanced Sciences and Technology

Cristina Alcaraz *Editor*

Security and Privacy Threats

Biblioteka Główna
Akademii Sztuki Wojennej

26668/III (CB)



03-026668-000-0

This book, written by leaders in the field, provides an extended overview of the technological and operative advantages together with the security problems and challenges of the new paradigm of the Internet of Things in today's industry, also known as the Industry Internet of Things (IIoT).

The incorporation of the new embedded technologies and the interconnected networking advances in the automation and monitoring processes, certainly multiplies the functional complexities of the underlying control system, whilst increasing security and privacy risks. The critical nature of the application context and its relevance for the well-being of citizens and their economy, attracts the attention of multiple, advanced attackers, with stealthy abilities to evade security policies, ex-filter information or exploit vulnerabilities. Some real-life events and registers in CERTs have already clearly demonstrated how the control industry can become vulnerable to multiple types of advanced threats whose focus consists in hitting the safety and security of the control processes.

This book, therefore, comprises a detailed spectrum of research papers with highly analytical content and actuation procedures to cover the relevant security and privacy issues such as data protection, awareness, response and resilience, all of them working at optimal times. Readers will be able to comprehend the construction problems of the fourth industrial revolution and are introduced to effective, lightweight protection solutions which can be integrated as part of the new IIoT-based monitoring ecosystem.

ISBN 978-3-030-12329-1

9 783030 123291

► [springer.com](https://www.springer.com)

