

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>

Apostolos P. Fournaris
Konstantinos Lampropoulos
Eva Marín Tordera (Eds.)

Information and Operational Technology Security Systems

First International Workshop, IOSec 2018, CIPSEC Project
Heraklion, Crete, Greece, September 13, 2018
Revised Selected Papers

Editors

Apostolos P. Fournaris
University of Patras
Patras, Greece

Konstantinos Lampropoulos
University of Patras
Patras, Greece

Eva Marín Tordera
Advanced Network Architectures Lab
Barcelona, Spain

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-12084-9 ISBN 978-3-030-12085-6 (eBook)
<https://doi.org/10.1007/978-3-030-12085-6>

Library of Congress Control Number: 2018968327

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

In the modern era most companies, enterprises, public services etc. use the recent ICT (information and communication technology) advances to become more flexible, lower their operational costs, and promote their products and services. In terms of infrastructure, this evolution has introduced new types of networks, systems, and architectures, which in many cases derive from the interconnection of new and legacy technologies. Especially for industrial systems like critical infrastructures (CIs), which until recently mainly used operational technologies (OT; automation-based, control-based systems) the recent advances of ICT have given them the ability to offer new and innovative services, improve their management procedures, lower their maintenance costs, and create new business opportunities. However, this adaptation of new technologies was made rather quickly without proper evaluation of its impact on security, exposing these systems (industrial systems and CIs) to various new kinds of cyberattacks.

Industrial systems and CIs have very specific requirements (e.g., high responsiveness, real-time monitoring, specialized hardware, low computational capabilities etc.). These requirements make the process of integrating new technologies and components more complicated compared with other domains. In particular, the adaptation of new cybersecurity products may impose additional delays on the system's performance, power consumption, complexity etc. Such products may also require additional components, thus increasing the complexity of the overall system and its maintenance costs. On the other hand, the absence of cybersecurity countermeasures in sensitive systems like industrial systems or CIs can lead to devastating damage with significant impact on public safety and welfare. In view of these issues, the research community must further work on addressing the cybersecurity issues that emerge from the ongoing integration between IT and OT systems. There is a need to model IT/OT system assets, identify possible cybersecurity vulnerabilities, and provide prevention, detection, response, and mitigation security strategies/policies.

The International Workshop on Information & Operational Technology (IT & OT) Security Systems (IOSEC) aims to bring together viewpoints from diverse areas to explore the commonalities of security problems and solutions for advancing the collective science and practice of IT and OT security protection. In 2018, the workshop took place in September in collocation with the RAID 2018 conference and had input from various security research fields that can be applicable in the IT/OT security strengthening. The workshop lasted one full day, had 22 submitted papers, of which 12 were accepted, thus achieving an acceptance rate of $\sim 54\%$.

This book presents the research outcomes of the IOSEC 2018 Workshop by including extended versions of all the scientific works that were presented during the workshop. IOSEC 2018 was sponsored by the CIPSEC European Union Innovation action project "Enhancing Critical Infrastructure Protection with innovative Security framework" that develops a cybersecurity framework for critical infrastructure systems.

This framework, apart from technical security tools, is also introducing a wide set of cybersecurity services (vulnerability tests and recommendations, key personnel training courses, public–private partnerships [PPPs] forensics analysis, standardization, and protection against cascading effects) making the CIPSEC solution a complete security ecosystem for critical infrastructure protection.

This book is divided into three sections, each one focused on the cybersecurity research problems of specific IT/OT environments. Since the CI domain constitutes the best example of where the IT/OT ecosystems interconnect and cybersecurity failures have the highest impact on society and public welfare, the first section of this book is specifically dedicated to this domain. In this section, there are four chapters where authors discuss and propose solutions on: how to achieve unclonable identities of security designs (based on hardware), how to introduce efficient and secure access control mechanisms on file systems, how to protect the cloud level that may exist in various critical infrastructure systems by pointing to their vulnerabilities, and finally how to detect attacks on CAN messages (a typical communication protocol on OT systems) using heuristics and neural networks.

The second section is focused on more generic concepts of IT/OT cybersecurity including cybersecurity threat modeling, vulnerability assessment based on questionnaires, and techniques in order to address privacy issues of IT/OT systems employees social network identities and interests.

Finally, the third section of this book is dedicated to malware threats in IT/OT systems. Malicious software is a very important problem in such systems and recently it has found fertile ground in OT systems since the latter were not originally designed for security (but mostly for safety). The authors of this section propose solutions on how to detect software vulnerabilities that can be used by malware as well as solutions on how to detect malwares in IT and OT environments. More specifically, this section describes mechanisms for automatic patching application software after detecting possible exploitable vulnerabilities, clustering of malware based on called API during runtime, malware context searching mechanisms for specific malware collections, and finally a cloud-focused anti-malware engine using graphic processing unit accelerated network monitoring.

We would like to thank all the people who contributed to the realization of the IOSEC 2018 Workshop, the RAID Organizing Committee that took care of all the local arrangements, the IOSEC Program Committee and reviewers who helped us with the review process, and finally Springer for aiding us with the post-conference proceedings publication.

December 2018

Konstantinos Lampropoulos
Apostolos P. Fournaris
Eva Marín Tordera

Organization

General Chairs

Kostas Lampropoulos	University of Patras, Greece
Eva Marín Tordera	Universitat Politècnica de Catalunya, Spain

Publication and Publicity Chair

Apostolos P. Fournaris	University of Patras, Greece
------------------------	------------------------------

Technical Program Committee

Antonio Álvarez	Atos, Spain
Rodrigo Díaz	Atos, Spain
Apostolos P. Fournaris	University of Patras, Greece
Odysseas Koufopavlou	University of Patras, Greece
Xavi Masip	Universitat Politècnica de Catalunya, Spain
Stefan Katzenbeisser	Technical University of Darmstadt, Germany
Neeraj Suri	Technical University of Darmstadt, Germany
Sotiris Ioannidis	Foundation for Research and Technology – Hellas, Greece
Christos Papachristos	Foundation for Research and Technology – Hellas, Greece
Vassilis Prevelakis	TU Braunschweig, Germany
Samuel Fricker	FHNW Fachhochschule Nordwestschweiz, Switzerland
Elias Athanasopoulos	University of Cyprus, Cyprus
Sharon Keidar-Barner	IBM Israel
Marco Spruit	Universiteit Utrecht, The Netherlands
Ciprian Oprisa	Bitdefender, Romania
Spyros Denazis	University of Patras, Greece
Dimitrios Serpanos	ISI/ATHENA, University of Patras, Greece
Nicolas Sklavos	University of Patras, Greece
Paris Kitsos	Technological Educational Institute of Western Greece

Sponsor



EU Horizon 2020 project CIPSEC
Enhancing Critical Infrastructure Protection with innovative
SECurity framework

Contents

Critical Infrastructure Cybersecurity Issues

A Cipher Class Based on Golden S-Boxes for Creating Clone-Resistant Identities	3
<i>Saleh Mulhem, Ayoub Mars, and Wael Adi</i>	
A Secure and Efficient File System Access Control Mechanism (FlexFS). . . .	15
<i>Jihane Najar and Vassilis Prevelakis</i>	
Protecting Cloud-Based CIs: Covert Channel Vulnerabilities at the Resource Level	27
<i>Tsvetoslava Vateva-Gurova, Salman Manzoor, Ruben Trapero, and Neeraj Suri</i>	
Detecting In-vehicle CAN Message Attacks Using Heuristics and RNNs	39
<i>Shahroz Tariq, Sangyup Lee, Huy Kang Kim, and Simon S. Woo</i>	

CyberSecurity Threats, Assessment and Privacy

A Questionnaire Model for Cybersecurity Maturity Assessment of Critical Infrastructures	49
<i>Bilge Yigit Ozkan and Marco Spruit</i>	
Threat Modeling the Cloud: An Ontology Based Approach	61
<i>Salman Manzoor, Tsvetoslava Vateva-Gurova, Ruben Trapero, and Neeraj Suri</i>	
Automated Measurements of Cross-Device Tracking	73
<i>Konstantinos Solomos, Panagiotis Ilia, Sotiris Ioannidis, and Nicolas Kourtellis</i>	
Incognitus: Privacy-Preserving User Interests in Online Social Networks	81
<i>Alexandros Kornilakis, Panagiotis Papadopoulos, and Evangelos Markatos</i>	

Vulnerability and Malware Detection

Deep Ahead-of-Threat Virtual Patching	99
<i>Fady Copt, Andre Kassis, Sharon Keidar-Barner, and Dov Murik</i>	
Malware Clustering Based on Called API During Runtime.	110
<i>Gergő János Széles and Adrian Coleșa</i>	

CloudNet Anti-malware Engine: GPU-Accelerated Network Monitoring for Cloud Services	122
<i>George Hatzivasilis, Konstantinos Fysarakis, Ioannis Askoxylakis, and Alexander Bilanakos</i>	
Full Content Search in Malware Collections	134
<i>Andrei Mihalca and Ciprian Oprea</i>	
Author Index	147