

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>

Habtamu Abie · Silvio Ranise ·
Luca Verderame · Enrico Cambiaso ·
Rita Ugarelli · Gabriele Giunta ·
Isabel Praça · Federica Battisti (Eds.)

Cyber-Physical Security for Critical Infrastructures Protection

First International Workshop, CPS4CIP 2020
Guildford, UK, September 18, 2020
Revised Selected Papers

Editors

Habtamu Abie 

Norwegian Computing Center
Oslo, Norway

Luca Verderame 

Università degli Studi di Genova
Genoa, Italy

Rita Ugarelli 

SINTEF A.S.
Oslo, Norway

Isabel Praça 

Instituto Superior de Engenharia do Porto
Porto, Portugal

Silvio Ranise 

University of Trento and Fondazione
Bruno Kessler
Trento, Italy

Enrico Cambiaso 

IEIIT Institute
Consiglio Nazionale delle Ricerche (CNR)
Genoa, Italy

Gabriele Giunta

Engineering Ingegneria Informatica S.p.A.
Rome, Italy

Federica Battisti 

University of Padua
Padua, Italy

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-030-69780-8

ISBN 978-3-030-69781-5 (eBook)

<https://doi.org/10.1007/978-3-030-69781-5>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2021

Chapters 5, 6, 10, 11, 13 and 14 are licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>). For further details see license information in the chapters.

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

Preface

CPS4CIP 2020 is a forum for researchers and practitioners working on cyber-physical security for critical infrastructures protection that supports finance, energy, health, air transport, communication, gas, and water. The secure operation of critical infrastructures is essential to the security of nations and, in an increasingly interconnected world, of unions of states sharing their infrastructures in order to develop their economies, and to public health and safety. Security incidents in critical infrastructures can directly lead to a violation of users' safety and privacy, physical damage, interference in the political and social life of citizens, significant economic impact on individuals and companies, and threats to human life while decreasing trust in institutions and questioning their social value. Because of the increasing interconnection between the digital and physical worlds, these infrastructures and services are more critical, sophisticated, and interdependent than ever before. The increased complexity makes each infrastructure increasingly vulnerable to attacks, as confirmed by the steady rise of cyber-security incidents, such as phishing or ransomware, and cyber-physical incidents, such as physical violation of devices or facilities in conjunction with malicious cyber activities. To make the situation even worse, interdependency may give rise to a domino effect with catastrophic consequences on multiple infrastructures.

To address these challenges, the workshop aimed to bring together security researchers and practitioners from the various verticals of critical infrastructures (such as the financial, energy, health, air transport, communication, gas, and water domains) and rethink cyber-physical security in the light of the latest technological developments (e.g., Cloud Computing, Blockchain, Big Data, AI, Internet-of-Things) by developing novel and effective approaches to increase the resilience of critical infrastructures and the related ecosystems of services.

The workshop attracted the attention of the critical infrastructures protection research communities and stimulated new insights and advances with particular attention to the integrated cyber and physical aspects of security in critical infrastructures. The first International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2020) was held online. The workshop was organized in conjunction with the 25th European Symposium on Research in Computer Security (ESORICS 2020), Guildford, the United Kingdom on 14–18 September 2020. The format of the workshop included two keynotes and technical presentations. The workshop was attended by around 28 people on average.

The workshop received 24 submissions, of which one was withdrawn and 23 were sent for reviews, from authors in 15 distinct countries. After a thorough peer-review process, 14 papers were selected for presentation at the workshop. The review process focused on the quality of the papers, their scientific novelty, and their applicability to the protection of critical financial infrastructure and services, and the acceptance rate was 58%. The accepted articles represent an interesting mix of techniques for security threat intelligence, data anomaly detection (predict and prevent), computer vision and

datasets for security, security management and governance, and impact propagation and power traffic analysis. The workshop was proactive with two important and stimulating keynotes in the areas of “Digital twins in industrial ecosystems: challenges, security issues, and countermeasures”, and “Cyber-physical security in automotive: the new challenge for smart cities”.

The workshop was supported by projects of the ECSCI (European Cluster for Securing Critical Infrastructures) cluster (<https://bit.ly/35YKnyE>), mainly FINSEC (www.finsec-project.eu), ANASTACIA (www.anastacia-h2020.eu/), DEFENDER (<https://defender-project.eu/>), InfraStress (www.infrastress.eu/), RESISTO (www.resistoproject.eu/), SAFECARE (www.safecare-project.eu/), SATIE (<http://satie-h2020.eu>), SecureGas (www.securegas-project.eu/), SPHINX (sphinx-project.eu/), and STOP-IT (stop-it-project.eu/). The organizers would like to thank these projects for supporting the CPS4CIP 2020 workshop.

Finally, the organizers of the CPS4CIP 2020 workshop would like to thank the CPS4CIP 2020 Program Committee, whose members made the workshop possible with their rigorous and timely review process. We would also like to thank the University of Surrey for hosting the workshop and the ESORICS 2020 workshop chair for valuable help and support.

December 2020

Habtamu Abie
Silvio Ranise
Luca Verderame
Enrico Cambiaso
Rita Ugarelli
Gabriele Giunta
Isabel Praça
Federica Battisti

Organization

General Chairs

Habtamu Abie
Silvio Ranise

Norwegian Computing Center, Norway
Fondazione Bruno Kessler (FBK), Italy

Program Committee Chairs

Luca Verderame
Enrico Cambiaso
Rita Ugarelli
Gabriele Giunta
Isabel Praça
Federica Battisti

University of Genoa, Italy
National Research Council (CNR), Italy
SINTEF, Norway
Engineering Ingegneria Informatica S.p.A., Italy
GECAD/ISEP, Portugal
Università degli Studi Roma Tre, Italy

Program Committee

Dieter Gollmann
Sokratis Katsikas

Hamburg University of Technology, Germany
Norwegian University of Science and Technology,
Norway

Javier Lopez
Fabio Martinelli
Einar Snekkenes

University of Malaga, Spain
IIT-CNR, Italy
Norwegian University of Science and Technology,
Norway

Omri Soceanu
Stamatis Karnouskos
Reijo Savola
Alessandro Armando
Alessio Merlo
Cristina Alcaraz
Giovanni Livraga
Gustavo G. Granadillo
Stefan Poslad
Shouhuai Xu
Christos Xenakis
Mauro Conti
Denis Čaleta
Ali Dehghantanha
Dušan Gabrijelčič
Nikolaus Wirtz
Theodore Zahariadis

IBM Research, Israel
SAP Research, Germany
VTT Technical Research Centre of Finland, Finland
University of Genoa, Italy
University of Genoa, Italy
University of Malaga, Spain
University of Milan, Italy
Atos Spain, Spain
Queen Mary University of London, UK
University of Texas at San Antonio, USA
University of Piraeus, Greece
University of Padua, Italy
Institute for Corporate Security Studies, Slovenia
University of Guelph, Canada
Jožef Stefan Institute, Slovenia
RWTH Aachen University, Germany
National and Kapodistrian University of Athens,
Greece

Adrien Bécue	AIRBUS CyberSecurity, France
Lorenzo Sutton	Engineering Ingegneria Informatica S.p.A., Italy
Harsha Ratnaweera	Norwegian University of Life Sciences, Norway
Volodymyr Tarabara	Michigan State University, USA
Christos Makropoulos	National Technical University of Athens, Greece
Alessandro Neri	Università degli Studi Roma Tre, Italy
Stefano Panzieri	Università degli Studi Roma Tre, Italy
David Tipping	DeftEdge, USA
Dionysis Nikolopoulos	National Technical University of Athens, Greece
Véronique Legrand	Cnam, France
Ioan Constantin	Orange Romania, Romania
Tim Stelkens-Kobsch	German Aerospace Center (DLR), Germany
Matteo Mangini	Network Integration and Solutions S.r.l., Italy
Mirjam Fehling-Kaschek	Fraunhofer Inst. for High-Speed Dynamics, Germany
Vasileios Kazoukas	Center for Security Studies (KEMEA), Greece

Contents

Security Threat Intelligence

Privacy-Preserving CCTV Analytics for Cyber-Physical Threat Intelligence.	3
<i>Jürgen Neises, Adrien Besse, and Jean-Baptiste Rouquier</i>	
TLSAssistant Goes FINSEC A Security Platform Integration Extending Threat Intelligence Language	16
<i>Salvatore Manfredi, Silvio Ranise, Giada Sciarretta, and Alessandro Tomasi</i>	
Cyber Threat Monitoring Systems - Comparing Attack Detection Performance of Ensemble Algorithms	31
<i>Eva Maia, Bruno Reis, Isabel Praça, Adrien Becue, David Lancelin, Samantha Dauguet Demailly, and Orlando Sousa</i>	
FINSTIX: A Cyber-Physical Data Model for Financial Critical Infrastructures	48
<i>Giorgia Gazzarata, Ernesto Troiano, Luca Verderame, Maurizio Aiello, Ivan Vaccari, Enrico Cambiaso, and Alessio Merlo</i>	

Data Anomaly Detection: Predict and Prevent

Inferring Anomaly Situation from Multiple Data Sources in Cyber Physical Systems.	67
<i>Sara Baldoni, Giuseppe Celozzi, Alessandro Neri, Marco Carli, and Federica Battisti</i>	
Fusing RGB and Thermal Imagery with Channel State Information for Abnormal Activity Detection Using Multimodal Bidirectional LSTM.	77
<i>Nikolaos Bakalos, Athanasios Voulodimos, Nikolaos Doulamis, Anastasios Doulamis, Kassiani Papisotiriou, and Matthaïos Bimpas</i>	
A Cloud-Based Anomaly Detection for IoT Big Data	87
<i>Omri Soceanu, Allon Adir, Ehud Aharoni, Lev Greenberg, and Habtamu Abie</i>	

Computer Vision and Dataset for Security

An Advanced Framework for Critical Infrastructure Protection Using Computer Vision Technologies	107
<i>Krishna Chandramouli and Ebroul Izquierdo</i>	

A Comprehensive Dataset from a Smart Grid Testbed for Machine Learning
Based CPS Security Research. 123
Chuadhry Mujeeb Ahmed and Nandha Kumar Kandasamy

Security Management and Governance

Cross-Domain Security Asset Management for Healthcare 139
*Federico Stirano, Francesco Lubrano, Giacomo Vitali,
Fabrizio Bertone, Giuseppe Varavallo, and Paolo Petrucci*

Towards a Global CIs' Cyber-Physical Security Management and Joint
Coordination Approach 155
*Vasiliki Mantzana, Eftichia Georgiou, Anna Gazi, Ilias Gkotsis,
Ioannis Chasiotis, and Georgios Eftychidis*

Toward a Context-Aware Methodology for Information Security
Governance Assessment Validation 171
*Marco Angelini, Silvia Bonomi, Claudio Ciccotelli,
and Alessandro Palma*

Impact Propagation and Power Traffic Analysis

Impact Propagation in Airport Systems 191
*Corinna Köpke, Kushal Srivastava, Louis König, Natalie Miller,
Mirjam Fehling-Kaschek, Kelly Burke, Matteo Mangini, Isabel Praça,
Alda Canito, Olga Carvalho, Filipe Apolinário, Nelson Escravana,
Nils Carstengerdes, and Tim Stelkens-Kobsch*

A Comparative Analysis of Emulated and Real IEC-104 Spontaneous
Traffic in Power System Networks 207
C.-Y. Lin and Simin Nadjm-Tehrani

Author Index 225