Lecture Notes in Computer Science 12618

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

Springer

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

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

Program Committee Chairs

Luca Verderame	University of Genoa, Italy
Enrico Cambiaso	National Research Council (CNR), Italy
Rita Ugarelli	SINTEF, Norway
Gabriele Giunta	Engineering Ingegneria Informatica S.p.A., Italy
Isabel Praça	GECAD/ISEP, Portugal
Federica Battisti	Università degli Studi Roma Tre, Italy

Program Committee

Dieter Gollmann	Hamburg University of Technology, Germany
Sokratis Katsikas	Norwegian University of Science and Technology, Norway
Javier Lopez	University of Malaga, Spain
Fabio Martinelli	IIT-CNR, Italy
Einar Snekkenes	Norwegian University of Science and Technology, Norway
Omri Soceanu	IBM Research, Israel
Stamatis Karnouskos	SAP Research, Germany
Reijo Savola	VTT Technical Research Centre of Finland, Finland
Alessandro Armando	University of Genoa, Italy
Alessio Merlo	University of Genoa, Italy
Cristina Alcaraz	University of Malaga, Spain
Giovanni Livraga	University of Milan, Italy
Gustavo G. Granadillo	Atos Spain, Spain
Stefan Poslad	Queen Mary University of London, UK
Shouhuai Xu	University of Texas at San Antonio, USA
Christos Xenakis	University of Piraeus, Greece
Mauro Conti	University of Padua, Italy
Denis Čaleta	Institute for Corporate Security Studies, Slovenia
Ali Dehghantanha	University of Guelph, Canada
Dušan Gabrijelčič	Jožef Stefan Institute, Slovenia
Nikolaus Wirtz	RWTH Aachen University, Germany
Theodore Zahariadis	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

Data Anomaly Detection: Predict and Prevent

Computer Vision and Dataset for Security

Security Management and Governance

Impact Propagation and Power Traffic Analysis