Lecture Notes in Computer Science **11260**

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
Gerhard Weikum
Max Planck Institute for Informatics, Saarbrücken, Germany

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

Eric Luiijf · Inga Žutautaitė
Bernhard M. Hämmerli (Eds.)

Critical Information Infrastructures Security

13th International Conference, CRITIS 2018
Kaunas, Lithuania, September 24–26, 2018
Revised Selected Papers

Springer

Editors
Eric Luiijf
TNO (retired) and Luiijf Consultancy
Zoetermeer, The Netherlands

Bernhard M. Hämmerli
Hochschule Luzern/Acris GmbH
Wettingen, Switzerland

Inga Žutautaitė
Vytautas Magnus University
Kaunas, Lithuania

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-05848-7 ISBN 978-3-030-05849-4 (eBook)
https://doi.org/10.1007/978-3-030-05849-4

Library of Congress Control Number: 2018952640

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

This volume contains the proceedings of the 13th International Conference on Critical Information Infrastructures Security (CRITIS 2018). The conference was held at the Vytautas Magnus University, Kaunas, Lithuania during September 24–26, 2018. The conference was organized by the Lithuanian Energy Institute and Vytautas Magnus University.

CRITIS 2018 continued the well-established series of successful CRITIS conferences. The conference contained the following keynote lectures:

- "Protecting Critical Information Infrastructure on National and EU Level – Lithuanian Approach" by Edvinas Kerza (Vice-Minister, Ministry of National Defense of the Republic of Lithuania)
- "Bridging the Gap Between ICS and Corporate IT Security: Finding Common Culture and Views" by Stefan Lüders (Head of Computer Security at CERN, Switzerland)
- "Comparison of Nordic and Continental Europe Grids from the Cyber Resilience Perspective" by Hayretdin Bahşi (Center for Digital Forensics and Cyber Security, Tallinn University of Technology, Estonia)

The main theme of the conference concerned the challenges for the energy sector as national and multinational critical infrastructure. Two special sessions addressed the technological and policy challenges for energy operators, policymakers, and other stakeholders. The following sessions were introduced by invited speakers:

- "The Necessity of Synchronization of the Baltic States' Electricity Network with the European System" by Ramūnas Bikulčius (Head of Strategy and Research Division, AB Litgrid, Lithuania)
- "Building a Network of Trust Among European Utilities to Foster Proactive Security Though Info Sharing" by Massimo Rocca (Enel Security representative and EE-ISAC Chair, Enel, Italy)
- "Securing BKW's Electrical Power Production and Distribution: A 3D Approach to Cyber Threats" by Ivo Maritz (Head, Cyber Security (CSO/CISO), BKW Group, Switzerland)
- "Emerging Threats for Energy Security" by Egidijus Purlys (Vice-Minister, Ministry of Energy of the Republic of Lithuania)
- "Cybersecurity in the Energy Sector – The EU Perspective" by Michaela Kollau (European Commission, Directorate-General for Energy)
- "Implications of Political and Policy Decisions to Energy Security" by Einari Kisel (Regional Manager for Europe, World Energy Council, Estonia)
- "Role of Public – Private Partnership in Critical Energy Infrastructure Protection: NATO ENSEC COE Perspective" by Artūras Petkus (Head of Strategic Analysis Division, NATO ENSECCOE, Lithuania)

Panel discussions led by the session chairman Marcelo Masera (European Commission, Joint Research Centre, Petten, The Netherlands) between these invited speakers and interactions with the audience stimulated the long-term debate between energy domain stakeholders and the research community.

As in previous years, the Program Committee received a large set of paper submissions. The Program Committee provided insightful reviews and comments to the authors of 51 papers. At least three, on average 4.6 independent reviews per submission took place resulting in the acceptance of 16 full papers. Therefore, the acceptance rate was 31%. Another three submissions were accepted as short papers. All these papers are published in this proceedings volume.

The selected reviewed papers and their presentations were grouped in the conference program under the topic sections "Advanced Analysis of Critical Energy Systems", "Strengthening Urban Resilience", "Securing Internet of Things and Industrial Control Systems", "Need and Tool Sets for Industrial Control System Security", "Advancements in Governance and Resilience of Critical Infrastructures", and "Short papers". The same outline can be found in this volume.

To stimulate international collaboration and exchange of ideas, the program chairs invited work-in-progress projects for a short presentation and poster session. There were three candidates for the Young CRITIS Award (YCA): Luca Faramondi, Davide Fauri, and Anamitra Pal. The intention of the YCA is building a virtual international community that allows junior researchers in the C(I)I domain to interact and network with peers and experienced researchers in the C(I)I domain. This stimulates faster and better research results and may also lead to further joint international research. The fifth YCA was presented by Marco Santarelli (Scientific Director ReS On Network, Italy) as chair of the YCA commission to Anamitra Pal (Pal Lab, SECEE, Arizona State University) for his contribution to the paper "Health Monitoring of Critical Power System Equipments Using Identifying Codes".

Organizing a conference like CRITIS entails an effort that is largely invisible to the participants. We, therefore, want to acknowledge the personal commitment of the local organizing team, general chairs, the contributions by the keynote speakers and invited speakers, as well as the support of the host organizations Vytautas Magnus University and the Lithuanian Energy Institute. The Program Committee chairs express their gratitude to the Technical Program Committee members who volunteered their services and devoted considerable time in preparing insightful reviews and comments to the authors of the papers. Together with the contributions to the discussions and interactions between all conference participants, this resulted in a very successful and stimulating CRITIS 2018.

November 2018

Eric Luiijf
Inga Žutautaitė
Bernhard M. Hämmerli

CRITIS 2018

13th International Workshop on Critical Information Infrastructures Security

Vytautas Magnus University, Kaunas, Lithuania
September 24–26, 2018
Organized by
The Lithuanian Energy Institute

Executive Committee

Programme Chair

Eric Luiijf	Luiijf Consultancy, The Netherlands

Supporting Chairs

Marcelo Masera	European Commission/Joint Research Centre, The Netherlands
Marianthi Theocharidou	European Commission/Joint Research Centre, Italy
Grigore Havarneanu	International Union of Railways, France
Simin Nadjm-Tehrani	Linköping University, Sweden
Erich Rome	2E!SAC; Fraunhofer IAIS, Germany
Enrico Zio	Politecnico di Milano, Italy; Ecole Centrale Paris, France
Sokratis K. Katsikas	Norwegian University of Science and Technology, Norway; University of Piraeus, Greece

Local Co-chairs

Inga Žutautaitė	Lithuanian Energy Institute, Lithuania
Ričardas Krikštolaitis	Vytautas Magnus University, Lithuania

Young CRITIS Award Chair

Marco Santarelli	Res on Networks, Italy

Honorary Chair

Algirdas Avižienis	Vytautas Magnus University, Lithuania; University of California, Los Angeles, USA

Publicity Chairs

Cristina Alcaraz	University of Malaga, Spain
Rolandas Urbonas	Lithuanian Energy Institute, Lithuania

Program Committee

Cristina Alcaraz	University of Malaga, Spain
John Andrews	University of Nottingham, UK
Juozas Augutis	Vytautas Magnus University, Lithuania
Fabrizio Baiardi	University of Pisa, Italy
Robin Bloomfield	CSR City University London, UK
Arslan Brömme	GI Biometrics Special Interest Group (BIOSIG), Germany
Emiliano Casalicchio	Blekinge Institute of Technology, Sweden
Simona Cavallini	Fondazione FORMIT, Italy
Michal Choras	ITTI Ltd., Poland
Gregorio D'Agostino	ENEA, Italy
Myriam Dunn	ETH Center for Security Studies Zurich, Switzerland
Mohamed Eid	CEA, France
Dimitris Gritzalis	Athens University of Economics and Business, Greece
Stefanos Gritzalis	University of the Aegean, Greece
Bernhard M. Hämmerli	Lucerne University of Applied Sciences and Arts, ACRIS GmbH, Switzerland
Chris Hankin	Imperial College London, UK
Grigore M. Havarneanu	International Union of Railways, France
Sokratis Katsikas	Center for Cyber and Information Security, NTNU, Norway
Elias Kyriakides	University of Cyprus, Cyprus
Marieke Klaver	Netherlands Organisation for Applied Scientific Research TNO, The Netherlands
Vytis Kopustinskas	European Commission/Joint Research Centre, Italy
Panayiotis Kotzanikolaou	University of Piraeus, Greece
Rafal Kozik	Institute of Telecommunications, UTP Bydgoszcz, Poland
Ričardas Krikštolaitis	Vytautas Magnus University, Lithuania
Javier Lopez	University of Malaga, Spain
Eric Luiijf	TNO (retired) and Luiijf Consultancy, The Netherlands
Jose Martí	UBC, Canada
Linas Martišauskas	Lithuanian Energy Institute, Lithuania
Raimundas Matulevičius	University of Tartu, Estonia
Richard McEvoy	NTNU and HPE Ltd., Norway
Hypatia Nassopoulos	EIVP, France
Eiji Okamoto	University of Tsukuba, Japan
Gabriele Oliva	Università Campus Bio-Medico di Roma, Italy
Evangelos Ouzounis	ENISA, Greece

Stefano Panzieri	Roma Tre University, Italy
Peter T. Popov	City University London, UK
Sigitas Rimkevičius	Lithuanian Energy Institute, Lithuania
Brendan Ryan	University of Nottingham, UK
Erich Rome	Fraunhofer IAIS, Germany
Vittorio Rosato	ENEA, Italy
Andre Samberg	i4-Flame OU (LLC), Estonia
Maria Paola Scaparra	Kent Business School, University of Kent, UK
Dominique Sérafin	CEA, France
Andrea Servida	European Commission/DG Connect, Belgium
Roberto Setola	Università Campus Bio-Medico di Roma, Italy
George Stergiopoulos	Athens University of Econ and Business, Greece
Nils Kalstad Svendsen	Gjøvik University College, Norway
André Teixeira	Uppsala Universitet, Sweden
Marianthi Theocharidou	European Commission, Joint Research Centre, Italy
Alberto Tofani	ENEA, Italy
Eugenijus Uspuras	Lithuanian Energy Institute, Lithuania
Simona Louise Voronca	Transelectrica, Romania
Stephen D. Wolthusen	Royal Holloway, University of London, UK; Norwegian University of Science and Technology, Norway
Christos Xenakis	University of Piraeus, Greece
Jianying Zhou	Singapore University of Technology and Design, Singapore
Enrico Zio	Politecnico di Milano, Italy
Urko Zurutuza	University of Mondragón, Spain
Inga Žutautaitė	Lithuanian Energy Institute, Lithuania

Local Organizing Committee CRITIS 2018

Juozas Augutis	Vytautas Magnus University, Lithuania
Sigitas Rimkevičius	Lithuanian Energy Institute, Lithuania
Rolandas Urbonas	Lithuanian Energy Institute, Lithuania
Inga Žutautaitė	Lithuanian Energy Institute, Lithuania
Ričardas Krikštolaitis	Vytautas Magnus University, Lithuania
Linas Martišauskas	Lithuanian Energy Institute, Lithuania
Rūta Užupytė	Vytautas Magnus University, Lithuania
Simona Staskevičiūtė	Vytautas Magnus University, Lithuania

Steering Committee

Chairs

Bernhard M. Hämmerli	Lucerne University of Applied Sciences and Arts, ACRIS GmbH, Switzerland
Javier Lopez	University of Malaga, Spain
Stephen D. Wolthusen	Royal Holloway, University of London, UK; Norwegian University of Science and Technology, Norway

Members

Robin Bloomfield	City University London, UK
Sandro Bologna	AIIC, Italy
Gregorio D'Agostino	ENEA, Italy
Grigore Havarneanu	International Union of Railways, France
Sokratis K. Katsikas	Norwegian University of Science and Technology, Norway; University of Piraeus, Greece
Elias Kyriakides	University of Cyprus, Cyprus
Eric Luiijf	Luiijf Consultancy, The Netherlands
Marios M. Polycarpou	University of Cyprus, Cyprus
Reinhard Posch	Technical University Graz, Austria
Saifur Rahman	Advanced Research Institute, Virginia Tech, USA
Erich Rome	2E!SAC; Fraunhofer IAIS, Germany
Antonio Scala	IMT – CNR, Italy
Roberto Setola	Università Campus Bio-Medico, Italy
Nils Kalstad Svendsen	Gjøvik University College, Norway
Marianthi Theocharidou	European Commission, Joint Research Centre, Italy

Contents

Advanced Analysis of Critical Energy Systems

Node Importance Analysis of a Gas Transmission Network with Evaluation of a New Infrastructure by ProGasNet 3
Pavel Praks and Vytis Kopustinskas

In-Cycle Sequential Topology Faults and Attacks: Effects on State Estimation 17
Ammara Gul and Stephen Wolthusen

Health Monitoring of Critical Power System Equipments Using Identifying Codes 29
Kaustav Basu, Malhar Padhee, Sohini Roy, Anamitra Pal, Arunabha Sen, Matthew Rhodes, and Brian Keel

Strengthening Urban Resilience

Towards Computer-Aided Security Life Cycle Management for Critical Industrial Control Systems 45
Florian Patzer, Ankush Meshram, Pascal Birnstill, Christian Haas, and Jürgen Beyerer

A Measure for Resilience of Critical Infrastructures 57
Sandra König, Thomas Schaberreiter, Stefan Rass, and Stefan Schauer

Earthquake Simulation on Urban Areas: Improving Contingency Plans by Damage Assessment 72
Gregorio D'Agostino, Antonio Di Pietro, Sonia Giovinazzi, Luigi La Porta, Maurizio Pollino, Vittorio Rosato, and Alberto Tofani

IVAVIA: Impact and Vulnerability Analysis of Vital Infrastructures and Built-Up Areas 84
Erich Rome, Oliver Ullrich, Daniel Lückerath, Rainer Worst, Jingquan Xie, and Manfred Bogen

Securing Internet of Things and Industrial Control Systems

SMuF: State Machine Based Mutational Fuzzing Framework for Internet of Things 101
Neeraj Karamchandani, Vinay Sachidananda, Suhas Setikere, Jianying Zhou, and Yuval Elovici

Leveraging Semantics for Actionable Intrusion Detection in Building Automation Systems 113
Davide Fauri, Michail Kapsalakis, Daniel Ricardo dos Santos, Elisa Costante, Jerry den Hartog, and Sandro Etalle

Need and Tool Sets for Industrial Control System Security

Cybersecurity Self-assessment Tools: Evaluating the Importance for Securing Industrial Control Systems in Critical Infrastructures 129
Georgia Lykou, Argiro Anagnostopoulou, George Stergiopoulos, and Dimitris Gritzalis

Gathering Intelligence Through Realistic Industrial Control System Honeypots: A Real-World Industrial Experience Report 143
Óscar Navarro, Servilio Alonso Joan Balbastre, and Stefan Beyer

A Comparison of ICS Datasets for Security Research Based on Attack Paths 154
Seungoh Choi, Jeong-Han Yun, and Sin-Kyu Kim

Advancements in Governance and Resilience of Critical Infrastructures

PPP (Public-Private Partnership)-Based Cyber Resilience Enhancement Efforts for National Critical Infrastructures Protection in Japan 169
Kenji Watanabe

Governance Models Preferences for Security Information Sharing: An Institutional Economics Perspective for Critical Infrastructure Protection 179
Alain Mermoud, Marcus Matthias Keupp, and Dimitri Percia David

Conceptual Framework for Hybrid Situational Awareness in Critical Port Infrastructures 191
Stefan Schauer, Benjamin Rainer, Nicolas Museux, David Faure, Javier Hingant, Federico Jesús Carvajal Rodrigo, Stefan Beyer, Rafael Company Peris, and Sergio Zamarripa Lopez

Discovering Vulnerabilities in Heterogeneous Interconnected Systems 204
Luca Faramondi, Gabriele Oliva, Stefano Panzieri, and Roberto Setola

Short Papers

RICS-el: Building a National Testbed for Research and Training on SCADA Security (Short Paper) 219
Magnus Almgren, Peter Andersson, Gunnar Björkman, Mathias Ekstedt, Jonas Hallberg, Simin Nadjm-Tehrani, and Erik Westring

Efficient Analysis to Protect Control into Critical Infrastructures 226
Shuo Zhang and Stephen D. Wolthusen

Denial of Service Attacks: Detecting the Frailties of Machine Learning Algorithms in the Classification Process 230
Ivo Frazão, Pedro Henriques Abreu, Tiago Cruz, Hélder Araújo, and Paulo Simões

Author Index 237