

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>

Gregorio D'Agostino · Antonio Scala (Eds.)

Critical Information Infrastructures Security

12th International Conference, CRITIS 2017
Lucca, Italy, October 8–13, 2017
Revised Selected Papers

Editors

Gregorio D'Agostino 
ENEA "Casaccia"
and Network of Networks - Netonets
Rome, Italy

Antonio Scala 
CNR - Institute for Complex Systems (ISC)
Rome, Italy

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-99842-8 ISBN 978-3-319-99843-5 (eBook)
<https://doi.org/10.1007/978-3-319-99843-5>

Library of Congress Control Number: 2018952640

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2018

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 papers presented at CRITIS 2017 – the 12th International Conference on Critical Information Infrastructures Security held during October 8–13, 2017, in Lucca.

CRITIS 2017 continued the tradition of presenting innovative research and exploring new challenges in the field of critical (information) infrastructures protection (C(I)IP) and fostering dialogue with stakeholders. CRITIS 2017 renewed efforts to bring together researchers and professionals from academia, industry, and governmental organizations working in the field of the security of critical (information) infrastructure systems.

As in previous years, distinguished invited speakers and special events complemented a program of original research contributions. According to the tradition, the conference invited the different research communities and disciplines involved in the C(I)IP space, and encouraged discussions and multi-disciplinary approaches to relevant C(I)IP problems.

This 2017 edition of CRITIS was hosted in Lucca, Italy, by the IMT School for Advanced Studies Lucca, an Italian public academic institution organized as a graduate school and research center that focuses on the analysis of economic, social, technological, and cultural systems.

Two satellite workshops on energy security and on water security took place on the closing days of the main conference.

Some specific innovations were introduced: beside the traditional sessions where original works and significant improvements were presented, specific sessions devoted to ongoing projects and operators took place. The “Projects Dissemination Session” provided an opportunity for the dissemination of ongoing project results both at the European and the Member States level for a total of 12 European and three Italian projects. The operators session in this edition was limited to the ICT sector and was led by TIM (the former Italian national telecommunication operator).

There were 63 papers submitted. Each submission was reviewed by at least two, and on average 2.8, Program Committee members. The committee decided to accept 21 full papers and four extended abstracts with a rejection rate of $\sim 67\%$ ($\sim 60\%$ accounting for the extended abstracts). Extended abstracts were selected among the 20 submissions accepted for poster presentation.

Each accepted full paper was allowed a 20-min slot for oral presentation. The program also included four keynote talks and one institutional talk; none of the invited speakers contributed with a non-reviewed proceedings paper.

As in previous editions, CRITIS 2017 awarded three prizes to the best contribution from young (<32 years) scientists. The winners were selected after a joint evaluation by both the audience and the academic committee of the Young CRITIS Award (YCA).

CRITIS 2017 received the endorsement of the Presidency of the Italian Council of Ministers (“patrocinio della Presidenza del Consiglio dei Ministri”) UCE F 735/2017.

The conference was organized by NetONets, a nonprofit organization fostering the diffusion of interdisciplinary research, especially on complexity science and critical infrastructures.

The organizers are indebted to IMT Lucca for providing the location of the conference and for supporting the event in several different forms, among which were the lodgings provided in the beautiful medieval complex of S. Francesco. We also thank the IMT press office for their support.

We thank our communication chair, Alberto Tofani, for creating and maintaining the conference's website and registration services.

The conference organization benefited from the contributions of the program co-chairs, Cristina Alcaraz and Grigore Havarneanu, of the poster co-chair, Fabiana Zollo, of the Young CRITIS Award chairs, Bernhard M. Hämmerli and Marco Santarelli, and of the CRITIS Steering Committee chairs, Bernhard M. Hämmerli, Javier Lopez, and Stephen D. Wolthusen. We also thank the Program Committee and all the experts who participated in the reviewing process.

The event was mainly sponsored by TIM with the secondary involvement of the Kaspersky Lab; the YCA prize was supported by Res On Networks, an international institute for research and development based in London.

The submission and reviewing process was performed through the EasyChair platform.

November 2017

Gregorio D'Agostino
Antonio Scala

Organization

Program Committee

| | |
|--------------------------|---|
| Cristina Alcaraz | UMA |
| Marc Antoni | International Union of Railways |
| Fabrizio Baiardi | Dipartimento di informatica, Università di Pisa |
| Robin Bloomfield | City, University of London, UK |
| Maria Cristina Brugnoli | CNIT |
| Arslan Brömme | GI Biometrics Special interest Group (BIOSIG) |
| Emiliano Casalicchio | Blekinge Institute of Technology, Sweden |
| Simona Cavallini | Fondazione Formit, Italy |
| Michal Choras | ITTI Ltd. |
| Kris Christmann | University of Huddersfield, UK |
| Gregorio D'Agostino | ENEA |
| Myriam Dunn | ETH Center for Security Studies Zurich, Switzerland |
| Mohamed Eid | commissariat à l'énergie atomique et aux énergies alternatives |
| Angelo Facchini | IMT |
| Adrian Gheorghe | Old Dominion University, USA |
| Dimitris Gritzalis | Athens University of Economics and Business, Greece |
| Stefanos Gritzalis | University of the Aegean, Greece |
| Bernhard Haemmerli | Lucerne University of Applied Sciences and Arts, Switzerland, and Acris GmbH |
| Chris Hankin | Imperial College London, UK |
| Grigore M. Havarneanu | International Union of Railways |
| Apiniti Jotisankasa | Kasetsart University, Bangkok |
| Sokratis Katsikas | Center for Cyber and Information Security, NTNU |
| Marieke Klaver | TNO |
| Panayiotis Kotzanikolaou | University of Piraeus, Greece |
| Rafal Kozik | UTP Bydgoszcz, Poland |
| Boban Krsic | DENIC eG |
| Elias Kyriakides | University of Cyprus, Cyprus |
| Javier Lopez | University of Malaga, Spain |
| Eric Luijff | TNO |
| Jose Marti | The University of British Columbia, Canada |
| Richard Mcevoy | NTNU, Norway and HPE Ltd. |
| Maddalen Mendizabal | Tecnalia R&I |
| Igor Nai Fovino | Joint Research Centre |
| Aristotelis Naniopoulos | Aristotle University of Thessaloniki, Greece |
| Hypatia Nassopoulos | EIVP |
| Eiji Okamoto | University of Tsukuba, Japan |

| | |
|------------------------|---|
| Gabriele Oliva | University Campus Biomedico of Rome, Italy |
| Evangelos Ouzounis | ENISA |
| Stefano Panzieri | Roma Tre University, Italy |
| Alexander Paz-Cruz | University of Nevada, Las Vegas, USA |
| Reinhard Posch | UNC Charlotte |
| Erich Rome | Fraunhofer |
| Vittorio Rosato | ENEA |
| Brendan Ryan | University of Nottingham |
| Andre Samberg | TIEMS International Program Committee |
| Antonio Scala | IMT, CNR, Italy |
| Maria Paola Scaparra | The University of Kent, UK |
| Eric Schellekens | ARCADIS |
| Roberto Setola | University Campus Biomedico of Rome, Italy |
| George Stergiopoulos | Athens University of Economics and Business, Greece |
| Nils Kalstad Svendsen | Gjøvik University College, Norway |
| Dominique Sérafin | CEA |
| André Teixeira | Delft University of Technology, The Netherlands |
| Marianthi Theocharidou | European Commission, Joint Research Centre |
| Alberto Tofani | ENEA |
| William J. Tolone | UNC Charlotte |
| Simona Louise Voronca | Transelectrica - POLITEHNICA University Bucharest |
| René Willems | Eindhoven University of Technology |
| Stephen D. Wolthusen | Royal Holloway, University of London, UK and 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 |
| Fabiana Zollo | University of Venice Ca' Foscari, Italy |
| Urko Zurutuza | Mondragon University, Spain |
| Inga Žutautaitė | Lithuanian Energy Institute, Lithuania |

Additional Reviewers

Kasse, Paraskevi
 Lykou, Georgia
 Lückerath, Daniel
 Malatras, Apostolos
 Mentzelioti, Despina
 Mohammadi, Farnaz
 Moulinos, Konstantinos
 Virvilis, Nick
 Xie, Jingquan

Contents

| | |
|--|-----|
| Resilience of Electrical Distribution Systems with Critical Load Prioritization. | 1 |
| <i>Zejun Yang and Jose R. Marti</i> | |
| Public Tolerance Levels of Transportation Resilience: A Focus on the Oresund Region Within the IMPROVER Project. | 13 |
| <i>Laura Petersen, Laure Fallou, Elisabete Carreira, and Andrei Utkin</i> | |
| Towards a Common Vocabulary for Crisis Management Scenarios | 25 |
| <i>Jingquan Xie, Betim Sojeva, Erich Rome, and Daniel Lückerath</i> | |
| Analysis and Classification of Adaptation Tools for Transport Sector Adaptation Planning | 37 |
| <i>Georgia Lykou, George Iakovakis, George Chronis, and Dimitris Gritzalis</i> | |
| Timing-Based Anomaly Detection in SCADA Networks | 48 |
| <i>Chih-Yuan Lin, Simin Nadjm-Tehrani, and Mikael Asplund</i> | |
| Operational Resilience Metrics for a Complex Electrical Network | 60 |
| <i>Alberto Tofani, Gregorio D'Agostino, Antonio Di Pietro, Giacomo Onori, Maurizio Pollino, Silvio Alessandrini, and Vittorio Rosato</i> | |
| The Influence of Load Characteristics on Early Warning Signs in Power Systems | 72 |
| <i>Steffen O. P. Blume and Giovanni Sansavini</i> | |
| DMA Optimal Layout for Protection of Water Distribution Networks from Malicious Attack | 84 |
| <i>Simeone Chianese, Armando Di Nardo, Michele Di Natale, Carlo Giudicianni, Dino Musmarra, and Giovanni Francesco Santonastaso</i> | |
| Role of Urban Interactions and Damage in Seismic Resilience of Historical Centers | 97 |
| <i>Anna Bozza, Domenico Asprone, Fulvio Parisi, and Gaetano Manfredi</i> | |
| Towards Blockchain-Based Collaborative Intrusion Detection Systems. | 107 |
| <i>Nikolaos Alexopoulos, Emmanouil Vasilomanolakis, Natália Réka Ivánkó, and Max Mühlhäuser</i> | |

| | |
|---|-----|
| Analysis of Cybersecurity Threats in Industry 4.0: The Case of Intrusion Detection | 119 |
| <i>Juan E. Rubio, Rodrigo Roman, and Javier Lopez</i> | |
| De-Synchronisation Attack Modelling in Real-Time Protocols Using Queue Networks: Attacking the ISO/IEC 61850 Substation Automation Protocol . . . | 131 |
| <i>James G. Wright and Stephen D. Wolthusen</i> | |
| Assessing Urban Rail Transit Systems Vulnerability: Metrics vs. Interdiction Models. | 144 |
| <i>Stefano Starita, Annunziata Esposito Amideo, and Maria Paola Scaparra</i> | |
| Automatically Generating Security Models from System Models to Aid in the Evaluation of AMI Deployment Options. | 156 |
| <i>Michael Rausch, Ken Keefe, Brett Feddersen, and William H. Sanders</i> | |
| A Gamified Approach to Participatory Modelling of Water System Risks. . . . | 168 |
| <i>Alex Coletti, Antonio De Nicola, Giordano Vicoli, and Maria Luisa Villani</i> | |
| Managing Gas and Electric Power Network Dependencies to secure Energy Supply: Application to the UK System | 181 |
| <i>Dominique Wassermann, Andrea Antenucci, and Giovanni Sansavini</i> | |
| What the Stack? On Memory Exploitation and Protection in Resource Constrained Automotive Systems | 185 |
| <i>Aljoscha Lautenbach, Magnus Almgren, and Tomas Olovsson</i> | |
| Dealing with Functional Safety Requirements for Automotive Systems: A Cyber-Physical-Social Approach | 194 |
| <i>Mohamad Gharib, Paolo Lollini, Andrea Ceccarelli, and Andrea Bondavalli</i> | |
| Side-Channel Based Intrusion Detection for Industrial Control Systems | 207 |
| <i>Pol Van Aubel, Kostas Papagiannopoulos, Łukasz Chmielewski, and Christian Doerr</i> | |
| Security Evaluation of Cyber-Physical Systems Using Automatically Generated Attack Trees | 225 |
| <i>Laurens Lemaire, Jan Vossaert, Bart De Decker, and Vincent Naessens</i> | |
| Faulty or Malicious Anchor Detection Criteria for Distance-Based Localization | 229 |
| <i>Federica Inderst, Gabriele Oliva, Stefano Panzieri, Federica Pascucci, and Roberto Setola</i> | |

One Step More: Automatic ICS Protocol Field Analysis 241
Yeop Chang, Seungoh Choi, Jeong-Han Yun, and SinKyu Kim

Motion Magnification for Urban Buildings 253
*Vincenzo Fioriti, Ivan Roselli, Angelo Tati, Roberto Romano,
and Gerardo De Canio*

Reputation Systems to Mitigate DoS Attack in Vehicular Network 261
Gianpiero Costantino, Fabio Martinelli, and Ilaria Matteucci

On the Security of Aircraft Communication Networks 266
Paul Berthier, Corentin Bresteau, and José Fernandez

Author Index 271