Preface

The 2016 International Conference on Critical Information Infrastructures Security (CRITIS 2016) was the 11th conference in the series, continuing a well-established tradition of successful annual conferences. Since its inception, CRITIS has been a global forum for researchers and practitioners to present and discuss the most recent innovations, trends, results, experiences, and concerns in selected perspectives of critical information infrastructure protection [C(I)IP] at large covering the range from small-scale cyber-physical systems security via information infrastructures and their interaction with national and international infrastructures, and ultimately also reaching policy-related aspects. In line with this tradition, CRITIS 2016 brought together experts from governments, regulators, scientists, and professionals from academia, industry, service providers, and other stakeholders in one conference to secure infrastructures and study ways to enhance their resilience to faults and deliberate attacks.

This volume contains the carefully reviewed proceedings of the 11th CRITIS conference, held in Paris, France, during October 10–12, 2016. The conference was organized by the International Union of Railways (Union Internationale des Chemins de Fer, UIC) — the worldwide professional association representing the railway sector and promoting rail transport. Following the call for papers, we received 58 high-quality submissions, which were thoroughly reviewed by the expert members of the international Program Committee (IPC). Out of the total submissions, 22 papers were accepted as full papers with eight further papers accepted as short papers offering work in progress; these short papers are also collected in this volume. Each paper was reviewed by at least three expert reviewers, and both full and short papers were retained for oral presentations during the conference. The technical papers were grouped into sessions that included topics on innovative responses for the protection of cyber-physical systems, procedures and organizational aspects in C(I)IP and advances in human factors, decision support, and cross-sector C(I)IP approaches. Furthermore, in continuation of an initiative first taken up at the 2014 CRITIS, the conference also included an award for young researchers in the area (the 3rd CIPRNet Young CRITIS Award), seeking to recognize and encourage the integration of talented younger researchers into the community. Five of the accepted papers were presented during a dedicated CYCA Session. This award was sponsored by the FP7 Network of Excellence CIPRNet. As in previous years, invited keynote speakers and special events complemented the three-day technical program. The five plenary talks were the following:

- Dr Artūras Petkus (NATO Energy Security Centre of Excellence, Lithuania) gave a CIPRNet Lecture entitled: “CEIP and Energy Security in Perspective of NATO Energy Security Center of Excellence.”
- Commander Cyril Stylianidis (Ministry of Interior, General Directorate for Civil Protection and Crisis Management, France), provided an overview of “The Crisis Interministerial Cell (CIC), the French Tool for Interministerial Level Crisis Management,” illustrated with recent examples from France.

- Mr. Kris Christmann (University of Huddersfield, Applied Criminology Centre, UK) offered “Findings from the PRE-EMPT Project: Establishing Best Practice for Reducing Serious Crime and Terrorism at Multi-Modal Passenger Terminals (MMPT).”
- Dr. Paul Theron (Thales Communications and Security, France) presented “A Way Towards a Fully Bridged European Certification of IACS Cyber Security,” related to the work of DG JRC’s ERNCIP Thematic Group on IACS cybersecurity certification.

In addition, the CRITIS 2016 participants had the opportunity to attend (with a limited number of places) an associated event organized at UIC the day after the main conference. The IMPROVER Workshop – “Meeting Public Expectations in Response to Crises” – addressed an important topic in C(I)IP, aiming to discuss how infrastructure operators meet these requirements today and how this can be improved.

It is our pleasure to express our gratitude to everybody that contributed to the success of CRITIS 2016. In particular, we would like to thank the general chair, Jean-Pierre Loubinoux (UIC Director-General), and the local UIC hosts, Jerzy Wisniewski (Fundamental Values Department Director) and Jacques Colliard (Head of UIC Security Division), for making CRITIS possible at the UIC headquarters in Paris – one of the most beautiful European capitals. Further, we would like to thank the members of the Program Committee, who did a tremendous job under strict time limitations during the review process. We also thank the members of the Steering Committee for the great effort and their continuous assistance in the organization of the conference. We are also grateful to the publicity chair and to the UIC Communications Department for their excellent dissemination support, and to the CIPRNet Network, which was an active supporting community. We are equally grateful to the keynote speakers who accepted our invitation and agreed to round off the conference program through presentations on hot topics of the moment. We would also like to thank the publisher, UIC-ETF, for their cooperation in publishing the selected papers from the pre-conference proceedings. Finally, we thank all the authors who submitted their work to CRITIS and who contributed to this volume for sharing their new ideas and results with the community. We hope that these ideas will generate further new ideas and innovations for securing our critical infrastructures for the benefit of the whole society.

September 2016

Grigore Havarneanu
Roberto Setola
Hypatia Nassopoulos
Stephen Wolthusen

http://www.springer.com/978-3-319-71367-0

Critical Information Infrastructures Security
11th International Conference, CRITIS 2016, Paris,
France, October 10–12, 2016, Revised Selected Papers
Havarneanu, G.; Setola, R.; Nassopoulos, H.;
Wolthusen, S. (Eds.)
2017, XI, 348 p. 103 illus., Softcover
ISBN: 978-3-319-71367-0