

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 <https://link.springer.com/bookseries/7410>


Dimitri Percia David · Alain Mermoud ·
Thomas Maillart (Eds.)

Critical Information Infrastructures Security

16th International Conference, CRITIS 2021
Lausanne, Switzerland, September 27–29, 2021
Revised Selected Papers

Editors

Dimitri Percia David 
University of Geneva
Geneva, Switzerland

Alain Mermoud 
armasuisse Science and Technology S+T
Thun, Switzerland

Thomas Maillart 
University of Geneva
Geneva, Switzerland

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-93199-5 ISBN 978-3-030-93200-8 (eBook)
<https://doi.org/10.1007/978-3-030-93200-8>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2021

Chapters “GNSS Positioning Security: Automatic Anomaly Detection on Reference Stations” and “The Cost of Incidents in Essential Services—Data from Swedish NIS Reporting” 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

This volume contains the proceedings of the 16th International Conference on Critical Information Infrastructures Security (CRITIS 2021). The conference was held during September 27–29, 2021, at the EPFL SwissTech Convention Center (STCC) in Lausanne, Switzerland. The CRITIS community was delighted to be back in Switzerland, as the 6th edition of the conference (CRITIS 2011) was held in Lucerne exactly 10 years ago.

CRITIS 2021 was hosted in hybrid mode at EPFL by Trust Valley, the University of Geneva, and the Cyber-Defence Campus of armasuisse S+T, the Swiss Federal Office for Defence Procurement. Despite the pandemic, over 130 participants registered for the onsite conference and about 100 participants registered for the online option. Overall, the conference enabled the connection of different continents and time zones, audiences, and scientific disciplines, as well as generations of researchers.

On the second day, the conference was held in conjunction with a Cyber-Defence (CYD) Campus conference. Indeed, the CYD Campus and CRITIS share an important goal: to provide a platform to bring together different audiences from academia, industry, and government. Ongoing discussions between these audiences can be found on social media with the hashtags #CRITIS2021 and/or #CYDCAMPUS, as well as on the conference Twitter account: @critis21.

The final conference program is available on the [conference website](#). The 40 conference podcasts are available for download (HD, 1080p) [here](#). As a thank you to the attendants, pre-proceedings, video recordings, slides and conference pictures are available in the following [shared drive](#), password: *SwissTech2021*. The conference program and podcasts, as well as conference pictures and slides are available on the conference website: critis2021.org

In total, 42 papers (full and short) were submitted on EasyChair, the scientific conference management platform used for CRITIS 2021. Each paper received a minimum of three double-blind reviews thanks to the thorough and generous work of the Technical Program Committee, which welcomed over 10 new active members this year.

As a result of this double-blind peer-review process, 12 full papers were accepted (one with shepherding) along with one short paper, which brings the overall acceptance rate to about 30%, thus maintaining the scientific quality of the conference. Additionally, eight keynotes, two testbeds, three demonstrations and five posters were accepted for presentation at the conference. Accepted papers were presented in four scientific sessions (reflected in the structure of this volume) organized around the following topics:

1. Protection of Cyber-Physical Systems and Industrial Control Systems (ICS)
2. C(I)IP Organisation, (Strategic) Management and Legal Aspects
3. Human Factor, Security Awareness and Crisis Management for C(I)IP and Critical Services
4. Future, TechWatch and Forecast for C(I)IP and Critical Services

Three industrial sessions (one per day) were chaired by David Baschung to allow major players from industry to present current challenges and solutions to better protect critical infrastructures and critical services. The panel discussions were particularly interesting for building bridges between the academic world and industry.

On September 28, the CYD Campus hosted its start-up challenge organized around the topic ‘Boost your Information Sharing and Analysis Center (ISAC)’. The three finalists were the following:

1. Decentriq
2. Constella Intelligence
3. Pandora Intelligence

Following in the footsteps of the previous years, CRITIS 2021 awarded prizes to the best young researchers:

1. Siddhant Shrivastava, Singapore University of Technology and Design
2. Santiago Anton Moreno, EPFL
3. Stéphanie Lebrun, CYD Campus

We thank the Master of Advanced Studies in Information Security of the University of Geneva for sponsoring the award, thus helping the event carry on through the years.

In summary, CRITIS 2021 continued the well-established series of successful CRITIS conferences. We hope it will remain a memorable edition that also tried to bring new features to the community: hybrid mode and podcasts, paper shepherding, a rump session, and a scientific session on technology market monitoring and forecasting.

Organizing a conference in the middle of a pandemic is a tough challenge. A big thank you goes to all our stakeholders for their trust and to all our sponsors for their precious support: Fortinet, ELCA, AWK Group, Monti Stampa Furrer & Partners AG, AdNovum, Kudelski Security, and the University of Geneva.

We wish Stefan Pickl every success as he takes over the role of general chair for CRITIS 2022, which will take place in Germany at the Bundeswehr University Munich. The CRITIS franchise is thus in good hands and its future is fully assured, thanks also to the good advice of Bernhard Hämmerli, head of the CRITIS Steering Committee.

October 2021

Alain Mermoud
Dimitri Percia David
Thomas Maillart

Organization

General Co-chairs

Alain Mermoud
Thomas Maillart

Cyber-Defence Campus armasuisse S+T, Switzerland
University of Geneva, Switzerland

Program Committee Co-chairs

Dimitri Percia David
Alain Mermoud

University of Geneva, Switzerland
Cyber-Defence Campus armasuisse S+T, Switzerland

Steering Committee

Bernhard Hämmerli (Chair)
Javier Lopez (Chair)
Stephen Wolthusen (Chair)
Robin Bloomfield
Sandro Bologna
Gregorio D'Agostino
Grigore Havarneanu
Sokratis Katsikas

Lucerne University of Applied Sciences, Switzerland
University of Malaga, Spain
Royal Holloway, University of London, UK
City University London, UK
AIIC, Italy
ENEA, Italy
International Union of Railways (UIC), France
Norwegian University of Science and Technology,
Norway

Eric Luijff
Alain Mermoud
Marios Polycarpou
Reinhard Posch
Erich Rome
Antonio Scala
Inga Šarūnienė
Roberto Setola
Nils Kalstad Svendsen
Marianthi Theodoridou

TNO (retired), The Netherlands
Cyber-Defence Campus armasuisse S+T, Switzerland
University of Cyprus, Cyprus
Technical University Graz, Austria
Fraunhofer IAIS, Germany
IMT-CNR, Italy
Lithuanian Energy Institute, Lithuania
Università Campus Bio-Medico di Roma, Italy
Gjøvik University College, Norway
European Commission Joint Research Centre, Italy

Technical Program Committee

Cristina Alcaraz
Magnus Almgren
Fabrizio Baiardi
Sandro Bologna
Tom Chothia

University of Malaga, Spain
Chalmers University of Technology, Sweden
University of Pisa, Italy
Association of Critical Infrastructure Experts, Italy
University of Birmingham, UK

Gregorio D'Agostino	Italian National Agency for New Technologies, Italy
Geert Deconinck	KU Leuven, Belgium
Steven Furnell	University of Nottingham, UK
Jairo Giraldo	University of Utah, USA
Dimitris Gritzalis	Athens University of Economics and Business, Greece
Bernhard Hämmerli	Lucerne University of Applied Sciences, Switzerland
Chris Hankin	Imperial College London, UK
Grigore Havarneanu	International Union of Railways (UIC), France
Chad Heitzenrater	US Air Force Research Laboratory, USA
Kévin Huguenin	University of Lausanne, Switzerland
Mathias Humbert	Cyber-Defence Campus armasuisse S+T, Switzerland
Mikel Iturbe	Mondragon Unibertsitatea, Spain
Zbigniew Kalbarczyk	University of Illinois, USA
Sokratis Katsikas	Norwegian University of Science and Technology, Norway
Marieke Klaver	TNO, The Netherlands
Vytis Kopustinskas	European Commission Joint Research Centre, Italy
Panayiotis Kotzanikolaou	University of Piraeus, Greece
Marina Krotofil	Hamburg University of Technology, Germany
Jean-Yves Le Boudec	EPFL, Switzerland
Vincent Lenders	Cyber-Defence Campus armasuisse S+T, Switzerland
Javier Lopez	University of Malaga, Spain
Thomas Maillart	University of Geneva, Switzerland
Linas Martišauskas	Lithuanian Energy Institute, Lithuania
Marcelo Masera	European Commission Joint Research Centre, Italy
Kieran McLaughlin	Queen's University Belfast, UK
Alain Mermoud	Cyber-Defence Campus armasuisse S+T, Switzerland
Simin Nadjm-Tehrani	Linköping University, Sweden
Sebastian Obermeier	Lucerne University of Applied Sciences, Switzerland
Diego Ortiz Yepes	Lucerne University of Applied Sciences, Switzerland
Stefano Panzieri	Roma Tre University, Italy
Mario Paolone	EPFL, Switzerland
Dimitri Percia David	University of Geneva, Switzerland
Adrian Perrig	ETH Zurich, Switzerland
Stefan Pickl	Universität der Bundeswehr München, Germany
Ludovic Pietre-Cambacedes	Électricité de France (EDF), France
Peter Popov	City University London, UK
Awais Rashid	University of Bristol, UK
Anne Remke	University of Münster, Germany
Brian Sadler	US Army Research Laboratory, USA
Andre Samberg	European Commission, Belgium
Henrik Sandberg	KTH Royal Institute of Technology, Sweden
Patrick Schaller	ETH Zurich, Switzerland
Roberto Setola	Università Campus Bio-Medico di Roma, Italy
Florian Skopik	Austrian Institute of Technology, Austria
Vladimir Stankovic	City University London, UK

Martin Strohmeier	Cyber-Defence Campus armasuisse S+T, Switzerland
Nils Ole Tippenhauer	Helmholtz Center for Information Security, Germany
Alberto Tofani	Italian National Agency for New Technologies, Italy
Claire Vishik	Intel Corporation, UK
Florian Wamser	University of Würzburg, Germany
Jiaying Zhou	Singapore University of Technology and Design, Singapore
Inga Žutautaitė	Lithuanian Energy Institute, Lithuania

Industrial/Practical Experience Reports Chair

David Baschung	Military Academy at ETH Zurich, Switzerland
----------------	---

Young CRITIS Award Chairs

Thomas Maillart	University of Geneva, Switzerland
Bernhard Hämmerli	Lucerne University of Applied Sciences, Switzerland

Local Organizing Chair

Lena Perrenoud	EPFL SwissTech Convention Center, Switzerland
----------------	---

Publicity, Communication, and Sponsorship Chair

Kilian Cuhe	Armed Forces Command Support Organisation of DDPS, Switzerland
-------------	---

Registration, Merchandising, and Social Events Chairs

Monia Khelifi	Cyber-Defence Campus armasuisse S+T, Switzerland
Sarah Frei	Cyber-Defence Campus armasuisse S+T, Switzerland

Sponsors



Contents

Protection of Cyber-Physical Systems and Industrial Control Systems (ICS)

Bank of Models: Sensor Attack Detection and Isolation in Industrial Control Systems	3
<i>Chuadhry Mujeeb Ahmed and Jianying Zhou</i>	
Super Detector: An Ensemble Approach for Anomaly Detection in Industrial Control Systems	24
<i>Madhumitha Balaji, Siddhant Shrivastava, Sridhar Adepu, and Aditya Mathur</i>	
Optimal Man-In-The-Middle Stealth Attack	44
<i>Luca Faramondi, Gabriele Oliva, and Roberto Setola</i>	
GNSS Positioning Security: Automatic Anomaly Detection on Reference Stations	60
<i>Stéphanie Lebrun, Stéphane Kaloustian, Raphaël Rollier, and Colin Barschel</i>	

C(I)IP Organisation, (Strategic) Management and Legal Aspects

Model-Based Risk Analysis Approach for Network Vulnerability and Security of the Critical Railway Infrastructure	79
<i>Himanshu Neema, Leqiang Wang, Xenofon Koutsoukos, CheeYee Tang, and Keith Stouffer</i>	
A Survey on Applications of Formal Methods in Analysis of SCADA Systems	99
<i>Mihael Marović, Ante Derek, and Stjepan Groš</i>	
The Cost of Incidents in Essential Services—Data from Swedish NIS Reporting	116
<i>Ulrik Franke, Johan Turell, and Ivar Johansson</i>	

Human Factor, Security Awareness and Crisis Management for C(I)IP and Critical Services

Impact Analysis of PLC Performance When Applying Cyber Security
Solutions Using Active Information Gathering 133
Yeop Chang, Taeyeon Kim, and Woonyon Kim

Multi-categorical Risk Assessment for Urban Critical Infrastructures 152
Sandra König, Stefan Schauer, and Stefan Rass

Use-Case Informed Task Analysis for Secure and Usable Design Solutions
in Rail 168
*Amna Altaf, Shamal Faily, Huseyin Dogan, Alexios Mylonas,
and Eylem Thron*

Studying Neutrality in Cyber-Space: a Comparative Geographical
Analysis of Honeypot Responses 186
Martin Strohmeier, James Pavur, Ivan Martinovic, and Vincent Lenders

Future, TechWatch & Forecast for C(I)IP and Critical Services

TABLEAU: Future-Proof Zoning for OT Networks 207
Piet De Vaere, Claude Hähni, Franco Monti, and Adrian Perrig

Link Prediction for Cybersecurity Companies and Technologies: Towards
a Survivability Score 228
Santiago Anton Moreno, Anita Mezzetti, and William Lacube

Author Index 235