

Editor-in-Chief

Kai Rannenber, Goethe University Frankfurt, Germany

Editorial Board

TC 1 – Foundations of Computer Science

Jacques Sakarovitch, Télécom ParisTech, France

TC 2 – Software: Theory and Practice

Michael Goedicke, University of Duisburg-Essen, Germany

TC 3 – Education

Arthur Tatnall, Victoria University, Melbourne, Australia

TC 5 – Information Technology Applications

Erich J. Neuhold, University of Vienna, Austria

TC 6 – Communication Systems

Aiko Pras, University of Twente, Enschede, The Netherlands

TC 7 – System Modeling and Optimization

Fredi Tröltzsch, TU Berlin, Germany

TC 8 – Information Systems

Jan Pries-Heje, Roskilde University, Denmark

TC 9 – ICT and Society

Diane Whitehouse, The Castlegate Consultancy, Malton, UK

TC 10 – Computer Systems Technology

Ricardo Reis, Federal University of Rio Grande do Sul, Porto Alegre, Brazil

TC 11 – Security and Privacy Protection in Information Processing Systems

Steven Furnell, Plymouth University, UK

TC 12 – Artificial Intelligence

Ulrich Furbach, University of Koblenz-Landau, Germany

TC 13 – Human-Computer Interaction

Jan Gulliksen, KTH Royal Institute of Technology, Stockholm, Sweden

TC 14 – Entertainment Computing

Matthias Rauterberg, Eindhoven University of Technology, The Netherlands

IFIP – The International Federation for Information Processing

IFIP was founded in 1960 under the auspices of UNESCO, following the first World Computer Congress held in Paris the previous year. A federation for societies working in information processing, IFIP's aim is two-fold: to support information processing in the countries of its members and to encourage technology transfer to developing nations. As its mission statement clearly states:

IFIP is the global non-profit federation of societies of ICT professionals that aims at achieving a worldwide professional and socially responsible development and application of information and communication technologies.

IFIP is a non-profit-making organization, run almost solely by 2500 volunteers. It operates through a number of technical committees and working groups, which organize events and publications. IFIP's events range from large international open conferences to working conferences and local seminars.

The flagship event is the IFIP World Computer Congress, at which both invited and contributed papers are presented. Contributed papers are rigorously refereed and the rejection rate is high.

As with the Congress, participation in the open conferences is open to all and papers may be invited or submitted. Again, submitted papers are stringently refereed.

The working conferences are structured differently. They are usually run by a working group and attendance is generally smaller and occasionally by invitation only. Their purpose is to create an atmosphere conducive to innovation and development. Refereeing is also rigorous and papers are subjected to extensive group discussion.

Publications arising from IFIP events vary. The papers presented at the IFIP World Computer Congress and at open conferences are published as conference proceedings, while the results of the working conferences are often published as collections of selected and edited papers.

IFIP distinguishes three types of institutional membership: Country Representative Members, Members at Large, and Associate Members. The type of organization that can apply for membership is a wide variety and includes national or international societies of individual computer scientists/ICT professionals, associations or federations of such societies, government institutions/government related organizations, national or international research institutes or consortia, universities, academies of sciences, companies, national or international associations or federations of companies.

More information about this series at <http://www.springer.com/series/6102>

Mason Rice · Sujeet Shenoi (Eds.)

Critical Infrastructure Protection X

10th IFIP WG 11.10 International Conference, ICCIP 2016
Arlington, VA, USA, March 14–16, 2016
Revised Selected Papers

Editors

Mason Rice
Air Force Institute of Technology
Wright-Patterson AFB, OH
USA

Sujeet Shenoj
Tandy School of Computer Science
University of Tulsa
Tulsa, OK
USA

ISSN 1868-4238 ISSN 1868-422X (electronic)
IFIP Advances in Information and Communication Technology
ISBN 978-3-319-48736-6 ISBN 978-3-319-48737-3 (eBook)
DOI 10.1007/978-3-319-48737-3

Library of Congress Control Number: 2016955510

© IFIP International Federation for Information Processing 2016

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.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

Contributing Authors	vii
Preface	xiii
PART I THEMES AND ISSUES	
1	
Cyberspace and Organizational Structure: An Analysis of the Critical Infrastructure Environment	3
<i>Michael Quigg, Juan Lopez, Mason Rice, Michael Grimaila and Benjamin Ramsey</i>	
2	
Critical Infrastructure Asset Identification: Policy, Methodology and Gap Analysis	27
<i>Christine Izuakor and Richard White</i>	
3	
Mitigating Emergent Vulnerabilities in Oil and Gas Assets via Resilience	43
<i>Stig Johnsen</i>	
4	
Legal Aspects of Protecting Intellectual Property in Additive Manufacturing	63
<i>Adam Brown, Mark Yampolskiy, Jacob Gatlin and Todd Andel</i>	
PART II CONTROL SYSTEMS SECURITY	
5	
Practical Application Layer Emulation in Industrial Control System Honeypots	83
<i>Kyle Girtz, Barry Mullins, Mason Rice and Juan Lopez</i>	
6	
Lightweight Journaling for SCADA Systems via Event Correlation	99
<i>Antoine Lemaq, Alireza Sadighian and Jose Fernandez</i>	

7

Forensic Analysis of a Siemens Programmable Logic Controller 117
Raymond Chan and Kam-Pui Chow

8

Division of Cyber Safety and Security Responsibilities Between 131
 Control System Owners and Suppliers
Ruth Skotnes

PART III INFRASTRUCTURE MODELING AND SIMULATION

9

Multigraph Critical Infrastructure Model 149
Bernhard Schneidhofer and Stephen Wolthusen

10

Enhancing Decision Support with Interdependency Modeling 169
Dario Masucci, Cosimo Palazzo, Chiara Foglietta and Stefano Panzieri

11

Integrating Simulated Physics and Device Virtualization in Control 185
 System Testbeds
Owen Redwood, Jason Reynolds and Mike Burmester

12

A Multidisciplinary Predictive Model for Managing Critical 203
 Infrastructure Disruptions
Carol Romanowski, Rajendra Raj, Jennifer Schneider, Sumita Mishra, Bernard Brooks, Jessica Pardee, Bharat Bhole and Nikolaus Robalino

PART IV RISK AND IMPACT ASSESSMENT

13

Towards a Comparable Cross-Sector Risk Analysis: RAMCAP 221
 Revisited
Richard White, Aaron Burkhart, Terrance Boulton and Edward Chow

14

Classification and Comparison of Critical Infrastructure Protection 239
 Tools
George Stergiopoulos, Efstratios Vasilellis, Georgia Lykou, Panayiotis Kotzanikolaou and Dimitris Gritzalis

Contributing Authors

Todd Aniel is an Associate Professor of Computer Science at the University of South Alabama, Mobile, Alabama. His research interests include computer and information security, side-channel analysis, hardware/software partitioning, network security protocols and formal methods.

Bharat Bhole is an Associate Professor of Economics at Rochester Institute of Technology, Rochester, New York. His research interests include industrial organization, law and economics, and applied microeconomics.

Terry Boulton is the El Pomar Endowed Chair of Innovation and Security and Professor of Computer Science at the University of Colorado Colorado Springs, Colorado Springs, Colorado. His research interests include biometrics, visual security systems, facial recognition and wireless networks.

Bernard Brooks is a Professor of Mathematical Sciences at Rochester Institute of Technology, Rochester, New York. His research interests include agent-based models, applied dynamical systems and modeling human systems and rumor flow in social networks.

Adam Brown is a Ph.D. student in Computing at the University of South Alabama, Mobile, Alabama. His research interests include cyber law, cyber security and formal methods.

Aaron Burkhart is a Ph.D. student in Computer Science at the University of Colorado Colorado Springs, Colorado; and a Software Engineer Associate at Lockheed Martin in Colorado Springs, Colorado. His research interests include web programming, cloud computing, computer graphics and software architectures.

Mike Burmester is a Professor of Computer Science at Florida State University, Tallahassee, Florida. His research interests include computer and network security, cyber-physical system protection, pervasive and ubiquitous systems, trust management and cryptography.

Raymond Chan is a Ph.D. student in Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include digital forensics and critical infrastructure protection.

Edward Chow is a Professor of Computer Science at the University of Colorado Colorado Springs, Colorado Springs, Colorado. His research focuses on improving the performance, reliability and security of networked systems.

Kam-Pui Chow is an Associate Professor of Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include information security, digital forensics, live system forensics and digital surveillance.

Jose Fernandez is an Associate Professor of Computer and Software Engineering at Ecole Polytechnique de Montreal, Montreal, Canada. His research interests include industrial control systems security, critical infrastructure security, cyber crime, cyber public health and cyber conflict.

Chiara Foglietta is a Researcher at the University of Roma Tre, Rome, Italy. Her research interests include industrial control systems (especially, energy management systems), resilient control algorithms for smart grids and data fusion techniques.

Jacob Gatlin is an undergraduate student in Computer Engineering at the University of South Alabama, Mobile, Alabama. His research interests include additive manufacturing security and additive manufactured circuits.

Kyle Girtz is an M.S. student in Cyber Operations at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include critical infrastructure protection and reverse engineering.

Michael Grimaila is a Professor of Systems Engineering and a Member of the Center for Cyberspace Research at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include computer engineering, mission assurance, quantum communications and cryptography, data analytics, network management and security, and systems engineering.

Dimitris Gritzalis is Associate Rector, Professor of Information Security and Director of the Information Security and Critical Infrastructure Protection Laboratory at Athens University of Economics and Business, Athens, Greece. His research interests include critical infrastructure protection, social media intelligence, smartphone security and privacy, and malware detection and prevention.

Christine Izuakor is a Ph.D. candidate in Security Engineering at the University of Colorado Colorado Springs, Colorado Springs, Colorado. Her research interests include critical infrastructure protection, vulnerability management and information technology compliance.

Stig Johnsen is a Senior Research Scientist in the Department of Technology and Society at SINTEF, Trondheim, Norway; and a Postdoctoral Researcher in the Faculty of Information Technology, Mathematics and Electrical Engineering at the Norwegian University of Science and Technology, Trondheim, Norway. His research interests include safety and information security (especially in offshore oil and gas facilities), human factors in complex operations, resilience engineering, and risk and safety analysis.

Panayiotis Kotzanikolaou is an Assistant Professor of Information and Communications Technology Security at the University of Piraeus, Piraeus, Greece. His research interests include network security and privacy, critical infrastructure protection and applied cryptography.

Antoine Lemay is a Researcher in the Department of Computer and Software Engineering at Ecole Polytechnique de Montreal, Montreal, Canada. His research interests include industrial control systems security, critical infrastructure protection, cyber crime ecosystems and cyber conflict.

Juan Lopez is a Research Engineer with Applied Research Solutions, Beavercreek, Ohio, who supports the Center for Cyberspace Research at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include critical infrastructure protection, radio frequency intelligence and telecommunications engineering.

Georgia Lykou is a Ph.D. candidate in Informatics and a Researcher in the Information Security and Critical Infrastructure Protection Laboratory at Athens University of Economics and Business, Athens, Greece. Her research interests include critical infrastructure protection, risk assessment and environmental threats.

Dario Masucci is a Research Collaborator in the Models for Critical Infrastructure Protection Laboratory at the University of Roma Tre, Rome, Italy. His research interests include multi-objective optimization (especially, multi-criteria decision making), energy sustainability and model development.

Sumita Mishra is an Associate Professor of Computing Security at Rochester Institute of Technology, Rochester, New York. Her research interests include critical infrastructure protection, resource-constrained networking and security.

Barry Mullins is a Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include cyber operations, critical infrastructure protection and computer/network/embedded systems security.

Cosimo Palazzo is a Ph.D. student in Computer Science and Automation at the University of Roma Tre, Rome, Italy. His research interests include critical infrastructure modeling and simulation, and robotics.

Stefano Panzieri is an Associate Professor of Automatic Control and the Head of the Models for Critical Infrastructure Protection Laboratory at the University of Roma Tre, Rome, Italy. His research interests include industrial control systems, robotics and sensor fusion.

Jessica Pardee is an Associate Professor of Science, Technology and Society at Rochester Institute of Technology, Rochester, New York. Her research focuses on how intersectional identities shape lived disaster experiences.

Michael Quigg is an M.S. student in Information Technology Management at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include organizational structure and cyber protection.

Rajendra Raj is a Professor of Computer Science at Rochester Institute of Technology, Rochester, New York. His research interests include real-world applications of data management, distributed computing and security.

Benjamin Ramsey is an Assistant Professor of Computer Science at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include wireless network security and critical infrastructure protection.

Owen Redwood is the Co-Founder and Chief Executive Officer of Hack All The Things, LLC, Orlando, Florida. His research interests include cyber-physical system vulnerability research, embedded systems reverse engineering, industrial control systems security, exploit development and cyber operations.

Jason Reynolds is the Chief Technology Officer of Hack All The Things, LLC, Orlando, Florida. His research interests include vulnerability research, operating system design and hardening, exploit development, web application exploitation and digital forensics.

Mason Rice is an Assistant Professor of Computer Science at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include network and telecommunications security, cyber-physical systems security and critical infrastructure protection.

Nikolaus Robalino is an Assistant Professor of Economics at Rochester Institute of Technology, Rochester, New York. His research interests include microeconomic theory and behavioral economics.

Carol Romanowski is an Associate Professor of Computer Science at Rochester Institute of Technology, Rochester, New York. Her research interests include applications of data science and data mining to critical infrastructure protection, cyber security and engineering design.

Alireza Sadighian is a Postdoctoral Fellow in Computer Engineering at Ecole de Technologie Supérieure, Montreal, Canada; and a Research and Development Leader at Groupe Access Company, Montreal, Canada. His research interests include network security, especially machine learning and data mining applications in network security.

Jennifer Schneider is the Eugene H. Fram Chair of Applied Critical Thinking and a Professor of Environmental Management, Health and Safety at Rochester Institute of Technology, Rochester, New York. Her research interests include community resilience, risk and disaster decision systems, and multidimensional sustainability.

Bernhard Schneidhofer is an Information Security Architect at Erste Group IT in Vienna, Austria. His research interests include modeling and analysis of critical infrastructure systems, especially in the energy and healthcare sectors.

Ruth Skotnes is a Research Scientist at the International Research Institute of Stavanger, Stavanger, Norway; and an Associate Professor at the Centre for Risk Management and Societal Safety, University of Stavanger, Stavanger, Norway. Her research interests include critical infrastructure protection, information and communications systems safety and security, risk regulation, risk perception and safety culture.

George Stergiopoulos is a Senior Researcher and Postdoctoral Fellow in the Information Security and Critical Infrastructure Protection Laboratory at Athens University of Economics and Business, Athens, Greece. His research interests include critical infrastructure protection, applications security, cryptography and software engineering.

Efstratios Vasilellis is an M.Sc. student in Informatics and an Assistant Researcher in the Information Security and Critical Infrastructure Protection Laboratory at Athens University of Economics and Business, Athens, Greece. His research interests include critical infrastructure protection and information security.

Richard White is an Assistant Research Professor of Security Engineering at the University of Colorado Colorado Springs, Colorado Springs, Colorado. His research interests include risk management and critical infrastructure protection.

Stephen Wolthusen is a Professor of Information Security in the Faculty of Information Technology, Mathematics and Electrical Engineering at the Norwegian University of Science and Technology, Gjøvik, Norway; and a Reader in Mathematics at Royal Holloway, University of London, London, United Kingdom. His research interests include critical infrastructure protection and cyber-physical systems security.

Mark Yampolskiy is an Assistant Professor of Computer Science at the University of South Alabama, Mobile, Alabama. His research focuses on the security aspects of additive manufacturing, cyber-physical systems and the Internet of Things.

Preface

The information infrastructure – comprising computers, embedded devices, networks and software systems – is vital to operations in every sector: information technology, telecommunications, energy, banking and finance, transportation systems, chemicals, agriculture and food, defense industrial base, public health and health care, national monuments and icons, drinking water and water treatment systems, commercial facilities, dams, emergency services, commercial nuclear reactors, materials and waste, postal and shipping, and government facilities. Global business and industry, governments, indeed society itself, cannot function if major components of the critical information infrastructure are degraded, disabled or destroyed.

This book, *Critical Infrastructure Protection X*, is the tenth volume in the annual series produced by IFIP Working Group 11.10 on Critical Infrastructure Protection, an active international community of scientists, engineers, practitioners and policy makers dedicated to advancing research, development and implementation efforts related to critical infrastructure protection. The book presents original research results and innovative applications in the area of infrastructure protection. Also, it highlights the importance of weaving science, technology and policy in crafting sophisticated, yet practical, solutions that will help secure information, computer and network assets in the various critical infrastructure sectors.

This volume contains fourteen revised and edited papers from the Tenth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, held at SRI International in Arlington, Virginia, USA on March 14–16, 2016. The papers were refereed by members of IFIP Working Group 11.10 and other internationally-recognized experts in critical infrastructure protection. The post-conference manuscripts submitted by the authors were rewritten to accommodate the suggestions provided by the conference attendees. They were subsequently revised by the editors to produce the final chapters published in this volume.

The chapters are organized into four sections: themes and issues, control systems security, infrastructure modeling and simulation, and risk and impact assessment. The coverage of topics showcases the richness and vitality of the discipline, and offers promising avenues for future research in critical infrastructure protection.

This book is the result of the combined efforts of several individuals and organizations. In particular, we thank Zach Tudor and Heather Drinan for their tireless work on behalf of IFIP Working Group 11.10. We gratefully acknowledge the Institute for Information Infrastructure Protection (I3P), managed by George Washington University, for its sponsorship of IFIP Working Group 11.10. We also thank the Department of Homeland Security, National Security Agency and SRI International for their support of IFIP Working Group 11.10 and its activities. Finally, we wish to note that all opinions, findings, conclusions and recommendations in the chapters of this book are those of the authors and do not necessarily reflect the views of their employers or funding agencies.

MASON RICE AND SUJEET SHENOI