

Editor-in-Chief

*A. Joe Turner, Seneca, SC, USA*

Editorial Board

Foundations of Computer Science

*Jacques Sakarovitch, Télécom ParisTech, France*

Software: Theory and Practice

*Michael Goedicke, University of Duisburg-Essen, Germany*

Education

*Arthur Tatnall, Victoria University, Melbourne, Australia*

Information Technology Applications

*Erich J. Neuhold, University of Vienna, Austria*

Communication Systems

*Aiko Pras, University of Twente, Enschede, The Netherlands*

System Modeling and Optimization

*Fredi Tröltzsch, TU Berlin, Germany*

Information Systems

*Jan Pries-Heje, Roskilde University, Denmark*

ICT and Society

*Diane Whitehouse, The Castlegate Consultancy, Malton, UK*

Computer Systems Technology

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

Security and Privacy Protection in Information Processing Systems

*Yuko Murayama, Iwate Prefectural University, Japan*

Artificial Intelligence

*Tharam Dillon, Curtin University, Bentley, Australia*

Human-Computer Interaction

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

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. An umbrella organization for societies working in information processing, IFIP's aim is two-fold: to support information processing within its member countries and to encourage technology transfer to developing nations. As its mission statement clearly states,

*IFIP's mission is to be the leading, truly international, apolitical organization which encourages and assists in the development, exploitation and application of information technology for the benefit of all people.*

IFIP is a non-profitmaking organization, run almost solely by 2500 volunteers. It operates through a number of technical committees, which organize events and publications. IFIP's events range from an international congress to local seminars, but the most important are:

- The IFIP World Computer Congress, held every second year;
- Open conferences;
- Working conferences.

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 small and 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.

Any national society whose primary activity is about information processing may apply to become a full member of IFIP, although full membership is restricted to one society per country. Full members are entitled to vote at the annual General Assembly, National societies preferring a less committed involvement may apply for associate or corresponding membership. Associate members enjoy the same benefits as full members, but without voting rights. Corresponding members are not represented in IFIP bodies. Affiliated membership is open to non-national societies, and individual and honorary membership schemes are also offered.

Jonathan Butts Sujeet Shenoi (Eds.)

# Critical Infrastructure Protection VIII

8th IFIP WG 11.10 International Conference, ICCIP 2014  
Arlington, VA, USA, March 17-19, 2014  
Revised Selected Papers

 Springer

## Volume Editors

Jonathan Butts

Air Force Institute of Technology

Wright-Patterson Air Force Base

Dayton, OH 45433-7765, USA

E-mail: jonathan.butts@afit.edu

Sujeet Sheno

University of Tulsa

Tulsa, OK 74104-3189, USA

E-mail: sujeet@utulsa.edu

ISSN 1868-4238

ISBN 978-3-662-45354-4

DOI 10.1007/978-3-662-45355-1

e-ISSN 1868-422X

e-ISBN 978-3-662-45355-1

Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014952306

© IFIP International Federation for Information Processing 2014

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. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

*Typesetting:* Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

# Contents

Contributing Authors	ix
Preface	xvii
PART I CONTROL SYSTEMS SECURITY	
1	
Detecting Integrity Attacks on Industrial Control Systems	3
<i>Chad Arnold, Jonathan Butts, and Krishnaprasad Thirunarayan</i>	
2	
Detecting Malicious Software Execution in Programmable Logic Controllers Using Power Fingerprinting	15
<i>Carlos Aguayo Gonzalez and Alan Hinton</i>	
3	
Timing of Cyber-Physical Attacks on Process Control Systems	29
<i>Marina Krotofil, Alvaro Cardenas, and Kishore Angrishi</i>	
4	
Recovery of Structural Controllability for Control Systems	47
<i>Cristina Alcaraz and Stephen Wolthusen</i>	
5	
Industrial Control System Traffic Data Sets for Intrusion Detection Research	65
<i>Thomas Morris and Wei Gao</i>	
6	
An Industrial Control System Testbed Based on Emulation, Physical Devices and Simulation	79
<i>Haihui Gao, Yong Peng, Zhonghua Dai, Ting Wang, Xuefeng Han, and Hanjing Li</i>	

## PART II INFRASTRUCTURE SECURITY

7

Evidence Theory for Cyber-Physical Systems 95  
*Riccardo Santini, Chiara Foglietta and Stefano Panzieri*

8

An Automated Dialog System for Conducting Security Interviews 111  
 for Access Control  
*Mohammad Ababneh, Malek Athamnah, Duminda Wijesekera and Paulo Costa*

9

A Survey of Critical Infrastructure Security 127  
*William Hurst, Madjid Merabti, and Paul Fergus*

## PART III INFRASTRUCTURE MODELING AND SIMULATION

10

A System Dynamics Framework for Modeling Critical 141  
 Infrastructure Resilience  
*Simona Cavallini, Cristina d'Alessandro, Margherita Volpe,  
 Stefano Armenia, Camillo Carlini, Elisabeth Brein,  
 and Pierluigi Assogna*

11

Reinforcement Learning Using Monte Carlo Policy Estimation for 155  
 Disaster Mitigation  
*Mohammed Talat Khouj, Sarbjit Sarkaria, Cesar Lopez,  
 and Jose Marti*

12

Accuracy of Service Area Estimation Methods Used for Critical 173  
 Infrastructure Recovery  
*Okan Pala, David Wilson, Russell Bent, Steve Linger,  
 and James Arnold*

## PART IV RISK AND IMPACT ASSESSMENT

13

A Decision Support Tool for a Unified Homeland Security Strategy 195  
*Richard White, Aaron Burkhart, Edward Chow,  
 and Logan Maynard*

<i>Contents</i>	vii
14	
Assessing the Impact of Cyber Attacks on Wireless Sensor Nodes That Monitor Interdependent Physical Systems	213
<i>Valerio Formicola, Antonio Di Pietro, Abdullah Alsubaie, Salvatore D'Antonio, and Jose Marti</i>	
15	
Assessing Potential Casualties in Critical Events	231
<i>Simona Cavallini, Fabio Bisogni, Marco Bardoscia, and Roberto Bellotti</i>	
PART V ADVANCED TECHNIQUES	
16	
Evaluation of Format-Preserving Encryption Algorithms for Critical Infrastructure Protection	245
<i>Richard Agbeyibor, Jonathan Butts, Michael Grimaila, and Robert Mills</i>	
17	
Asynchronous Binary Byzantine Consensus over Graphs with Power-Law Degree Sequence	263
<i>Goitom Weldehawaryat and Stephen Wolthusen</i>	

# Contributing Authors

**Mohammad Ababneh** recently received his Ph.D. degree in Information Technology from George Mason University, Fairfax, Virginia. His research interests include information security and assurance, command and control, semantic web and information systems.

**Richard Agbeyibor** is an M.S. student in Electrical Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include computer and network security, digital systems and avionics.

**Carlos Aguayo Gonzalez** is the Founder and Chief Technology Officer of PFP CyberSecurity, Vienna, Virginia. His research interests include cyber security, critical infrastructure protection, side channel information, machine learning and signal processing.

**Cristina Alcaraz** is a Marie Curie Postdoctoral Researcher at the School of Mathematics and Information Security at Royal Holloway, University of London, London, United Kingdom. Her research interests include critical information infrastructure protection, SCADA systems, smart grids and wireless sensor networks.

**Abdullah Alsubaie** is a Ph.D. student in Electrical Engineering at the University of British Columbia, Vancouver, Canada; and a Researcher at King Abdulaziz City for Science and Technology, Riyadh, Saudi Arabia. His research interests include power systems operation, smart grids and critical infrastructure simulation.

**Kishore Angrishi** is an IT Consultant with T-Systems International in Hamburg, Germany. His research interests include security and traffic engineering in data networks.



**Stefano Armenia** is a Research Fellow in the Department of Computer, Control and Management Engineering at Sapienza University of Rome, Rome, Italy. His research interests include cyber security, critical infrastructure protection, policy modeling, risk management, system dynamics and complex systems analysis.

**Chad Arnold** is a Ph.D. student in Computer Science at Wright State University, Dayton, Ohio. His research interests include computer and network security, critical infrastructure protection and malware analysis.

**James Arnold** received his M.S. degree in Geography from the University of Utah, Salt Lake City, Utah. His research interests include spatial analysis, geographic information systems and remote sensing.

**Pierluigi Assogna** is a Senior Consultant with Theorematica SpA, Rome, Italy. His research interests include knowledge management, control systems and decision support systems.

**Malek Athamnah** is a Ph.D. student in Computer Science at Temple University, Philadelphia, Pennsylvania. His research interests include information security and voice-based services.

**Marco Bardoscia** is a Postdoctoral Fellow at the Abdus Salam International Centre for Theoretical Physics, Trieste, Italy. His research focuses on applications of statistical physics to socio-economic systems.

**Roberto Bellotti** is an Associate Professor of Experimental Physics at the University of Bari Aldo Moro, Bari, Italy. His research interests include econophysics, medical physics and astroparticle physics.

**Russell Bent** is a Research Scientist in the Energy and Infrastructure Analysis Group at Los Alamos National Laboratory, Los Alamos, New Mexico. His research focuses on algorithms for planning, operating and designing the next generation of critical infrastructure systems.

**Fabio Bisogni** is a Member of the Board of the FORMIT Foundation, Rome, Italy. His research interests include information security economics, critical infrastructure protection and information disclosure policy.

**Elisabeth Brein** is a Researcher at the Rotterdam School of Management, Erasmus University Rotterdam, Rotterdam, The Netherlands. Her research focuses on the identification of social system variables, such as human behavior and leadership, during crisis situations.

**Aaron Burkhart** is an M.S. student in Computer Science at the University of Colorado at Colorado Springs, 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.

**Jonathan Butts**, Chair, IFIP Working Group 11.10 on Critical Infrastructure Protection, is an Assistant Professor of Computer Science and the Research Director of 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 and cyber-physical systems security.

**Alvaro Cardenas** is an Assistant Professor of Computer Science at the University of Texas at Dallas, Richardson, Texas. His research interests include the security and privacy of cyber-physical systems and network security monitoring.

**Camillo Carlini** is a Research Fellow in the Department of Computer, Control and Management Engineering at Sapienza University of Rome, Rome, Italy. His research interests include system dynamics, critical infrastructure protection, policy modeling, simulation, cyber security and complex systems analysis.

**Simona Cavallini** is the Head of the Research and Innovation Area at the FORMIT Foundation, Rome, Italy. Her research interests include critical infrastructure protection, interdependency analysis, economics of security and macroeconomics modeling.

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

**Paulo Costa** is an Associate Professor of Systems Engineering and Operations Research at George Mason University, Fairfax, Virginia. His research interests are in the area of Bayesian probabilistic reasoning, with a focus on decision support and multi-source data fusion.

**Zhonghua Dai** is a Researcher at the China Information Technology Security Evaluation Center, Beijing, China. His research focuses on industrial control system security.

**Cristina d'Alessandro** is a Senior Researcher at the FORMIT Foundation, Naples, Italy. Her research interests include critical infrastructure protection, urban and transportation infrastructures, innovation and technology transfer.

**Salvatore D'Antonio** is an Assistant Professor of Web Systems at the University of Naples Parthenope, Naples, Italy. His research interests include network and information security, critical infrastructure protection and cloud security.

**Antonio Di Pietro** is a Researcher with ENEA, Rome, Italy. His research interests include critical infrastructure modeling, decision support systems and data fusion.

**Paul Fergus** is a Senior Lecturer of Computer Science at Liverpool John Moores University, Liverpool, United Kingdom. His research interests include artificial intelligence, semantic web, bioinformatics and data science.

**Chiara Foglietta** is a Researcher at the University of Roma Tre, Rome, Italy. Her research interests include industrial control systems (especially energy management systems), critical infrastructure interdependencies and data fusion techniques.

**Valerio Formicola** is a Postdoctoral Researcher in the Department of Engineering at the University of Naples Parthenope, Naples, Italy. His research interests include network and information security, critical infrastructure protection and cyber-physical systems.

**Haihui Gao** is a Researcher at the China Information Technology Security Evaluation Center, Beijing, China. His research interests include critical infrastructure protection, network testbeds, cyber-physical systems and information processing.

**Wei Gao** is an Industrial Control Systems Security Research Engineer at Siemens Corporation, Atlanta, Georgia. His research interests include SCADA system security, malware analysis and software vulnerability discovery.

**Michael Grimaila** is an Associate Professor of Systems Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include computer and network security, data analytics, quantum information, quantum key distribution and systems engineering.

**Xuefeng Han** is a Researcher at the China Information Technology Security Evaluation Center, Beijing, China. His research interests include industrial control system security and security testing.

**Alan Hinton** is a Principal Systems Engineer at PFP CyberSecurity, Vienna, Virginia. His research interests include side channel information processing for cyber security applications and signal processing architectures.

**William Hurst** is a Senior Lecturer of Computer Science at Liverpool John Moores University, Liverpool, United Kingdom. His research interests include cyber security, data classification and critical infrastructure simulation.

**Mohammed Talat Khouj** is a Postdoctoral Fellow in the Department of Electrical and Computer Engineering at the University of British Columbia, Vancouver, Canada. His research interests include the real-time simulation of complex systems with a focus on resource allocation optimization in inter-dependent systems.

**Marina Krotofil** is a Research Assistant at the Institute for Security in Distributed Applications, Hamburg University of Technology, Hamburg, Germany. Her research interests include cyber-physical system security and process-aware risk assessment of industrial control systems.

**Hanjing Li** is an M.E. student in Electronic Information Engineering at the Beijing University of Technology, Beijing, China. Her research interests include signal processing and digital image processing.

**Steve Linger** is an R&D Engineer at Los Alamos National Laboratory, Los Alamos, New Mexico. His research interests include electric power systems, water systems and atmospheric modeling.

**Cesar Lopez** is a Ph.D. student in Electrical and Computer Engineering at the University of British Columbia, Vancouver, Canada. His research interests include the real-time simulation of complex systems with a focus on infrastructure interdependencies in problems involving energy systems and disaster response scenarios.

**Jose Marti** is a Professor of Electrical and Computer Engineering at the University of British Columbia, Vancouver, Canada. His research interests include complex systems, power systems and critical infrastructures.

**Logan Maynard** is an Instructor and Researcher with Navy Cyber Forces in Colorado Springs, Colorado. His research interests include space systems security, self-healing networks and anti-jamming techniques.

**Madjid Merabti** is the Director and Head of Research at the School of Computing and Mathematical Sciences, Liverpool John Moores University, Liverpool, United Kingdom. His research interests include distributed multimedia systems, computer networks, operating systems and computer security.

**Robert Mills** is an Associate Professor of Electrical Engineering and the Director of the Center for Cyberspace Research at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include network security and management, cyber situational awareness and electronic warfare.

**Thomas Morris** is an Associate Professor of Electrical and Computer Engineering and the Director of the Critical Infrastructure Protection Center at Mississippi State University, Mississippi State, Mississippi. His research interests include industrial control systems and power system security.

**Okan Pala** is a Ph.D. student in Software and Information Systems at the University of North Carolina at Charlotte, Charlotte, North Carolina. His research interests include intelligent software systems, spatial decision support systems, geographic information systems, critical infrastructure protection, computational geometry and accuracy assessment.

**Stefano Panzieri** is an Associate Professor of Engineering and the Head of the Automation Laboratory at the University of Roma Tre, Rome, Italy. His research interests include industrial control systems, robotics and sensor fusion.

**Yong Peng** is a Research Fellow at the China Information Technology Security Evaluation Center, Beijing, China. His research interests include critical infrastructure protection, SCADA systems and complex systems analysis.

**Riccardo Santini** is a Ph.D. student in Computer Science and Automation at the University of Roma Tre, Rome, Italy. His research interests are in the area of control theory with an emphasis on renewable resources, smart grids, robotics and data fusion techniques.

**Sarbjit Sarkaria** is a Sessional Lecturer of Electrical and Computer Engineering at the University of British Columbia, Vancouver, Canada. His research interests include machine learning and critical infrastructure protection.

**Krishnaprasad Thirunarayan** is a Professor of Computer Science and Engineering at Wright State University, Dayton, Ohio. His research interests include big data analytics, Web 3.0, information retrieval, trust networks and programming languages.

**Margherita Volpe** is a Researcher at the FORMIT Foundation, Rome, Italy. Her research interests include critical infrastructure protection, crisis management, public-private entity interactions, international law and macroeconomics policies.

**Ting Wang** is a Researcher at the China Information Technology Security Evaluation Center, Beijing, China. Her research focuses on industrial control system security.

**Goitom Weldehawaryat** is a Ph.D. student in Information Security at the Norwegian Information Security Laboratory, Gjøvik University College, Gjøvik, Norway. His research interests include the modeling and analysis of critical infrastructure networks, Byzantine fault tolerance and digital forensics.

**Richard White** is the Director of Academic Programs at Everest University Online in Colorado Springs, Colorado. His research interests include risk management and critical infrastructure protection.

**Duminda Wijesekera** is a Professor of Computer Science at George Mason University, Fairfax, Virginia. His research interests include information security, safety and security of wireless-controlled trains, security and privacy of healthcare applications, and financial crime.

**David Wilson** is an Associate Professor of Software and Information Systems at the University of North Carolina at Charlotte, Charlotte, North Carolina. His research interests include intelligent software systems and the application of intelligent systems techniques to geographic, multimedia, database, Internet and communications systems.

**Stephen Wolthusen** is a Professor of Information Security at the Norwegian Information Security Laboratory, Gjøvik University College, Gjøvik, Norway; and a Reader in Mathematics at Royal Holloway, University of London, London, United Kingdom. His research interests include the modeling and analysis of critical infrastructure networks, and distributed systems security.

# 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 VIII*, is the eighth 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 seventeen edited papers from the Eighth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, held at SRI International in Arlington, Virginia, USA on March 17–19, 2014. The papers were refereed by members of IFIP Working Group 11.10 and other internationally-recognized experts in critical infrastructure protection.

The chapters are organized into five sections: control systems security, infrastructure security, infrastructure modeling and simulation, risk and impact assessment, and advanced techniques. 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, Richard George, Heather Drinan and Nicole Hall Hewett for their tireless work on behalf of IFIP Working Group 11.10. We gratefully acknowledge the Institute for Information Infra-



structure Protection (I3P), managed by Dartmouth College, for its sponsorship of IFIP Working Group 11.10. We also thank the Department of Homeland Security, the 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.

JONATHAN BUTTS AND SUJEET SHENOI