IFIP Advances in Information and Communication Technology 466

Editor-in-Chief

Kai Rannenberg, Goethe University Frankfurt, Germany

Editorial Board

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.

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

Mason Rice · Sujeet Shenoi (Eds.)

Critical Infrastructure Protection IX

9th IFIP 11.10 International Conference, ICCIP 2015
Arlington, VA, USA, March 16–18, 2015
Revised Selected Papers

Springer

Editors
Mason Rice
Department of Electrical and
Computer Engineering
Air Force Institute of Technology
Wright-Patterson AFB, Ohio
USA

Sujeet Shenoi
Tandy School of Computer Science
University of Tulsa
Tulsa, Oklahoma
USA

ISSN 1868-4238 ISSN 1868-422X (electronic)
IFIP Advances in Information and Communication Technology
ISBN 978-3-319-26566-7 ISBN 978-3-319-26567-4 (eBook)
DOI 10.1007/978-3-319-26567-4

Library of Congress Control Number: 2015954603

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media
(www.springer.com)

Contents

Contributing Authors ix

Preface xvii

PART I THEMES AND ISSUES

1
A Model for Characterizing Cyberpower 3
Adrian Venables, Siraj Ahmed Shaikh and James Shuttleworth

2
Cyber Attacks and Political Events: The Case of the Occupy Central Campaign 17
Kam-Pui Chow, Ken Yau and Frankie Li

3
On the Sharing of Cyber Security Information 29
Eric Luiijf and Marieke Klaver

PART II CONTROL SYSTEMS SECURITY

4
Modeling Message Sequences for Intrusion Detection in Industrial Control Systems 49
Marco Caselli, Emmanuele Zambon, Jonathan Petit and Frank Kargl

5
Industrial Control System Fingerprinting and Anomaly Detection 73
Yong Peng, Chong Xiang, Haihui Gao, Dongqing Chen and Wang Ren

6
Traffic-Locality-Based Creation of Flow Whitelists for SCADA Networks 87
Seungoh Choi, Yeop Chang, Jeong-Han Yun and Woonyon Kim

7
A Symbolic Honeynet Framework for SCADA System Threat Intelligence 103
Owen Redwood, Joshua Lawrence and Mike Burmester

8
Enhancing a Virtual SCADA Laboratory Using Simulink 119
Zach Thornton and Thomas Morris

9
How Industrial Control System Security Training is Falling Short 135
Jonathan Butts and Michael Glover

PART III CYBER-PHYSICAL SYSTEMS SECURITY

10
Runtime Integrity for Cyber-Physical Infrastructures 153
Jonathan Jenkins and Mike Burmester

11
Security Challenges of Additive Manufacturing with Metals and Alloys 169
Mark Yampolskiy, Lena Schutzle, Uday Vaidya and Alec Yasinsac

12
Using Information Flow Methods to Secure Cyber-Physical Systems 185
Gerry Howser

PART IV INFRASTRUCTURE SECURITY

13
Evaluating ITU-T G.9959 Based Wireless Systems Used in Critical Infrastructure Assets 209
Christopher Badenhop, Jonathan Fuller, Joseph Hall, Benjamin Ramsey and Mason Rice

14
Implementing Cyber Security Requirements and Mechanisms in Microgrids 229
Apurva Mohan and Himanshu Khurana

15
A Cyber Security Architecture for Microgrid Deployments 245
Apurva Mohan, Gregory Brainard, Himanshu Khurana and Scott Fischer

PART V INFRASTRUCTURE MODELING AND SIMULATION

16
Allocation and Scheduling of Firefighting Units in Large Petrochemical Complexes 263
Khaled Alutaibi, Abdullah Alsubaie and Jose Marti

17
Situational Awareness Using Distributed Data Fusion with Evidence Discounting 281
Antonio Di Pietro, Stefano Panzieri and Andrea Gasparri

PART VI RISK AND IMPACT ASSESSMENT

18
Using Centrality Measures in Dependency Risk Graphs for Efficient Risk Mitigation 299
George Stergiopoulos, Marianthi Theocharidou, Panayiotis Kotzanikolaou and Dimitris Gritzalis

19
Assessing Cyber Risk Using the CISIApro Simulator 315
Chiara Foglietta, Cosimo Palazzo, Riccardo Santini and Stefano Panzieri

Contributing Authors

Abdullah Alsubaie is a Ph.D. candidate in Electrical and Computer 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 protection.

Khaled Alutaibi is a Ph.D. candidate in Electrical and Computer Engineering at the University of British Columbia, Vancouver, Canada; and a Senior Officer at the Civil Defense Headquarters, Riyadh, Saudi Arabia. His research interests include decision support systems, critical infrastructure protection and emergency response.

Christopher Badenhop is a Ph.D. student in Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include computer network security, embedded systems security and RF communications.

Gregory Brainard is a Technical Manager at Honeywell Defense and Space, Albuquerque, New Mexico. His research interests include microgrid design and construction, and microgrid security.

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.

Jonathan Butts, Chair, IFIP Working Group 11.10 on Critical Infrastructure Protection, is the Founder of QED Secure Solutions, Coppell, Texas. His research interests include critical infrastructure protection and cyber-physical systems security.

Marco Caselli is a Ph.D. student in Computer Security at the University of Twente, Enschede, The Netherlands. His research interests include industrial control systems and building automation, with a focus on critical infrastructures.

Yeop Chang is a Senior Member of the Engineering Staff at the National Security Research Institute, Daejeon, South Korea. His research interests include industrial control systems security and reverse engineering.

Dongqing Chen is a Researcher at the China Information Technology Security Evaluation Center, Beijing, China. Her research interests include critical infrastructure protection, cyber-physical system testbeds and complex systems analysis.

Seungoh Choi is a Member of the Engineering Staff at the National Security Research Institute, Daejeon, South Korea. His research interests include critical infrastructure protection and network security.

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.

Antonio Di Pietro is a Staff Scientist at the Laboratory for the Analysis and Protection of Critical Infrastructures, ENEA, Rome, Italy. His research interests include critical infrastructure modeling, decision support systems and data fusion algorithms.

Scott Fischer is a Principal Systems Engineer at Honeywell Defense and Space, Glendale, Arizona. His research interests include microgrid design and construction, and microgrid security.

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

Jonathan Fuller is an M.S. student in Computer Science at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include wireless sensor networks and computer and network security.

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 cloud computing.

Andrea Gasparri is an Assistant Professor of Engineering at the University of Roma Tre, Rome, Italy. His research interests include robotics, sensor networks and networked multiagent systems.

Michael Glover is the Managing Partner of Fox Three, McKinney, Texas. His research interests include SCADA systems security, risk analysis and strategic policies.

Dimitris Gritzalis is a Professor of Information Security and the Director of the Information Security and Critical Infrastructure Protection Laboratory at the Athens University of Economics and Business, Athens, Greece. His research interests include critical infrastructure protection, open source intelligence, advanced persistent threats and digital forensics.

Joseph Hall is an M.S. student in Cyberspace Operations at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include network security and wireless sensor networks.

Gerry Howser is an Assistant Professor of Computer Science at Kalamazoo College, Kalamazoo, Michigan. His research interests include computer and network security, cyber-physical system protection, trust management and applications of modal logic to system security and assurance.

Jonathan Jenkins is a Ph.D. student in Computer Science at Florida State University, Tallahassee, Florida. His research interests include computer security and integrity, cyber-physical systems security and trust management.

Frank Kargl is the Director of the Institute of Distributed Systems at Ulm University, Ulm, Germany; and a Professor of Security and Privacy at the University of Twente, Enschede, The Netherlands. His research interests are in the area of mobile and self-organizing networks, and security and privacy of information technology systems, with a special focus on vehicular ad-hoc networks and industrial control systems.

Himanshu Khurana is the Director of Engineering at Honeywell Building Solutions, Golden Valley, Minnesota. His research interests are in the area of secure building automation and control systems.

Woonyon Kim is a Principal Member of the Engineering Staff at the National Security Research Institute, Daejeon, South Korea. His research interests include critical infrastructure protection and SCADA systems security.

Marieke Klaver is a Program Manager at the Netherlands Organisation for Applied Scientific Research (TNO), The Hague, The Netherlands. Her research interests include critical infrastructure protection and resilience.

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.

Joshua Lawrence is a Ph.D. student in Computer Science at Florida State University, Tallahassee, Florida. His research interests include critical infrastructure security, cyber-physical systems security and network security.

Frankie Li is a Research Staff Member at the Center for Information Security and Cryptography, University of Hong Kong, Hong Kong, China. His research interests include malware analysis and digital forensics.

Eric Luiijf is a Principal Consultant at the Netherlands Organisation for Applied Scientific Research (TNO), The Hague, The Netherlands. His research interests include information assurance and critical infrastructure protection.

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 infrastructure protection.

Apurva Mohan is a Cybersecurity Research Scientist at Honeywell Automation and Control Solutions Labs, Golden Valley, Minnesota. His research interests are in the areas of security and privacy for smart grids, industrial control systems, critical infrastructures, cloud computing, mobile computing and healthcare informatics.

Thomas Morris is an Associate Professor of Electrical and Computer Engineering, and the Director of the Center for Cybersecurity Research and Education at the University of Alabama in Huntsville, Huntsville, Alabama. His research interests include industrial control systems security, intrusion detection, machine learning and vulnerability testing.

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 Engineering 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.

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.

Jonathan Petit is a Research Fellow with the Computer Security Group at University College Cork, Cork, Ireland. His research interests include the security and privacy of cyber-physical systems, network security and intelligent transportation systems.

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 a Ph.D. student in Computer Science at Florida State University, Tallahassee, Florida. His research interests include computer and network security, vulnerability analysis and cyber-physical systems security.

Wang Ren is a Researcher at the China Information Technology Security Evaluation Center, Beijing, China. Her research interests include critical infrastructure protection, network security and complex systems analysis.

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.

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 cyber-physical systems from a control point of view with an emphasis on the topological properties of interconnected networks.

Lena Schutzle is an M.S. student in Mechanical Engineering at the Technical University of Munich, Munich, Germany. Her research interests are in the area of additive manufacturing.

Siraj Ahmed Shaikh is a Reader in Cyber Security at Coventry University, Coventry, United Kingdom. His research interests include cyber defense and systems security engineering focused on problems in the automotive and transportation domain.

James Shuttleworth is the Associate Head of the Department of Computing and the Digital Environment at Coventry University, Coventry, United Kingdom. His research interests include image analysis, wireless sensor networks, data visualization, in-network processing and systems integration.

George Stergiopoulos is a Ph.D. candidate in Informatics at the Athens University of Economics and Business, Athens, Greece. His research interests include critical infrastructure protection, applications security and software engineering.

Marianthi Theocharidou is a Scientific/Technical Support Officer at the Institute for the Protection and Security of the Citizen, European Commission Joint Research Center, Ispra, Italy. Her research interests include critical infrastructure protection, dependency modeling and risk assessment.

Zach Thornton received his M.S. degree in Electrical and Computer Engineering from Mississippi State University, Mississippi State, Mississippi. His research interests include virtual SCADA systems and industrial control systems security.

Uday Vaidya is the UT/ORNL Governor's Chair of Advanced Composites Manufacturing at the University of Tennessee at Knoxville, Knoxville, Tennessee. His research interests include advanced composites, applications development, prototyping and the commercialization of composites.

Adrian Venables is a Ph.D. student in Cyber Security at Coventry University, Coventry, United Kingdom. His research interests include cyberpower modeling, in particular, the role of innovation in the projection of influence in cyberspace.

Chong Xiang is a Researcher at the China Information Technology Security Evaluation Center, Beijing, China. His research interests include critical infrastructure protection, complex systems analysis, cyber-physical systems and cloud computing.

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.

Alec Yasinsac is a Professor and the Dean of the School of Computing at the University of South Alabama, Mobile, Alabama. His research interests include cyber security, critical infrastructure protection, Internet voting and digital forensics.

Ken Yau is a Research Staff Member at the Center for Information Security and Cryptography, University of Hong Kong, Hong Kong, China. His research interests include information security and digital forensics.

Jeong-Han Yun is a Senior Member of the Engineering Staff at the National Security Research Institute, Daejeon, South Korea. His research interests include industrial control systems security and network anomaly detection.

Emmanuele Zambon is a Postdoctoral Researcher with the Services, Cybersecurity and Safety Group at the University of Twente, Enschede, The Netherlands; and the Founder of SecurityMatters, Eindhoven, The Netherlands. His research interests include industrial control systems security and information technology risk management.

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 IX*, is the ninth 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 nineteen revised and edited papers from the Ninth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, held at SRI International in Arlington, Virginia, USA on March 16–18, 2015. 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 six sections: themes and issues, control systems security, cyber-physical systems security, infrastructure 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, 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 Infrastructure Protection (I3P), managed by Dartmouth College, 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