IFIP Advances in Information and Communication Technology 512

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 XI

11th IFIP WG 11.10 International Conference, ICCIP 2017
Arlington, VA, USA, March 13–15, 2017
Revised Selected Papers

Springer

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

Sujeet Shenoi
University of Tulsa
Tulsa, OK
USA

ISSN 1868-4238 ISSN 1868-422X (electronic)
IFIP Advances in Information and Communication Technology
ISBN 978-3-319-70394-7 ISBN 978-3-319-70395-4 (eBook)
https://doi.org/10.1007/978-3-319-70395-4

Library of Congress Control Number: 2017959615

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 ix

Preface xv

PART I INFRASTRUCTURE PROTECTION

1
Protecting the Transportation Sector from the Negative Impacts of Climate Change 3
Georgia Lykou, George Stergiopoulos, Antonios Papachrysanthou and Dimitris Gritzalis

2
Evaluation of Additive and Subtractive Manufacturing from the Security Perspective 23
Mark Yampolskiy, Wayne King, Gregory Pope, Sofia Belikovetsky and Yuval Elovici

3
Detecting Data Manipulation Attacks on the Substation Interlocking Function Using Direct Power Feedback 45
Eniye Tebekaemi, Edward Colbert and Duminda Wijesekera

4
Network Forensic Analysis of Electrical Substation Automation Traffic 63
Megan Leierzapf and Julian Rrushi

PART II INFRASTRUCTURE MODELING AND SIMULATION

5
Multiple Security Domain Model of a Vehicle in an Automated Platoon 81
Uday Kanteti and Bruce McMillin

6
Distributed Data Fusion for Situational Awareness in Critical Infrastructures with Link Failures 99
Antonio Di Pietro, Stefano Panzieri and Andrea Gasparri

7
Exploiting Web Ontologies for Automated Critical Infrastructure Data Retrieval 119
Luca Galbusera and Georgios Giannopoulos

PART III INDUSTRIAL CONTROL SYSTEM SECURITY

8
Enforcing End-to-End Security in SCADA Systems via Application-Level Cryptography 139
Adrian-Vasile Duka, Bela Genge, Piroska Haller and Bogdan Crainicu

9
Software Defined Response and Network Reconfiguration for Industrial Control Systems 157
Hunor Sandor, Bela Genge, Piroska Haller and Flavius Graur

10
Threat Analysis of an Elevator Control System 175
Raymond Chan and Kam-Pui Chow

11
Generating Honeypot Traffic for Industrial Control Systems 193
Htein Lin, Stephen Dunlap, Mason Rice and Barry Mullins

12
Challenges to Automating Security Configuration Checklists in Manufacturing Environments 225
Joshua Lubell and Timothy Zimmerman

13
Categorization of Cyber Training Environments for Industrial Control Systems 243
Evan Plumley, Mason Rice, Stephen Dunlap and John Pecarina

14
Multi-Controller Exercise Environments for Training Industrial Control System First Responders 273
Joseph Daoud, Mason Rice, Stephen Dunlap and John Pecarina

PART IV INTERNET OF THINGS SECURITY

15
Defending Building Automation Systems Using Decoy Networks 297
Caleb Mays, Mason Rice, Benjamin Ramsey, John Pecarina and Barry Mullins

16
Securing Bluetooth Low Energy Locks from Unauthorized Access and Surveillance 319
Anthony Rose, Jason Bindewald, Benjamin Ramsey, Mason Rice and Barry Mullins

Contributing Authors

Sofia Belikovetsky is a Ph.D. student in Information Systems Engineering at Ben-Gurion University of the Negev, Beer-Sheva, Israel. Her research focuses on the security of additive manufacturing processes and systems.

Jason Bindewald is an Assistant Professor of Computer Science at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include autonomous systems, machine learning, multi-agent system design and human-machine teaming.

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.

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.

Edward Colbert is a Cyber Security Researcher at the U.S. Army Research Laboratory in Adelphi, Maryland. His research interests include cyber-physical system security and Internet of Things security, especially in tactical environments.

Bogdan Crainicu is an Assistant Professor of Computer Science at Petru Maior University of Tirgu-Mures, Mures, Romania. His research interests include network and computer security, cryptography, software-defined networking and cloud computing architectures.

Joseph Daoud 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 cyber operations and critical infrastructure protection.

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 decision support systems for emergency management, geographical information systems and infrastructure modeling.

Adrian-Vasile Duka is an Assistant Professor of Engineering at Petru Maior University of Tirgu-Mures, Mures, Romania. His research interests include control systems engineering and cyber-physical system protection.

Stephen Dunlap is a Cyber Security Research Engineer at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include embedded system security, cyber-physical system security and critical infrastructure protection.

Yuval Elovici is a Professor of Information Systems Engineering, Director of the Telekom Innovation Laboratories and Head of the Cyber Security Research Center at Ben-Gurion University of the Negev, Beer-Sheva, Israel. His research interests include computer security and network security.

Luca Galbusera is a Scientific/Technical Support Officer at the Joint Research Centre of the European Commission, Ispra, Italy. His research interests include optimal and robust control, networked and multi-agent control systems, and critical infrastructure modeling and analysis.

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

Bela Genge is an Associate Professor of Computer Science and a Marie Curie Fellow at Petru Maior University of Tirgu-Mures, Mures, Romania. His research interests include critical infrastructure protection, secure and resilient design of critical control systems and network security.

Georgios Giannopoulos is a Scientific Officer at the Joint Research Centre of the European Commission, Ispra, Italy. His current research focuses on computational tools for analyzing risk, interdependencies and the economic impacts of critical infrastructure disruptions.

Flavius Graur is an M.Sc. student in Information Technology at Petru Maior University of Tirgu-Mures, Mures, Romania. His research interests include computer and network security, penetration testing and software-defined networking.

Dimitris Gritzalis is the Associate Rector for Research, 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 and smartphone security and privacy.

Piroska Haller is an Associate Professor of Computer Science at Petru Maior University of Tirgu-Mures, Mures, Romania. Her research interests include industrial control system security and distributed systems.

Uday Kanteti is an M.S. student in Computer Science at the Missouri University of Science and Technology, Rolla, Missouri. His research interests include information assurance, critical infrastructure protection and formal methods.

Wayne King is a Project Leader at Lawrence Livermore National Laboratory, Livermore, California. His research focuses on the physics, material science, engineering and control aspects of additive manufacturing.

Megan Leierzapf is a System Validation Engineer at Intel Corporation, San Jose, California. Her research interests include cyber security and systems engineering.

Htein Lin 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 network security and critical infrastructure protection.

Joshua Lubell is a Computer Scientist in the Systems Integration Division at the National Institute of Standards and Technology, Gaithersburg, Maryland. His research interests include model-based engineering, cyber security, cyber-physical systems, information modeling and markup technologies.

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.

Caleb Mays 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 wireless network security and critical infrastructure protection.

Bruce McMillin is a Professor of Computer Science at the Missouri University of Science and Technology, Rolla, Missouri. His research interests include critical infrastructure protection, computer security, formal methods and distributed systems.

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 and embedded system security.

Stefano Panzieri is an Associate Professor of Automatic Control and 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.

Antonios Papachrysanthou is 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.

John Pecarina is an Assistant Professor of Computer Science at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include distributed systems, cryptographic protocols, cyber-physical system security and critical infrastructure protection.

Evan Plumley 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 network security, cyber security training and critical infrastructure protection.

Gregory Pope is a Group Leader at Lawrence Livermore National Laboratory, Livermore, California. His research interests include vulnerability analyses of additive manufacturing and Internet of Things software control systems.

Benjamin Ramsey is a Cyberspace Operations Officer in the U.S. Air Force, Washington, DC. His research interests include wireless network security and critical infrastructure protection.

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 system security and critical infrastructure protection.

Anthony Rose 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 wireless network security and Internet of Things security.

Julian Rrushi is an Assistant Professor of Computer Science at Western Washington University, Bellingham, Washington. His research interests include industrial control system security and defensive cyber deception.

Hunor Sandor is a Ph.D. student in Computer Science at the Technical University of Cluj-Napoca, Cluj-Napoca, Romania; and a Researcher in the Department of Computer Science at Petru Maior University of Tirgu-Mures, Mures, Romania. His research interests include cyber security and cyber-physical security, and designing response and reconfiguration techniques to mitigate threats and vulnerabilities in large-scale systems.

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 and cryptography.

Eniye Tebekaemi is a Ph.D. candidate in Information Technology and a Researcher in the Radio and Radar Engineering Laboratory at George Mason University, Fairfax, Virginia. His research interests include cyber security, cyber-physical systems and intrusion detection systems.

Duminda Wijesekera is a Professor of Computer Science at George Mason University, Fairfax, Virginia; and a Visiting Research Scientist at the National Institute of Standards and Technology, Gaithersburg, Maryland. His research interests include cyber security, digital forensics and transportation systems.

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.

Timothy Zimmerman is a Computer Engineer in the Intelligent Systems Division at the National Institute of Standards and Technology, Gaithersburg, Maryland. His research focuses on cyber security in the manufacturing sector with an emphasis on industrial control systems and robotics.

Preface

The information infrastructure – comprising computers, embedded devices, networks and software systems – is vital to operations in every sector: chemicals, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waste, transportation systems, and water and wastewater systems. 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 XI*, is the eleventh 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 sixteen revised and edited papers from the Eleventh Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, held at SRI International in Arlington, Virginia, USA on March 13–15, 2017. 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: (i) infrastructure protection; (ii) infrastructure modeling and simulation; (iii) industrial control system security; and (iv) Internet of Things security. 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 David Balenson, Molly Keane and Zachary Tudor for their tireless work on behalf of IFIP Working Group 11.10. We gratefully acknowledge Idaho National Laboratory and the Institute for Information Infrastructure Protection (I3P), managed by George Washington University, for their sponsorship of IFIP Working Group 11.10. We also thank the U.S. 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