IFIP Advances in Information and Communication Technology 542

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

Jason Staggs · Sujeet Shenoi (Eds.)

Critical Infrastructure Protection XII

12th IFIP WG 11.10 International Conference, ICCIP 2018
Arlington, VA, USA, March 12–14, 2018
Revised Selected Papers

Springer

Editors
Jason Staggs
Tandy School of Computer Science
University of Tulsa
Tulsa, OK, USA

Sujeet Shenoi
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 978-3-030-04536-4 ISBN 978-3-030-04537-1 (eBook)
https://doi.org/10.1007/978-3-030-04537-1

Library of Congress Control Number: 2018963824

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. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

Contents

Contributing Authors ix

Preface xv

PART I THEMES AND ISSUES

1
A Theory of Homeland Security 3
Richard White

2
An Evidence Quality Assessment Model for Cyber Security Policymaking 23
Atif Hussain, Siraj Shaikh, Alex Chung, Sneha Dawda and Madeline Carr

3
Liability Exposure when 3D-Printed Parts Fall from the Sky 39
Lynne Graves, Mark Yampolskiy, Wayne King, Sofia Belikovetsky and Yuval Elovici

PART II INFRASTRUCTURE PROTECTION

4
Error Propagation After Reordering Attacks on Hierarchical State Estimation 67
Ammara Gul and Stephen Wolthusen

5
Securing Data in Power-Limited Sensor Networks Using Two-Channel Communications 81
Clark Wolfe, Scott Graham, Robert Mills, Scott Nykl and Paul Simon

6
Reversing a Lattice ECP3 FPGA for Bitstream Protection 91
Daniel Celebucki, Scott Graham and Sanjeev Gunawardena

7
Protecting Infrastructure Data via Enhanced Access Control, Blockchain and Differential Privacy 113
Asma Alnemari, Suchith Arodi, Valentina Rodriguez Sosa, Soni Pandey, Carol Romanowski, Rajendra Raj and Sumita Mishra

8
A New SCAP Information Model and Data Model for Content Authors 127
Joshua Lubell

PART III INFRASTRUCTURE MODELING AND SIMULATION

9
Modeling a Midstream Oil Terminal for Cyber Security Risk Evaluation 149
Rishabh Das and Thomas Morris

10
A Cyber-Physical Testbed for Measuring the Impacts of Cyber Attacks on Urban Road Networks 177
Marielba Urdaneta, Antoine Lemay, Nicolas Saunier and Jose Fernandez

11
Persistent Human Control in a Reservation-Based Autonomous Intersection Protocol 197
Karl Bentjen, Scott Graham and Scott Nykl

PART IV INDUSTRIAL CONTROL SYSTEMS SECURITY

12
A History of Cyber Incidents and Threats Involving Industrial Control Systems 215
Kevin Hemsley and Ronald Fisher

13
An Integrated Control and Intrusion Detection System for Smart Grid Security 243
Eniye Tebekaemi, Duminda Wijesekera and Paulo Costa

14
Generating Abnormal Industrial Control Network Traffic for Intrusion Detection System Testing 265
Joo-Yeop Song, Woomyo Lee, Jeong-Han Yun, Hyunjae Park, Sin-Kyu Kim and Young-June Choi

15
Variable Speed Simulation for Accelerated Industrial Control System Cyber Training 283
Luke Bradford, Barry Mullins, Stephen Dunlap and Timothy Lacey

Contributing Authors

Asma Alnemari is a Ph.D. student in Computing and Information Sciences at Rochester Institute of Technology, Rochester, New York. Her research interests include differential privacy and its application in real-world systems.

Suchith Arodi is a Software Engineer with the Office of Architecture, State Street Corporation, Raleigh, North Carolina. His research interests include blockchain, cyber security and data science.

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.

Karl Bentjen recently completed his M.S. degree in Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include vehicular network security and critical infrastructure protection.

Luke Bradford 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.

Madeline Carr is an Associate Professor of International Relations and Cyber Security, and the Director of the Research Institute for the Science of Cyber Security at University College London, London, United Kingdom. Her research interests include global cyber security, cyber norms, the Internet of Things and board/policy decision making on cyber risk.

Daniel Celebucki recently completed his M.S. degree in Cyber Operations at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include embedded systems, reconfigurable computing, reverse engineering and critical infrastructure protection.

Young-June Choi is a Professor of Computer Engineering at Ajou University, Suwon, Republic of Korea. His research interests include network security and cyber-physical systems.

Alex Chung is a Research Associate in the Department of Science, Technology, Engineering and Public Policy, University College London, London, United Kingdom. His research interests include cyber security policy, organized crime, and digital economy and society.

Paulo Costa is an Associate Professor of Systems Engineering and Operations Research at George Mason University, Fairfax, Virginia. His research interests include cyber security, transportation systems and multi-sensor data fusion.

Rishabh Das is a Ph.D. student in Computer Engineering at the University of Alabama in Huntsville, Huntsville, Alabama. His research interests include industrial control system virtualization, machine learning and embedded intrusion detection systems.

Sneha Dawda is a Research Associate in Digital Business Strategy at Forrester Research, London, United Kingdom. Her research interests include geopolitical cyber security and digital financial services security.

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 systems security, cyber-physical systems 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.

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.

Ronald Fisher is the Director of the Infrastructure Assurance and Analysis Division at Idaho National Laboratory, Idaho Falls, Idaho. His research interests include critical infrastructure protection and resilience, including industrial control systems.

Scott Graham is an Assistant Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include vehicle cyber security, critical infrastructure protection and embedded systems security.

Lynne Graves is a Ph.D. student in Computer Science at the University of South Alabama, Mobile, Alabama. Her research focuses on additive manufacturing security.

Ammara Gul is a Ph.D. student in Information Security at Royal Holloway, University of London, Egham, United Kingdom. Her research interests include graph theory and control theory, in particular, the security of state estimation systems.

Sanjeev Gunawardena is a Research Assistant Professor of Electrical Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include satellite navigation and timing systems, embedded systems, reconfigurable computing and software-defined radio.

Kevin Hemsley is a Project Manager at Idaho National Laboratory, Idaho Falls, Idaho. His research interests include critical infrastructure protection and industrial control systems security.

Atif Hussain is a Cyber Security Researcher at the Future Transport and Cities Research Institute, Coventry University, Coventry, United Kingdom. His research interests include penetration testing, digital forensics and cyber security policymaking.

Sin-Kyu Kim is a Senior Engineering Staff Member at the National Security Research Institute, Daejeon, Republic of Korea. His research focuses on critical infrastructure protection.

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.

Timothy Lacey is an Adjunct Assistant Professor of Computer Science at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include cyber operations, critical infrastructure protection, mobile device security, and computer, network and embedded systems security.

Woomyo Lee is an Engineering Staff Member at the National Security Research Institute, Daejeon, Republic of Korea. Her research interests include applied cryptography, cyber security and cyber-physical systems.

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.

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.

Robert Mills is a Professor of Electrical Engineering 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.

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

Thomas Morris is a 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 system virtualization, intrusion detection, machine learning and vulnerability testing of cyber-physical 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-physical systems security, cyber operations, critical infrastructure protection, computer, network and embedded systems security, wired and wireless networking, and code reverse engineering.

Scott Nykl is an Assistant Professor of Computer Science at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include visualization and the use of synthetic environments for evaluating computer vision algorithms.

Soni Pandey recently completed her M.S. degree in Computer Science at Rochester Institute of Technology, Rochester, New York. Her research interests include data management and cyber security.

Hyunjae Park is a Ph.D. candidate in Computer Engineering at Ajou University, Suwon, Republic of Korea. His research areas include cyber-physical systems and artificial intelligence.

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

Valentina Rodriguez Sosa is an M.S. student in Computer Science at Rochester Institute of Technology, Rochester, New York. Her research interests include enterprise system security, secure coding and cyber security education.

Carol Romanowski is a 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.

Nicolas Saunier is a Professor of Transportation Engineering at Ecole Polytechnique de Montreal, Montreal, Canada. His research interests include intelligent transportation systems, road safety and information technology for transportation.

Siraj Shaikh is a Professor of Systems Security at the Future Transport and Cities Research Institute, Coventry University, Coventry, United Kingdom. His research interests include stealthy threat detection, cyber-physical systems security, especially transportation and cyber security policymaking.

Paul Simon is a Ph.D. student in Electrical Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include embedded systems security, computer communications security and critical infrastructure protection.

Joo-Yeop Song is an M.S. student in Computer Engineering at Ajou University, Suwon, Republic of Korea. His research areas include network security and artificial intelligence.

Eniye Tebekaemi is an Assistant Professor of Computer Science at Mercer University, Macon, Georgia. His research interests include cyber security, cyber-physical systems and intrusion detection systems.

Marielba Urdaneta is an M.S. student in Computer Engineering at Ecole Polytechnique de Montreal, Montreal, Canada. Her research interests include industrial control systems security and critical infrastructure protection.

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.

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.

Clark Wolfe recently completed his M.S. degree in Electrical Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include computer communications security 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, Gjovik, Norway; and a Professor of Information Security at Royal Holloway, University of London, Egham, 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.

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

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 XII*, is the twelfth 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 fifteen revised and edited papers from the Twelfth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, held at SRI International in Arlington, Virginia, USA on March 12–14, 2018. 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) themes and issues; (ii) infrastructure protection; (iii) infrastructure modeling and simulation; and (iv) industrial control systems 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 and Molly Keane 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 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.

JASON STAGGS AND SUJEET SHENOI