IFIP Advances in Information and Communication Technology 417

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 VII

7th IFIP WG 11.10 International Conference
ICCIP 2013
Washington, DC, USA, March 18-20, 2013
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 Shenoi
University of Tulsa
Tulsa, OK 74104-3189, USA
E-mail: sujeet@utulsa.edu

ISSN 1868-4238 e-ISSN 1868-422X
ISBN 978-3-642-45329-8 e-ISBN 978-3-642-45330-4
DOI 10.1007/978-3-642-45330-4
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2013955033

CR Subject Classification (1998): K.6.5, J.7, K.4, I.6, D.4.6, K.5.1, C.2, H.4, H.3, K.6

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

Saed Alajlouni is a Researcher in the Department of Electrical Engineering at Texas Tech University, Lubbock, Texas. His research interests include cyber-physical systems security, control systems, autonomous systems, industrial automation, renewable energy systems and power electronics.

Abdullah Alsubaie is a Ph.D. student in Electrical Engineering at the University of British Columbia, Vancouver, Canada. His research interests include power systems operation and critical infrastructure simulation.

Aaron Alva is a J.D. candidate and an M.S. student in Information Management at the University of Washington, Seattle, Washington. His research interests include cloud forensics, digital evidence admissibility and legal barriers to critical infrastructure resilience.

Tara Anderson is a member of the Senior Professional Staff at the Johns Hopkins University Applied Physics Laboratory in Laurel, Maryland. Her research interests include information security, modeling and simulation, and mission risk assessment.

Daniel Arnaudo is a Senior Research Fellow at the Jackson School of International Studies, University of Washington, Seattle, Washington. His research interests include Internet governance, information assurance and Brazilian telecommunications policy.

Damindra Bandara is a Ph.D. student in Computer Science at George Mason University, Fairfax, Virginia. Her research interests include the security of software-defined radios and wireless-controlled trains, and protocol verification.

Andre Bondi is a Senior Staff Engineer at Siemens Corporate Technology, Princeton, New Jersey. His research interests include computer performance engineering, modeling and simulation.

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 an Assistant Professor of Computer Science and the Chief of the Computer Science and Engineering Division 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, Dallas, Texas. His research interests include the security and privacy of control systems, SCADA systems, the smart grid and other cyber-physical critical infrastructures.

Richard Chow is a Security Researcher and Privacy Architect at Intel Corporation, Santa Clara, California. His research interests include privacy-enhancing technologies using machine learning and applied cryptography.

Emiliano De Cristofaro is a Research Scientist at PARC (a Xerox company), Palo Alto, California. His research interests include security, privacy and applied cryptography.

Yi Deng is a Research Scientist in the Department of Electrical and Computer Engineering, Arlington Research Center, Virginia Polytechnic Institute and State University, Arlington, Virginia. His research interests include smart grid security, PMU-based wide area measurement, SCADA systems security, software security and software modeling and meta-modeling.

Antonio Di Pietro is a Researcher at ENEA Casaccia Research Centre, Rome, Italy. His research interests include critical infrastructure interdependency modeling and simulation, and SCADA systems security.

Clay Dubendorfer 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 signals exploitation and critical infrastructure protection.

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

Rajni Goel is an Associate Professor and Chairman of the Department of Information Systems at Howard University, Washington, DC. Her research interests include railroad security, supply chain networks and applications security.

Dimitris Gritzalis is a Professor of Information and Communications Technology Security and the Director of the Information Security and Critical Infrastructure Protection Laboratory, Department of Informatics, Athens University of Economics and Business, Athens, Greece. His research interests include critical infrastructure protection, privacy in social media, digital forensics and cloud security.

Robert Jaromin is a Developmental Electrical Engineer with the U.S. Air Force. His research interests include critical infrastructure protection and signals exploitation.

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 system security and trust management.

Pranab Kini is a Research Engineer in the School of Engineering and Computer Science at the University of British Columbia, Vancouver, Canada. His research focuses on software engineering solutions for disaster and relief management.

Panayiotis Kotzanikolaou is a Lecturer of Information and Communications Technology Security in the Department of Informatics, University of Piraeus, Piraeus, Greece. His research interests include network security and privacy, critical infrastructure protection and applied cryptography.

Ting Fu Lin is a Research Assistant in the Power Systems Laboratory at the School of Engineering and Computer Science, University of British Columbia, Vancouver, Canada. His research interests include the analysis and design of complex systems.

Thomas Llanso is a member of the Principal Professional Staff at the Johns Hopkins University Applied Physics Laboratory in Laurel, Maryland; and a Ph.D. student in Information Systems at Dakota State University, Madison, South Dakota. His research interests include quantitative risk assessment and cyber investment analysis.

Juan Lopez is a Research Engineer with 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 radio frequency identification.

Jose Marti is a Professor of Electrical and Computer Engineering at the University of British Columbia, Vancouver, Canada. His research interests include critical infrastructure modeling and the real-time simulation of large-scale systems.

Barry Mullins is an Associate Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include cyber operations, software reverse engineering, computer and network security, SCADA systems security and reconfigurable computing systems.

Simone Palmieri is a Ph.D. student in Computer Science and Automation at the University of Roma Tre, Rome, Italy. His research interests include telecommunications networks and SCADA systems, with a special focus on power systems.

Stefano Panzieri is an Associate Professor of Automation and Process Control Engineering at the University of Roma Tre, Rome, Italy. His research interests are in the areas of industrial control systems, robotics and sensor fusion.

Benjamin Ramsey is a Ph.D. student in 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.

Vittal Rao is a Professor of Electrical and Computer Engineering and the Director of the Smart Grid Energy Center at Texas Tech University, Lubbock, Texas. His research interests include cyber security, critical infrastructure protection, smart grid and microgrid systems, wind turbine control and robust control systems.

Aunshul Rege is an Assistant Professor of Criminal Justice at Temple University, Philadelphia, Pennsylvania. Her research interests include cyber crime, organized crime, offender decision-making, and surveillance and regulation.

Sandeep Shukla is a Professor of Electrical and Computer Engineering at the Arlington Research Center, Virginia Polytechnic Institute and State University, Arlington, Virginia. His research interests include formal methods, system-level design languages and frameworks, component-based and platform-based design, smart grid systems, formal verification and its applications to critical infrastructure systems.

Michael Silberglitt is a member of the Principal Professional Staff at the Johns Hopkins University Applied Physics Laboratory in Laurel, Maryland. His research interests include mission-focused risk assessment methodologies, modeling and simulation, and security engineering.

Michael Smith is a Requirements and System Design Manager with the Rail Automation Unit of Siemens, New York, New York. His research interests include software engineering and computer architecture.

Gregg Tally is a member of the Senior Professional Staff at the Johns Hopkins University Applied Physics Laboratory in Laurel, Maryland. His research interests include cyber security engineering methodologies and malware defense.

Michael Temple is a Professor of Electrical Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include radio frequency systems, wireless networks and critical infrastructure protection.

Marianthi Theoharidou is a Post-Doctoral Researcher in the Information Security and Critical Infrastructure Protection Laboratory, Department of Informatics, Athens University of Economics and Business, Athens, Greece. Her research interests include critical infrastructure protection, risk assessment and cloud security.

Alberto Tofani is a Researcher in the Computing and Technological Infrastructures Laboratory at ENEA Casaccia Research Centre, Rome, Italy. His research interests include critical infrastructure vulnerability assessment and decision support systems for crisis preparedness and mitigation.

Jan Whittington is an Assistant Professor of Urban Design and Planning and an Associate Director of the Center for Information Assurance and Cybersecurity at the University of Washington, Seattle, Washington. Her research interests are in the areas of economics, planning and infrastructure management, including privacy and security issues.

Duminda Wijesekera is a Professor of Computer Science at George Mason University, Fairfax, Virginia. His research includes information security and its application to logical models of security policies, safety and security of wireless-controlled trains, security and privacy of healthcare applications, and financial crime.

Phillip Wood received his M.S. degree in Information Management from the University of Washington, Seattle, Washington. His research interests include technology valuation and the economic impact of political insecurity.

Yanjun Zuo is an Associate Professor of Computer Information Systems at the University of North Dakota, Grand Forks, North Dakota. His research interests include system survivability, trustworthy computing and RFID security and privacy.

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 VII*, is the seventh 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 edited papers from the Seventh Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, held at George Washington University, Washington, DC, March 18–20, 2013. 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: themes and issues, control systems security, infrastructure security, infrastructure modeling and simulation, and risk 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 Richard George, Heather Drinan, Nicole Hall Hewett, Lance Hoffman and Firoozeh Rahimian for their tireless work on behalf of IFIP Working Group 11.10. We gratefully acknowledge the Insti-

tute 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 and the National Security Agency 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