IFIP Advances in Information and Communication Technology 390

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 VI

6th IFIP WG 11.10 International Conference
ICCIP 2012
Washington, DC, USA, March 19-21, 2012
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 978-3-642-35763-3 e-ISBN 978-3-642-35764-0
DOI 10.1007/978-3-642-35764-0
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012954250

CR Subject Classification (1998): K.6.5, D.4.6, K.5.1, K.4.1, I.6.3-5, C.2.0, H.4.2-3, H.3.4-5, K.6.1

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

Anas Abou El Kalam is a Professor of Computer and Network Security at the National School of Applied Sciences, Marrakesh, Morocco. His research interests include embedded systems security, network security, wireless security, security models and intrusion detection.

Abdellah Ait Ouahman is a Professor of Telecommunication Networks and the Director of the National School of Applied Sciences, Marrakesh, Morocco. His research interests include logistics, telecommunications and information networks.

Hasan Ali is an Assistant Professor of Electrical and Computer Engineering at the University of Memphis, Memphis, Tennessee. His research interests include advanced power systems, smart grid and micro grid systems, renewable energy systems, energy storage systems and flexible AC transmission systems.

Abdeljebar Ameziane El Hassani is a Ph.D. student in Network Security Science at Cadi Ayyad University, Marrakesh, Morocco, and at the National Polytechnic Institute, Toulouse, France. His research interests are in the area of access control for distributed critical infrastructures.

Michael Berg is a Principal Member of the Technical Staff at Sandia National Laboratories, Albuquerque, New Mexico. His research interests include optimization and embedded systems design.

Ron Berndsen is the Head of the Oversight Department at The Netherlands Bank, Amsterdam, The Netherlands; and an Endowed Professor of Financial Infrastructure and Systemic Risk at the University of Tilburg, Tilburg, The Netherlands. His research interests are in the area of financial market infrastructures.

Fabio Bisogni is a Member of the Board of the Formit Foundation, Rome, Italy. His research interests include critical infrastructure protection, cyber security, critical event management and information disclosure policy.

Henry Bushey 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 SCADA systems security and protocol verification.

Jonathan Butts, Chair, IFIP Working Group 11.10 on Critical Infrastructure Protection, is an Assistant Professor of Computer Science 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.

Emiliano Casalicchio is a Researcher in the Department of Computer Science, University of Rome – Tor Vergata, Rome, Italy; and a Senior Advisor at the Global Cyber Security Center, Rome, Italy. His research interests include performance-oriented design and evaluation of large-scale distributed systems, and analysis, modeling and simulation of critical information infrastructures.

Marco Caselli is a Ph.D. student in Computer Science at the University of Twente, Enschede, The Netherlands. His research interests are mainly in the field of cyber security applied to industrial infrastructures.

Simona Cavallini is a Senior Researcher at the Formit Foundation, Rome, Italy. Her research interests include critical infrastructure protection, interdependency analysis, economics of security and macroeconomics modeling.

Alessio Coletta is a Researcher at the Global Cyber Security Center, Rome, Italy. His research interests include critical infrastructure protection, industrial control systems security and malware analysis.

Dipankar Dasgupta is a Professor of Computer Science at the University of Memphis, Memphis, Tennessee. His research interests include evolutionary and immunological computation, intrusion detection and fault detection.

Marco Del Pra is a Software Designer with Stratiqo, Milan, Italy; and an External Consultant at the Institute for the Protection and Security of the Citizen, Joint Research Centre of the European Commission, Ispra, Italy. His research interests include the modeling and simulation of industrial applications, and the development of applied mathematics and real-time software.

Salvatore Di Blasi is a Researcher at the Global Cyber Security Center, Rome, Italy. His research interests are in the area of information and communications systems security.

Ian Ellefsen is a Senior Lecturer in the Academy of Computer Science and Software Engineering at the University of Johannesburg, Johannesburg, South Africa. His research interests include critical infrastructure protection and critical information infrastructure protection models for developing nations.

Chiara Foglietta is a Ph.D. student in Computer Science and Automation at the University of Roma Tre, Rome, Italy. Her research interests include data fusion techniques, situational awareness and the application of multi-agent systems to critical infrastructure protection, especially power systems and smart grid security.

Luisa Franchina is the Director General of the Critical Infrastructure Secretariat in the Office of the Military Advisor to the Italian Presidency of the Council of the Ministers, Rome, Italy. Her research interests include security and business continuity.

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

Bela Genge is a Post-Doctoral Researcher at the Institute for the Protection and Security of the Citizen, Joint Research Centre of the European Commission, Ispra, Italy. His research interests include critical infrastructure protection, intrusion detection systems, and the security and resilience of networked industrial control systems.

Michael Gosnell is a Ph.D. student in Computer Science at Missouri University of Science and Technology, Rolla, Missouri. His research interests include fault detection, tolerance, prognostics and diagnostics, parallel and distributed computing, and wireless and unmanned systems.

James Graham is the Henry Vogt Professor of Computer Science and Engineering at the University of Louisville, Louisville, Kentucky. His research interests include information security, digital forensics, critical infrastructure protection, high performance computing and intelligent systems.

Jeffrey Hieb is an Assistant Professor of Engineering Fundamentals at the University of Louisville, Louisville, Kentucky. His research interests include information security, honeypots, digital forensics, secure operating systems and the use of technology in engineering education.

Marc Hohenadel is an Action Leader at the Institute for the Protection and Security of the Citizen, Joint Research Centre of the European Commission, Ispra, Italy. His research interests include the security of networked critical infrastructures.

Chun Hu is a Ph.D. student in Computer Science at Missouri University of Science and Technology, Rolla, Missouri. His research interests include privacy-preserving data mining and information assurance.

Wei Jiang is an Assistant Professor of Computer Science at Missouri University of Science and Technology, Rolla, Missouri. His research interests include privacy-preserving data mining, data integration, text sanitization and applied cryptography.

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.

Thomas McEvoy is a Ph.D. student in Mathematics at Royal Holloway, University of London, London, United Kingdom; and a Technical Manager at HP Information Security, Bracknell, United Kingdom. His research interests include the modeling and simulation of critical infrastructures and hybrid systems in relation to security properties.

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

Lucille McMinn is an M.S. student in Computer Science at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. Her research interests include malware analysis and embedded device security.

John Mulder is a Senior Member of the Technical Staff at Sandia National Laboratories, Albuquerque, New Mexico. His research interests include computer networks and industrial control systems security.

Igor Nai Fovino is the Head of the Research Division at the Global Cyber Security Center, Rome, Italy. His research interests include critical infrastructure protection, intrusion detection, secure communication protocols and industrial informatics.

Paul Ngo is a Ph.D. candidate in Computer Science at George Mason University, Fairfax, Virginia; and the Next Generation Network (NGN) Security Lead at the National Communications System in Arlington, Virginia. His research interests are in the area of emergency communications systems.

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

Alex Pease is a Member of the Technical Staff at Sandia National Laboratories, Albuquerque, New Mexico. His research interests include memory and kernel security and integrity.

Giovanni Saja is a Security Manager at Telecom Italia, Milan, Italy. His research interests are in the area of critical infrastructure protection.

Jacob Schreiver is an M.S. student in Computer Engineering at the University of Louisville, Louisville, Kentucky. His interests include computer security, image processing and the use of computer games in education.

Moses Schwartz is a Member of the Technical Staff at Sandia National Laboratories, Albuquerque, New Mexico. His research interests include supply chain risk management, visualization, formal methods and embedded systems.

Christos Siaterlis is a Scientific Officer at the Institute for the Protection and Security of the Citizen, Joint Research Centre of the European Commission, Ispra, Italy. His research interests include various aspects of the security, stability and resilience of complex systems, especially critical infrastructures such as the Internet and smart grid.

Leon Strous, IFIP President, is an IT Auditor in the Cash and Payment Systems Division of The Netherlands Bank, Amsterdam, The Netherlands. His research interests include business continuity, operational crisis management and critical infrastructure protection, with special emphasis on the financial sector.

Jorge Mario Urrea is a Senior Member of the Technical Staff at Sandia National Laboratories, Albuquerque, New Mexico. His research interests include information assurance, wireless networks and microcontroller development.

Jonathan Van Houten is a Senior Member of the Technical Staff at Sandia National Laboratories, Albuquerque, New Mexico. His research interests include digital design and embedded software security.

Matthijs van Oers is a Senior Policy Advisor with The Netherlands Bank, Amsterdam, The Netherlands. His research interests are in the broad area of financial infrastructure protection, in particular payment and securities, and business continuity and crisis management.

Sebastiaan von Solms is a Research Professor in the Academy of Computer Science and Software Engineering at the University of Johannesburg, Johannesburg, South Africa. His research interests include information security and critical information infrastructure protection.

Duminda Wijesekera is an Associate Professor of Information and Software Engineering at George Mason University, Fairfax, Virginia. His research interests include information, network, telecommunications and control systems security.

Stephen Wolthusen is a Professor of Information Security at the Norwegian Information Security Laboratory, Gjovik University College, Gjovik, Norway; and a Reader in Mathematics at Royal Holloway, University of London, London, United Kingdom. His research interests include critical infrastructure modeling and simulation, and network 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 VI*, is the sixth 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 edited papers from the Sixth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, held at the National Defense University, Washington, DC, March 19–21, 2012. 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 four sections: themes and issues, control systems security, infrastructure security, and infrastructure modeling and simulation. 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 Robert Miller, Heather Drinan, Nicole Hall Hewett and Firoozeh Rahimian 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 supporting 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