IFIP Advances in Information and Communication Technology 342

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 less 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 in information 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.

Tyler Moore Sujeet Shenoi (Eds.)

Critical Infrastructure Protection IV

Fourth Annual IFIP WG 11.10 International Conference
on Critical Infrastructure Protection, ICCIP 2010
Washington, DC, USA, March 15-17, 2010
Revised Selected Papers

Springer

Volume Editors

Tyler Moore
Harvard University
Cambridge, MA 02138, USA
E-mail: tmoore@seas.harvard.edu

Sujeet Shenoi
University of Tulsa, Department of Computer Science
Tulsa, OK 74104, USA
E-mail: sujeet@utulsa.edu

Library of Congress Control Number: 2010937784

CR Subject Classification (1998): B.8, C.4, B.1.3, B.2.3, B.7.3, C.2, I.6

ISSN 1868-4238
ISBN-10 3-642-16805-1 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-16805-5 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 219/3180

Contents

PART V RISK MANAGEMENT

Contributing Authors

Craig Allwardt is a Research Scientist at the Pacific Northwest National Laboratory, Richland, Washington. His research interests include knowledge systems, visualization and software architectures.

Ainara Alvarez is a Researcher in the Department of Industrial Organization at the University of Navarra, San Sebastian, Spain. Her research interests include innovation, marketing and risk assessment.

Maria Jesus Alvarez is a Professor of Operations Research at the University of Navarra, San Sebastian, Spain. Her research interests include operations research applied to logistics and systems productivity.

Dan Assaf is a Doctor of Juridical Science (S.J.D.) degree candidate in the Faculty of Law, University of Toronto, Toronto, Canada. His research interests are in the intersection of law, economics and security, in particular, the regulation and governance of information security.

Zaw Zaw Aung is a Ph.D. student in Information Science and Control Engineering at Nagaoka University of Technology, Nagaoka, Japan. His research interests include operational risk management, interdependency analysis and critical infrastructure modeling.

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

Thomas Brandstetter is a Program Manager at Siemens CERT, Siemens Corporate Research and Technology, Munich, Germany. His research interests include vulnerabilities in critical infrastructures, incident handling methods and economic aspects of IT security.

Peter Burge is an Associate Director at RAND Europe, Cambridge, United Kingdom. His research focuses on modeling choice making behavior, the design and administration of surveys, and the estimation of discrete choice models.

Jonathan Butts 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, telecommunications and SCADA systems security.

Andrea Carcano is a Ph.D. student in Computer Science at the University of Insubria, Varese, Italy. His research interests include industrial SCADA protocols and architectures.

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

Yousu Chen is a Research Engineer at the Pacific Northwest National Laboratory, Richland, Washington. His research interests include high-performance computing applications, power system operation and decision support, and power system modeling and analysis.

Maria Carla De Maggio is a Researcher at the Complex Systems and Security Laboratory at University Campus Bio-Medico of Rome, Rome, Italy. Her research interests include critical infrastructure protection, risk analysis and risk management.

Ian Ellefsen is a Ph.D. student in Computer Science at the University of Johannesburg, Johannesburg, South Africa. His research interests include critical infrastructure protection and critical information infrastructure protection models for developing nations.

Aaron Engel received his M.S. degree in Computer Science from the University of Tulsa, Tulsa, Oklahoma. His research interests include information assurance, and network and telecommunications system security.

Rajni Goel is an Associate Professor of Information Systems and Decision Sciences at Howard University, Washington, DC. Her research interests include information assurance, digital forensics, control systems security and data mining.

Frank Greitzer is a Chief Scientist at the Pacific Northwest National Laboratory, Richland, Washington. His research interests include situational awareness and decision making in grid operations, cyber security and the insider threat, and applications of cognitive informatics to decision making.

Daniel Guernsey is a Ph.D. student in Computer Science at the University of Tulsa, Tulsa, Oklahoma. His research interests include information assurance, and network and telecommunications system security.

Michele Guglielmi is a Research Trainee at the Joint Research Centre of the European Commission, Ispra, Italy. His research interests include industrial SCADA protocols and architectures.

Mark Hartong is a Senior Electronics Engineer with the Office of Safety, Federal Railroad Administration, U.S. Department of Transportation, Washington, DC. His research interests include information assurance, control systems security, risk analysis and regulatory development.

Zhenyu Huang is a Staff Engineer at the Pacific Northwest National Laboratory, Richland, Washington. His research interests include high performance computing, wide-area measurement technology, information visualization, and power system stability and simulation.

Stig Johnsen is a Senior Research Scientist at SINTEF, Trondheim, Norway. His research interests include information security, SCADA systems, integrated oil and gas operations, and plant safety.

Chong Kim is a Researcher at RAND Europe, Cambridge, United Kingdom. His main research areas are discrete choice modeling and stated preference research in the transportation and health domains.

Ray Klump is an Associate Professor of Mathematics and Computer Science at Lewis University, Romeoville, Illinois; and a Visiting Research Scientist at the Information Trust Institute at the University of Illinois at Urbana-Champaign, Urbana, Illinois. His research interests include electric power system stability and smart grid security.

Konstantin Knorr is a Professor of IT Security in the Computer Science Department at Trier University of Applied Sciences, Trier, Germany. His research interests include SCADA security, authorization models of information and communications systems, and patch management.

Matthew Kwiatkowski is the Cyber Operations Lead in the Cyber Security Program Office at Argonne National Laboratory, Argonne, Illinois; and an Adjunct Professor of Information Security at Lewis University, Romeoville, Illinois. His research focuses on intrusion detection and response mechanisms.

Hans Lund received his B.Sc. degree in Computer Science from Gjovik University College, Gjovik, Norway. His research interests include critical infrastructure protection and communication systems security.

Nils Lunden received his B.Sc. degree in Computer Science from Gjovik University College, Gjovik, Norway. His research interests include security modeling and visualization.

Jian Ma is a Research Engineer at the Pacific Northwest National Laboratory, Richland, Washington. His research interests include power system stability and reliability, renewable integration, wide-area measurement technology and applications of artificial intelligence in power systems.

Patrick Mackey is a Research Scientist at the Pacific Northwest National Laboratory, Richland, Washington. His research interests include visual analytics, data visualization, scientific computation, auditory displays and human-computer interaction.

Marcelo Masera is a Scientific Officer at the Institute for the Protection and Security of the Citizen, Joint Research Center of the European Commission, Ispra, Italy. His research interests include securing networked systems and systems of systems, risk governance and control systems security.

Thomas McEvoy is a Ph.D. student in Mathematics at Royal Holloway, University of London, London, United Kingdom; and a Principal Consultant at Vistorm Ltd., Warrington, United Kingdom. His research interests include the modeling and simulation of critical infrastructures and hybrid systems in relation to security properties.

Igor Nai Fovino is a Scientific Officer at the Institute for the Protection and Security of the Citizen, Joint Research Center of the European Commission, Ispra, Italy; and an Adjunct Professor of Operating Systems at the University of Insubria, Varese, Italy. His research interests include critical infrastructure protection, intrusion detection, secure communication protocols and industrial informatics.

Ainhoa Oses is a Researcher in the Department of Industrial Organization at the University of Navarra, San Sebastian, Spain. Her research interests include manufacturing processes, supply chain management and risk analysis.

Dimitris Potoglou is a Researcher at RAND Europe, Cambridge, United Kingdom. His research involves the design of discrete choice stated preference experiments for understanding individuals' choices and valuations of goods and services.

Mason Rice is a Ph.D. student in Computer Science at the University of Tulsa, Tulsa, Oklahoma. His research interests include network and telecommunications security, and cyberspace deterrence strategies.

Neil Robinson is a Researcher at RAND Europe, Cambridge, United Kingdom. His research interests include critical infrastructure protection, cyber crime and information assurance.

Ute Rosenbaum is a Senior Consultant in IT security at Siemens CERT, Siemens Corporate Research and Technology, Munich, Germany. Her research interests include control systems security, and enhancing development and service processes using security methodologies.

Roberto Setola is the Director of the Complex Systems and Security Laboratory at University Campus Bio-Medico of Rome, Rome, Italy. His research interests include critical infrastructure modeling and analysis, critical infrastructure protection, risk assessment and control strategies for complex systems.

Sujeet Shenoi, Chair, IFIP Working Group 11.10 on Critical Infrastructure Protection, is the F.P. Walter Professor of Computer Science at the University of Tulsa, Tulsa, Oklahoma. His research interests include information assurance, digital forensics, critical infrastructure protection, reverse engineering and intelligent control.

Sean Smith is an Associate Professor of Computer Science at Dartmouth College, Hanover, New Hampshire. His research interests include trusted computing and usable security.

Rouslan Solomakhin is a Software Engineer at Microsoft, Redmond, Washington. His research interests include information assurance, network security and cloud computing.

Robin Sveen received his B.Sc. degree in Computer Science from Gjovik University College, Gjovik, Norway. His research interests include software security and critical infrastructure protection.

Nils Svendsen is an Associate Professor of Computer Science at the Norwegian Information Security Laboratory, Gjovik University College, Gjovik, Norway. His research interests include the modeling and simulation of critical infrastructures, graph theory, cryptography and coding theory.

Alberto Trombetta is an Assistant Professor of Computer Science and Communication at the University of Insubria, Varese, Italy. His research interests include data security and privacy, data integration, query languages, imprecise data management and systems security.

Marcella Trombetta is a Professor of Chemical Fundamentals in Technology at University Campus Bio-Medico of Rome, Rome, Italy. Her research interests include the synthesis and characterization of new materials for biomedical applications, energy and the environment.

Patrick Tsang, who passed away on October 27, 2009, was a Ph.D. student in Computer Science at Dartmouth College, Hanover, New Hampshire. His research interests included cryptography, network security and privacy-enhancing technologies.

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

Richard Warnes is a Researcher at RAND Europe, Cambridge, United Kingdom. His research interests include counterterrorism, policing and intelligence.

Kenji Watanabe is a Professor in the Graduate School of Social Engineering, Nagoya University of Technology, Nagoya, Japan. His research areas include IT risk management, business continuity and critical 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.

Pak-Chung Wong is a Chief Scientist and Project Manager at the Pacific Northwest National Laboratory, Richland, Washington. His research interests include visual analytics, power grid analytics, graph and network analytics, and multimedia analytics.

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 IV*, is the fourth 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 seventeen edited papers from the Fourth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, held at the National Defense University, Washington, DC, March 15–17, 2010. 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 management. 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 Daniel Guernsey, Jonathan Butts, Mason Rice, 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 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.

Tyler Moore and Sujeet Shenoi