IFIP Advances in Information and Communication Technology 367

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 ist member countries and to encourage technology transfer to developing nations. As ist 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.

Jonathan Butts Sujeet Shenoi (Eds.)

Critical Infrastructure Protection V

5th IFIP WG 11.10 International Conference
on Critical Infrastructure Protection, ICCIP 2011
Hanover, NH, USA, March 23-25, 2011
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
Department of Computer Science
Tulsa, OK 74104-3189, USA
E-mail: sujeet@utulsa.edu

ISSN 1868-4238 e-ISSN 1868-422X
ISBN 978-3-642-24863-4 e-ISBN 978-3-642-24864-1
DOI 10.1007/978-3-642-24864-1
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011938839

CR Subject Classification (1998): D.4.6, K.6.5, E.3, C.2, H.4, H.3, I.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

Sergey Bratus is a Research Assistant Professor of Computer Science at Dartmouth College, Hanover, New Hampshire. His research interests include Linux kernel security, wireless network security and security-related visualization tools.

Jim Chen is a Professor of Computer Science at George Mason University, Fairfax, Virginia. His research interests include computer graphics, networking and visualization.

Adam Comella is an undergraduate student in Computer Science at Rensselaer Polytechnic Institute, Troy, New York. His research interests include secure systems, open source software applications and operating systems.

Qi Fang is an M.S. student in Information Sciences and Technology at Pennsylvania State University, University Park, Pennsylvania. Her research interests are in the area of network science.

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, design methods and composition of security protocols.

Daniel Guernsey received his Ph.D. degree in Computer Science from the University of Tulsa, Tulsa, Oklahoma. His research interests include information assurance, and network and telecommunications systems security.

Joshua Haines is an Assistant Leader of the Cyber Systems and Technology Group at MIT Lincoln Laboratory, Lexington, Massachusetts. His research interests include system analysis, secure and robust architectures, network-centric cyber systems and automated network vulnerability analysis.

Carl Hauser is an Associate Professor of Computer Science at Washington State University, Pullman, Washington. His research interests include concurrent and distributed systems, especially as applied to secure wide-area control systems.

Eric Koziel 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 offensive and defensive cyber security analysis.

Anyi Liu is a Ph.D. student in Information Technology at George Mason University, Fairfax, Virginia. His research interests include information assurance, and intrusion detection and correlation.

Peng Liu is a Professor of Information Sciences and Technology and Director of the Center for Cyber Security, Information Privacy and Trust at Pennsylvania State University, University Park, Pennsylvania. His research interests include computer security and network security.

Michael Locasto is an Assistant Professor of Computer Science at the University of Calgary, Alberta, Canada. His research interests include machine intelligence and trustworthy systems.

Marcelo Masera is the Head of the Energy Security Unit at the Institute for Energy, Joint Research Centre, Petten, The Netherlands. 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 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.

Peter Michaleas is a Systems Engineer in the Embedded and High Performance Computing Group at MIT Lincoln Laboratory, Lexington, Massachusetts. His research interests include kernel development and high performance computing.

Jonathan Morgan is a Research Assistant and Manager of the Applied Cognitive Science Laboratory at Pennsylvania State University, University Park, Pennsylvania. His research interests include modeling small-team dynamics, the effects of social moderators and organizational learning.

Igor Nai Fovino is the Head of the Research Division of 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. student 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.

Hamed Okhravi is a Technical Staff Member in the Cyber Systems and Technology Group at MIT Lincoln Laboratory, Lexington, Massachusetts. His research interests include cyber security, cyber trust, high assurance systems, virtualization and operating systems.

Andres Perez-Garcia is a Network Security Specialist at the Institute for the Protection and Security of the Citizen, Joint Research Centre of the European Commission, Ispra, Italy. His research interests include inter-domain routing protocols and critical information infrastructure protection.

Sanaz Rahimi is a Ph.D. candidate in Computer Science at Southern Illinois University, Carbondale, Illinois. Her research interests include cyber security, software reliability and cyber trust.

Ashwin Ramaswamy is an Analyst at Bloomberg, New York. His research interests include operating system security and patch deployment systems.

Jason Reeves is an M.S. student in Computer Science at Dartmouth College, Hanover, New Hampshire. His research interests include system security and human-computer interaction.

Mason Rice received his Ph.D. degree in Computer Science from the University of Tulsa, Tulsa, Oklahoma. His research interests include network and telecommunications systems security, and cyberspace deterrence strategies.

Frank Ritter is a Professor of Information Sciences and Technology, Computer Science and Engineering, and Psychology at Pennsylvania State University, University Park, Pennsylvania. His research interests include models of cognition and cognitive architectures.

David Robinson is an Assistant Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include cyber and cyber physical systems security.

Eric Robinson is a Technical Staff Member in the Embedded and High Performance Computing Group at MIT Lincoln Laboratory, Lexington, Massachusetts. His research interests include high performance computing, distributed systems and compilers.

Edmond Rogers is a Smart Grid Cyber Security Engineer at the University of Illinois Information Trust Institute, Urbana, Illinois. His research interests include critical infrastructure vulnerability assessment, penetration testing of SCADA systems and persistent attack detection.

Rebecca Shapiro is a Ph.D. student in Computer Science at Dartmouth College, Hanover, New Hampshire. Her research interests are in the area of systems security.

Donald Shemanski is a Professor of Practice of Information Sciences and Technology at Pennsylvania State University, University Park, Pennsylvania. His research interests include information law and policy, privacy law, system science and global prescience.

Sujeet Shenoi 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.

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 the security, stability and resilience of computer networks.

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

Yujue Wang is a Ph.D. student in Computer Science at Washington State University, Pullman, Washington. His research interests include trust assessment, network security and distributed systems.

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.

Li Yang is an Associate Professor of Computer Science at the University of Tennessee at Chattanooga, Chattanooga, Tennessee. Her research interests include computer security, software design and engineering, and database management.

Stephen Yannalfo is a Subcontractor in the Cyber Systems and Technology Group at MIT Lincoln Laboratory, Lexington, Massachusetts. His research interests include software engineering and virtualization.

John Yen is a University Professor and Director of Strategic Research Initiatives for the College of Information Sciences and Technology at Pennsylvania State University, University Park, Pennsylvania. His research interests include cognitive agents, social network analysis and artificial intelligence.

Mehdi Zargham is a Professor and Chair of Computer Science at Southern Illinois University, Carbondale, Illinois. His research interests include mobile learning, pattern recognition and data mining.

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 V*, is the fifth 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 fourteen edited papers from the Fifth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, held at Dartmouth College, Hanover, New Hampshire, March 23–25, 2011. 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 Daniel Guernsey, 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.

Jonathan Butts and Sujeet Shenoi