IFIP Advances in Information and Communication Technology 596

Editor-in-Chief

Kai Rannenberg, Goethe University Frankfurt, Germany

Editorial Board Members

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 XIV

14th IFIP WG 11.10 International Conference, ICCIP 2020
Arlington, VA, USA, March 16–17, 2020
Revised Selected Papers

Springer

Editors
Jason Staggs
University of Tulsa
Tulsa, OK, USA

Sujeet Shenoi
University of Tulsa
Tulsa, OK, USA

ISSN 1868-4238 ISSN 1868-422X (electronic)
IFIP Advances in Information and Communication Technology
ISBN 978-3-030-62839-0 ISBN 978-3-030-62840-6 (eBook)
https://doi.org/10.1007/978-3-030-62840-6

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

David Balenson is a Senior Computer Scientist in the Infrastructure Security Group at SRI International, Arlington, Virginia. His research interests include critical infrastructure protection, experimentation and testing, and technology transition.

Elena Bernardini is an M.Sc. student in Management and Automation Engineering at the University of Roma Tre, Rome, Italy. Her research interests include modeling critical infrastructures and telecommunications networks.

Addison Betances is an Assistant Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include software-defined radios, device fingerprinting, programmable hardware, embedded systems security and critical infrastructure protection.

Zachary Birnbaum is a Senior Professional Staff Member at Johns Hopkins University Applied Physics Laboratory, Laurel, Maryland. His research interests include quantitative cyber and resilience modeling and simulation, and behavior-based anomaly detection in cyber-physical systems.

Brett Borghetti is an Associate Professor of Computer Science at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include applying machine learning to problem spaces such as human-machine teaming in cyber security.

Chun-Fai Chan is a Ph.D. student in Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include penetration testing, digital forensics and Internet of Things security.

Raymond Chan is a Lecturer of Information and Communications Technology at Singapore Institute of Technology, Singapore. His research interests include cyber security, digital forensics and critical infrastructure protection.

Kam-Pui Chow is an Associate Professor of Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include information security, digital forensics, live system forensics and digital surveillance.

David Crow recently completed his M.S. degree in Computer Science at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include machine learning, cyber-physical systems security and critical infrastructure protection.

Matthew Dallmeyer is a Research Engineer at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include programmable hardware, cyber-physical systems security and embedded systems security.

Matthew Davis is a Senior Professional Staff Member at Johns Hopkins University Applied Physics Laboratory, Laurel, Maryland. His research interests include information security, modeling and simulation, and cyber-physical systems 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.

Tim Ellis is a Senior Principal Research Engineer at SRI International, San Diego, California. His research interests include critical infrastructure protection and information system privacy and security.

Chiara Foglietta is an Assistant Professor of Automatic Control at the University of Roma Tre, Rome, Italy. Her research interests include industrial control systems, data fusion techniques and controls for energy management systems.

Yanan Gong is an M.Phil. student in Computer Science at the University of Hong Kong, Hong Kong, China. Her research interests include cyber security and digital forensics.

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

Micah Hayden 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 computer communications, avionics security and critical infrastructure protection.

Nicholas Kovach is a Senior Research Engineer at the Air Force Research Laboratory, Wright-Patterson Air Force Base, Ohio. His research interests include avionics security, critical infrastructure protection and embedded systems security.

Brandon Kow is a B.Sc. student in Computing Science at the University of Glasgow, Glasgow, United Kingdom. His research interests include the Internet of Things and cyber security.

Rajesh Kumar is an Assistant Professor of Computer Science at Birla Institute of Technology and Science, Pilani, India. His research interests include information security risk management, and safety and security risk analysis using formal models and model checking.

Jennifer Leopold is an Associate Professor of Computer Science at Missouri University of Science and Technology, Rolla, Missouri. Her research interests include data mining, especially graph data mining, and cyber-physical systems.

Michael Locasto is a Principal Computer Scientist at SRI International, New York. His research focuses on understanding software faults and developing fixes.

Nathan Lutes is a Ph.D. student in Mechanical Engineering at Missouri University of Science and Technology, Rolla, Missouri. His research interests include automatic control and machine learning, with an emphasis on intelligent control and decision making.

Jake Magness 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 cyber-physical systems security, avionics security and critical infrastructure protection.

Yonghao Mai is a Professor of Information Technology at Hubei Police University, Wuhan, China. His research interests include digital forensics and cyber law.

Bruce McMillin is a Professor of Computer Science at Missouri University of Science and Technology, Rolla, Missouri. His research interests include cyber-physical systems security, distributed systems and formal methods.

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.

Lucas Mireles 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 communications systems security, avionics security and critical infrastructure protection.

Stefano Panzieri is a Professor of Automatic Control and Head of the Models for Critical Infrastructure Protection Laboratory at the University of Roma Tre, Rome, Italy. His research interests include industrial control systems, robotics, sensor fusion and models for critical infrastructure protection.

Shruti Paul is a Cyber Security Engineer at PayPal, Scottsdale, Arizona. Her research interests include cyber security, network security and penetration testing.

Dillon Pettit 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 cyber security risk management, unmanned aerial vehicles and cyber-physical systems security.

Stefan Rass is an Associate Professor of Computer Science at the University of Klagenfurt, Klagenfurt, Austria. His research interests include decision theory and game theory applications in security, complexity theory and applied cryptography.

Salman Salman is a Cyber Security Engineer at Aerospace Corporation, Chantilly, Virginia. His research interests include operational technology/information technology cyber defense, high latency network optimization, penetration testing and networking.

James Schaffter is a D.Eng. student at Johns Hopkins University, Baltimore, Maryland. His research interests include cyber-physical systems security, virtualization, fog computing and penetration testing.

Stefan Schauer is a Senior Scientist at the Austrian Institute of Technology, Klagenfurt, Austria. His research interests include mathematical models for risk and security management, and the assessment of cascading effects in critical infrastructures.

Rachel Stiffler is a Ph.D. student in Mechanical Engineering at Missouri University of Science and Technology, Rolla, Missouri. Her research interests include combustion and cyclic dynamics in internal combustion engines.

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

Forest Tan is a Cluster Director and Associate Professor of Information and Communications Technology at Singapore Institute of Technology, Singapore. His research interests include the Internet of Things, and intelligent and secure systems.

Ulric Teo is a B.Sc. student in Computing Science at the University of Glasgow, Glasgow, United Kingdom. His research interests include industrial control systems and cyber security.

Simon Thougaard is a Ph.D. student in Computer Science at Missouri University of Science and Technology, Rolla, Missouri. His research interests include cyber-physical systems security, consensus systems and emergent behavior in distributed systems.

Anusha Thudimilla recently completed her Ph.D. degree in Computer Science at Missouri University of Science and Technology, Rolla, Missouri. Her research interests include cyber-physical systems security and deep learning.

Matthew Wagner recently completed his Ph.D. degree in Computer Science at Missouri University of Science and Technology, Rolla, Missouri. His research interests include cyber-physical systems security and cryptography.

Lanier Watkins is an Associate Research Scientist at the Information Security Institute, Whiting School of Engineering, Johns Hopkins University, Baltimore, Maryland; and a Senior Professional Staff Member at Johns Hopkins University Applied Physics Laboratory, Laurel, Maryland. His research interests include algorithms and frameworks for defending critical infrastructure networks and systems.

Saikiran Yamajala is a Software Engineer at Cisco Systems, Research Triangle Park, North Carolina. Her research interests include information security, cryptosystems and cloud security.

Jun Zhang is a Professor of Information Technology at Hubei Police University, Wuhan, China. His research interests include information security and digital forensics.

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 XIV*, is the fourteenth 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 critical 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 selected papers from the Fourteenth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, held at SRI International in Arlington, Virginia, USA on March 16–17, 2020. 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. The sixteen selected papers were subsequently revised by the editors to produce the final chapters published in this volume.

The chapters are organized into six sections: (i) aviation infrastructure security; (ii) vehicle infrastructure security; (iii) telecommunications systems security; (iv) industrial control systems security; (v) cyber-physical systems security; and (vi) 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 David Balenson for his tireless work on behalf of IFIP Working Group 11.10. We also thank the National Science Foundation, 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