IFIP Advances in Information and Communication Technology 570

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 XIII

13th IFIP WG 11.10 International Conference, ICCIP 2019
Arlington, VA, USA, March 11–12, 2019
Revised Selected Papers

Springer

Editors
Jason Staggs
Tandy School of Computer Science
University of Tulsa
Tulsa, OK, USA

Sujeet Shenoi
Tandy School of Computer Science
University of Tulsa
Tulsa, OK, USA

ISSN 1868-4238 ISSN 1868-422X (electronic)
IFIP Advances in Information and Communication Technology
ISBN 978-3-030-34646-1 ISBN 978-3-030-34647-8 (eBook)
https://doi.org/10.1007/978-3-030-34647-8

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

Prashant Anantharaman is a Ph.D. student in Computer Science at Dartmouth College, Hanover, New Hampshire. His research interests include smart grid and Internet of Things protocol security, and eliminating input-handling vulnerabilities in code.

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

Robert Borrelli is an Assistant Professor of Nuclear Engineering at the University of Idaho, Idaho Falls, Idaho. His research interests include assessing and safeguarding advanced nuclear fuel cycles, including securing industrial control systems.

J. Peter Brady is a Ph.D. student in Computer Science at Dartmouth College, Hanover, New Hampshire. His research interests include improving systems and data security via the application of formal verification techniques.

Sergey Bratus is a Research Associate Professor of Computer Science at Dartmouth College, Hanover, New Hampshire. His research interests include computing system exploitation and its formalization as a distinct research and engineering discipline.

Manan Buddhadev is a Software Engineer at Microsoft Corporation, Redmond, Washington. His research interests include natural language processing and data privacy.

Timothy Carbino is an Adjunct Assistant Professor of Electrical Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include digital communications protocols, physical layer device fingerprinting and critical infrastructure protection.

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.

Seungoh Choi is a Senior Researcher at the Affiliated Institute of ETRI, Daejeon, South Korea. His research interests include critical infrastructure protection and network security.

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.

Luis Cintron 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 embedded systems, critical infrastructure protection, distributed computing applications and software engineering.

Siddharth Dongre is an M.S. student in Computing Security at Rochester Institute of Technology, Rochester, New York. His research interests include data privacy and security, and their applications in critical infrastructure protection.

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.

James Graham is a Co-Founder and the Chief Executive Officer of True Secure SCADA, Goshen, Kentucky. His research interests include information security, digital forensics, critical infrastructure protection, high performance computing and intelligent systems.

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 vehicle cyber security, critical infrastructure protection and embedded systems security.

Kenneth Hacker 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 automotive embedded systems, critical infrastructure protection and distributed computing applications.

Michael Haney is an Assistant Professor of Computer Science at the University of Idaho, Idaho Falls, Idaho; and a Cyber Security Researcher at Idaho National Laboratory, Idaho Falls, Idaho. His research interests include critical infrastructure protection and active defenses for industrial control 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 engineering education.

Douglas Hodson is an Associate Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include computer engineering, software engineering, real-time distributed simulation and quantum communications.

Keith Holt is the Vice President of Northeast Division Rail Systems at HNTB Corporation, Philadelphia, Pennsylvania; and a retired Deputy Chief Engineer at Amtrak, Philadelphia, Pennsylvania. His research interests are in the area of rail systems.

Matthew Jablonski is a Ph.D. student in Information Technology at George Mason University, Fairfax, Virginia. His research interests include attack modeling, secure system design and transportation systems security.

HyoungChun Kim is a Principal Researcher at the Affiliated Institute of ETRI, Daejeon, South Korea. His research interests include cyber security and critical infrastructure protection.

Yesol Kim is a Researcher at the Affiliated Institute of ETRI, Daejeon, South Korea. Her research interests include cyber security and industrial control systems security.

Rahn Lassiter recently completed his M.S. degree in Electrical Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include digital communications protocols, physical layer device fingerprinting and critical infrastructure protection.

Adrian Lauf is an Assistant Professor of Computer Engineering and Computer Science at the University of Louisville, Louisville, Kentucky. His research interests include the integration of embedded computing, networking and security applications in airborne robotics.

Xiang Liu is an Assistant Professor of Civil and Environmental Engineering at Rutgers University, Piscataway, New Jersey. His research interests include rail systems safety and security.

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

Trevor MacLean is an M.E. student in Mechanical Engineering at the University of Idaho, Idaho Falls, Idaho. His research interests include industrial control systems security, especially in the nuclear sector.

Michael Millian is a Ph.D. student in Computer Science at Dartmouth College, Hanover, New Hampshire. His research interests include language-theoretic security for network-level and bootloader-level protocols.

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.

Byung-Gil Min is a Senior Researcher at the Affiliated Institute of ETRI, Daejeon, South Korea. His research interests include security monitoring, industrial control systems and critical infrastructure protection.

Sumita Mishra is a Professor of Computing Security at Rochester Institute of Technology, Rochester, New York. Her research interests include critical infrastructure protection, smart grid privacy and resource-constrained network security.

Barry Mullins is a Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include cyber-physical systems security, cyber operations, critical infrastructure protection, computer, network and embedded systems security, wired and wireless networking, and code reverse engineering.

Carol Romanowski is a Professor of Computer Science at Rochester Institute of Technology, Rochester, New York. Her research interests include applications of data science and data mining to critical infrastructure protection, cyber security and engineering design.

Mehdi Sabraoui is a Ph.D. student in Computer Science and Engineering at the University of Louisville, Louisville, Kentucky. His research interests include the formal modeling and verification of security in industrial control systems.

Daryl Schmitt 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 network security and management, cyber situational awareness and cyber defense.

Sujeet Shenoi is the F.P. Walter Professor of Computer Science and a Professor of Chemical Engineering at the University of Tulsa, Tulsa, Oklahoma. His research interests include critical infrastructure protection, industrial control systems and digital forensics.

Sean Smith is a Professor of Computer Science at Dartmouth College, Hanover, New Hampshire. His research interests include industrial Internet of Things security, trusted computing and human-computer interaction security.

Jason Staggs is an Adjunct Assistant Professor of Computer Science at the University of Tulsa, Tulsa, Oklahoma. His research interests include telecommunications networks, industrial control systems, critical infrastructure protection, security engineering and digital forensics.

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.

Yongxin Wang is a Ph.D. student in Computer Science at George Mason University, Fairfax, Virginia. His research interests include applications of cyber security and sensor systems to transportation systems.

Zezhou Wang is a Ph.D. student in Civil Engineering at Rutgers University, Piscataway, New Jersey. His research interests include rail systems safety and security.

Duminda Wijesekera is a Professor of Computer Science at George Mason University, Fairfax, Virginia; and a Visiting Research Scientist at the National Institute of Standards and Technology, Gaithersburg, Maryland. His research interests include cyber security, digital forensics and transportation systems.

Ken Yau is a Ph.D. student in Computer Science at the University of Hong Kong, Hong Kong, China. His research interests are in the area of digital forensics, with an emphasis on industrial control system forensics.

Chaitanya Yavvari recently completed his Ph.D. degree in Computer Science at George Mason University, Fairfax, Virginia. His research areas include cyber security, and transportation systems safety and security.

Siu-Ming Yiu is an Associate Professor of Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include security, cryptography, digital forensics and bioinformatics.

Jeong-Han Yun is a Senior Researcher at the Affiliated Institute of ETRI, Daejeon, South Korea. His research interests include network security, cyber security and industrial control systems security.

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 XIII*, is the thirteenth 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 revised and edited papers from the Thirteenth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, held at SRI International in Arlington, Virginia, USA on March 11–12, 2019. 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. They were subsequently revised by the editors to produce the final chapters published in this volume.

The chapters are organized into six sections: (i) themes and issues; (ii) infrastructure protection; (iii) vehicle infrastructure security; (iv) telecommunications infrastructure security; (v) cyber-physical systems security; and (vi) industrial control systems security. 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 gratefully acknowledge the Institute for Information Infrastructure Protection (I3P), managed by George Washington University, for its sponsorship 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