IFIP Advances in Information and Communication Technology 462

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.

More information about this series at http://www.springer.com/series/6102

Gilbert Peterson · Sujeet Shenoi (Eds.)

Advances in Digital Forensics XI

11th IFIP WG 11.9 International Conference
Orlando, FL, USA, January 26–28, 2015
Revised Selected Papers

Springer

Editors
Gilbert Peterson
Department of Electrical and Computer Engineering
Air Force Institute of Technology
Wright-Patterson Air Force Base, Ohio
USA

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

ISSN 1868-4238 ISSN 1868-422X (electronic)
IFIP Advances in Information and Communication Technology
ISBN 978-3-319-24122-7 ISBN 978-3-319-24123-4 (eBook)
DOI 10.1007/978-3-319-24123-4

Library of Congress Control Number: 2015951345

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media (www.springer.com)

Contents

Contributing Authors

Sudhir Aggarwal is a Professor of Computer Science at Florida State University, Tallahassee, Florida. His research interests include password cracking, information security and building software tools and systems for digital forensics.

Monis Akhlaq is an Assistant Professor of Information Security at the National University of Sciences and Technology, Islamabad, Pakistan. His research interests include digital forensics, network security, incident handling and risk management.

Panagiotis Andriotis is a Ph.D. student in Computer Science at the University of Bristol, Bristol, United Kingdom. His research interests include digital forensics, text mining, content analysis and systems security.

Baber Aslam is an Assistant Professor and Head of the Department of Information Security at the National University of Sciences and Technology, Islamabad, Pakistan. His research interests include computer security, network security and digital forensics.

Stefan Axelsson is a Senior Lecturer of Computer Science at the Blekinge Institute of Technology, Karlskrona, Sweden. His research interests include digital forensics, intrusion and fraud detection, visualization and digital surveillance.

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.

Fred Cohen is the Chief Executive Officer of Management Analytics, Pebble Beach, California; a Member of Fearless Security, Pebble Beach, California; and Acting Director of the Webster University CyberLab, St. Louis, Missouri. His research interests include digital forensics, information assurance and critical infrastructure protection.

David Dampier is a Professor of Computer Science and Engineering, and Director of the Distributed Analytics and Security Institute at Mississippi State University, Mississippi State, Mississippi. His research interests include digital forensics, information assurance and software engineering.

Xiao-Xi Fan is a Ph.D. student in Computer Science at the University of Hong Kong, Hong Kong, China. Her research interests include digital forensics, digital profiling and data mining.

Junbin Fang is an Associate Professor of Optoelectronics Engineering at Jinan University, Guangzhou, China. His research interests include information security and forensics, and quantum cryptography.

Peter Fruhwirt is a Researcher at SBA Research, Vienna, Austria. His research interests include digital forensics, mobile security and applied security.

Glenn Fryklund is a Security Analyst at Coresec Systems, Malmo, Sweden. His research interests include computer and network security, and digital forensics.

Sara Ghorbanian is a Security Analyst at Coresec Systems, Malmo, Sweden. Her research interests include computer and network security, and digital forensics.

Dae Glendowne is an Assistant Research Professor at the Distributed Analytics and Security Institute at Mississippi State University, Mississippi State, Mississippi. His research interests include malware reverse engineering, memory forensics and machine learning.

Jayaprakash Govindaraj is a Senior Technology Architect at Infosys Labs, Bangalore, India; and a Ph.D. student in Computer Science and Engineering at Indraprastha Institute of Information Technology, New Delhi, India. His research interests include mobile security, mobile device forensics and anti-forensics, mobile cloud computing security and forensics, and security in emerging technologies.

Stefan Gruner is an Associate Professor of Computer Science at the University of Pretoria, Pretoria, South Africa. His research interests include software science, formal methods and the philosophy of science.

Yong Guan is an Associate Professor of Electrical and Computer Engineering at Iowa State University, Ames, Iowa. His research interests include digital forensics, system security and privacy.

Gaurav Gupta is a Scientist D in the Department of Electronics and Information Technology, Ministry of Information Technology, New Delhi, India. His research interests include digitized document fraud detection, mobile device forensics and cloud forensics.

Qi Han is an Associate Professor of Computer Science and Technology at Harbin Institute of Technology, Shenzhen, China. His research fields include digital video forensics, hiding communications and digital watermarking.

Ragib Hasan is an Assistant Professor of Computer and Information Sciences at the University of Alabama at Birmingham, Birmingham, Alabama. His research interests include computer security, cloud computing security, secure provenance, trustworthy databases and digital forensics.

Werner Hauger is an M.Sc. student in Computer Science at the University of Pretoria, Pretoria, South Africa. His research interests include digital forensics and computer security.

Shiva Houshmand is a Ph.D. candidate in Computer Science at Florida State University, Tallahassee, Florida. Her research interests include computer and network security, authentication, digital forensics and machine learning.

Umit Karabiyik is a Ph.D. candidate in Computer Science at Florida State University, Tallahassee, Florida. His research interests include digital forensics, cyber security, expert systems and computer and network security.

Peter Kieseberg is a Researcher at SBA Research, Vienna, Austria. His research interests include digital forensics, cryptography and mobile security.

Irwin King is the Associate Dean (Education) of the Faculty of Engineering and a Professor of Computer Science and Engineering at the Chinese University of Hong Kong, Hong Kong, China. His research interests include machine learning, social computing, web intelligence, data mining and multimedia information processing.

Changwei Liu is a Ph.D. candidate in Computer Science at George Mason University, Fairfax, Virginia. Her research interests include cyber security and network forensics.

Rashmi Mata is a Technology Lead at Infosys Labs, Bangalore, India. Her research interests include web and mobile applications security.

Wesley McGrew is an Assistant Research Professor at the Distributed Analytics and Security Institute at Mississippi State University, Mississippi State, Mississippi. His research interests include cyber operations, reverse engineering, vulnerability analysis and digital forensics.

Cody Miller is a Research Associate at the Distributed Analytics and Security Institute at Mississippi State University, Mississippi State, Mississippi. His research interests include cloud computing, computer security and digital forensics.

Shariq Murtuza is an M.Tech. student in Computer Science and Engineering at Indraprastha Institute of Information Technology, New Delhi, India. His research interests include digital forensics, mobile device forensics and cloud forensics.

Xiamu Niu is a Professor of Computer Science and Technology at Harbin Institute of Technology, Shenzhen, China. His research interests include computer and information security, hiding communications, cryptography, digital watermarking, signal processing and image processing.

George Oikonomou is a Research Associate in Security for the Internet of Things at the University of Bristol, Bristol, United Kingdom. His research interests include Internet forensics, computer networks and security for the Internet of Things.

Martin Olivier is a Professor of Computer Science at the University of Pretoria, Pretoria, South Africa. His research interests include digital forensics and privacy.

Oluwasayo Oyelami is an M.Sc. student in Computer Science at the University of Pretoria, Pretoria, South Africa. His research interests include digital forensics and information security.

Anoop Singhal is a Senior Computer Scientist in the Computer Security Division at the National Institute of Standards and Technology, Gaithersburg, Maryland. His research interests include network security, network forensics, web services security and data mining systems.

Zheng Tan is a Research Assistant in Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include distributed storage systems and parallel data processing systems.

Yanbin Tang is a Ph.D. student in Computer Science at the University of Hong Kong, Hong Kong, China. Her research interests include digital forensics and file carving.

Segen Tewelde is an M.Sc. student in Computer Science at the University of Pretoria, Pretoria, South Africa. Her research interests include digital forensics and requirements engineering.

Philip Trenwith is an M.Sc. student in Computer Science at the University of Pretoria, Pretoria, South Africa. His research interests include digital forensics and cloud computing.

Theo Tryfonas is a Senior Lecturer in Systems Engineering at the University of Bristol, Bristol, United Kingdom. His research interests are in the areas of smart cities, cyber security, systems engineering and technologies for sustainable development.

Hein Venter is a Professor of Computer Science at the University of Pretoria, Pretoria, South Africa. His research interests are in the area of digital forensics, with a current focus on digital forensic standardization and the construction of an ontology for digital forensic techniques.

Robin Verma is a Ph.D. student in Computer Science and Engineering at Indraprastha Institute of Information Technology, New Delhi, India. His research interests include digital forensics, data privacy and mobile device forensics.

Edgar Weippl is the Research Director at SBA Research, Vienna, Austria; and an Associate Professor of Computer Science at Vienna University of Technology, Vienna, Austria. His research focuses on information security and e-learning.

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

Xianyan Wu is a Ph.D. student in Computer Science and Technology at Harbin Institute of Technology, Shenzhen, China. Her research interests include figure-ground segmentation, image file carving, image processing and security.

Fei Xu is an Assistant Professor of Computer Science at the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. Her research interests include information security and digital forensics.

Min Yang is a Ph.D. student in Computer Science at the University of Hong Kong, Hong Kong, China. Her research interests include digital forensics and data mining.

Ken Yau is a Research Staff Member at the Center for Information Security and Cryptography, University of Hong Kong, Hong Kong, China. His research interests include information security and digital forensics.

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

Muhammad Sharjeel Zareen is an M.S. student in Information Security at the National University of Sciences and Technology, Islamabad, Pakistan. His research interests include digital forensics, vulnerability assessment, penetration testing and the Internet of Things.

Shams Zawoad is a Ph.D. student in Computer and Information Sciences at the University of Alabama at Birmingham, Birmingham, Alabama. His research interests include cloud forensics, cyber crime, secure provenance and mobile malware.

Ping Zhang is a Lecturer at the Guangdong Police College, Guangzhou, China. Her research interests include information security, digital forensics and secure data mining.

Chen Zhao is an M.S. student in Electrical and Computer Engineering at Iowa State University, Ames, Iowa. His research interests include digital forensics, in particular, Bitcoin system analysis and forensic investigations.

Preface

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every type of crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence in legal proceedings. Digital forensics also has myriad intelligence applications; furthermore, it has a vital role in information assurance – investigations of security breaches yield valuable information that can be used to design more secure and resilient systems.

This book, *Advances in Digital Forensics XI*, is the eleventh volume in the annual series produced by IFIP Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book presents original research results and innovative applications in digital forensics. Also, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations.

This volume contains twenty revised and edited chapters based on papers presented at the Eleventh IFIP WG 11.9 International Conference on Digital Forensics, held in Orlando, Florida, USA on January 26-28, 2015. The papers were refereed by members of IFIP Working Group 11.9 and other internationally-recognized experts in digital forensics. 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: Themes and Issues, Internet Crime Investigations, Forensic Techniques, Mobile Device Forensics, Cloud Forensics, and Forensic Tools. The coverage of topics highlights the richness and vitality of the discipline, and offers promising avenues for future research in digital forensics.

This book is the result of the combined efforts of several individuals. In particular, we thank Mark Pollitt for his tireless work on behalf of IFIP Working Group 11.9. We also acknowledge the support provided by the National Science Foundation, National Security Agency, Immigration and Customs Enforcement, Internal Revenue Service and U.S. Secret Service.

Gilbert Peterson and Sujeet Shenoi