IFIP Advances in Information and Communication Technology 383

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.

Gilbert Peterson Sujeet Shenoi (Eds.)

Advances in Digital Forensics VIII

8th IFIP WG 11.9 International Conference on Digital Forensics
Pretoria, South Africa, January 3-5, 2012
Revised Selected Papers

Springer

Volume Editors

Gilbert Peterson
Air Force Institute of Technology
Wright-Patterson Air Force Base, OH 45433-7765, USA
E-mail: gilbert.peterson@afit.edu

Sujeet Shenoi
University of Tulsa
Tulsa, OK 74104-3189, USA
E-mail: sujeet@utulsa.edu

ISSN 1868-4238 e-ISSN 1868-422X
ISBN 978-3-642-33961-5 e-ISBN 978-3-642-33962-2
DOI 10.1007/978-3-642-33962-2
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012948200

CR Subject Classification (1998): K.6.5, H.3.2, H.3.4-5, J.1, C.2, C.5.3, E.3, H.2.7, D.2.11, F.2, E.5

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

Saif Al-Kuwari is an Information Security Officer with the Ministry of Foreign Affairs in Doha, Qatar. His research interests are in the area of computational forensics, particularly clandestine localization in multimodal environments.

Aaron Alva is an M.S. student in Information Management and a Juris Doctorate student at the University of Washington, Seattle, Washington. His research interests include digital evidence admissibility in U.S. courts and the creation of federal laws in cybersecurity.

Lamine Aouad is a Researcher at the Center for Cybersecurity and Cyber Crime Investigation, University College Dublin, Dublin, Ireland. His research interests include parallel and distributed computing, data mining and analytics, and digital forensics.

Joe Carthy is the Dean of Science and a Professor of Computer Science and Informatics at University College Dublin, Dublin, Ireland. His research interests include cloud forensics and cyber crime investigations.

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.

John Christiansen is an Attorney with Christiansen IT Law in Seattle, Washington. His specialties in the field of information technology law include legal compliance, and security and technology due diligence and administration.

Waldo Delport 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.

Barbara Endicott-Popovsky is the Director of the Center for Information Assurance and Cybersecurity at the University of Washington, Seattle, Washington. Her research interests include enterprise-wide information systems security and compliance management, forensically-ready networks and secure coding practices.

Junbin Fang is an Associate Professor of Optoelectronic Engineering at the Guangdong Higher Education Institute, Jinan University, Guangzhou, China; and a Visiting Scholar in the Department of Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include mobile forensics, information security and quantum cryptography.

Oluwasola Mary Fasan is a Lecturer and Ph.D. student in Computer Science at the University of Pretoria, Pretoria, South Africa. Her research interests include digital forensics and database security.

Stephen Flowerday is a Professor of Information Systems at the University of Fort Hare, East London, South Africa. His research interests include information security management, trust and digital forensics.

Mark-Anthony Fouche is an M.Sc. student in Computer Science at the University of Pretoria, Pretoria, South Africa. His research interests include digital image forensics and steganography.

Felix Freiling is a Professor of Computer Science at Friedrich Alexander University, Erlangen-Nuremberg, Germany. His research interests cover the theory and practice of secure and dependable computing.

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.

Mengfei He is an M.S. student in Computer Science and Technology at Shenzhen Graduate School, Harbin Institute of Technology, Shenzhen, China. His research interests include digital forensics and information security.

Bruno Hoelz is a Ph.D. student in Electrical Engineering at the University of Brasilia, Brasilia, Brazil; and a Computer Forensics Expert at the National Institute of Criminalistics, Brazilian Federal Police, Brasilia, Brazil. His research interests include multiagent systems and artificial intelligence applications in digital forensics.

Markus Huber is a Ph.D. student in Computer Science at the Vienna University of Technology, Vienna, Austria; and a Computer Security Researcher at SBA Research, Vienna, Austria. His research focuses on security and privacy issues in social networks.

Lucas Hui is an Associate Professor of Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include information security and digital forensics.

Ricci Ieong is a Ph.D. student in Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include live forensics, peer-to-peer forensics and time correlation analysis.

Joshua James is a Researcher at the Center for Cybersecurity and Cyber Crime Investigation, University College Dublin, Dublin, Ireland. His research interests include cyber crime investigation process models and standards, evidence correlation techniques, human inference and event reconstruction.

Zoe Jiang is a Postdoctoral Researcher in the School of Computer Science and Technology at Shenzhen Graduate School, Harbin Institute of Technology, Shenzhen, China. Her research interests include digital forensics and applied cryptography.

Tahar Kechadi is a Professor of Computer Science and Informatics at University College Dublin, Dublin, Ireland. His research interests include data extraction and analysis, and data mining in digital forensics and cyber crime investigations.

Thomas Kemmerich is a Lecturer of Computer Science at the University of Bremen, Bremen, Germany. His research interests include information security management, digital evidence and digital forensics.

Nicolai Kuntze is a Researcher at the Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany. His research interests include trusted computing, network security architectures and forensic readiness of embedded devices.

Michael Kwan is an Honorary Assistant Professor of Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include digital forensics, digital evidence evaluation and the application of probabilistic models in digital forensics.

Pierre Lai is a Guest Lecturer and a Research Project Manager in the Department of Computer Science at the University of Hong Kong, Hong Kong, China. Her research interests include cryptography, peer-to-peer networks and digital forensics.

Himal Lalla received his M.Com. degree in Information Systems from the University of Fort Hare, East London, South Africa. His research interests include digital forensics and stylometry.

Nhien-An Le-Khac is a Researcher in the School of Computer Science and Informatics, University College Dublin, Dublin, Ireland. His research interests include data mining in criminal investigations, cloud security and privacy, and grid and high-performance computing.

Martin Mulazzani is a Ph.D. student in Computer Science at the Vienna University of Technology, Vienna, Austria; and a Computer Security Researcher at SBA Research, Vienna, Austria. His research interests include privacy, digital forensics and applied security.

Teja Myneedu is a Software Engineer with Union Pacific in Omaha, Nebraska. His research interests include digital forensics and system security.

Alex Nelson is a Ph.D. student in Computer Science at the University of California Santa Cruz, Santa Cruz, California. His research interests include digital forensics, computer security, indexing, long-term data management and archival storage.

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

Grant Osborne is a Defense Scientist at the Defense Science and Technology Organization, Adelaide, Australia. His research interests include digital forensics and visualization.

Heloise Pieterse is an M.Sc. student in Computer Science at the University of Pretoria, Pretoria, South Africa. Her research interests include digital forensics and mobile botnets.

Celia Ralha is an Associate Professor of Computer Science at the University of Brasilia, Brasilia, Brazil. Her research interests include data mining and multiagent system applications in specialized domains such as digital forensics.

Dirk Ras is a B.Sc. (Honors) student in Computer Science at the University of Pretoria, Pretoria, South Africa. His research interests include digital forensics applied to cloud computing and databases.

Vassil Roussev is an Associate Professor of Computer Science at the University of New Orleans, New Orleans, Louisiana. His research interests are in the area of large-scale digital forensics, particularly performance, scalability, automated sampling and triage, and visual analytics support.

Keyun Ruan is a Researcher in the School of Computer Science and Informatics, University College Dublin, Dublin, Ireland. Her research interests include cloud computing, cloud security and digital forensics.

Marcelo Ruback is an M.Sc. student in Electrical Engineering at the University of Brasilia, Brasilia, Brazil; and a Computer Forensics Expert at the National Institute of Criminalistics, Brazilian Federal Police, Brasilia, Brazil. His research interests include cryptographic hash functions and data mining applications in digital forensics.

Carsten Rudolph is the Head of the Secure Engineering Research Department at the Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany. His research interests include security modeling and validation, model-based security engineering, cryptographic protocols and trusted computing.

Tendai Sanyamahwe is an M.Com. student in Information Systems at the University of Fort Hare, East London, South Africa. His research interests include digital forensics and networking.

Sven Schmitt is a Ph.D. student in Computer Science at Friedrich Alexander University, Erlangen-Nuremberg, Germany. His research interests include database forensics and live forensics.

Jill Slay is the Dean of Research and a Professor of Forensic Computing at the University of South Australia, Adelaide, Australia. Her research interests include information assurance, digital forensics, critical infrastructure protection and complex system modeling.

Luigi Sportiello is an Information Security Researcher at the Joint Research Center of the European Commission, Ispra, Italy. His research interests include cryptography, and security and privacy in RFID systems and digital forensics.

Michael Spreitzenbarth is a Ph.D. student in Computer Science at Friedrich Alexander University, Erlangen-Nuremberg, Germany. His research interests include mobile phone forensics and malware analysis.

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

Paul Tarwireyi is a Lecturer of Information Systems at the University of Fort Hare, East London, South Africa. His research interests include computer security and networking.

Hannah Thinyane is an Associate Professor of Computer Science at Rhodes University, Grahamstown, South Africa; and an Adjunct Senior Research Fellow at the University of South Australia, Adelaide, Australia. Her research interests include visualization and augmented reality, and information technologies for development.

Justin Trentesaux is an M.Sc. student in Computer Science and Informatics at University College Dublin, Dublin, Ireland. His research interests include digital forensics and information security.

Hayson Tse is a Computer Science Researcher at the University of Hong Kong, Hong Kong, China. His research interests include digital forensics, and artificial intelligence and the law.

Franscois van Staden is an M.Sc. student in Computer Science and an Academic Systems Administrator at the University of Pretoria, Pretoria, South Africa. His research interests include digital forensic readiness and process standardization.

Hein Venter is an Associate Professor of Computer Science and the Leader of the Information and Computer Security Architectures Research Group at the University of Pretoria, Pretoria, South Africa. His research interests include digital forensics, privacy and network security.

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

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.

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

Stefano Zanero is a Research Assistant Professor of Computer Security at Politecnico di Milano, Milan, Italy. His research interests include malware analysis, systems security and digital forensics.

Gang Zhou is the Director of the Computer Applications Laboratory at the Wuhan Engineering Science and Technology Institute, Wuhan, China. His research interests include digital forensics, large-scale network storage and embedded encryption systems.

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 VIII*, is the eighth 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-two edited papers from the Eighth IFIP WG 11.9 International Conference on Digital Forensics, held at the University of Pretoria, Pretoria, South Africa, January 3–5, 2012. The papers were refereed by members of IFIP Working Group 11.9 and other internationally-recognized experts in digital forensics.

The chapters are organized into six sections: themes and issues, forensic techniques, mobile phone forensics, cloud forensics, network forensics and advanced forensic techniques. 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 Hein Venter, Rene Venter and Mark Pollitt for their 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