IFIP Advances in Information and Communication Technology 433

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 X

10th IFIP WG 11.9 International Conference
Vienna, Austria, January 8-10, 2014
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 978-3-662-44951-6 e-ISBN 978-3-662-44952-3
DOI 10.1007/978-3-662-44952-3
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014948941

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

Oluwasola Mary Adedayo 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.

Sadia Afroz is a Postdoctoral Researcher in the Computer Science Division at the University of California at Berkeley, Berkeley, California. Her research interests include security, privacy and machine learning.

Waqas Ali is an M.S./M.Phil. student in Information Security at the National University of Sciences and Technology, Islamabad, Pakistan. His research interests include vulnerability discovery, penetration testing and digital forensics.

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

Ibrahim Baggili is an Assistant Professor of Computer Science at the University of New Haven, West Haven, Connecticut. His research interests include digital forensics and cyber crime.

Harald Baier is a Professor of Internet Security at the Darmstadt University of Applied Sciences, Darmstadt, Germany; and a Principal Investigator at the Center for Advanced Security Research Darmstadt, Darmstadt, Germany. His research areas include digital forensics, network-based anomaly detection and security protocols.

Stefanie Beyer received her M.Sc. degree in Computer Science from the Vienna University of Technology, Vienna, Austria. Her research interests are in the area of digital forensics, with a focus on the reliability of digital alibis.

Clive Blackwell is a Research Fellow in Digital Forensics at Oxford Brookes University, Oxford, United Kingdom. His research interests include cyber security and digital forensics, with a focus on developing a scientific basis for digital forensics.

Frank Breitinger is a Ph.D. student in Computer Science at the Darmstadt University of Applied Sciences, Darmstadt, Germany; and a Researcher at the Center for Advanced Security Research Darmstadt, Darmstadt, Germany. His research interests include digital forensics, file analysis and approximate matching.

Patrick Brennan is the Chief Executive Officer of Juola and Associates, Pittsburgh, Pennsylvania. His research interests include digital forensics and stylometry.

Vivien Chan is a Research Project Manager at the University of Hong Kong, Hong Kong, China. Her research interests include cyber criminal profiling and digital forensics.

Ahmad Raza Cheema is an Assistant Professor of Information Security at the National University of Sciences and Technology, Islamabad, Pakistan. His research interests include network security and digital forensics.

Kim-Kwang Choo is a Senior Lecturer of Cyber Security at the University of South Australia, Adelaide, Australia. His research interests include anti-money laundering, cyber crime, digital forensics and information 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.

Philip Craiger is an Associate Professor of Engineering Technology at Daytona State College, Daytona Beach, Florida. His research interests include the technical and behavioral aspects of information security and digital forensics.

Quang Do is a Ph.D. student in Computer and Information Science at the University of South Australia, Adelaide, Australia. His research interests include user privacy preservation and mobile device security.

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.

Tobias Fink is an M.Sc. student in Computer Science at the Darmstadt University of Applied Sciences, Darmstadt, Germany. His research interests include embedded systems and cryptography.

Guy Fong is a Senior Official with the Hong Kong Customs and Excise Department, Hong Kong, China. His research interests include intellectual property rights protection and intellectual property rights infringement in cyber platforms.

Alex Fridman is a Ph.D. student in Electrical and Computer Engineering at Drexel University, Philadelphia, Pennsylvania. His research interests include machine learning, numerical optimization, robotics and communications networks.

Simson Garfinkel is an Associate Professor of Computer Science at the Naval Postgraduate School (National Capital Region Office) in Arlington, Virginia. His research interests include security and privacy.

Kyle Gorak is a Cadet majoring in Computer Science at the U.S. Military Academy, West Point, New York. His research interests include security exploitation and encryption techniques.

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 anti-forensic and anti-anti-forensic techniques for mobile devices.

Lukas Graner is a B.S. student in Computer Science at the Technical University of Darmstadt, Darmstadt, Germany. His research interests include digital forensic tool testing using synthetic test data.

Rachel Greenstadt is an Assistant Professor of Computer Science at Drexel University, Philadelphia, Pennsylvania. Her research centers on the privacy and security properties of intelligent systems and the economics of electronic privacy and information security.

Gaurav Gupta is an Assistant Professor of Computer Science at Indraprastha Institute of Information Technology, New Delhi, India. His research interests include digital forensics, digitized document fraud detection and mobile device forensics.

Aubin Heffernan is a Cadet majoring in Computer Science at the U.S. Military Academy, West Point, New York. His research interests include cyber security and digital forensics.

Scott Horras is a Cadet majoring in Computer Science at the U.S. Military Academy, West Point, New York. His research interests include artificial intelligence and data processing.

Markus Huber is a Computer Security Researcher at SBA Research, Vienna, Austria. His research focuses on security and privacy issues in social networks.

Aleksandar Hudic is a Researcher at the Austrian Institute of Technology, Vienna, Austria. His research interests are in the area of autonomic security management systems for distributed environments.

Michael Hui is a Senior Inspector with the Hong Kong Customs and Excise Department, Hong Kong, China. His research interests are in the area of intellectual property rights protection.

Ricci Ieong is the Director of eWalker Consulting, a digital forensics consultancy in Hong Kong, China; and a Researcher in Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include live forensics, peer-to-peer forensics, cloud forensics and time correlation analysis.

Mian Muhammad Waseem Iqbal is a Lecturer of Information Security at the National University of Sciences and Technology, Islamabad, Pakistan. His research interests include network security and digital forensics.

Yasser Jafar received an M.S. degree in Information Technology (Cyber Security Specialization) from Zayed University, Abu Dhabi, United Arab Emirates. His research interests include digital forensics and information security.

Patrick Juola is a Co-Founder of Juola and Associates, Pittsburgh, Pennsylvania; and a Professor of Computer Science at Duquesne University, Pittsburgh, Pennsylvania. His research interests include humanities computing, computational psycholinguistics, and digital and linguistic forensics.

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.

Katharina Krombholz is a Computer Security Researcher at SBA Research, Vienna, Austria; and a Ph.D. student in Computer Science at the Vienna University of Technology, Vienna, Austria. Her research interests include usable security and digital forensics.

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.

Steffen Lange is a Professor of Theoretical Computer Science at the Darmstadt University of Applied Sciences, Darmstadt, Germany. His research interests include algorithmic learning theory, formal language theory and information technology security.

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

Wee-Yong Lim is a Researcher in the Cybercrime and Security Intelligence Department at the Institute for Infocomm Research, Singapore. His research interests include predictive intelligence, text analysis, object recognition and machine learning.

Jonathan Looi received his Bachelor's degree in Information Technology from the University of South Australia, Adelaide, Australia. His research interests are in the area of digital forensics.

Andrew Marrington is an Assistant Professor of Information Technology at Zayed University, Dubai, United Arab Emirates. His research interests include digital forensics and information security.

Ben Martini is the Digital Forensics Research Administrator and a Ph.D. student in Computer and Information Science at the University of South Australia, Adelaide, Australia. His research interests include cyber security and digital forensics.

Martin Mulazzani is a Postdoctoral Researcher at SBA Research, Vienna, Austria. His research interests include digital forensics, privacy and applied security.

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

Thomas Otterbein is a Researcher in the Secure Systems Laboratory at the Vienna University of Technology, Vienna, Austria. His research interests are in the area of digital forensics.

Rebekah Overdorf is a Ph.D. student in Computer Science at Drexel University, Philadelphia, Pennsylvania. Her research interests include security and privacy, machine learning and stylometry.

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

Christian Platzer is a Senior Researcher and Head of the Secure Systems Laboratory at the Vienna University of Technology, Vienna, Austria. His research areas include malware analysis, digital forensics and network security.

Mark Pollitt recently retired from his position as an Associate Professor of Engineering Technology at Daytona State College, Daytona Beach, Florida. His research interests include digital forensics, textual and narrative theory, and knowledge management.

Mark Roeloffs is a Forensic Examiner at the Netherlands Forensic Institute, The Hague, The Netherlands. His research interests include digital forensics of mobile phones, navigation systems and other embedded systems.

Amit Sachan is a Researcher in the Cybercrime and Security Intelligence Department at the Institute for Infocomm Research, Singapore. His research interests include information security, digital forensics and digital rights management.

Sebastian Schrittwieser is a Lecturer of Information Security at the St. Polten University of Applied Sciences, St. Polten, Austria; and a Ph.D. candidate in Computer Science at the Vienna University of Technology, Vienna, Austria. His research interests include digital forensics, software protection and code obfuscation.

Michael Seefried is an M.Sc. student in Computer Science at the Darmstadt University of Applied Sciences, Darmstadt, Germany. His research interests include digital forensics and information security.

Martin Steinebach is the Head of Media Security and IT Forensics at the Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany. His research interests include digital watermarking and robust hashing.

Ariel Stolerman is a Ph.D. student in Computer Science at Drexel University, Philadelphia, Pennsylvania. His research interests include security and privacy, applied machine learning and text analysis.

Atsuhiro Takasu is a Professor in the Digital Content and Media Services Research Division at the National Institute of Informatics, Tokyo, Japan. His research interests include symbol sequence and time series analysis based on statistical models and their application to information integration.

Jemy Tang is a Training Officer at the Electronic Crime Investigation Centre of the Hong Kong Customs and Excise Department, Hong Kong, China. His research interests include digital forensics and the analysis of cyber crime investigations.

Vrizlynn Thing leads the Cybercrime and Security Intelligence Department at the Institute for Infocomm Research, Singapore. Her research interests include network security, systems security, mobile device security, digital forensics and security analytics.

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 defense and security systems, and technologies for sustainable development.

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 digitized document fraud detection, mobile device forensics and cloud forensics.

Yu Wang received his Bachelor's degree in Information Technology from the University of South Australia, Adelaide, Australia. His research interests are in the area of digital forensics.

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.

Christian Winter is a Research Associate in IT Forensics at the Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany. His research interests include statistical forensics and fuzzy hashing.

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.

York Yannikos is a Research Associate in IT Forensics at the Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany. His research interests include digital forensic tool testing, synthetic test data generation and multimedia file carving.

Carolina Zarate is an undergraduate student in Computer Science at Carnegie Mellon University, Pittsburgh, Pennsylvania. Her research interests include cyber security and digital forensics.

Georg Ziroff received his B.Sc. degree in Computer Science from the Darmstadt University of Applied Sciences, Darmstadt, Germany. His research interests include approximate string matching and similarity hashing, and their applications in malware detection.

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 X*, is the tenth 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 Tenth IFIP WG 11.9 International Conference on Digital Forensics, held at the Vienna University of Technology in Vienna, Austria on January 8–10, 2014. 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 four sections: Internet crime investigations, forensic techniques, mobile device forensics, and forensic tools and training. 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 Martin Mulazzani and Yvonne Poul 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