IFIP Advances in Information and Communication Technology 361

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 ist member countries and to encourage technology transfer to developing nations. As ist 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 less 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 in information 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 VII

7th IFIP WG 11.9 International Conference
on Digital Forensics
Orlando, FL, USA, January 31 – February 2, 2011
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 978-3-642-24211-3 e-ISBN 978-3-642-24212-0
DOI 10.1007/978-3-642-24212-0
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011936376

CR Subject Classification (1998): H.3, C.2, K.6.5, D.4.6, F.2, E.3

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

PART V ADVANCED FORENSIC TECHNIQUES

Contributing Authors

Rafael Accorsi is a Lecturer of Computer Science and the Head of the Business Process Security Group at the University of Freiburg, Freiburg, Germany. His interests include information security and compliance in process-aware information systems, with an emphasis on automated certification, forensics and auditing.

Irfan Ahmed is a Postdoctoral Research Fellow at the Information Security Institute, Queensland University of Technology, Brisbane, Australia. His research interests include digital forensics, intrusion detection, malware analysis and control systems security.

Andre Arnes is the Head of Enterprise Security and Connectivity at Telenor Key Partner, Oslo, Norway; and an Associate Professor of Computer Science at the Norwegian Information Security Laboratory, Gjovik University College, Gjovik, Norway. His research interests include digital and memory forensics, forensic reconstruction and computer security.

Hector Beyers is an M.Eng. student in Computer Engineering at the University of Pretoria, Pretoria, South Africa; and a Technical Systems Engineer with Dimension Data, Johannesburg, South Africa. His research interests include computer security, digital forensics and artificial intelligence.

Clive Blackwell is a Research Fellow in Digital Forensics at Oxford Brookes University, Oxford, United Kingdom. His research interests include the application of formal methods such as logic, finite automata and process calculi to digital forensics and information security.

Shane Bracher is an eBusiness Researcher at SAP Research, Brisbane, Australia. His research interests include fraud detection and business intelligence.

Joe Carthy is 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.

Andrew Clark is an Adjunct Associate Professor of Information Technology at Queensland University of Technology, Brisbane, Australia. His research interests include digital forensics, intrusion detection and network security.

Fred Cohen is the Chief Executive Officer of Fred Cohen and Associates; and the President of California Sciences Institute, Livermore, California. His research interests include digital forensics, information assurance and critical infrastructure protection.

Scott Conrad was a Senior Digital Forensics Research Assistant at the National Center for Forensic Science, University of Central Florida, Orlando, Florida. His research interests include personal gaming devices and virtualization technologies.

Malcolm Corney is a Lecturer of Computer Science at Queensland University of Technology, Brisbane, Australia. His research interests include insider misuse, digital forensics and computer science education.

Philip Craiger is an Associate Professor of Engineering Technology at Daytona State College, Daytona Beach, Florida; and the Assistant Director for Digital Evidence at the National Center for Forensic Science, University of Central Florida, Orlando, Florida. His research interests include the technical and behavioral aspects of information security and digital forensics.

Mark Crosbie is a Security Architect with IBM in Dublin, Ireland. His research interests include cloud security, software security, penetration testing and mobile device security.

Greg Dorn is a Senior Digital Forensics Research Assistant at the National Center for Forensic Science, University of Central Florida, Orlando, Florida. His research interests include virtualization technologies and personal gaming devices.

Anders Flaglien is a Security Consultant at Accenture in Oslo, Norway. His research interests include digital forensics, malware analysis, data mining and computer security.

Ulrich Flegel is a Professor of Computer Science at HFT Stuttgart University of Applied Sciences, Stuttgart, Germany. His research focuses on privacy-respecting reactive security solutions.

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.

Katrin Franke is a Professor of Computer Science at the Norwegian Information Security Laboratory, Gjovik University College, Gjovik, Norway. Her research interests include digital forensics, computational intelligence and robotics.

Gerhard Hancke is a Professor of Computer Engineering at the University of Pretoria, Pretoria, South Africa. His research interests are in the area of advanced sensor networks.

Andrew Hay is an M.S. student in Cyber Operations at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include intrusion detection and SCADA 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.

Man-Pyo Hong is a Professor of Information and Computer Engineering at Ajou University, Suwon, South Korea. His research interests are in the area of information security.

David Irwin is a Ph.D. student in Computer Science at the University of South Australia, Adelaide, Australia. His research interests include digital forensics and information security.

Asadul Islam is a Research Fellow in Information Security at Queensland University of Technology, Brisbane, Australia. His research interests include information security, digital forensics and XML.

Ramesh Joshi is a Professor of Electronics and Computer Engineering at the Indian Institute of Technology, Roorkee, India. His research interests include parallel and distributed processing, data mining, information systems, information security and digital forensics.

Patrick Juola is an Associate 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.

Dennis Krill is an M.S. student in Cyber Warfare at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research focuses on integrating space, influence and cyber operations.

Benjamin Kuhar is an M.S. student in Cyber Operations at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include malware collection and analysis.

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 Ph.D. student in Computer Science at the University of Hong Kong, Hong Kong, China. Her research interests include cryptography, peer-to-peer networks and digital forensics.

Frank Law is a Ph.D. student in Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include digital forensics and time analysis.

Kyung-Suk Lhee, formerly an Assistant Professor of Information and Computer Engineering at Ajou University, Suwon, South Korea, is an Independent Researcher based in Seoul, South Korea. His research interests include computer security and network security.

Julie Lowrie is a Ph.D. student in Digital Forensics at California Sciences Institute, Livermore, California. Her research interests include digital forensics, cyber crime and economic crime investigations, and criminal profiling.

Heather McCalley is an M.S. student in Computer Science and a candidate for a Certificate in Computer Forensics at the University of Alabama at Birmingham, Birmingham, Alabama. Her research interests include phishing and cyber crime investigations.

Frederico Mesquita 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 live forensics and malware analysis.

Robert Mills is an Associate Professor of Electrical Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include network management, network security and insider threat mitigation.

George Mohay is an Adjunct Professor of Computer Science at Queensland University of Technology, Brisbane, Australia. His research interests include digital forensics and intrusion detection.

Barry Mullins is an Associate Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include cyber operations, computer and network security, and reconfigurable computing systems.

Rajdeep Niyogi is an Assistant Professor of Electronics and Computer Engineering at the Indian Institute of Technology, Roorkee, India. His research interests include automated planning, formal methods and distributed systems.

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

Richard Overill is a Senior Lecturer of Computer Science at King's College London, London, United Kingdom. His research interests include digital forensics, cyber crime analysis, cyber attack analysis and information assurance.

Gilbert Peterson is an Associate Professor of Computer Science at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include digital forensics and statistical machine learning.

Emmanuel Pilli is a Research Scholar with the Department of Electronics and Computer Engineering at the Indian Institute of Technology, Roorkee, India. His research interests include information security, intrusion detection, network forensics and cyber crime investigations.

Charles Preston is the Chief Operating Officer of SysWisdom LLC, Anchorage, Alaska. His research interests include information assurance, network security and wireless network design.

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.

Tobias Raub is the Team Lead of Business Development at SAP Research, Brisbane, Australia. His research interests are in the area of business intelligence.

Keyun Ruan is a Ph.D. student in Computer Science and Informatics at University College Dublin, Dublin, Ireland. Her research interests include cloud computing, cloud security and digital forensics.

Markus Schneider is the Deputy Director of the Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany. His research interests include digital forensics and information security.

Hyun-Jung Shin is an Associate Professor of Industrial and Information Systems Engineering at Ajou University, Suwon, South Korea. Her research interests include hospital fraud detection, oil/stock price prediction and bioinformatics.

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.

Jon Stewart is the Chief Technology Officer and Co-Founder of Lightbox Technologies, Arlington, Virginia. His research interests include string searching, large-scale forensic analysis, distributed systems and machine learning.

Brennon Thomas received his M.S. degree in Cyber Operations from the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include computer and network defense, and embedded systems.

Hayson Tse 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.

Joel Uckelman is a Partner in Lightbox Technologies, Arlington, Virginia. His research interests include rule specification and preference specification languages, logic and social choice.

Hein Venter is an Associate Professor of Computer Science at the University of Pretoria, Pretoria, South Africa. His research interests include network security, digital forensics and information privacy.

Darren Vescovi is an M.S. student in Computational Mathematics at Duquesne University, Pittsburgh, Pennsylvania. His research interests include humanities computing, data mining and regression analysis.

Ickin Vural is an M.Sc. student in Computer Science at the University of Pretoria, Pretoria, South Africa; and a Software Developer with Absa Capital, Johannesburg, South Africa. His research interests include artificial intelligence and mobile botnets.

Brad Wardman is a Ph.D. student in Computer and Information Sciences at the University of Alabama at Birmingham, Birmingham, Alabama. His research interests include digital forensics and phishing.

Gary Warner is the Director of Computer Forensics Research at the University of Alabama at Birmingham, Birmingham, Alabama. His research interests include digital investigations, with an emphasis on email-based crimes such as spam, phishing and malware, and very large data set analysis.

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

Claus Wonnemann is a Ph.D. student in Computer Science at the University of Freiburg, Freiburg, Germany. His research focuses on the security certification and forensic analysis of business process models.

York Yannikos is a Research Assistant in IT Forensics at the Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany. His research interests include forensic tool testing, live forensics and mobile device forensics.

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 VII*, is the seventh 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-one edited papers from the Seventh IFIP WG 11.9 International Conference on Digital Forensics, held at the National Center for Forensic Science, Orlando, Florida, January 31 – February 2, 2011. 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 five sections: themes and issues, forensic techniques, fraud and malware investigations, 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 Daniel Guernsey, Philip Craiger, Jane Pollitt 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, and U.S. Secret Service.

Gilbert Peterson and Sujeet Shenoi