IFIP Advances in Information and Communication Technology 337

Editor-in-Chief

A. Joe Turner, Seneca, SC, USA

Editorial Board

Foundations of Computer Science
Mike Hinchey, Lero, Limerick, Ireland

Software: Theory and Practice
Bertrand Meyer, ETH Zurich, Switzerland

Education
Bernard Cornu, CNED-EIFAD, Poitiers, France

Information Technology Applications
Ronald Waxman, EDA Standards Consulting, Beachwood, OH, USA

Communication Systems
Guy Leduc, Université de Liège, Belgium

System Modeling and Optimization
Jacques Henry, Université de Bordeaux, France

Information Systems
Barbara Pernici, Politecnico di Milano, Italy

Relationship between Computers and Society
Chrisanthi Avgerou, London School of Economics, UK

Computer Systems Technology
Paolo Prinetto, Politecnico di Torino, Italy

Security and Privacy Protection in Information Processing Systems
Kai Rannenberg, Goethe University Frankfurt, Germany

Artificial Intelligence
Max A. Bramer, University of Portsmouth, UK

Human-Computer Interaction
Annelise Mark Pejtersen, Center of Cognitive Systems Engineering, Denmark

Entertainment Computing
Ryohei Nakatsu, National University of Singapore

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 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.

Kam-Pui Chow Sujeet Shenoi (Eds.)

Advances in Digital Forensics VI

Sixth IFIP WG 11.9 International Conference on Digital Forensics
Hong Kong, China, January 4-6, 2010
Revised Selected Papers

Springer

Volume Editors

Kam-Pui Chow
University of Hong Kong, Department of Computer Science
Hong Kong, China
E-mail: chow@cs.hku.hk

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

Library of Congress Control Number: 2010934317

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

ISSN 1868-4238
ISBN-10 3-642-15505-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-15505-5 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 219/3180

Contents

Contributing Authors

Saif Al-Kuwari is a Ph.D. student in Mathematics with the Information Security Group at Royal Holloway, University of London, London, United Kingdom. His research interests are in the area of digital forensics, particularly clandestine localization and tracking in MANET and VANET environments.

Ivan Burke is an M.Sc. student in Computer Science at the University of Pretoria, Pretoria, South Africa; and a Researcher with the Council for Scientific and Industrial Research, Pretoria, South Africa. His research interests include wireless networks and agent-based modeling.

Hilton Chan is an Adjunct Assistant Professor of Information Systems, Business Statistics and Operations Management at the Hong Kong University of Science and Technology, Hong Kong, China. His research interests include cyber crime investigations, digital forensics, incident response and crisis management.

Patrick Chan is an M.Phil. student in Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include web security, applied cryptography and network security.

Jenny Chen is a Research Engineer with the Center for Information Security and Cryptography at the University of Hong Kong, Hong Kong, China. Her research interests include digital forensics and peer-to-peer networks.

Lijuan Chen is an Associate Researcher at the Shandong Computer Science Center, Jinan, China. Her research interests include information security, digital forensics and database systems.

Zhenya Chen is an Associate Researcher at the Shandong Computer Science Center, Jinan, China. Her research interests include digital forensics and grid computing.

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 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.

Michael Cohen is a Data Specialist with the Australian Federal Police in Brisbane, Australia. His research interests include network forensics, memory forensic analysis, large-scale forensic frameworks and the AFF4 forensic file format.

Scott Conrad is 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/entertainment devices and virtualization technologies.

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.

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/entertainment devices.

Isao Echizen is an Associate Professor of Computer Science at the National Institute of Informatics, Tokyo, Japan. His research interests include media security, information processing and information hiding.

Ryo Furukawa is a Researcher at NEC Corporation, Tokyo, Japan. His research interests include access control, privacy management and optimization.

Pavel Gladyshev is a Lecturer of Computer Science and Informatics at University College Dublin, Dublin, Ireland. His research interests include information security and digital forensics.

Paolo Gubian is an Associate Professor of Electrical Engineering at the University of Brescia, Brescia, Italy. His research areas include integrated circuit design, digital forensics and embedded systems security.

Murat Gunestas is a Police Major with the General Directorate of Security in Ankara, Turkey. His research interests include web services security, computer and network forensics, and software engineering.

Yinghua Guo is a Postdoctoral Research Fellow at the School of Computer and Information Science, University of South Australia, Adelaide, Australia. His research interests include digital forensics, information assurance, network security, intrusion detection systems and wireless networking.

Wing-Kai Hon is an Assistant Professor of Computer Science at National Tsing Hua University, Hsinchu, Taiwan. His research interests include data compression, design and analysis of algorithms, and combinatorial optimization.

Lucas Hui is an Associate Professor of Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include computer security, cryptography 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 digital forensics, peer-to-peer forensics and time correlation analysis.

Joshua James is a Ph.D. student in Computer Science and Informatics at University College Dublin, Dublin, Ireland. His research interests include cyber crime investigation process models and standards, evidence correlation techniques, human inference and event reconstruction.

Masahiro Kawato is an Assistant Manager at NEC Corporation, Tokyo, Japan. His research interests include distributed computing, enterprise systems security and privacy management.

Michael Kwan is a Ph.D. student in 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.

Frankie Li is an M.Sc. student in Electronic Commerce and Internet Computing at the University of Hong Kong, Hong Kong, China. His research interests include digital forensics and malware analysis.

Fumio Machida is an Assistant Manager at NEC Corporation, Tokyo, Japan. His research interests include dependable computing, autonomic computing and systems management.

Yoshiharu Maeno is a Principal Researcher at NEC Corporation, Tokyo, Japan. His research interests include the analysis and control of complex distributed systems for communications and computing.

Murad Mehmet is a Ph.D. student in Information Technology at George Mason University, Fairfax, Virginia. His research interests include network security, digital forensics and web services security.

Yuki Nakayama is an M.S. student in Computer Science at Keio University, Kanagawa, Japan. His research interests include network security and digital forensics.

Sipho Ngobeni is an M.Sc. student in Computer Science at the University of Pretoria, Pretoria, South Africa; and a Researcher with the Council for Scientific and Industrial Research, Pretoria, South Africa. His research interests include network security, digital forensics and information security.

Kenichi Okada is a Professor of Information and Computer Science at Keio University, Kanagawa, Japan. His research interests include computer-supported cooperative work, groupware, human-computer interaction and ubiquitous computing.

James Okolica is a Ph.D. student in Computer Science at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include text mining and memory forensics.

Richard Overill is a Senior Lecturer in Computer Science at King's College London, London, United Kingdom. His research interests include digital forensics, cyber crime analysis, anomaly detection, cyber warfare and information security management.

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, steganography and machine learning.

Mark Pollitt, Chair, IFIP Working Group 11.9 on Digital Forensics, is an Associate Professor of Engineering Technology at Daytona State College, Daytona Beach, Florida; and a principal with the National Center for Forensic Science, University of Central Florida, Orlando, Florida. His research interests include forensic processes, knowledge management, information security and forensic quality management.

Vassil Roussev is an Assistant 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.

Antonio Savoldi is an Associate Researcher in the Department of Information Engineering at the University of Brescia, Brescia, Italy. His research interests include digital forensics, embedded systems security and counter-forensic methodologies.

Bradley Schatz is the Director of Schatz Forensic, a digital forensics consultancy; and an Adjunct Associate Professor at the Information Security Institute, Queensland University of Technology, Brisbane, Australia. His research interests include volatile memory acquisition, scaling storage forensics and the development of the new AFF4 forensic evidence container.

Seiji Shibaguchi is a Software Developer with Nintendo in Kyoto, Japan. His research interests include network security and digital forensics.

Jantje Silomon is a Research Associate in the Department of Computer Science, King's College London, London, United Kingdom. Her research interests are in the area of digital 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.

Kumiko Tadano is a Researcher at NEC Corporation, Tokyo, Japan. Her research interests include dependable computing, systems management and enterprise systems security.

Benjamin Tang is an undergraduate student in Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include digital forensics.

Vrizlynn Thing leads the Digital Forensics Research Group at the Institute for Infocomm Research, Singapore. Her research interests include digital forensics, network security, intrusion detection and mitigation, networking protocols and optical fiber communications.

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.

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.

Chunxiao Wang is an Associate Researcher at the Shandong Computer Science Center, Jinan, China. Her research interests include cryptography, digital forensics and software engineering.

Kenny Wang is a Ph.D. candidate in Law at the University of Hong Kong, Hong Kong, China. His research interests include digital evidence, cyber crime and legal jurisdiction.

Duminda Wijesekera is an Associate Professor of Information and Software Engineering at George Mason University, Fairfax, Virginia. His research interests include information, network, telecommunications and control systems security.

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 the modeling and simulation of critical infrastructures, and network and distributed systems security.

Ying Yang is an Associate Professor of Information Security at the Shandong Computer Science Center, Jinan, China. Her research interests include computer security, digital forensics and software systems.

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

Yuandong Zhu is a Ph.D. student in Computer Science and Informatics at University College Dublin, Dublin, Ireland. His research interests include user activity analysis and forensic tool development.

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 VI*, is the sixth 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 Sixth IFIP WG 11.9 International Conference on Digital Forensics, held at the University of Hong Kong, Hong Kong, January 4–6, 2010. 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, Internet crime investigations, live forensics, advanced forensic techniques 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 Daniel Guernsey, Pierre Lai and Catherine Chan for their tireless work on behalf of IFIP Working Group 11.9. We also acknowledge the support provided by the University of Hong Kong, Hong

Kong Police Force, Hong Kong Forensic Science Foundation, National Security Agency, Immigration and Customs Enforcement, and U.S. Secret Service.

Kam-Pui Chow and Sujeet Shenoi