IFIP Advances in Information and Communication Technology 569

Editor-in-Chief

Kai Rannenberg, Goethe University Frankfurt, Germany

Editorial Board Members

TC 1 – Foundations of Computer Science
Jacques Sakarovitch, Télécom ParisTech, France

TC 2 – Software: Theory and Practice
Michael Goedicke, University of Duisburg-Essen, Germany

TC 3 – Education
Arthur Tatnall, Victoria University, Melbourne, Australia

TC 5 – Information Technology Applications
Erich J. Neuhold, University of Vienna, Austria

TC 6 – Communication Systems
Aiko Pras, University of Twente, Enschede, The Netherlands

TC 7 – System Modeling and Optimization
Fredi Tröltzsch, TU Berlin, Germany

TC 8 – Information Systems
Jan Pries-Heje, Roskilde University, Denmark

TC 9 – ICT and Society
David Kreps, University of Salford, Greater Manchester, UK

TC 10 – Computer Systems Technology
Ricardo Reis, Federal University of Rio Grande do Sul, Porto Alegre, Brazil

TC 11 – Security and Privacy Protection in Information Processing Systems
Steven Furnell, Plymouth University, UK

TC 12 – Artificial Intelligence
Ulrich Furbach, University of Koblenz-Landau, Germany

TC 13 – Human-Computer Interaction
Marco Winckler, University of Nice Sophia Antipolis, France

TC 14 – Entertainment Computing
Rainer Malaka, University of Bremen, Germany

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. A federation for societies working in information processing, IFIP's aim is two-fold: to support information processing in the countries of its members and to encourage technology transfer to developing nations. As its mission statement clearly states:

> *IFIP is the global non-profit federation of societies of ICT professionals that aims at achieving a worldwide professional and socially responsible development and application of information and communication technologies.*

IFIP is a non-profit-making organization, run almost solely by 2500 volunteers. It operates through a number of technical committees and working groups, which organize events and publications. IFIP's events range from large international open conferences to working conferences and local seminars.

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 generally smaller and occasionally 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.

IFIP distinguishes three types of institutional membership: Country Representative Members, Members at Large, and Associate Members. The type of organization that can apply for membership is a wide variety and includes national or international societies of individual computer scientists/ICT professionals, associations or federations of such societies, government institutions/government related organizations, national or international research institutes or consortia, universities, academies of sciences, companies, national or international associations or federations of companies.

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

Gilbert Peterson · Sujeet Shenoi (Eds.)

Advances in Digital Forensics XV

15th IFIP WG 11.9 International Conference
Orlando, FL, USA, January 28–29, 2019
Revised Selected Papers

Springer

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

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

ISSN 1868-4238 ISSN 1868-422X (electronic)
IFIP Advances in Information and Communication Technology
ISBN 978-3-030-28751-1 ISBN 978-3-030-28752-8 (eBook)
https://doi.org/10.1007/978-3-030-28752-8

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

Contributing Authors

Temilola Aderibigbe recently received his M.S. degree in Computer Science from Florida A&M University, Tallahassee, Florida. His research interests are in the area of digital forensics.

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

Gunnar Alendal is a Special Investigator with Kripos/NCIS Norway, Oslo, Norway; and a Ph.D. student in Computer Security at the Norwegian University of Science and Technology, Gjovik, Norway. His research interests include digital forensics, reverse engineering, security vulnerabilities, information security and cryptography.

Albert Antwi-Boasiako is the National Cybersecurity Advisor, Republic of Ghana, Ghana, Accra; and the Founder of the e-Crime Bureau, Accra, Ghana. His research interests are in the area of digital forensics, with a focus on digital forensic process standardization.

Stefan Axelsson is an Associate Professor of Digital Forensics at the Norwegian University of Science and Technology, Gjovik, Norway; and an Associate Professor of Digital Forensics at Halmstad University, Halmstad, Sweden. His research interests include digital forensics, data analysis and digital investigations.

Ramesh Babu Battula is an Assistant Professor of Computer Science and Engineering at Malaviya National Institute of Technology, Jaipur, India. His research interests include secure communications, cyber security, performance modeling and next generation networks.

Chun-Fai Chan is a Ph.D. student in Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include penetration testing, digital forensics and Internet of Things security.

Raymond Chan is a Lecturer of Information and Communications Technology at the Singapore Institute of Technology, Singapore. His research interests include cyber security, digital forensics and critical infrastructure protection.

Ramaswamy Chandramouli is a Senior Computer Scientist in the Computer Security Division at the National Institute of Standards and Technology, Gaithersburg, Maryland. His research interests include security for virtualized infrastructures, and smart card interface specification and testing.

Saheb Chhabra is a Ph.D. student in Computer Science and Engineering at Indraprastha Institute of Information Technology, New Delhi, India. His research interests include image processing and computer vision, and their applications to document fraud detection.

Hongmei Chi is an Associate Professor of Computer and Information Sciences at Florida A&M University, Tallahassee, Florida. Her research interests include information assurance, scientific computing, Monte Carlo and quasi Monte Carlo techniques, and data science.

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.

Gokila Dorai is a Ph.D. student in Computer Science at Florida State University, Tallahassee, Florida. Her research interests include computer, mobile device and Internet of Things forensics.

Geir Olav Dyrkolbotn is a Major in the Norwegian Armed Forces, Lillehammer, Norway; and an Associate Professor of Cyber Defense at the Norwegian University of Science and Technology, Gjovik, Norway. His research interest include cyber defense, reverse engineering, malware analysis, side-channel attacks and machine learning.

Struan Gray is an Associate Professor of Physics at Halmstad University, Halmstad, Sweden. His research interests include scanning tunneling microscopy and atomic force microscopy.

Zachary Grimmett is a Computer Engineer with the U.S. Department of Defense in Washington, DC. His research interests include mobile communications devices, digital forensics and malware analysis.

Nicholas Guerra is an M.S. student in Computer Science at the University of Tulsa, Tulsa, Oklahoma. His research interests include digital forensics, cyber security and reverse engineering.

Garima Gupta is a Postdoctoral Researcher in Computer Science and Engineering at Indraprastha Institute of Information Technology, New Delhi, India. Her research interests include image processing and computer vision, and their applications to document fraud detection.

Gaurav Gupta is a Scientist E in the Ministry of Information Technology, New Delhi, India. His research interests include mobile device security, digital forensics, web application security, Internet of Things security and security in emerging technologies.

Monika Gupta is a Visiting Assistant Professor of Optical Physics at Miranda House, Delhi University, India. Her research interests include image processing and computer vision, and their applications to document fraud detection.

Manuel Hernandez is a Software Engineer at Microsoft, Redmond, Washington. His research interests include software engineering and computer hardware.

Yongheng Jia is an M.S. student in Computer Science at Tianjin University, Tianjin, China. His research interests include malware detection and classification.

Umit Karabiyik is an Assistant Professor of Computer and Information Technology at Purdue University, West Lafayette, Indiana. His research interests include digital forensics, user and data privacy, machine learning, and computer and network security.

Martin Karresand is a Senior Scientist at the Swedish Defence Research Agency, Linkoping, Sweden; and a Ph.D. student in Computer Security at the Norwegian University of Science and Technology, Gjovik, Norway. His research interests include digital forensics, file carving, data analysis, machine learning and intrusion detection.

Yuze Li is an M.S. student in Computer Science at Tianjin University, Tianjin, China. His research interests include digital forensics and deep learning.

David Lindahl is a Research Engineer at the Swedish Defence Research Agency, Linkoping, Sweden. His research interests include cyber warfare, critical infrastructure protection and digital forensics.

Changwei Liu is a Postdoctoral Researcher in the Department of Computer Science at George Mason University, Fairfax, Virginia. Her research interests include network security, cloud security and digital forensics.

Jingcheng Liu is an M.S. student in Computer Science at Tianjin University, Tianjin, China. His research interests include data privacy and intrusion detection.

Liangfu Lu is an Assistant Professor of Mathematics at Tianjin University, Tianjin, China. His research interests include compressed sensing, sparse representation and image processing.

Cesar Mak is a Research Programmer at the Logistics and Supply Chain MultiTech R&D Centre, Hong Kong, China. His research interests include digital forensics, machine learning and data analytics.

Tathagata Mukherjee is an Assistant Professor of Computer Science at the University of Alabama in Huntsville, Huntsville, Alabama. His research interests include cyber security, adversarial machine learning, large-scale digital forensics, cyber law, computational geometry, graph theory and optimization.

Martin Olivier is a Professor of Computer Science at the University of Pretoria, Pretoria, South Africa. His research focuses on digital forensics – in particular, the science of digital forensics and database forensics.

James Parsons is a Software Engineer at Microsoft, Redmond, Washington. His research interests include digital forensics and software engineering.

Heloise Pieterse is a Senior Researcher and Software Developer at the Council for Scientific and Industrial Research, Pretoria, South Africa; and a Ph.D. student in Computer Science at the University of Pretoria, Pretoria, South Africa. Her research interests include digital forensics and cyber security.

Emmanuel Pilli is an Associate Professor of Computer Science and Engineering at Malaviya National Institute of Technology, Jaipur, India. His research interests include cyber security, digital forensics, cloud computing, big data, blockchains and the Internet of Things.

Khushboo Rathi is a Senior Software Engineer with Dell Technologies, Round Rock, Texas. Her research interests include digital forensics, mobile forensics and machine learning.

Lakshminarayana Sadineni is a Ph.D. student in Computer Science and Engineering at Malaviya National Institute of Technology, Jaipur, India. His research interests include Internet of Things security and forensics.

Sujeet Shenoi is the F.P. Walter Professor of Computer Science and a Professor of Chemical Engineering at the University of Tulsa, Tulsa, Oklahoma. His research interests include critical infrastructure protection, industrial control systems and digital forensics.

Bhupendra Singh is an Assistant Professor of Computer Science and Engineering at the Indian Institute of Information Technology, Pune, India. His research interests include digital forensics, filesystem analysis and user activity analysis in Windows and Linux systems.

Shweta Singh is an Integrated Software System Engineer at Elkosta Security Systems, New Delhi, India. Her research interests include machine learning and its applications to document fraud detection.

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

Jason Staggs is an Adjunct Assistant Professor of Computer Science at the University of Tulsa, Tulsa, Oklahoma. His research interests include telecommunications networks, industrial control systems, critical infrastructure protection, security engineering and digital forensics.

Renier van Heerden is the Science Engagement Officer at the South African Research and Education Network in Pretoria, South Africa. His research interests include network security, password security and network attacks.

Wynand van Staden is a Senior Lecturer of Computer Science at the University of South Africa, Florida Park, South Africa. His research interests include digital forensics, anonymity and privacy.

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 focus on digital forensic process standardization.

Asalena Warnqvist is a Forensics Expert at the National Forensic Centre, Swedish Police Authority, Linkoping, Sweden. Her research interests include digital forensics and data recovery.

Duminda Wijesekera is a Professor of Computer Science at George Mason University, Fairfax, Virginia. His research interests include systems security, digital forensics and transportation systems.

Rodney Wilson is a Software Developer at IBM, Research Triangle Park, North Carolina. His research interests are in the area of software engineering and test automation.

Yaping Zhang is an Assistant Professor of Computer Science at Tianjin University, Tianjin, China. His research interests include network security, data mining and digital forensics.

Preface

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Computer networks, cloud computing, smartphones, embedded devices and the Internet of Things have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every 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 cyber security – investigations of security breaches yield valuable information that can be used to design more secure and resilient systems.

This book, *Advances in Digital Forensics XV*, is the fifteenth volume in the annual series produced by the 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 fourteen revised and edited chapters based on papers presented at the Fifteenth IFIP WG 11.9 International Conference on Digital Forensics, held in Orlando, Florida, USA on January 28-29, 2019. 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 five sections: Forensic Models, Mobile and Embedded Device Forensics, Filesystem Forensics, Image Forensics, and 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 Mark Pollitt and Jane Pollitt for their tireless work on behalf of IFIP Working Group 11.9. We also acknowledge the support provided by the U.S. National Science Foundation, U.S. National Security Agency and U.S. Secret Service.

GILBERT PETERSON AND SUJEET SHENOI