IFIP Advances in Information and Communication Technology 532

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 XIV

14th IFIP WG 11.9 International Conference
New Delhi, India, January 3–5, 2018
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 978-3-319-99276-1 ISBN 978-3-319-99277-8 (eBook)
https://doi.org/10.1007/978-3-319-99277-8

Library of Congress Control Number: 2018951631

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

Contents

PART V MOBILE AND EMBEDDED DEVICE FORENSICS

Contributing Authors

Gail-Joon Ahn is a Professor of Computer Science and Engineering, and Director of the Center for Cybersecurity and Digital Forensics at Arizona State University, Tempe, Arizona. His research interests include security analytics and big-data-driven security intelligence, vulnerability and risk management, access control and security architectures for distributed systems, identity and privacy management, cyber crime analysis, security-enhanced computing platforms and formal models for computer security devices.

Saad Alabdulsalam is a Ph.D. student in Computer Science at University College Dublin, Dublin, Ireland. His research interests include Internet of Things security and forensics.

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

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.

Wenhao Chen is a Ph.D. student in Computer Engineering at Iowa State University, Ames, Iowa. His research interests include program analysis and digital forensics.

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.

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.

Spyridon Dosis is a Security Engineer at NetEnt, Stockholm, Sweden. His research interests include network security, digital forensics, cloud computing and semantic web technologies.

Adam Doupé is an Assistant Professor of Computer Science and Engineering, and Associate Director of the Center for Cybersecurity and Digital Forensics at Arizona State University, Tempe, Arizona. His research interests include vulnerability analysis, web security, mobile security, network security and ethical hacking.

Binxing Fang is a Member of the Chinese Academy of Engineering, Beijing, China; and a Professor of Information Engineering at the University of Electronic Science and Technology, Guangdong, China. His research interests are in the area of cyber security.

Thomas Göbel is a Ph.D. student in Computer Science at Darmstadt University of Applied Sciences, Darmstadt, Germany; and a Researcher at the Center for Research in Security and Privacy, Darmstadt, Germany. His research interests include digital forensics, anti-forensics and network forensics.

Mahesh Govil is a Professor of Computer Science and Engineering at Malaviya National Institute of Technology, Jaipur, India; and Director of National Institute of Technology Sikkim, Ravangla, India. His research interests include real-time systems, parallel and distributed systems, fault-tolerant systems and cloud computing.

Yong Guan is a Professor of Electrical and Computer Engineering at Iowa State University, Ames, Iowa. His research interests include digital forensics and information security.

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 D 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 recently received her Ph.D. degree in Physics from National Institute of Technology Kurukshetra, Kurukshetra, India. Her research interests include image processing and computer vision, and their applications to document fraud detection.

Irvin Homem is a Ph.D. student in Computer and Systems Sciences at Stockholm University, Stockholm, Sweden; and a Threat Intelligence Analyst with IBM, Stockholm, Sweden. His research interests include network security, digital forensics, mobile forensics, machine learning, virtualization and cloud computing.

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

Nhien-An Le-Khac is a Lecturer of Computer Science, and Director of the Forensic Computing and Cybercrime Investigation Program at University College Dublin, Dublin, Ireland. His research interests include digital forensics, cyber security and big data analytics.

Xiang Li is a Researcher at the Bank of China, Beijing, China. Her research interests include web application security and digital forensics.

Ondrej Lichtner is a Ph.D. student in Information Technology at Brno University of Technology, Brno, Czech Republic. His research interests include network architecture design and secure network architectures.

Li Lin is a Ph.D. student in Applied Mathematics at Iowa State University, Ames, Iowa. His research interests include digital image forensics and statistical machine learning.

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.

Danjun Liu is an M.S. student in Computer Science and Technology at the National University of Defense Technology, Changsha, China. His research interests include cyber security and software reliability.

Qingyun Liu is a Professor of Information Engineering at the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. His research interests include information security and network security.

Mike Mabey recently received his Ph.D. in Computer Science from Arizona State University, Tempe, Arizona. His research interests include digital forensics, threat intelligence sharing and security in emerging technologies.

Anand Kumar Mishra is a Ph.D. student in Computer Science and Engineering at Malaviya National Institute of Technology, Jaipur, India; and a Guest Researcher in the Information Technology Laboratory at the National Institute of Standards and Technology, Gaithersburg, Maryland. His research interests include digital forensics and cyber security, especially related to cloud computing and container technology.

Nour Moustafa is a Postdoctoral Research Fellow at the Australian Centre for Cyber Security, University of New South Wales, Canberra, Australia. His research interests include cyber security, intrusion detection and machine learning.

Rajender Nath is a Professor of Computer Science and Engineering at Kurukshetra University, Kurukshetra, India. His research interests include computer architecture, parallel processing, object-oriented modeling and aspect-oriented programming.

Jijnasa Nayak is a B.Tech. student in Computer Science and Engineering at National Institute of Technology Rourkela, Rourkela, India. Her research interests include computer vision, image processing, natural language processing and their applications to document fraud detection.

Jennifer Newman is an Associate Professor of Mathematics at Iowa State University, Ames, Iowa. Her research interests include digital image forensics and image processing.

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

Panagiotis Papapetrou is a Professor of Computer and Systems Sciences at Stockholm University, Stockholm, Sweden; and an Adjunct Professor of Computer Science at Aalto University, Helsinki, Finland. His research interests include algorithmic data mining with a focus on mining and indexing sequential data, complex metric and non-metric spaces, biological sequences, time series and sequences of temporal intervals.

Slobodan Petrovic is a Professor of Information Security at the Norwegian University of Science and Technology, Gjovik, Norway. His research interests include cryptology, intrusion detection and digital forensics.

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, privacy and forensics, computer networks, cloud computing, big data and the Internet of Things.

Jan Pluskal is a Ph.D. student in Information Technology at Brno University of Technology, Brno, Czech Republic. His research interests include network forensics, machine learning and distributed computing.

Kyle Porter is a Ph.D. student in Information Security and Communications Technology at the Norwegian University of Science and Technology, Gjovik, Norway. His research interests include approximate string matching algorithms, and applications of machine learning and data reduction mechanisms in digital forensics.

Stephanie Reinders is a Ph.D. student in Applied Mathematics at Iowa State University, Ames, Iowa. Her research interests include steganalysis and machine learning.

Ondrej Rysavy is an Associate Professor of Information Systems at Brno University of Technology, Brno, Czech Republic. His research interests are in the area of computer networks, especially, network monitoring, network security, network forensics and network architectures.

Mark Scanlon is an Assistant Professor of Computer Science, and Co-Director of the Forensic Computing and Cybercrime Investigation Program at University College Dublin, Dublin, Ireland. His research interests include artificial-intelligence-based digital evidence processing, digital forensics as a service and remote evidence processing.

Kevin Schaefer is an Information Technology and Forensics Investigator at the Land Office of Criminal Investigation Baden-Wuerttemberg in Stuttgart, Germany. His research interests include mobile phone and smartwatch forensics.

Pankaj Sharma is an Assistant Professor of Computer Science and Engineering at Chitkara University, Punjab, India. His research interests include digital forensics, security and privacy.

Ambika Shrestha Chitrakar is a Ph.D. student in Information Security and Communications Technology at the Norwegian University of Science and Technology, Gjovik, Norway. Her research interests include approximate search algorithms, intrusion detection and prevention, big data, machine learning and digital forensics.

Bhupendra Singh is a Ph.D. student in Computer Science and Engineering at the Defence Institute of Advanced Technology, Pune, India. His research interests include digital forensics, filesystem analysis and user activity analysis in Windows and Linux systems.

Shweta Singh is a B.Tech. student in Computer Science at Maharishi Dayanand University, Rohtak, India. Her research interests include machine learning and their applications to digitized document fraud.

Upasna Singh is an Assistant Professor of Computer Science and Engineering at the Defence Institute of Advanced Technology, Pune, India. Her research interests include data mining and knowledge discovery, machine intelligence, soft computing, digital forensics, social network analysis and big data analytics.

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.

Jill Slay is the La Trobe Optus Chair of Cyber Security at La Trobe University, Melbourne, Australia. Her research interests include digital forensics, cyber intelligence and cyber skilling.

Yong Sun is a Professor of Information Engineering at the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. His research interests include information security and network security.

Yong Tang is an Associate Researcher in the Network Research Institute at the National University of Defense Technology, Changsha, China. His research interests include cyber security and software reliability.

Erwin van de Wiel is a Digital Forensic Investigator with the Dutch Police in Breda, The Netherlands. His research interests are in the area of digital forensics.

Baosheng Wang is a Researcher in the Network Research Institute at the National University of Defense Technology, Changsha, China. His research interests include computer networks and software reliability.

Yangxiao Wang recently received his B.S. degree in Computer Engineering from Iowa State University, Ames, Iowa. His research interests include digital forensics and information security.

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.

Wei Xie is an Assistant Researcher in the Network Research Institute at the National University of Defense Technology, Changsha, China. His research interests include cyber security and software reliability.

Ken Yau 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, with an emphasis on industrial control system forensics.

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

Bo Yu is an Assistant Researcher in the Network Research Institute at the National University of Defense Technology, Changsha, China. His research interests include cyber security and software reliability.

Ziming Zhao is an Assistant Research Professor in the School of Computing, Informatics and Decision Systems Engineering at Arizona State University, Tempe, Arizona. His research interests include system and network security.

Chao Zheng is an Associate Professor of Information Engineering at the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. His research interests include deep packet inspection, digital forensics, protocols and network security.

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 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 XIV*, is the fourteenth 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 nineteen revised and edited chapters based on papers presented at the Fourteenth IFIP WG 11.9 International Conference on Digital Forensics, held in New Delhi, India on January 3-5, 2018. 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: Themes and Issues, Forensic Techniques, Network Forensics, Cloud Forensics, and Mobile and Embedded Device Forensics. 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 Gaurav Gupta and Robin Verma for their tireless work on behalf of IFIP Working Group 11.9 on Digital Forensics. We also acknowledge the conference sponsors, Cellebrite, Magnet Forensics and Lab Systems, as well as the support provided by the Department of Electronics and Information Technology (Ministry of Communications and Information Technology, Government of India), U.S. National Science Foundation, U.S. National Security Agency and U.S. Secret Service.

Gilbert Peterson and Sujeet Shenoi