IFIP Advances in Information and Communication Technology 511

Editor-in-Chief

Kai Rannenberg, Goethe University Frankfurt, Germany

Editorial Board

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
Diane Whitehouse, The Castlegate Consultancy, Malton, 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 Paul Sabatier, Toulouse, France

TC 14 – Entertainment Computing
Matthias Rauterberg, Eindhoven University of Technology, The Netherlands

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 XIII

13th IFIP WG 11.9 International Conference
Orlando, FL, USA, January 30 – February 1, 2017
Revised Selected Papers

Springer

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

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

ISSN 1868-4238 ISSN 1868-422X (electronic)
IFIP Advances in Information and Communication Technology
ISBN 978-3-319-67207-6 ISBN 978-3-319-67208-3 (eBook)
DOI 10.1007/978-3-319-67208-3

Library of Congress Control Number: 2016950753

Printed on acid-free paper

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

Contents

Contributing Authors ix

Preface xvii

PART I THEMES AND ISSUES

1
Establishing Findings in Digital Forensic Examinations: A Case Study Method 3
Oluwasayo Oyelami and Martin Olivier

2
A Model for Digital Evidence Admissibility Assessment 23
Albert Antwi-Boasiako and Hein Venter

PART II MOBILE AND EMBEDDED DEVICE FORENSICS

3
Evaluating the Authenticity of Smartphone Evidence 41
Heloise Pieterse, Martin Olivier and Renier van Heerden

4
Forensic Evaluation of an Amazon Fire TV Stick 63
Logan Morrison, Huw Read, Konstantinos Xynos and Iain Sutherland

5
Detecting Anomalous Programmable Logic Controller Events Using Machine Learning 81
Ken Yau and Kam-Pui Chow

PART III NETWORK AND CLOUD FORENSICS

6
A Forensic Methodology for Software-Defined Network Switches 97
Tommy Chin and Kaiqi Xiong

7
Identifying Evidence for Cloud Forensic Analysis 111
Changwei Liu, Anoop Singhal and Duminda Wijesekera

PART IV THREAT DETECTION AND MITIGATION

8
Digital Forensic Implications of Collusion Attacks on the Lightning Network 133
Dmytro Piatkivskyi, Stefan Axelsson and Mariusz Nowostawski

9
Insider Threat Detection Using Time-Series-Based Raw Disk Forensic Analysis 149
Nicole Beebe, Lishu Liu and Zi Ye

10
Anti-Forensic Threat Modeling 169
Bruno Hoelz and Marcelo Maues

PART V MALWARE FORENSICS

11
A Behavior-Based Approach for Malware Detection 187
Rayan Mosli, Rui Li, Bo Yuan and Yin Pan

12
Categorizing Mobile Device Malware Based on System Side-Effects 203
Zachary Grimmett, Jason Staggs and Sujeet Shenoi

PART VI IMAGE FORENSICS

13
Semantic Video Carving Using Perceptual Hashing and Optical Flow 223
Junbin Fang, Sijin Li, Guikai Xi, Zoe Jiang, Siu-Ming Yiu, Liyang Yu, Xuan Wang, Qi Han and Qiong Li

14
Detecting Fraudulent Bank Checks 245
Saheb Chhabra, Garima Gupta, Monika Gupta and Gaurav Gupta

PART VII FORENSIC TECHNIQUES

15
Automated Collection and Correlation of File Provenance Information 269
Ryan Good and Gilbert Peterson

16
Using Personal Information in Targeted Grammar-Based Probabilistic Password Attacks 285
Shiva Houshmand and Sudhir Aggarwal

Contributing Authors

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

Albert Antwi-Boasiako is the Principal Consultant at e-Crime Bureau, Accra, Ghana and Cyber Security Advisor to the Government of Ghana, Accra, Ghana; he is also a Ph.D. student in 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.

Stefan Axelsson is an Associate Professor of Computer Science at the Norwegian University of Science and Technology, Gjovik, Norway; and an Associate Professor with the Norwegian National Criminal Police, Oslo, Norway. His research interests include digital forensics, intrusion and fraud detection, visualization and digital surveillance.

Nicole Beebe is an Associate Professor of Cyber Security at the University of Texas at San Antonio, San Antonio, Texas. Her research interests include digital forensics, cyber security and advanced analytics.

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

Tommy Chin is an M.S. student in Computing Security at Rochester Institute of Technology, Rochester, New York. His research interests include cyber security and digital forensics.

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.

Junbin Fang is an Associate Professor of Optoelectronic Engineering at Jinan University, Guangzhou, China; and a Visiting Professor in the Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, Toronto, Canada. His research interests include digital forensics, quantum cryptography and visible light communications.

Ryan Good is an M.S. student in Computer Science at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include digital forensics and network security.

Zachary Grimmett recently received his Ph.D. degree in Computer Engineering from the University of Tulsa, Tulsa, Oklahoma. His research interests include mobile communications devices, digital forensics and malware analysis.

Garima Gupta is a Post Doctoral Researcher in Computer Science and Engineering at Indraprastha Institute of Information Technology, 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 the National Institutes of Technology, Kurukshetra, India. Her research interests include image processing and computer vision and their applications to document fraud detection

Qi Han is an Associate Professor of Computer Science and Technology at Harbin Institute of Technology, Harbin, China. His research interests include digital video forensics, hiding communications and digital watermarking.

Bruno Hoelz is 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.

Shiva Houshmand is an Assistant Professor of Computer Science at Southern Illinois University, Carbondale, Illinois. Her research interests include computer and network security, authentication, digital forensics and usable security.

Zoe Jiang is an Assistant Professor of Computer Science and Technology at the Shenzhen Graduate School, Harbin Institute of Technology, Shenzhen, China. Her research interests include cryptography and digital forensics.

Qiong Li is a Professor of Computer Science and Technology at Harbin Institute of Technology, Harbin, China. Her research interests include quantum cryptography, multimedia security and biometrics.

Rui Li is a Visiting Assistant Professor in the Golisano College of Computing and Information Sciences at Rochester Institute of Technology, Rochester, New York. His research attempts to address multidisciplinary data analytics challenges by developing scalable statistical procedures and efficient learning algorithms.

Sijin Li is a B.S. student in Information Engineering at Jinan University, Guangzhou, China. His research interests include digital forensics, computer vision and deep learning.

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

Lishu Liu is a Machine Learning Engineer at RetailMeNot, Austin, Texas. Her research interests involve the application of machine learning algorithms to locate, extract and present relevant information from massive data sets.

Marcelo Maues is a Computer Forensics Expert at the Renato Chaves Center of Forensic Sciences, Belem/Para, Brazil. His research interests include computer and network forensics.

Logan Morrison is a Computer Scientist with the U.S. Department of Defense in Washington, DC. His research interests include digital forensics, computer security and data recovery.

Rayan Mosli is a Ph.D. student in Computing and Information Sciences at Rochester Institute of Technology, Rochester, New York. His research interests include memory-based malware detection and digital forensics.

Mariusz Nowostawski is an Associate Professor of Computer Science at the Norwegian University of Science and Technology, Gjovik, Norway. His research interests include machine learning, code generation, autonomous and biology-inspired computing, blockchain and distributed ledger technology, and mobile and heterogeneous peer-to-peer computing.

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.

Oluwasayo Oyelami is an M.Sc. student in Computer Science at the University of Pretoria, Pretoria, South Africa; and an Information Security Analyst at Performanta, Midrand, South Africa. His research interests include digital forensics, information security and threat intelligence.

Yin Pan is a Professor of Computing Security at Rochester Institute of Technology, Rochester, New York. Her research interests include game-based digital forensics and memory-based malware detection.

Gilbert Peterson, Chair, IFIP Working Group 11.9 on Digital Forensics, is a Professor of Computer Science at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include digital forensics, artificial intelligence and statistical machine learning.

Dmytro Piatkivskyi is a Ph.D. student in Cyber and Information Security at the Norwegian University of Science and Technology, Gjovik, Norway. His research focuses on the analysis of off-chain scalability solutions for Bitcoin and other crypto-currencies with an emphasis on security.

Heloise Pieterse is a Senior Researcher 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 mobile device security.

Huw Read is an Associate Professor of Digital Forensics and Director of the Center for Advanced Computing and Digital Forensics at Norwich University, Northfield, Vermont. His research interests include digital forensics and computer security.

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.

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

Jason Staggs recently received his Ph.D. degree in Computer Science from the University of Tulsa, Tulsa, Oklahoma. His research interests include telecommunications networks, industrial control systems, critical infrastructure protection, security engineering and digital forensics.

Iain Sutherland is a Professor of Digital Forensics at Noroff University College, Kristiansand, Norway. His research interests include digital forensics and data recovery.

Renier van Heerden is a Principal Researcher at the Council for Scientific and Industrial Research, Pretoria, South Africa. His research interests include network security, password security and network attacks.

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.

Xuan Wang is a Professor and Ph.D. Supervisor in the Computer Application Research Center at the Shenzhen Graduate School, Harbin Institute of Technology, Shenzhen, China. His research interests include artificial intelligence, computer vision, computer security and computational linguistics.

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.

Guikai Xi is a B.S. student in Information Engineering at Jinan University, Guangzhou, China. His research interests include digital forensics, deep learning and machine intelligence.

Kaiqi Xiong is an Associate Professor of Cybersecurity, Mathematics and Electrical Engineering at the University of South Florida, Tampa, Florida. His research interests include computer and network security.

Konstantinos Xynos is a Senior Researcher and Senior Manager at DarkMatter LLC, Dubai, United Arab Emirates. His research interests include digital forensics and computer security.

Ken Yau is an M.Phil. 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.

Zi Ye is a Data Analyst at Andorra Life in Los Angeles, California. Her research interests include the application of machine learning algorithms to locate, extract and present relevant information from massive data sets.

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.

Liyang Yu is a Lecturer of Software and Microelectronics at Harbin University of Science and Technology, Harbin, China. His research interests include digital image and video forensics.

Bo Yuan is a Professor and Chair of Computing Security at Rochester Institute of Technology, Rochester, New York. His research focuses on applications of computational intelligence in cyber security.

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 XIII*, is the thirteenth 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 sixteen revised and edited chapters based on papers presented at the Thirteenth IFIP WG 11.9 International Conference on Digital Forensics, held in Orlando, Florida on January 30 to February 1, 2017. 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 seven sections: Themes and Issues, Mobile and Embedded Device Forensics, Network and Cloud Forensics, Threat Detection and Mitigation, Malware 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