

Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering

259

Editorial Board

Ozgur Akan

Middle East Technical University, Ankara, Turkey

Paolo Bellavista

University of Bologna, Bologna, Italy

Jiannong Cao

Hong Kong Polytechnic University, Hong Kong, Hong Kong

Geoffrey Coulson

Lancaster University, Lancaster, UK

Falko Dressler

University of Erlangen, Erlangen, Germany

Domenico Ferrari

Università Cattolica Piacenza, Piacenza, Italy

Mario Gerla

UCLA, Los Angeles, USA

Hisashi Kobayashi

Princeton University, Princeton, USA

Sergio Palazzo

University of Catania, Catania, Italy

Sartaj Sahni

University of Florida, Florida, USA

Xuemin Sherman Shen

University of Waterloo, Waterloo, Canada

Mircea Stan

University of Virginia, Charlottesville, USA

Jia Xiaohua

City University of Hong Kong, Kowloon, Hong Kong

Albert Y. Zomaya

University of Sydney, Sydney, Australia

More information about this series at <http://www.springer.com/series/8197>


Frank Breitingner · Ibrahim Baggili (Eds.)

Digital Forensics and Cyber Crime

10th International EAI Conference, ICDF2C 2018
New Orleans, LA, USA, September 10–12, 2018
Proceedings

Editors

Frank Breitingner 
Tagliatela College of Engineering
University of New Haven
West Haven, CT, USA

Ibrahim Baggili 
Tagliatela College of Engineering
University of New Haven
West Haven, CT, USA

ISSN 1867-8211 ISSN 1867-822X (electronic)
Lecture Notes of the Institute for Computer Sciences, Social Informatics
and Telecommunications Engineering
ISBN 978-3-030-05486-1 ISBN 978-3-030-05487-8 (eBook)
<https://doi.org/10.1007/978-3-030-05487-8>

Library of Congress Control Number: 2018963584

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2019
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

Preface

We are delighted to introduce the proceedings of the 10th edition of the 2018 European Alliance for Innovation (EAI) International Conference on Digital Forensics and Cyber Crime (ICDF2C). This conference continues to bridge the gap in the domain, and is truly international and quite visible worldwide. More importantly, this event bridges the gap between industry and researchers.

This year's keynotes are also to be proud of. Our first keynote speaker was Deborah Frincke, the director of research at the National Security Agency (NSA), followed by a pioneer in memory forensics, Golden Richard III from Louisiana State University.

The program was strong and extremely relevant for 2018. One important highlight of the program was a hands-on workshop by Riscure on extracting secrets from encrypted devices using side channel attacks, reverse engineering, fault injection, and the exploitation of weaknesses in secure firmware. Furthermore, the forensic analysis of cryptocurrencies was also a hot topic covered at this event. These topics are becoming ever so important in digital forensics as practitioners are dealing with more devices and applications that are encrypted. The rest of the program covered areas that are of high importance as well; carving and data hiding, Android security and forensics, memory forensic, industry presentations, forensic readiness, hard drive data distribution, and artifact correlation.

Overall, we accepted papers from the following countries and states: Germany, USA (Connecticut, Texas, California, Virginia, Ohio), South Africa, Estonia, Spain, China, and Ireland. The conference further boasted participants from a larger number of countries. The TPC committee accepted only 11 quality double-blind peer-reviewed papers (three were accepted after shepherding), out of 33 submissions (33% acceptance rate), and one short paper. Each paper had an average of four reviews, and best paper awards were selected after review by individuals with no conflict of interest in the selection process.

The conference is now positioned to grow, and we anticipate that next year we will be expanding the event to include topics that go beyond digital forensics.

We are very proud of this year's event, and we hope to continue the success of ICDF2C in the future. We would like to thank everyone who made this conference successful this year, and we look forward to seeing participants at next year's event.

November 2018

Ibrahim Baggili
Frank Breitingner

Organization

Steering Committee

Imrich Chlamtac	Bruno Kessler Professor, University of Trento, Italy
Ibrahim Baggili	University of New Haven, USA
Joshua I. James	DFIRE Labs, Hallym University, South Korea
Frank Breitingner	University of New Haven, USA

Organizing Committee

General Co-chairs

Irfan Ahmed	University of New Orleans, USA
Vassil Roussev	University of New Orleans, USA

TPC Chair and Co-chair

Frank Breitingner	University of New Haven, USA
Mark Scanlon	University College Dublin, Ireland

Local Chair

Minhaz Zibran	University of New Orleans, USA
---------------	--------------------------------

Workshops Chair

Ibrahim Baggili	University of New Haven, USA
-----------------	------------------------------

Publicity and Social Media Chair

Hyunguk Yoo	University of New Orleans, USA
-------------	--------------------------------

Publications Chair

Joshua I. James	DFIRE Labs, Hallym University, South Korea
-----------------	--

Web Chair

Manish Bhatt	University of New Orleans, USA
--------------	--------------------------------

Conference Manager

Radka Pincakova	European Alliance for Innovations
-----------------	-----------------------------------

Technical Program Committee

Ashley Podhradsky	Dakota State University, USA
David Lillis	University College Dublin, Ireland
Nhien An Le Khac	University College Dublin, Ireland
Golden Richard	Louisiana State University, USA
Krzysztof Szczypiorski	Warsaw University of Technology, Poland
Kim-Kwang Raymond Choo	The University of Texas at San Antonio, USA
Michael Losavio	University of Louisville, USA
Petr Matousek	Brno University of Technology, Czech Republic
Sebastian Schinzel	Münster University of Applied Sciences, Germany
Richard E. Overill	King's College London, UK
Joshua I. James	Digital Forensic Investigation Research Laboratory
Michael Spreitzenbarth	Siemens CERT
Ibrahim Baggili	University of New Haven, USA
Vik Harichandran	MITRE
Pavel Gladyshev	University College Dublin, Ireland
Virginia Franqueira	University of Derby, UK
Umit Karabiyik	Sam Houston State University, USA
Timothy Vidas	Carnegie Mellon University, USA
Bruce Nikkel	UBS AG
David Dampier	Mississippi State University, USA
Neil Rowe	U.S. Naval Postgraduate School, USA
Alex Nelson	National Institute of Standards and Technology
Harald Baier	CASED
Irfan Ahmed	University of New Orleans, USA
Vassil Roussev	University of New Orleans, USA
David Baker	DFRWS
Frank Adelstein	NFA Digital
Nicole Beebe	University of Texas at San Antonio, USA
Ondrej Rysavy	Brno University of Technology, Czech Republic
Christian Winter	Fraunhofer Gesellschaft
Spiridon Bakiras	Hamad Bin Khalifa University, Qatar
Bradley Schatz	Queensland University of Technology, Australia
Vladimir Vesely	Brno University of Technology, Czech Republic
Stig Mjolsnes	Norwegian University of Science and Technology NTNU, Norway
John Sheppard	Waterford Institute of Technology, Ireland

Contents

Carving and Data Hiding

On Efficiency and Effectiveness of Linear Function Detection Approaches for Memory Carving	3
<i>Lorenz Liebler and Harald Baier</i>	
fishy - A Framework for Implementing Filesystem-Based Data Hiding Techniques	23
<i>Thomas Göbel and Harald Baier</i>	

Android

If I Had a Million Cryptos: Cryptowallet Application Analysis and a Trojan Proof-of-Concept.	45
<i>Trevor Haigh, Frank Breitingner, and Ibrahim Baggili</i>	
AndroParse - An Android Feature Extraction Framework and Dataset	66
<i>Robert Schmicker, Frank Breitingner, and Ibrahim Baggili</i>	

Forensic Readiness

Digital Forensic Readiness Framework for Ransomware Investigation	91
<i>Avinash Singh, Adeyemi R. Ikuesan, and Hein S. Venter</i>	
Forensics Analysis of an On-line Game over Steam Platform	106
<i>Raquel Tabuyo-Benito, Hayretdin Bahsi, and Pedro Peris-Lopez</i>	
A Digital Forensic Investigation and Verification Model for Industrial Espionage	128
<i>Jieun Dokko and Michael Shin</i>	

Hard Drives and Digital Forensics

Solid State Drive Forensics: Where Do We Stand?	149
<i>John Vieyra, Mark Scanlon, and Nhien-An Le-Khac</i>	
Associating Drives Based on Their Artifact and Metadata Distributions	165
<i>Neil C. Rowe</i>	

Artefact Correlation

Digital Forensics Event Graph Reconstruction 185
Daniel J. Schelkoph, Gilbert L. Peterson, and James S. Okolica

Multi-item Passphrases: A Self-adaptive Approach Against
Offline Guessing Attacks 204
Jaryn Shen, Kim-Kwang Raymond Choo, and Qingkai Zeng

Short Paper

Hybrid Intrusion Detection System for Worm Attacks Based on Their
Network Behavior 225
Hassan Hadi Latheeth AL-Maksousy and Michele C. Weigle

Author Index 235