

Pavel Gladyshev
Sanjay Goel
Joshua James
George Markowsky
Daryl Johnson (Eds.)



441

LNICST

Digital Forensics and Cyber Crime

12th EAI International Conference, ICDF2C 2021
Virtual Event, Singapore, December 6–9, 2021
Proceedings



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

441

Editorial Board Members

Ozgur Akan

Middle East Technical University, Ankara, Turkey

Paolo Bellavista

University of Bologna, Bologna, Italy

Jiannong Cao

Hong Kong Polytechnic University, Hong Kong, China

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, Gainesville, USA

Xuemin Shen 

University of Waterloo, Waterloo, Canada

Mircea Stan

University of Virginia, Charlottesville, USA

Xiaohua Jia

City University of Hong Kong, Kowloon, Hong Kong

Albert Y. Zomaya

University of Sydney, Sydney, Australia

More information about this series at <https://link.springer.com/bookseries/8197>

Pavel Gladyshev · Sanjay Goel · Joshua James ·
George Markowsky · Daryl Johnson (Eds.)

Digital Forensics and Cyber Crime

12th EAI International Conference, ICDF2C 2021
Virtual Event, Singapore, December 6–9, 2021
Proceedings

Editors

Pavel Gladyshev
School of Computer Science
University College Dublin
Dublin, Ireland

Sanjay Goel
State University of New York
University at Albany
Albany, NY, USA

Joshua James
DFIR Science
Champaign, IL, USA

George Markowsky
Missouri University
Rolla, MO, USA

Daryl Johnson
Rochester Institute of Technology
Rochester, NY, USA

ISSN 1867-8211 ISSN 1867-822X (electronic)
Lecture Notes of the Institute for Computer Sciences, Social Informatics
and Telecommunications Engineering
ISBN 978-3-031-06364-0 ISBN 978-3-031-06365-7 (eBook)
<https://doi.org/10.1007/978-3-031-06365-7>

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2022

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, expressed 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 12th edition of the European Alliance for Innovation (EAI) International Conference on Digital Forensics and Cyber Crime (ICDF2C 2021). This conference brought together researchers and practitioners around the world who are developing and using digital forensic technologies and techniques for a variety of applications in criminal investigations, incident response, and broader information security. The focus of ICDF2C 2021 was on various applications of digital evidence and forensics beyond “traditional” cyber crime investigations and litigation.

The technical program of ICDF2C 2021 consisted of 22 full papers presented over three days at the main conference track. Aside from the high-quality technical paper presentations, the technical program also featured three keynote speeches and two technical workshops. The three keynote speeches were given by Joe Weiss, the author of *Protecting Industrial Control Systems from Electronic Threats*, Vitaly Kamluk, the lead threat researcher for Kaspersky APAC, and Jonathan Pan, the head of the Disruptive Technologies Office of the Home Team Science and Technology Agency (HTX), Singapore. The two workshops were *Password Cracking and Rainbow Tables*, organized by George Markowsky, and *Intelligence Gathering Through the Internet and Dark Web*, organized by Lu Liming, Jacob Abraham, Selvakulasingam Thiruneepan, and James Ng Hian from the Singapore Institute of Technology and Feixiang He from Group-IB.

Coordination with EAI was essential for the success of the conference. We sincerely appreciate their constant support and guidance. We are grateful to Conference Managers Natasha Onofrei and Lenka Ležanská, Managing Editor Lucia Sedlářová, and all the authors who submitted their papers to the ICDF2C 2021 conference.

March 2022

Pavel Gladyshev
Sanjay Goel
Joshua James
George Markowsky
Daryl Johnson

Organization

Steering Committee

Imrich Chlamtac
Sanjay Goel

University of Trento, Italy
University at Albany, SUNY, USA

Organizing Committee

General Chair

Pavel Gladyshev

University College Dublin, Ireland

General Co-chair

Sanjay Goel

University at Albany, SUNY, USA

Vice-Chair

Alexey Chilikov

Bauman Moscow State Technical University,
Russia

Technical Program Committee Chairs

Daryl Johnson
George Markowsky

Rochester Institute of Technology, SUNY, USA
Missouri University of Science and Technology,
USA

Joshua Isaac James

DFIR Science, LLC, USA

Sponsorship and Exhibit Chair

Nikolay Akatyev

Horangi Cyber Security, Singapore

Local Chair

Nikolay Akatyev

Horangi Cyber Security, Singapore

Workshops Chair

Paulo Roberto Nunes de Souza

Federal University of Espírito Santo, Brazil

Outreach Co-chairs

Afrah Almansoori Dubai Police, UAE
Emil Tan Division Zero, Singapore

Publications Chair

Xiaoyu Du University College Dublin, Ireland

Web Chair

Pavel Gladyshev University College Dublin, Ireland

Technical Program Committee

Ahmed Shosha Microsoft, UK
Ahmed Hamza Rochester Institute of Technology, USA
Ambika N. SSMRV College, India
Anca Delia Jurcut University College Dublin, Ireland
Anthony Cheuk Tung Lai VX Research Limited, Hong Kong
Babak Habibnia University College Dublin, Ireland
Bill Stackpole Rochester Institute of Technology, USA
Bo Chen Michigan Technological University, USA
David Lillis University College Dublin, Ireland
Ding Wang Nankai University, China
Fahim Khan University of Tokyo, Japan
Farkhund Iqbal Zayed University, UAE
Glenn Dardick Longwood University, USA
John Sheppard Waterford Institute of Technology, Ireland
M. P. Gupta Indian Institute of Technology Delhi, India
Mengjun Xie University of Tennessee at Chattanooga, USA
Nhien An Le Khac University College Dublin, Ireland
Nickkisha Farrell Concordia University of Edmonton, Canada
Omid Mirzaei Elastic, Boston, USA
Pavol Zavorsky Concordia University College of Alberta, Canada
Pradeep Atrey University of Albany, USA
Prakash G. Amrita Vishwa Vidyapeetham University, India
Sai Mounika Errapotu University of Texas at El Paso, USA
Seungjoo Kim Korea University, South Korea
Shaikh Akib Shahriyar Rochester Institute of Technology, USA
Spiridon Bakiras Hamad Bin Khalifa University, Qatar
Stig Mjolsnes Norwegian University of Science and Technology,
Norway
Umit Karabiyik Purdue University, USA

Vinod Bhattathiripad

Vivienne Mee

Xianzhi Wang

Xiaochun Cheng

G J Software Forensics, India

VMGroup, Ireland

University of Technology Sydney, Australia

Middlesex University London, UK

Contents

Quantifying Paging on Recoverable Data from Windows User-Space Modules	1
<i>Miguel Martín-Pérez and Ricardo J. Rodríguez</i>	
Forensic Investigations of Google Meet and Microsoft Teams – Two Popular Conferencing Tools in the Pandemic	20
<i>M. A. Hannan Bin Azhar, Jake Timms, and Benjamin Tilley</i>	
On Exploring the Sub-domain of Artificial Intelligence (AI) Model Forensics	35
<i>Tiffanie Edwards, Syria McCullough, Mohamed Nassar, and Ibrahim Baggili</i>	
Auto-Parser: Android Auto and Apple CarPlay Forensics	52
<i>Andrew Mahr, Robert Serafin, Cinthya Grajeda, and Ibrahim Baggili</i>	
Find My IoT Device – An Efficient and Effective Approximate Matching Algorithm to Identify IoT Traffic Flows	72
<i>Thomas Göbel, Frieder Uhlig, and Harald Baier</i>	
Accessing Secure Data on Android Through Application Analysis	93
<i>Richard Burke and Nhien-An Le-Khac</i>	
Research on the Method of Selecting the Optimal Feature Subset in Big Data for Energy Analysis Attack	109
<i>Xiaoyi Duan, You Li, Chengyuan Liu, Xiuying Li, Wenfeng Liu, and Guoqian Li</i>	
Cheating Sensitive Security Quantum Bit Commitment with Security Distance Function	127
<i>Weicong Huang, Qisheng Guang, Dong Jiang, and Lijun Chen</i>	
Towards Mitigation of Data Exfiltration Techniques Using the MITRE ATT&CK Framework	139
<i>Michael Mundt and Harald Baier</i>	
PCWQ: A Framework for Evaluating Password Cracking Wordlist Quality	159
<i>Aikaterini Kanta, Iwen Coisel, and Mark Scanlon</i>	

No Pie in the Sky: The Digital Currency Fraud Website Detection	176
<i>Haoran Ou, Yongyan Guo, Chaoyi Huang, Zhiying Zhao, Wenbo Guo, Yong Fang, and Cheng Huang</i>	
Understanding the Brains and Brawn of Illicit Streaming App	194
<i>Kong Huang, Ke Zhang, Jiongyi Chen, Menghan Sun, Wei Sun, Di Tang, and Kehuan Zhang</i>	
Fine-Grained Obfuscation Scheme Recognition on Binary Code	215
<i>Zhenzhou Tian, Hengchao Mao, Yaqian Huang, Jie Tian, and Jinrui Li</i>	
Backdoor Investigation and Incident Response: From Zero to Profit	229
<i>Anthony Cheuk Tung Lai, Ken Wai Kin Wong, Johnny Tsz Wun Wong, Austin Tsz Wai Lau, Alan Po Lun Ho, Shuai Wang, and Jogesh Muppala</i>	
Automated Software Vulnerability Detection via Pre-trained Context Encoder and Self Attention	248
<i>Na Li, Haoyu Zhang, Zihui Hu, Guang Kou, and Huadong Dai</i>	
A CNN-Based HEVC Video Steganalysis Against DCT/DST-Based Steganography	265
<i>Zhenzhen Zhang, Henan Shi, Xinghao Jiang, Zhaohong Li, and Jindou Liu</i>	
Do Dark Web and Cryptocurrencies Empower Cybercriminals?	277
<i>Milad Taleby Ahvanooy, Mark Xuefang Zhu, Wojciech Mazurczyk, Max Kilger, and Kim-Kwang Raymond Choo</i>	
Lightweight On-Demand Honeypot Deployment for Cyber Deception	294
<i>Jaime C. Acosta, Anjon Basak, Christopher Kiekintveld, and Charles Kamhoua</i>	
Gotta Catch'em All! Improving P2P Network Crawling Strategies	313
<i>Alexander Mühle, Andreas Grüner, and Christoph Meinel</i>	
Parcae: A Blockchain-Based PRF Service for Everyone	328
<i>Elizabeth Wyss and Drew Davidson</i>	
A Hybrid Cloud Deployment Architecture for Privacy-Preserving Collaborative Genome-Wide Association Studies	342
<i>Fatima-zahra Boujdad, David Niyitegeka, Reda Bellafqira, Gouenou Coatrieux, Emmanuelle Genin, and Mario Südholt</i>	

Understanding the Security of Deepfake Detection 360
Xiaoyu Cao and Neil Zhenqiang Gong

Author Index 379