2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW 2019)

Stockholm, Sweden
17 – 19 June 2019

IEEE Catalog Number: CFP19N35-POD
ISBN: 978-1-7281-3027-9

Copyright © 2019 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number: CFP19N35-POD
ISBN (Print-On-Demand): 978-1-7281-3027-9
ISBN (Online): 978-1-7281-3026-2

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

2019 IEEE European Symposium on Security and Privacy Workshops

EuroSPW 2019

Table of Contents

Message from the General Chairs ..... **xi**
Organizing Committee ..... **xiii**

2019 European Workshop on Security and Privacy in Edge Computing (EuroSPEC 2019)

Edge and Fog Computing in Critical Infrastructures: Analysis, Security Threats, and Research Challenges 1
Pietro Tedeschi (Hamad Bin Khalifa University) and Savio Sciancalepore (Hamad Bin Khalifa University)

ANTIBIOTIC 2.0: A Fog-based Anti-Malware for Internet of Things 11
Michele De Donno (Technical University of Denmark), Juan Manuel Donaire Felipe (Technical University of Denmark), and Nicola Dragoni (Technical University of Denmark)

SeCoNetBench: A modular framework for Secure Container Networking Benchmarks 21
Amr Osman (TU Dresden), Simon Hanisch (TU Dresden), and Thorsten Strufe (TU Dresden)

Towards Multi-party Policy-based Access Control in Federations of Cloud and Edge Microservices 29
Davy Preuveneers (KU Leuven) and Wouter Joosen (KU Leuven)

IEEE EuroS&P Workshop on Software Security for Internet of Things (SSIoT 2019)

An Auditing Framework for Vulnerability Analysis of IoT System 39
Ibrahim Nadir (National University of Computer & Emerging Sciences, Lahore, Pakistan), Zafeer Ahmad (Al-Khawarizmi Institute of Computer Science, University of Engineering and Technology, Lahore, Pakistan), Haroon Mahmood (National University of Computer & Emerging Sciences, Lahore, Pakistan), Ghalib Asadullah Shah (Al-Khawarizmi Institute of Computer Science, University of Engineering and Technology, Lahore, Pakistan), Farrukh Shahzad (Ebryx LLC, Lahore, Pakistan), Muhammad Umair (Al-Khawarizmi Institute of Computer Science, University of Engineering and Technology, Lahore, Pakistan), Hassam Khan (Al-Khawarizmi Institute of Computer Science, University of Engineering and Technology, Lahore, Pakistan), and Usman Gulzar (Al-Khawarizmi Institute of Computer Science, University of Engineering and Technology, Lahore, Pakistan)

oneM2M Architecture Based Secure MQTT Binding in Mbed OS .48
Ahsan Muhammad (Al-Khawarizmi Institute of Computer Science, University of Engineering and Technology Lahore), Bilal Afzal (Al-Khawarizmi Institute of Computer Science, University of Engineering and Technology Lahore), Bilal Imran (Al-Khawarizmi Institute of Computer Science, University of Engineering and Technology Lahore), Asim Tanwir (Al-Khawarizmi Institute of Computer Science, University of Engineering and Technology Lahore), Ali Hammad Akbar (Department of Computer Science, University of Engineering and Technology Lahore), and Ghalib Shah (Al-Khawarizmi Institute of Computer Science, University of Engineering and Technology Lahore)

Network Reconnaissance and Vulnerability Excavation of Secure DDS Systems .57
Ruffin White (UC San Diego), Gianluca Caiazza (Ca' Foscari University of Venice), Chenxu Jiang (UC San Diego), Xinyue Ou (UC San Diego), Zhiyue Yang (UC San Diego), Agostino Cortesi (Ca' Foscari University of Venice), and Henrik Christensen (UC San Diego)

Workshop on Cyber Range Applications and Technologies (CACOE 2019)

Realistic Cybersecurity Training via Scenario Progression Management .67
Razvan Beuran (Japan Advanced Institute of Science and Technology), Takuya Inoue (Japan Advanced Institute of Science and Technology), Yasuo Tan (Japan Advanced Institute of Science and Technology), and Yoichi Shinoda (Japan Advanced Institute of Science and Technolog)

Becoming Invisible Hands of National Live-Fire Attack-Defense Cyber Exercise .77
Joonsoo Kim (National Security Research Institute), Youngjae Maeng (National Security Research Institute), and Moonsu Jang (National Security Research Institute)

Designing Serious Games for Cyber Ranges: A Socio-technical Approach .85
Mazaher Kianpour (Norwegian University of Science and Technology), Stewart Kowalski (Norwegian University of Science and Technology), Erjon Zoto (Norwegian University of Science and Technology), Christopher Frantz (Norwegian University of Science and Technology), and Harald Øverby (Norwegian University of Science and Technology)

Cybersecurity Experimentation at Program Scale: Guidelines and Principles for Future Testbeds .94
Stephen Schwab (USC Information Sciences Institute) and Erik Kline (USC Information Sciences Institute)

Pedagogical Aspects of Cyber Security Exercises .103
Mika Karjalainen (JAMK University of Applied Sciences), Tero Kokkonen (JAMK University of Applied Sciences), and Samir Puuska (JAMK University of Applied Sciences)

4th European Workshop on Usable Security (EuroUSEC 2019))

Why Johnny Fails to Protect his Privacy .109
Nina Gerber (SECUSO, Karlsruhe Institute of Technology), Verena Zimmermann (FAI, Technische Universität Darmstadt), and Melanie Volkamer (SECUSO, Karlsruhe Institute of Technology)

Don't Punish all of us: Measuring User Attitudes about Two-Factor Authentication .119
Jonathan Dutson (Brigham Young University), Danny Allen (Brigham Young University), Dennis Eggett (Brigham Young University), and Kent Seamons (Brigham Young University)

A Survey on Developer-Centred Security .129
Mohammad Tahaei (University of Edinburgh) and Kami Vaniea (University of Edinburgh)

How Could Serious Games Support Secure Programming? Designing a Study Replication and Intervention .139
Manuel Maarek (Heriot-Watt University), Léon McGregor (Heriot-Watt University), Sandy Louchart (Glasgow School of Art), and Ross McMenemy (Glasgow School of Art)

Vision: Shining Light on Smart Homes – Supporting Informed Decision-Making of End Users .149
Verena Zimmermann (Technische Universität Darmstadt), Ernestine Dickhaut (Technische Universität Darmstadt), Paul Gerber (Technische Universität Darmstadt), and Joachim Vogt (Technische Universität Darmstadt)

Vision: Exploring Challenges and Opportunities for Usable Authentication in the Smart Home.154
Sarah Prange (Bundeswehr University), Emanuel von Zezschwitz (University of Bonn), and Florian Alt (Bundeswehr University)

Comparative Analysis of Three Language Spheres: Are Linguistic and Cultural Differences Reflected in Password Selection Habits? .159
Keika Mori (Waseda University), Takuya Watanabe (NTT Secure Platform Laboratories), Yunao Zhou (Waseda University), Ayako Akiyama Hasegawa (NTT Secure Platform Laboratories), Mitsuaki Akiyama (NTT Secure Platform Laboratories), and Tatsuya Mori (Waseda University / RIKEN AIP / NICT)

Detecting Misalignments between System Security and User Perceptions: A Preliminary Socio-technical Analysis of an E2E email Encryption System .172
Borce Stojkovski (SnT, University of Luxembourg), Itzel Vazquez Sandoval (SnT, University of Luxembourg), and Gabriele Lenzini (SnT, University of Luxembourg)

A Review of Human- and Computer-Facing URL Phishing Features .182
Kholoud Althobaiti (University of Edinburgh & Taif University), Ghaidaa Rummani (Hood College), and Kami Vaniea (University of Edinburgh)

2 Fast 2 Secure: A Case Study of Post-Breach Security Changes .192
Albese Demjaha (University College London/The Alan Turing Institute), Tristan Caulfield (University College London/The Alan Turing Institute), M. Angela Sasse (University College London/The Alan Turing Institute), and David Pym (University College London/The Alan Turing Institute)

Workshop on Machine Learning for Cyber-Crime Investigation and Cybersecurity (MaL2CSec 2019)

Feature Selection Strategies for HTTP Botnet Traffic Detection .202
Ivan Letteri (University of L'Aquila), Giuseppe Della Penna (University of L'Aquila), and Pasquale Caianiello (University of L'Aquila)

Recessive Social Networking: Preventing Privacy Leakage against Reverse Image Search .211..
Jiajie Zhang (Lancaster University), Bingsheng Zhang (United Kingdom), and Jiancheng Lin (Guangdong Technology Normal University)

Generation of Static YARA-Signatures Using Genetic Algorithm .220.....
Alexander Zhdanov (INRIA)

AutoAttacker: A reinforcement learning approach for black-box adversarial attacks .229.....
Ilias Tsingenopoulos (Katholieke Universiteit Leuven), Davy Preuveneers (Katholieke Universiteit Leuven), and Wouter Joosen (Katholieke Universiteit Leuven)

An Semi-supervised Learning Methodology for Malware Categorization using Weighted Word Embeddings .238.....
Hugo Leonardo Duarte-Garcia (Instituto Politecnico Nacional), Carlos Domenick Morales-Medina (Instituto Politecnico Nacional), Aldo Hernandez-Suarez (Instituto Politecnico Nacional), Gabriel Sanchez-Perez (Instituto Politecnico Nacional), Karina Toscano-Medina (Instituto Politecnico Nacional), Hector Perez-Meana (Instituto Politecnico Nacional), and Victor Sanchez (University of Warwick)

Malware Detection Using 1-Dimensional Convolutional Neural Networks .247.....
Arindam Sharma (Queen Mary University of London), Pasquale Malacaria (Queen Mary University of London), and MHR Khouzani (Queen Mary University of London)

Towards Fully Integrated Real-time Detection Framework for Online Contents Analysis - RED-Alert Approach .257.....
Syed Naqvi (Birmingham City University), Ian Williams (Birmingham City University), Sean Enderby (Birmingham City University), Peter Pollner (Hungarian Academy of Sciences), Daniel Abel (Hungarian Academy of Sciences), Berta Biescas (INSIKT Intelligence), Oscar Garcia (Information Catalyst for Enterprise), Monica Florea (SIVECO), and Cristi Potlog (SIVECO)

CRC-PUF: A Machine Learning Attack Resistant Lightweight PUF Construction .264.....
Elena Dubrova (KTH Royal Institute of Technology), Oscar Näslund (KTH Royal Institute of Technology), Bernhard Degen (KTH Royal Institute of Technology), Anders Gawell (KTH Royal Institute of Technology), and Yang Yu (KTH Royal Institute of Technology)

Adversarial Out-domain Examples for Generative Models .272.....
Dario Pasquini (Sapienza University; IAC-CNR), Marco Mingione (Sapienza University; IAC-CNR), and Massimo Bernaschi (Institute for Applied Computing (IAC); CNR Rome)

Exploiting the Auto-Encoder Residual Error for Intrusion Detection .281.....
Giuseppina Andresini (Università degli Studi di Bari Aldo Moro), Annalisa Appice (Università degli Studi di Bari Aldo Moro), Nicola Di Mauro (Università degli Studi di Bari Aldo Moro), Corrado Loglisci (Università degli Studi di Bari Aldo Moro), and Donato Malerba (Università degli Studi di Bari Aldo Moro)

Using a Deep-Learning Approach for Smart IoT Network Packet Analysis .291.....
John Yoon (Mercy College)

IEEE Security & Privacy on the Blockchain (IEEE S&B 2019)

Eclipsing Ethereum Peers with False Friends .300
Sebastian Henningsen (Weizenbaum-Institute for the Networked Society/Humboldt-Universität zu Berlin), Daniel Teunis (Weizenbaum-Institute for the Networked Society/Humboldt-Universität zu Berlin), Martin Florian (Weizenbaum-Institute for the Networked Society/Humboldt-Universität zu Berlin), and Björn Scheuermann (Weizenbaum-Institute for the Networked Society/Humboldt-Universität zu Berlin)

Empirically Analyzing Ethereum's Gas Mechanism .310
Renlord Yang (University of Melbourne), Toby Murray (University of Melbourne), Paul Rimba (Data61, CSIRO), and Udaya Parampalli (University of Melbourne)

Resolving the Multiple Withdrawal Attack on ERC20 Tokens .320
Reza Rahimian (Concordia University), Shayan Eskandari (Concordia University), and Jeremy Clark (Concordia University)

MProve: A Proof of Reserves Protocol for Monero Exchanges .330
Arijit Dutta (Indian Institute of Technology Bombay) and Saravanan Vijayakumaran (Indian Institute of Technology Bombay)

Towards Automatically Penalizing Multimedia Breaches (Extended Abstract) .340
Easwar Vivek Mangipudi (Purdue University), Krutarth Rao (Hewlett Packard), Jeremy Clark (Concordia University), and Aniket Kate (Purdue University)

Discharged Payment Channels: Quantifying the Lightning Network's Resilience to Topology-Based Attacks .347
Elias Rohrer (Technical University of Berlin), Julian Malliaris (Technical University of Berlin), and Florian Tschorsch (Technical University of Berlin)

Temporary Censorship Attacks in the Presence of Rational Miners .357
Fredrik Winzer (Robert Bosch GmbH), Benjamin Herd (Robert Bosch GmbH), and Sebastian Faust (Technical University Darmstadt)

Erasing Data from Blockchain Nodes .367
Martin Florian (Humboldt Universität zu Berlin / Weizenbaum Institute), Sebastian Henningsen (Humboldt Universität zu Berlin / Weizenbaum Institute), Sophie Beaucamp (Humboldt Universität zu Berlin / Weizenbaum Institute), and Björn Scheuermann (Humboldt Universität zu Berlin / Weizenbaum Institute)

Is Stellar As Secure As You Think? .377
Minjeong Kim (KAIST), Yujin Kwon (KAIST), and Yongdae Kim (KAIST)

Agent-Based Simulations of Blockchain protocols illustrated via Kadena’s Chainweb .386
Tarun Chitra (Gauntlet Networks, Inc), Monica Quaintance (Kadena LLC), Stuart Haber (Stuart Haber Crypto LLC), and Will Martino (Kadena LLC)

TULIP: A Fully Incentive Compatible Blockchain Framework Amortizing Redundant Communication .396
Oguzhan Ersoy (Delft University of Technology), Erkin Zekeriya (Delft University of Technology), and Reginald L. Lagendijk (Delft University of Technology)

The First Workshop on Attackers and Cyber-Crime Operations (WACCO 2019)

Geost Botnet. Operational Security Failures of a New Android Banking Threat .406.....
Sebastian Garcia (Czech Technical University), Maria Jose Erquiaga (Universidad Nacional de Cuyo), Anna Shirokova (Avast Software), and Carlos Garcia Garino (Universidad Nacional de Cuyo)

Youth Hackers and Adult Hackers in South Korea: An Application of Cybercriminal Profiling .410.
Sinchul Back (University of Scranton), Jennifer LaPrade (University of Texas at Dallas), Lana Shehadeh (Florida International University), and Minju Kim (Dongkuk University)

Master of Sheets: A Tale of Compromised Cloud Documents .414.....
Jeremiah Onaolapo (Northeastern University), Martin Lazarov (University College London), and Gianluca Stringhini (Boston University)

Iniquitous Cord-Cutting: An Analysis of Infringing IPTV Services .423.....
Prakhar Pandey (NYU), Maxwell Aliapoulios (NYU), and Damon McCoy (NYU)

CARONTE: Crawling Adversarial Resources Over Non-Trusted, High-Profile Environments .433.
Michele Campobasso (Alma Mater Studiorum - Università degli Studi di Bologna), Pavlo Burda (Technische Universiteit Eindhoven - TU/e), and Luca Allodi (Technische Universiteit Eindhoven - TU/e)

Cascade and Chain Effects in Big Data Cybercrime: Lessons from the TalkTalk hack .443.....
Maria Grazia Porcedda (University of Leeds) and David S. Wall (University of Leeds)

A Qualitative Evaluation of Two Different Law Enforcement Approaches on Dark Net Markets .453
Cerys Bradley (UCL) and Gianluca Stringhini (Boston University)

Machete: Dissecting the Operations of a Cyber Espionage Group in Latin America .464.....
Veronica Valeros (Czech Technical University in Prague), Maria Rigaki (Czech Technical University in Prague), and Sebastian Garcia (Czech Technical University in Prague)

Beneath the Dark Web: Excavating the Layers of Cybercrime's Underground Economy .474.....
Jonathan Lusthaus (University of Oxford)

Inside out: Characterising Cybercrimes Committed Inside and Outside the Workplace .481.....
Alice Hutchings (Computer Laboratory, University of Cambridge) and Ben Collier (Computer Laboratory, University of Cambridge)

Author Index 491 . . . . . .