

# **8th International Conference on Information Systems Security and Privacy (ICISSP 2022)**

Online

9 - 11 February 2022

**Editors:**

**Paolo Mori**

**Gabriele Lenzini**

**Steven Furnell**

ISBN: 978-1-7138-5316-9

**Printed from e-media with permission by:**

Curran Associates, Inc.  
57 Morehouse Lane  
Red Hook, NY 12571



**Some format issues inherent in the e-media version may also appear in this print version.**

Copyright© (2022) by SCITEPRESS – Science and Technology Publications, Lda.  
All rights reserved.

Printed with permission by Curran Associates, Inc. (2022)

For permission requests, please contact SCITEPRESS – Science and Technology Publications, Lda.  
at the address below.

SCITEPRESS – Science and Technology Publications, Lda.  
Avenida de S. Francisco Xavier, Lote 7 Cv. C,  
2900-616 Setúbal, Portugal

Phone: +351 265 520 185

Fax: +351 265520 186

[info@scitepress.org](mailto:info@scitepress.org)

**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  
Email: [curran@proceedings.com](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

# CONTENTS

---

## INVITED SPEAKERS

### KEYNOTE SPEAKERS

- Why Rigorous Underpinnings for Cyber Security Education and Training Matter? Experiences from CyBOK: The Cyber Security Body of Knowledge 5  
*Awais Rashid*
- Data Security and Privacy in Emerging Scenarios 7  
*Pierangela Samarati*
- Why Usability Has Become Privacy's Biggest Challenge and What We Can Do About It 9  
*Norman Sadeh*

### PAPERS

#### FULL PAPERS

- "Fake News Detector": An Automatic System for the Reliability Evaluation of Digital News 15  
*Claudio Cilli, Giulio Magnanini, Lorenzo Manduca and Fabrizio Venettoni*
- Network Intrusion Detection: A Comprehensive Analysis of CIC-IDS2017 25  
*Arnaud Rosay, Eloïse Cheval, Florent Carlier and Pascal Leroux*
- Privacy-preserving Parallel Computation of Shortest Path Algorithms with Low Round Complexity 37  
*Mohammad Anagreh, Peeter Laud and Eero Vainikko*
- Systematic Analysis of Programming Languages and Their Execution Environments for Spectre Attacks 48  
*Amir Naseredini, Stefan Gast, Martin Schwarzl, Pedro Miguel Sousa Bernardo, Amel Smajic, Claudio Canella, Martin Berger and Daniel Gruss*
- Semantic Attack on Disassociated Transactions 60  
*Asma AlShuhail and Jianhue Shao*
- Implementing Post-quantum Cryptography for Developers 73  
*Julius Hekkala, Kimmo Halunen and Visa Vallivaara*
- Security Issue Classification for Vulnerability Management with Semi-supervised Learning 84  
*Emil Wåreus, Anton Dupplis, Magnus Tullberg and Martin Hell*
- Estimating the Time-To-Compromise of Exploiting Industrial Control System Vulnerabilities 96  
*Engla Rencelj Ling and Mathias Ekstedt*
- Containment Strategy Formalism in a Probabilistic Threat Modelling Framework 108  
*Per Fahlander, Mathias Ekstedt, Preetam Mukherjee and Ashish Kumar Dwivedi*
- Culturally-sensitive Cybersecurity Awareness Program Design for Iranian High-school Students 121  
*Rooya Karimnia, Kaie Maennel and Mahtab Shahin*
- Analysis and Enhancement of Self-sovereign Identity System Properties Compiling Standards and Regulations 133  
*Charnon Pattiyanon and Toshiaki Aoki*

Public Key Compression and Fast Polynomial Multiplication for NTRU using the Corrected Hybridized NTT-Karatsuba Method <i>Rohon Kundu, Alessandro de Piccoli and Andrea Visconti</i>	145
Intent-aware Permission Architecture: A Model for Rethinking Informed Consent for Android Apps <i>Md Rashedur Rahman, Elizabeth Miller, Moinul Hossain and Aisha Ali-Gombe</i>	154
A Fast and Cost-effective Design for FPGA-based Fuzzy Rainbow Tradeoffs <i>Leonardo Veronese, Francesco Palmarini, Riccardo Focardi and Flaminia L. Luccio</i>	165
Detecting Obfuscated Malware using Memory Feature Engineering <i>Tristan Carrier, Princy Victor, Ali Tekeoglu and Arash Habibi Lashkari</i>	177
Comparing the Detection of XSS Vulnerabilities in Node.js and a Multi-tier JavaScript-based Language via Deep Learning <i>Héloïse Maurel, Santiago Vidal and Tamara Rezk</i>	189
Differential-linear Attacks on Permutation Ciphers Revisited: Experiments on Ascon and DryGASCON <i>Aslı Başak Civek and Cihangir Tezcan</i>	202
On Tracking Ransomware on the File System <i>Luigi Catuogno and Clemente Galdi</i>	210
SecTL: Secure and Verifiable Transfer Learning-based inference <i>Abbass Madi, Oana Stan, Renaud Sirdey and Cédric Gouy-Pailler</i>	220
TEEm: A Tangle-based Elastic Emulator for Storing Connected Vehicle Data in a Distributed Ledger Technology <i>David Werden, Matthew Muccioli and Anyi Liu</i>	230
Game Theoretic Analysis of Ransomware: A Preliminary Study <i>Rudra Prasad Baksi and Shambhu Upadhyaya</i>	242
<b>SHORT PAPERS</b>	
On the LPSE Password Meter's Discrepancies among Different Datasets <i>Agnieszka Rucka and Wojciech Wodo</i>	255
Classifying COVID-19 Disinformation on Twitter using a Convolutional Neural Network <i>Mohamad Nabeel and Christine Große</i>	264
Utility of Anonymised Data in Decision Tree Derivation <i>Jack R. Davies and Jianhua Shao</i>	273
Formalizing Real-world Threat Scenarios <i>Paul Tavalato, Robert Luh and Sebastian Eresheim</i>	281
Side Channel Identification using Granger Time Series Clustering with Applications to Control Systems <i>Matthew Lee, Joshua Sylvester, Sunjoli Aggarwal, Aviraj Sinha, Michael Taylor, Nathan Srirama, Eric C. Larson and Mitchell A. Thornton</i>	290
An Analysis of Cloud Certifications' Performance on Privacy Protections <i>Tian Wang and Masooda Bashir</i>	299

Efficient and Secure Encryption Adjustment for JSON Data <i>Maryam Almarwani, Boris Konev and Alexei Lisitsa</i>	307
Towards a Better Understanding of Machine Learning based Network Intrusion Detection Systems in Industrial Networks <i>Anne Borcherdig, Lukas Feldmann, Markus Karch, Ankush Meshram and Jürgen Beyerer</i>	314
Digital Supply Chain Vulnerabilities in Critical Infrastructure: A Systematic Literature Review on Cybersecurity in the Energy Sector <i>Mari Aarland and Terje Gjøsæter</i>	326
Cluster Crash: Learning from Recent Vulnerabilities in Communication Stacks <i>Anne Borcherdig, Philipp Takacs and Jürgen Beyerer</i>	334
PREUNN: Protocol Reverse Engineering using Neural Networks <i>Valentin Kiechle, Matthias Börsig, Sven Nitzsche, Ingmar Baumgart and Jürgen Becker</i>	345
An Exploratory Study of Why UMLsec Is Not Adopted <i>Shouki A. Ebad</i>	357
A Tailored Model for Cyber Security Education Utilizing a Cyber Range <i>Gregor Langner, Florian Skopik, Steven Furnell and Gerald Quirchmayr</i>	365
Android Data Storage Locations and What App Developers Do with It from a Security and Privacy Perspective <i>Kris Heid, Tobias Tefke, Jens Heider and Ralf C. Staudemeyer</i>	378
SpamFender: A Semi-supervised Incremental Spam Classification System across Social Networks <i>Shengyuan Wen and Weiqing Sun</i>	388
A Novel Key Exchange Protocol using Logic Algebra for the Factorization Problem <i>Junhui Xiao, Ashish Neupane, Hiba F. Fayoumi and Weiqing Sun</i>	396
Cyber Exercises in Computer Science Education <i>Melisa Gafic, Simon Tjoa, Peter Kieseberg, Otto Hellwig and Gerald Quirchmayr</i>	404
Construction of a Support Tool for User Reading of Privacy Policies and Assessment of its User Impact <i>Sachiko Kanamori, Hirotsune Sato, Naoya Tabata and Ryo Nojima</i>	412
Impact of Cross-standard Cell Libraries on Machine Learning based Hardware Trojan Detection <i>Shang-Wen Chen, Jian-Wei Liao, Chia-Wei Tien and Jung-Hsin Hsiao</i>	420
Benchmarking Consumer Data and Privacy Knowledge in Connected and Autonomous Vehicles <i>Flora Barber and Steven Furnell</i>	426
Evaluating Deep Learning-based NIDS in Adversarial Settings <i>Hesamodin Mohammadian, Arash Habibi Lashkari and Ali A. Ghorbani</i>	435
Effective & Efficient Access Control in Smart Farms: Opportunities, Challenges & Potential Approaches <i>Ghadeer I. Yassin and Lakshmish Ramaswamy</i>	445
Feature Importance and Deep Learning for Android Malware Detection <i>A. Talbi, A. Viens, L.-C. Leroux, M. François, M. Caillol and N. Nguyen</i>	453

SMPG: Secure Multi Party Computation on Graph Databases <i>Nouf Aljuaid, Alexei Lisitsa and Sven Schewe</i>	463
Age Bias in Finger Vein Biometric Research <i>Joanne L. Hall, Jomin John, Jessica Liebig and Anju Skariah</i>	472
Industrial and Automation Control System Cyber Range Prototype for Offensive Capability Development <i>Austris Uljāns and Bernhards Blumbergs</i>	478
Planning for Cryptographic Readiness in an Era of Quantum Computing Advancement <i>David Ott, Dennis Moreau and Manish Gaur</i>	491
Incentivisation of Outsourced Network Testing: View from Platform Perspective <i>Sultan Alasmari, Weichao Wang and Yu Wang</i>	499
Protecting Shared Virtualized Environments against Cache Side-channel Attacks <i>Abdullah Albalawi, Vassilios G. Vassilakis and Radu Calinescu</i>	507
Revisiting Ontology Based Access Control: The Case for Ontology Based Data Access <i>Ozgu Can and Murat Osman Unalir</i>	515
Linguistic Steganography for Messaging Applications <i>Elsa Serret, Antoine Lesueur and Alban Gabillon</i>	519
DeDup.js: Discovering Malicious and Vulnerable Extensions by Detecting Duplication <i>Pablo Picazo-Sanchez, Maximilian Algehed and Andrei Sabelfeld</i>	528
Survey and Guidelines about Learning Cyber Security Risk Assessment <i>Christophe Ponsard and Philippe Massonet</i>	536
Comparing Perception of Disclosure of Different Types of Information Related to Automated Tools <i>Vanessa Bracamonte and Takamasa Isohara</i>	544
Post Quantum Cryptography Analysis of TLS Tunneling on a Constrained Device <i>Jon Barton, William J. Buchanan, Nikolaos Pitropakis, Sarwar Sayeed and Will Abramson</i>	551
PDF Malware Detection based on Stacking Learning <i>Maryam Issakhani, Princy Victor, Ali Tekeoglu and Arash Habibi Lashkari</i>	562
The GDPR Compliance and Access Control Systems: Challenges and Research Opportunities <i>Said Daoudagh and Eda Marchetti</i>	571
Who Watches the Watchers: A Multi-Task Benchmark for Anomaly Detection <i>Phil Demetriou, Ingolf Becker and Stephen Hailes</i>	579
Cyber Attack Stage Tracing System based on Attack Scenario Comparison <i>Masahito Kumazaki, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada and Hiroki Takakura</i>	587
Malware in Motion <i>Robert Choudhury, Zhiyuan Luo and Khuong An Nguyen</i>	595
Cryptanalysis of Some Electronic Checkbook Schemes <i>Isa Sertkaya and Oznur Kalkar</i>	603

The Role of Information Deserts in Information Security Awareness and Behaviour <i>D. P. Snyman and H. A. Kruger</i>	613
iProfile: Collecting and Analyzing Keystroke Dynamics from Android Users <i>Haytham Elmiligi and Sherif Saad</i>	621
WhatsApp Web Client Live Forensics Technique <i>Alberto Magno Muniz Soares</i>	629
A Privacy-Preserving Auction Platform with Public Verifiability for Smart Manufacturing <i>Thomas Lorünser, Florian Wohner and Stephan Krenn</i>	637
Can We Formally Catch Cheating in E-exams? <i>Itzel Vazquez Sandoval and Gabriele Lenzini</i>	648
Ransomware Detection with Deep Neural Networks <i>Matan Davidian, Natalia Vanetik and Michael Kiperberg</i>	656
<b>6TH INTERNATIONAL SPECIAL SESSION ON FORMAL METHODS FOR SECURITY ENGINEERING</b>	
<b>FULL PAPERS</b>	
On the Influence of Image Settings in Deep Learning-based Malware Detection <i>Francesco Mercaldo, Fabio Martinelli, Antonella Santone and Vinod P.</i>	669
Tamer: A Sandbox for Facilitating and Automating IoT Malware Analysis with Techniques to Elicit Malicious Behavior <i>Shun Yonamine, Yuzo Taenaka and Youki Kadobayashi</i>	677
Profile Hidden Markov Model Malware Detection and API Call Obfuscation <i>Muhammad Ali, Monem Hamid, Jacob Jasser, Joachim Lerman, Samod Shetty and Fabio Di Troia</i>	688
NLP-based User Authentication through Mouse Dynamics <i>Hoseong Asher Lee, Nikhil Prathapani, Rajesh Paturi, Sarp Parmaksiz and Fabio Di Troia</i>	696
AUTHOR INDEX	703