

10th International Conference on Information Systems Security and Privacy (ICISSP 2024)

Rome, Italy
26-28 February 2024

Editors:

**Gabriele Lenzini
Paolo Mori
Steven Furnell**

ISBN: 978-1-7138-9750-7

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© (2024) by SCITEPRESS – Science and Technology Publications, Lda.
All rights reserved.

Printed with permission by Curran Associates, Inc. (2025)

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

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
Web: www.proceedings.com

CONTENTS

INVITED SPEAKERS

KEYNOTE SPEAKERS

Safeguarding Industry 5.0 Ecosystems Through Digital Twins 5
Cristina Alcaraz

Covert & Side Stories: Threats Evolution in Traditional and Modern Technologies 7
Mauro Conti

Security, Privacy and the “Human Factor”: Making Sense of the Paradoxes of Security and Privacy Behaviour 9
Spyros Kokolakis

INVITED LECTURE

Integrating Post-Quantum Cryptography into Trusted Computing Group Standards 15
Thorsten P. Stremlau

MANAGEMENT AND OPERATIONS

FULL PAPERS

Anywhere on Earth: A Look at Regional Characteristics of DRDoS Attacks 21
Tiago Heinrich, Newton C. Will, Rafael R. Obelheiro and Carlos A. Maziero

The Role of Heuristics and Biases in Linux Server Administrators’ Information Security Policy Compliance at Healthcare Organizations 30
John McConnell, Yair Levy, Marti Snyder and Ling Wang

Automating IoT Security Standard Testing by Common Security Tools 42
Rauli Kaksonen, Kimmo Halunen, Marko Laakso and Juha Röning

FeedMeter: Evaluating the Quality of Community-Driven Threat Intelligence 54
Andreas Ruedlinger, Rebecca Klauser, Pavlos Lamprakis, Markus Happe, Bernhard Tellenbach, Onur Veyisoglu and Ariane Trammell

CPE-Identifier: Automated CPE Identification and CVE Summaries Annotation with Deep Learning and NLP 67
Wanyu Hu and Vrizlynn L. L. Thing

SHORT PAPERS

Policy-Driven XACML-Based Architecture for Dynamic Enforcement of Multiparty Computation <i>Arghavan Hosseinzadeh, Jessica Chwalek and Robin Brandstädter</i>	81
Analysis of Payload Confidentiality for the IoT/ LPWAN Technology ‘Lora’ <i>Bernard McWeeney, Ilya Mudritskiy and Renaat Verbruggen</i>	90
Security Contracts a Property-Based Approach to Support Security Patterns <i>Sylvain Guérin, Joel Champeau, Salvador Martínez and Raul Mazo</i>	103
Revolutionizing Board Cyber-Risk Management Using Collaborative Gaming <i>Tony Delvecchio, Sander Zeijlemaker, Giancarlo De Bernardis and Michael Siegel</i>	112
Towards Automated Information Security Governance <i>Ariane Trammell, Benjamin Gehring, Marco Isele, Yvo Spielmann and Valentin Zahnd</i>	120
An Open-Source Approach to OT Asset Management in Industrial Environments <i>Luca Pöhler, Marko Schuba, Tim Höner, Sacha Hack and Georg Neugebauer</i>	128
The Classification and Impact of Cyber Attacks Targeting Critical Service Providers <i>Josefin Andersson and Elias Seid</i>	137
An Empirical Study of Ransomware Vulnerabilities Descriptions <i>Claudia Lanza, Abdelkader Lahmadi and Fabian Osmond</i>	146
Evaluating the Security and Privacy Risk Postures of Virtual Assistants <i>Borna Kalhor and Sanchari Das</i>	154
Effectiveness of Malware Incident Management in Security Operations Centres: Trends, Challenges and Research Directions <i>Dakouri Gazo, Asma Patel and Mohammad Hasan</i>	162
ADMIn: Attacks on Dataset, Model and Input: A Threat Model for AI Based Software <i>Vimal Kumar, Juliette Mayo and Khadija Bahiss</i>	170
Merging Policy and Practice: Crafting Effective Social Engineering Awareness-Raising Policies <i>Eliana Stavrou, Andriani Piki and Panayiotis Varnava</i>	179
Perceptions of Cyber Security Risk of the Norwegian Advanced Metering Infrastructure <i>Eirik Lien, Karl Magnus Grønning Bergh and Sokratis Katsikas</i>	187
Interpretable Android Malware Detection Based on Dynamic Analysis <i>Arunab Singh, Maryam Tanha, Yashvi Girdhar and Aaron Hunter</i>	195
ArkThor: Threat Categorization Based on Malware’s C2 Communication <i>Mohammed Jawed, Sriram Parameshwaran, Nitesh Kumar, Anand Handa and Sandeep K. Shukla</i>	203
Comparing the Effectivity of Planned Cyber Defense Controls in Order to Support the Selection Process <i>Paul Tavolato, Robert Luh, Sebastian Eresheim, Simon Gmeiner and Sebastian Schrittwieser</i>	211
Your Robot Might Be Inadvertently or Deliberately Spying on You: A Critical Analysis of Privacy Practices in the Robotics Industry <i>Farida Elethin, Patrick Iradukunda, David Ishimwe Ruberomitwe and Eric Ishimwe</i>	219

Privacy-Aware Single-Nucleotide Polymorphisms (SNPs) Using Bilinear Group Accumulators in Batch Mode	226
<i>William J. Buchanan, Sam Grierson and Daniel Uribe</i>	
The Right Tool for the Job: Contextualization of Cybersecurity Education and Assessment Methods	234
<i>Daniel Köhler and Christoph Meinel</i>	
An Automated Adaptive Security Framework for Cyber-Physical Systems	242
<i>Elias Seid, Oliver Popov and Fredrik Blix</i>	
Detecting eBPF Rootkits Using Virtualization and Memory Forensics	254
<i>Nezer Jacob Zaidenberg, Michael Kiperberg, Eliav Menachi and Asaf Eitani</i>	
Cybersecurity Incident Response Readiness in Organisations	262
<i>Aseel Aldabjan, Steven Furnell, Xavier Carpent and Maria Papadaki</i>	
APPLICATIONS AND SERVICES	
FULL PAPERS	
A Categorical Data Approach for Anomaly Detection in WebAssembly Applications	275
<i>Tiago Heinrich, Newton C. Will, Rafael R. Obelheiro and Carlos A. Maziero</i>	
Supporting CAN Bus Anomaly Detection with Correlation Data	285
<i>Beatrix Koltai, András Gazdag and Gergely Ács</i>	
IoT Device Classification Using Link-Level Features for Traditional Machine Learning and Large Language Models	297
<i>Gabriel Morales, Farhan Tajwar Romit, Adam Bienek-Parrish, Patrick Jenkins and Rocky Slavin</i>	
Banking Malware Detection: Leveraging Federated Learning with Conditional Model Updates and Client Data Heterogeneity	309
<i>Nahid Ferdous Aurna, Md Delwar Hossain, Hideya Ochiai, Yuzo Taenaka, Latifur Khan and Youki Kadobayashi</i>	
Visual Attention and Privacy Indicators in Android: Insights from Eye Tracking	320
<i>Michele Guerra, Roberto Milanese, Michele Deodato, Vittorio Perozzi and Fausto Fasano</i>	
SHORT PAPERS	
Ethical Design for Data Privacy and User Privacy Awareness in the Metaverse	333
<i>Ophelia Prillard, Costas Boletsis and Shukun Tokas</i>	
Deep Q-Networks for Imbalanced Multi-Class Malware Classification	342
<i>Antonio Maci, Giuseppe Urbano and Antonio Coscia</i>	
Desktop Crypto Wallets: A Digital Forensic Investigation and Analysis of Remnants and Traces on end-User Machines	350
<i>David Debono and Aleandro Sultana</i>	
Build a Computationally Efficient Strong Defense Against Adversarial Example Attacks	358
<i>Changwei Liu, Louis DiValentin, Aolin Ding and Malek Ben Salem</i>	
Botnet Detection by Integrating Multiple Machine Learning Models	366
<i>Thanawat Tejapijaya, Prarinya Siritanawan, Karin Sumongkayothin and Kazunori Kotani</i>	

Robust Image Deepfake Detection with Perceptual Hashing <i>Chun-Shien Lu and Chao-Hsuan Lin</i>	374
Federated Learning with Differential Privacy and an Untrusted Aggregator <i>Kunlong Liu and Trinabh Gupta</i>	379
A Recommender System to Detect Distributed Denial of Service Attacks with Network and Transport Layer Features <i>Kağan Özgün, Ayşe Tosun and Mehmet Tahir Sandıkkaya</i>	390
Silicon-Integrated Security Solutions Driving IoT Security <i>Stephan Spitz and Alexander Lawall</i>	398
Vulnerability Information Sharing Platform for Securing Hardware Supply Chains <i>Kento Hasegawa, Katsutoshi Hanahara, Hiroshi Sugisaki, Minoru Kozu, Kazuhide Fukushima, Yosuke Murakami and Shinsaku Kiyomoto</i>	403
Off-Chaining Approaches for Cost-Efficiency in Threshold-Based Elliptic Curve Systems over Blockchains <i>Visakh K. Vijayan, Maria Francis and Kotaro Kataoka</i>	411
High Throughput Neural Network for Network Intrusion Detection on FPGAs: An Algorithm-Architecture Interaction <i>Muhammad Ali Farooq, Syed Muhammad Fasih Ul Hassan, Muhammad Umer Farooq and Abid Rafique</i>	423
Comparative Analysis of Feature Selection Algorithms for Automated IoT Device Fingerprinting <i>Ahmet Aksoy, Sundeep Varma, Ganesh Moorthy, Enya Pan and Gorkem Kar</i>	430
Cybersecurity-Related Tweet Classification by Explainable Deep Learning <i>Giacomo Iadarola, Fabio Martinelli, Francesco Mercaldo, Luca Petrillo and Antonella Santone</i>	438
Fuzzing Matter(s): A White Paper for Fuzzing the Matter Protocol <i>Marcello Maugeri</i>	446
Exploring BERT for Predicting Vulnerability Categories in Device Configurations <i>Dmitry Levshun and Dmitry Vesnin</i>	452

TECHNOLOGIES AND FOUNDATIONS

FULL PAPERS

Security Analysis of an Image Encryption Based on the Kronecker Xor Product, the Hill Cipher and the Sigmoid Logistic Map <i>George Teșeleanu</i>	467
Enclave Management Models for Safe Execution of Software Components <i>Newton Carlos Will and Carlos Alberto Maziero</i>	474
APP-CEP: Adaptive Pattern-Level Privacy Protection in Complex Event Processing Systems <i>Majid Lotfian Delouee, Victoria Degeler, Peter Amthor and Boris Koldehofe</i>	486
PenGym: Pentesting Training Framework for Reinforcement Learning Agents <i>Thanh Huynh Phuong Nguyen, Zhi Chen, Kento Hasegawa, Kazuhide Fukushima and Razvan Beuran</i>	498

Gradient-Based Clean Label Backdoor Attack to Graph Neural Networks <i>Ryo Meguro, Hiroya Kato, Shintaro Narisada, Seira Hidano, Kazuhide Fukushima, Takuo Suganuma and Masahiro Hiji</i>	510
Performance Evaluation of Polynomial Commitments for Erasure Code Based Information Dispersal <i>Antoine Stevan, Thomas Lavour, Jérôme Lacan, Jonathan Detchart and Tanguy Pérennou</i>	522
Feasibility of Random Forest with Fully Homomorphic Encryption Applied to Network Data <i>Shusaku Uemura and Kazuhide Fukushima</i>	534
Exploring Errors in Binary-Level CFG Recovery <i>Anjali Pare and Prasad A. Kulkarni</i>	546
RoomKey: Extracting a Volatile Key with Information from the Local WiFi Environment Reconstructable Within a Designated Area <i>Philipp Jakubeit, Andreas Peter and Maarten van Steen</i>	558
The Design and Implementation of a Semantic Web Framework for the Event-Centric Digital Forensics Analysis <i>Pavel Chikul, Hayretdin Bahşi and Olaf Maennel</i>	570
Secure Multiparty Computation of the Laplace Mechanism <i>Amir Zarei and Staal A. Vinterbo</i>	582
Towards Generalized Diffie-Hellman-esque Key Agreement via Generic Split KEM Construction <i>Brian Goncalves and Atefeh Mashatan</i>	594
LSTM Autoencoder-Based Insider Abnormal Behavior Detection Using De-Identified Data <i>Seo-Yi Kim and Il-Gu Lee</i>	609
Blockchain for Privacy-Preserving Data Distribution in Healthcare <i>Amitesh Singh Rajput and Arnav Agrawal</i>	621
SHORT PAPERS	
Smart Home Privacy: A Scoping Review <i>Ali Ahmed, Victor Ungureanu, Tarek Gaber, Craig Watterson and Fatma Masmoudi</i>	635
Comparing Phishing Training and Campaign Methods for Mitigating Malicious Emails in Organizations <i>Jackie Scott, Yair Levy, Wei Li and Ajoy Kumar</i>	643
User Re-Authentication via Mouse Movements and Recurrent Neural Networks <i>Paul R. B. Houssel and Luis A. Leiva</i>	652
UPSS: A Global, Least-Privileged Storage System with Stronger Security and Better Performance <i>Arastoo Bozorgi, Mahya Soleimani Jadidi and Jonathan Anderson</i>	660
KAIME: Central Bank Digital Currency with Realistic and Modular Privacy <i>Ali Dogan and Kemal Bicakci</i>	672
Enhancing Cybersecurity Through Comparative Analysis of Deep Learning Models for Anomaly Detection <i>Kateřina Macková, Dominik Benk and Martin Šrotýř</i>	682

Evaluating the Influence of Multi-Factor Authentication and Recovery Settings on the Security and Accessibility of User Accounts <i>Andre Büttner and Nils Gruschka</i>	691
Attestation with Constrained Relying Party <i>Mariam Moustafa, Arto Niemi, Philip Ginzboorg and Jan-Erik Ekberg</i>	701
Forgery Resistance of User Authentication Methods Using Location, Wi-Fi and Their Correlation <i>Ryosuke Kobayashi and Rie Shigetomi Yamaguchi</i>	709
Machine Learning-Based Classification of Hardware Trojans in FPGAs Implementing RISC-V Cores <i>Stefano Ribes, Fabio Malatesta, Grazia Garzo and Alessandro Palumbo</i>	717
An Improved PUF-Based Privacy-Preserving IoT Protocol for Cloud Storage <i>Cédric De Pauw, Jan Tobias Mühlberg and Jean-Michel Dricot</i>	725
Anonymous Multi-Receiver Certificateless Hybrid Signcryption for Broadcast Communication <i>Alia Umrani, Apurva K. Vangujar and Paolo Palmieri</i>	733
Security Analysis of an Image Encryption Scheme Based on a New Secure Variant of Hill Cipher and 1D Chaotic Maps <i>George Teşeleanu</i>	745
A Framework for E2E Audit Trails in System Architectures of Different Enterprise Classes <i>Luca Patzelt, Georg Neugebauer, Meik Döll, Sacha Hack, Tim Höner and Marko Schuba</i>	750
Differential Privacy for Distributed Traffic Monitoring in Smart Cities <i>Marcus Gelderie, Maximilian Luff and Lukas Brodschelm</i>	758
Using ILP to Learn AppArmor Policies <i>Lukas Brodschelm and Marcus Gelderie</i>	766
Learning from the Dark Side About How (not) to Engineer Privacy: Analysis of Dark Patterns Taxonomies from an ISO 29100 Perspective <i>Philippe Valoggia, Anastasia Sergeeva, Arianna Rossi and Marietjie Botes</i>	774
AnonEmoFace: Emotion Preserving Facial Anonymization <i>Jan Hintz, Jacob Rühle and Ingo Siegert</i>	785
The Status and Management of Web-Related Security at Higher Education Institutions in Poland <i>Jackson Barreto, Paulina Rutecka, Karina Cicha and Pedro Pinto</i>	789
A Decentralized Federated Learning Using Reputation <i>Olive Chakraborty and Aymen Boudguiga</i>	799
Pure Multi Key BGV Implementation <i>Justine Paillet, Olive Chakraborty and Marina Checri</i>	807
EMplifier: Hybrid Electromagnetic Probe for Side Channel and Fault Injection Analysis <i>Fabrizia Marrucco, Mosabbah Mushir Ahmed, Bechir Bouali and Alieeldin Mady</i>	815
Vision Based Malware Classification Using Deep Neural Network with Hybrid Data Augmentation <i>Md. Mahbubur Rahman, Md. Delwar Hossain, Hideya Ochiai, Youki Kadobayashi, Tanjim Sakib and Syed Taha Yeasin Ramadan</i>	823

Conceptualising an Anti-Digital Forensics Kill Chain for Smart Homes <i>Mario Raciti</i>	831
PETRIoT - A Privacy Enhancing Technology Recommendation Framework for IoT Computing <i>Fatema Rashid, Ali Miri and Atefeh Mashatan</i>	838
Preserving Privacy in High-Dimensional Data Publishing <i>Narges Alipourjeddi and Ali Miri</i>	845
Security Evaluation of Decision Tree Meets Data Anonymization <i>Ryousuke Wakabayashi, Lihua Wang, Ryo Nojima and Atsushi Waseda</i>	853
Implementation and Analysis of Covert Channel Using iBeacon <i>Ye-Sol Oh, Yeon-Ji Lee, Jiwon Jang, Hyunwoo Choi and Il-Gu Lee</i>	861
Smart Homes as Digital Ecosystems: Exploring Privacy in IoT Contexts <i>Sally Bagheri, Andreas Jacobsson and Paul Davidsson</i>	869
Efficient Secure Computation of Edit Distance on Genomic Data <i>Andrea Migliore, Stelvio Cimato and Gabriella Trucco</i>	878
GPU-Based Brute Force Cryptanalysis of KLEIN <i>Cihangir Tezcan</i>	884
A Brief Reflection on Trusted Platform Module Support <i>Martin Pirker and Robert Haas</i>	890
Feasibility of Privacy Preserving Minutiae-Based Fingerprint Matching <i>Julia Mader and Thomas Lorünser</i>	899
What's Your Purpose? An Approach to Incorporating GDPR Purposes into Requirements Analysis <i>Evangelia Vanezi, Georgia Kapitsaki and Anna Philippou</i>	907
AUTHOR INDEX	915