11th International Conference on Information Systems Security and Privacy (ICISSP 2025)

Volume 2

Porto, Portugal
20-22 February 2025

Editors:

Robert Di Pietro
Karen Renaud
Paolo Mori

ISBN: 979-8-3313-1862-8

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© (2025) 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

Rethinking Privacy Protection in Federated Learning in the Face of Model Inversion Attacks 5
Wenjing Lou

Securing Ultra-Large Scale Infrastructures: Challenges and Opportunities 7
Awais Rashid

Turing's Echo on Deceptive Machines: The Challenge of Distinguishing Human and AI Creations 9
Ahmad-Reza Sadeghi

APPLICATIONS AND SERVICES

FULL PAPERS

A Hybrid Approach for Detecting SQL-Injection Using Machine Learning Techniques 15
Hari Krishna, Jared Oluoch and Junghwan Kim

CyLLM-DAP: Cybersecurity Domain-Adaptive Pre-Training Framework of Large Language Models 24
Khang Mai, Razvan Beuran and Naoya Inoue

Assessing the Effectiveness of an LLM-Based Permission Model for Android 36
Roberto Milanese, Michele Guerra, Michele Daniele, Giovanni Fabbrocino and Fausto Fasano

Scrooge: Detection of Changes in Web Applications to Enhance Security Testing 48
Fabio Büsser, Jan Kressebuch, Martín Ochoa, Valentin Zahnd and Ariane Trammell

Privacy Policies in Medium-Sized European Town Administrations: A Comparative Analysis of English and German-Speaking Countries 60
Henry Hosseini

HybridMTD: Enhancing Robustness Against Adversarial Attacks with Ensemble Neural Networks and Moving Target Defense 72
Kimia Tahayori, Sherif Saad, Mohammad Mamun and Saeed Samet

Telosian: Reducing False Positives in Real-Time Cyber Anomaly Detection by Fast Adaptation to Concept Drift 84
Iker Antonio Olarra Maldonado, Erik Meeuwissen, Puck de Haan and Rob van der Mei

Large Language Models in Cybersecurity: State-of-the-Art 98
Farzad Nourmohammadzadeh Motlagh, Mehrdad Hajizadeh, Mehryar Majd, Pejman Najafi, Feng Cheng and Christoph Meinel

SGX-PrivInfer: A Secure Collaborative System for Quantifying and Mitigating Attribute Inference Risks in Social Networks 111
Hervais Simo and Michael Kreutzer

SHORT PAPERS

The Dual-Edged Sword: The Impact of Large Language Models in Network Infrastructure Security 125
David Debono and Anastasia Sare

Investigating the Effectiveness of Zero–Trust Architecture for Satellite Cybersecurity 133
Masrur Masqub Utsash, Georgios Kavallieratos, Konstantinos Antonakopoulos and Sokratis Katsikas

Dynamic-Differential Privacy based on Feature Selection with Improved Usability and Security 141
Sun-Jin Lee, Hye-Yeon Shim, Jung-Hwa Rye and Il-Gu Lee

Attackers' Profiling Based on Multi-Attack Patterns in SSH Service 150
Kriti Majumdar, Nitesh Kumar, Anand Handa and Sandeep K. Shukla

Defense Against Backdoor Attacks on Image Retrieval Models Through Strategic Manipulations 160
Hung-Lei Lee, Chun-Shien Lu and Jia-Ching Wang

RiVS: Reputation in VoIP Systems 167
Bruno Freitas Cruz and Bruno Sousa

Cybersecurity Fundamentals Training Among Middle School Students: Building a Strong Foundation 176
Qingsong Zhao, Urska Cvek and Kevin Zhao

Autonomous Cyber Defence by Quantum-Inspired Deep Reinforcement Learning 184
Wenbo Feng, Sanyam Vyas and Tingting Li

Distributed Machine Learning and Multi-Agent Systems for Enhanced Attack Detection and Resilience in IoT Networks 192
Gustavo Funchal, Tiago Pedrosa, Fernando de la Prieta and Paulo Leitão

LLM-Based Fine-Grained ABAC Policy Generation 204
Khang Mai, Nakul Ghate, Jongmin Lee and Razvan Beuran

The Digital Loophole: Evaluating the Effectiveness of Child Age Verification Methods on Social Media 213
Fatmaelzahraa Eltaher, Rahul Krishna Gajula, Luis Miralles-Pechuán, Christina Thorpe and Susan Mckeever

Adaptive Ensemble Defense: Mitigating NLP Adversarial Attacks with Data-Augmented Voting Mechanisms 223
Amira Abdelbaky, Sherif Saad and Mohammad Mamun

Hybrid Classical Quantum Learning Model Framework for Detection of Deepfake Audio 231
Atul Pandey and Bhawana Rudra

Navigating the Security Challenges of LLMs: Positioning Target-Side Defenses and Identifying Research Gaps 240
Malte Josten, Matthias Schaffeld, René Lehmann and Torben Weis

Comprehensive Feature Selection for Machine Learning-Based Intrusion Detection in Healthcare IoMT Networks 248
Muaan Ur Rehman, Rajesh Kalakoti and Hayretdin Bahşi

Randomizing Forger Selection to Improve Decentralization in Proof of Stake Consensus Protocol 260
Syed Badruddoja, Sasi Kiran Kanduri and Ram Dantu

Evaluating and Defending Backdoor Attacks in Image Recognition Systems
Syed Badruddoja, Bashar Najah Allwza and Ram Dantu 268

Exploring Efficiency of Machine Learning in Profiling of Internet of Things Devices for Malicious Activity Detection
Daniil Legkodymov and Dmitry Levshun 276

TECHNOLOGIES AND FOUNDATIONS

FULL PAPERS

Flow Exporter Impact on Intelligent Intrusion Detection Systems
Daniela Pinto, João Vitorino, Eva Maia, Ivone Amorim and Isabel Praça 289

VBSF: A Visual-Based Spam Filtering Technique for Obfuscated Emails
Ali Hossary and Stefano Tomasin 299

Gram Root Decomposition over the Polynomial Ring: Application to Sphericalization of Discrete Gaussian
Hiroki Okada and Tsuyoshi Takagi 306

Privacy- & Utility-Preserving Data Releases over Fragmented Data Using Individual Differential Privacy
Luis Del Vasto-Terrientes, Sergio Martínez and David Sánchez 318

A Deontic Logic Model of Attribute-Based Information Flows in Database-Defined Networks with Application to Healthcare Monitoring
Benjamin Aziz, Ukamaka Oragwu and Safa Tharib 330

Securing the Device Lifecycle Management: A Scalable and Cost-Efficient Public Key Infrastructure Through Microservices
Sara Sumaidaa, Hamda Almenhali, Rajkumar Ramasamy, Oleksii Voronin, Mohammed Alazzani and Kyusuk Han 342

Exploit the Leak: Understanding Risks in Biometric Matchers
Dorine Chagnon, Axel Durbet, Paul-Marie Grollemund and Kevin Thiry-Atighehchi 353

Enhanced Predictive Clustering of User Profiles: A Model for Classifying Individuals Based on Email Interaction and Behavioral Patterns
Peter Wafik, Alessio Botta, Luigi Gallo, Gennaro Esposito Mocerino, Cornelia Herbert, Ivan Annicchiarico, Alia El Bolock and Slim Abdennadher 363

X-Ray Radiation Effects on SRAM-Based TRNG and PUF
Martin Holec, Jan Bělohoubek, Pavel Rous, Tomáš Pokorný, Róbert Lórencz and František Steiner 375

Management of Customized Privacy Policies
Jens Leicht and Maritta Heisel 385

Precise Detection of Security Checks in Program Binaries
Koyel Pramanick and Prasad A. Kulkarni 397

SHORT PAPERS

A Secret Key Spreading Protocol for Extending ETSI Quantum Key Distribution 411
Thomas Prévost, Bruno Martin and Olivier Alibart

Quantum-Resilient IoT: Integrating Hardware-Based Post-Quantum Cryptography for Robust Device Security 419
Stephan Spitz, Alexander Lawall and Michal Andrzejczak

A2CT: Automated Detection of Function and Object-Level Access Control Vulnerabilities in Web Applications 425
Michael Schlaubitz, Onur Veyisoglu and Marc Rennhard

(Deep) Learning About Elliptic Curve Cryptography 437
Diana Maimuţ, Cristian Matei and George Teşeleanu

Approximations of the Sigmoid Function Beyond the Approximation Domains for Privacy-Preserving Neural Networks 445
Shusaku Uemura, Kazuhide Fukushima and Shinsaku Kiyomoto

A Targeting Attack by Dynamic Fake QR Code Using Invisible Laser Irradiation 455
Dai Itakura, Taiga Manabe, Yuki Kamata, Ayana Oku, Hiroshi Yamamoto, Yoshihisa Takayama and Toshihiro Ohigashi

Logic Locking for Random Forests: Securing HDL Design and FPGA Accelerator Implementation 463
Rupesh Raj Karn, Johann Knechtel and Ozgur Sinanoglu

Is My Data in Your Retrieval Database? Membership Inference Attacks Against Retrieval Augmented Generation 474
Maya Anderson, Guy Amit and Abigail Goldsteen

Exploring Attack Paths Using Graph Theory: Case - Microsoft Entra ID Pass-Through Authentication 486
Nestori Syynimaa

Objective- and Utility-Based Negotiation for Access Control 493
Aditya Sissodiya, Ulf Bodin and Olov Schelén

Towards Efficient Cloud Data Processing: A Comprehensive Guide to CKKS Parameter Selection 502
Modjtaba Gharibyar, Clemens Krüger and Dominik Schoop

On the Effect of Dataset Size and Composition for Privacy Evaluation 510
Danai Georgiou, Carlos Franzreb and Tim Polzehl

Evaluating the Efficacy of LINDDUN GO for Privacy Threat Modeling for Local Renewable Energy Communities 518
Oliver Langthaler, Günther Eibl, Lars-Kevin Klüver and Andreas Unterweger

Improving Locally Differentially Private Graph Statistics Through Sparseness-Preserving Noise-Graph Addition 526
Sudipta Paul, Julián Salas and Vicenç Torra

Secure Visual Data Processing via Federated Learning 534
Pedro Santos, Tânia Carvalho, Filipe Magalhães and Luís Antunes

Leash: A Transparent Capability-Based Sandboxing Supervisor for Unix 542
Mahya Soleimani Jadidi and Jonathan Anderson

Flexible Noise Based Robustness Certification Against Backdoor Attacks in Graph Neural Networks 552
Hiroya Kato, Ryo Meguro, Seira Hidano, Takuo Suganuma and Masahiro Hiji

Security Analysis of a Color Image Encryption Scheme Based on a Fractional-Order Hyperchaotic System 564
George Teşeleanu

Security Analysis of Biased Basis for Efficient BB84 571
Hiroki Yamamuro, Shohei Beppu, Kazuhide Fukushima and Shinsaku Kiyomoto

EK-Means: Towards Making Ensemble K-Means Work for Image-Based Data Analysis Without Prior Knowledge of K 575
Danping Niu, Yuan Ping, Yujian Liu, Fanxi Wei and Wenhong Wu

User Authentication on Remote Connections with Siamese Networks Using Keyboard Usage Behavior and Corresponding Noise Performances 585
Mehmet Fide and Emin Anarim

De-Anonymization of Health Data: A Survey of Practical Attacks, Vulnerabilities and Challenges 595
Hamza Aguelal and Paolo Palmieri

Privacy Preservation for Machine Learning in IIoT Data via Manifold Learning and Elementary Row Operations 607
E. Fatih Yetkin and Tuğçe Ballı

Using Compact DNSSEC and Self-Signed Certificate to Improve Security and Privacy for Second-Level Domain Resolution 615
Lanlan Pan, Ruonan Qiu and Minghui Yang

Analytical Evaluation of Time-Based Cryptography 624
Mohammed Ramadan, Pranit Gadekar, Veit Hagenmeyer and Ghada Elbez

Memory-Saving Oblivious RAM for Trajectory Data via Hierarchical Generation of Dummy Access over Untrusted Cloud Environment 635
Taisho Sasada and Bernard Ousmane Sane

Connected Vehicles Data Classification and the Influence of a Sustainable Data Governance for Optimal Utilisation of In-Vehicle Data 643
Ali Karimi, Asma Adnane, Iain W. Phillips and Elhadj Benkhelifa

Device-Bound vs. Synced Credentials: A Comparative Evaluation of Passkey Authentication 651
Andre Büttner and Nils Gruschka

AUTHOR INDEX 661