# 12th International Conference on Information Systems Security and Privacy (ICISSP 2026)

Volume 2

Marbella, Spain
4-6 March 2026

ISBN: 979-8-3313-3346-1

**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© (2026) by SCITEPRESS – Science and Technology Publications, Lda.
All rights reserved.

Printed with permission by Curran Associates, Inc. (2026)

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**

Cracking the Code: Detecting the Next Generation of Social Bots 3
*Salil Kanhere*

Humans and Hybrids: Repositioning the Social Threat to Network Security in the 21st Century 5
*Michael McGuire*

Data Privacy and Security in Distributed Collaborative Scenarios 7
*Pierangela Samarati*

**TECHNOLOGIES AND FOUNDATIONS**

**FULL PAPERS**

Revisiting ISD Algorithms and New Decoding Records for Large Weight Syndrome Decoding over $F_q$ 13
*Takeshi Wakao, Yusuke Aikawa, Shintaro Narisada and Tsuyoshi Takagi*

Plug'n'Trust: Fine-Grained USB Device Isolation for ARM TrustZone 25
*Julian Funk, Yvonne Kothmeier, Jonas Röckl, Christian Lindenmeier and Tilo Müller*

Sequential Pattern Recognition Attacks against Deployed Topic-Based Mechanisms 37
*Saranya Vijayakumar, Norman Sadeh and Matt Fredrikson*

On the Hardness of Decoding Quasi-Cyclic Codes and the Security of Code-Based Public-Key Cryptosystems 49
*Alessandro Annechini, Alessandro Barenghi and Gerardo Pelosi*

Practical Private Approximate Similarity Computation 61
*Ryo Nojima and Lihua Wang*

Private Multivariate Function Evaluation Using CKKS-Based Homomorphic Encrypted Lookup Tables 70
*Haoyun Zhu, Takuya Suzuki and Hayato Yamana*

ERAHE: Edge-Offloaded Robust Attribute-Based Aggregate Scheme Enhanced with Homomorphic Encryption for 5G-Connected Delivery Drones 84
*Aagii Mariam Thomas and Sana Belguith*

QAGC: A Hybrid Quantum Walk Compiler for Scalable and High-Precision Attack Graph Analytics 100
*Mahesh Babu Chittem, Sriramulu Bojjagani and Anup Kumar Maurya*

Avatar Motion Signatures: Evaluating Linkability of Expressive De-Identification 112
*Fenja Schulz, Jan Marquenie, Carlos Franzreb, Tim Polzehl, Ingo Siegert and Sebastian Möller*

Transformers Can Do It: Recovering Types from Executables Using Transformer Based LLMs 119
*Ruturaj Vaidya and Prasad A. Kulkarni*

**SHORT PAPERS**


Securing Mobile Devices: An Analysis of Security Subsystems and Supply Chain Risks 133
*Stephan Spitz and Alexander Lawall*

Exploring Large Language Models for Trustworthy Use: Insights from Research and Development 141
*Sandeep Kalari, Sahithi Padidela, Vikas Ashok and Ravi Mukkamala*

Rotating Arrows Scheme: Shoulder Surfing Resistant Graphical Password System 149
*Hanadi Asfour, Hafez Barghouthi and Abdallah Karakra*

SoK: Challenges for Implementing Automated Cryptography Discovery and Inventory Tool 157
*Hiroki Yamamuro, Shusaku Uemura and Kazuhide Fukushima*

Enhancing Certified Robustness in Few-Shot Classification with Contrastive Loss and Defensive Noise in Fine-Tuning 169
*Hiroya Kato, Seira Hidano, Takao Murakami and Hideitsu Hino*

Decentralized Secure Authentication with DIDs and Ethereum Signatures: A Case Study in Immersive Environments 181
*Amira Talha, Faten Chaabane, Tarek Frikha, Claude Duvallet and Mohamed Ben Aouicha*

Cyberinfrastructure Resilience Index against Ransomware Using Markov Chain Modeling and Tensor Computation 189
*Fred Kembamba and Javed I. Khan*

Security and Detectability Analysis of Unicode Text Watermarking Methods against Large Language Models 197
*Malte Hellmeier*

Attacking a Segmented CFB Mode with a Predictable IV 205
*Novák Vojtěch, Kokeš Josef and Lórencz Róbert*

Scaling Android Hooking: Usability and Performance of Frida and Xposed for Mass API Interception 210
*Kris Heid, Dávid Zsolt Balatoni and Jens Heider*

WuppieFuzz: Coverage-Guided, Stateful REST API Fuzzing 221
*Thomas Rooijakkers, Anne Nijsten, Cristian Daniele, Erieke Weitenberg, Ringo Groenewegen and Arthur Melissen*

Systematic Construction and Experimental Evaluation of a Cybersecurity Threat Catalogue 232
*Finn Siegismund-Poschmann and Jörn Eichler*

Show Me What You Got: Vulnerabilities of Industrial Components Revealed by Automated Blackbox Testing 240
*Anne Borcherding, Mark Leon Giraud and Laura Tzigiannis*

HEALED: Hybrid Homomorphic Encryption for Analysis of Large-Scale Encrypted Data 252
*Maria João Dias, Ivan Costa, Ivone Amorim, Eva Maia and Isabel Praça*

Privacy-Preserving Protocol for Computing Majority with Adjustable Threshold 260
*Kittiphop Phalakarn*

LLM-Driven Python-to-Rust Translation for Efficient and Safe Code for Neural Networks: llm4py2rs 268
*Rupesh Raj Karn, Johann Knechtel, Siddharth Garg, Ramesh Karri and Ozgur Sinanoglu*

Enhancing Robustness against Transient Variability in Touch-Based Authentication via Cluster-Wise Feature Dropout Ensemble 278
*Taiki Furukawa and Hayato Yamana*

Securing Hyper-Dimensional Computing: A Locking Mechanism with FPGA Implementation 289
*Rupesh Raj Karn, Paul R. Genssler, Hussam Amrouch and Ozgur Sinanoglu*

Simple Power Analysis of Polynomial Multiplication in HQC 299
*Pavel Velek, Tomáš Rabas and Jiří Buček*

Method for Reducing Atmospheric Turbulence Effects Using Multiple Invisible Laser Irradiation for Dynamic Fake QR Codes 307
*Ayari Higashiizumi, Dai Itakura, Masayoshi Matsui, Taiga Manabe, Hiroshi Yamamoto, Yoshihisa Takayama and Toshihiro Ohigashi*

Log-Based Authentication via Cybernetic Avatars: Data Type Categorization Focused on Authenticated Game Character Information 315
*Ryosuke Kobayashi, Mhd Irvan, Franziska Zimmer, Maharage Nisansala Sevwandi Perera and Rie Shigetomi Yamaguchi*

When Only Parts Matter: Efficient Privacy-Preserving Analytics with Fully Homomorphic Encryption 323
*Alexandros Bakas and Dimitrios Schoinianakis*

A Comparison of Selected Image Transformation Techniques for Malware Classification 334
*Rishit Agrawal, Kunal Bhatnagar, Andrew Do, Ronnit Rana, Martin Jureček and Mark Stamp*

Towards AI-Driven Framework of Automating Cloud Security Orchestration 345
*Hamza Aabirouche, Eddy Caron and Redhouane Messaoud*

Detecting Cryptographically Relevant Software Packages with Collaborative LLMs 354
*Eduard Hirsch, Kristina Raab, Tobias J. Bauer and Daniel Loebenberger*

Anonymous Location-Based Advertising with Fine-Grained Statistics 366
*Gizem Akman, Kuan Eeik Tan and Valtteri Niemi*

Automated Distribution of Out-of-Band Key Material in Virtual Private Networks 376
*David Schatz, Hedwig Koerfgen and Guenter Schaefer*

Prevention of Bitcoin Loot in Bitcoin Lightning Network 388
*Sujit Sangram Sahoo, Akash Kumar, Pravas Ranjan Bal and Abinash Mishra*

Multi-Modal Model for Embedding Network and Audit Data for IoT Anomaly Detection 396
*Pratyush Singh, Yuxiang Huang, Haoxiang Li, George Oikonomou and James Pope*

Ontology-Driven Detection of Traffic Light Manipulation in Intelligent Transportation Systems 406
*Elena Cardillo, Marco De Vincenzi, Maria Taverniti and Ilaria Matteucci*

Non-Authorized User Detection Using Pupils Position Information During Inputting PIN Codes 414
*Sachi Fujimoto and Masaki Inamura*

A Pragmatic Comparison of Cryptographic Computation Technologies for Machine Learning 422
*Marcus Taubert, Adam Skuta and Thomas Lorünser*

G.H.O.S.T: A Scalable Framework for Metadata-Resistant Messaging with Token-Based Incentives 431
*Igor Khokhlov, Yuriy Khokhlov and Owen Weissman*

Physical Privacy through Reconfigurable Intelligent Surfaces on Visible Light Communication Systems 439
*Everton Alex Matos, Lucas Dias Hiera Sampaio and Luiz Carlos Pessoa Albini*

Offensive Security Testing of Aviation Systems: A Case Study of SWIM and Air Traffic Control Using the MITRE ATT&CK Framework 447
*Borna Radojčić, Severen Fernandes, Hannes Künstner, Jens Myrup Pedersen and Rasmus Løvenstein Olsen*

SyMoGen: A Python-Based Synthetic Mobility Generator for Privacy-Preserving Trajectory Research 459
*Fatih S. Bayram, Matvii Shevchenko, Clemens Krüger, Tim Mencin and Dominik Schoop*

On RBAC Maintenance for Preserving Confidentiality 467
*Franck Fotso Kuate, Omer Nguena Timo and Florent Avellaneda*

AUTHOR INDEX 475