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

Volume 1

Marbella, Spain
4-6 March 2026

ISBN: 979-8-3313-3345-4

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

MANAGEMENT AND OPERATIONS

FULL PAPERS

It Runs and It Hides: A Function-Hiding Construction for Private-Key Multi-Input Functional Encryption 13
Antonis Michalas and Alexandros Bakas

A Resource-Aware Cyber Emergency Response Framework for SMEs 27
Amar Almaini, Jakob Folz, Stefan Anthuber, Martin Schramm and Icyer Abdurrahman

Competency Requirements for Cybersecurity Professionals in Canadian Job Market: Organizational Convergences and Divergences 38
Sylvestre Uwizeyemungu, Thang Le Dinh and Tran Duc Le

Cybersecurity Maturity Assessment of the Northern Portugal: A NIST CSF–Aligned Baseline of SMEs and Public Bodies 49
Rogério Silva, António Pinto, Ivone Amorim and Isabel Praça

Effective Analysis of Encrypted Traffic for Mining Detection 61
Masahiro Ishii, Satoshi Shibuya and Keisuke Tanaka

Can Synthetic Spam Beat Real-World Detectors? Evaluating LLMs' Dual Role in Spam Generation and Detection 73
Tianyu Wang, Nianjun Zhou and Zhixiong Chen

Green by Design: Embedding Sustainability into Cybersecurity Architectures 85
Ângelo Borges and João Rafael Almeida

Incremental Federated Learning for Intrusion Detection in IoT Networks under Evolving Threat Landscape 97
Muaan Ur Rehman, Hayretdin Bahsi and Rajesh Kalakoti

SHORT PAPERS

The Assessment of Human Vulnerability in Cybersecurity on Efficacy, Awareness, Knowledge and Advocacy: A New Perspective 111
V. Sithira Vadivel, Peik Foong Yeap, Geoff Skinner and Noryanti Binti Muhammad

Do Japanese FemTech Users Consent without Reading Privacy Policies? Reasons for Use and Privacy Concerns of FemTech 118
Sachiko Kanamori, Hirotsune Sato and Naoya Tabata

Silent Shield: Dynamic Instrumentation of Privacy Breaches in Oculus VR Applications 127
Fadi Yilmaz, Bilge Kelesoglu, Kursat Korkmaz, Beyza Karakurt and Gurkan Agir

Tackling over Privilege: Resolving Access Concerns in Android Mobile Applications 136
Osamah Taha and Abdallah Karakra

A Framework for near-Real-Time Intrusion Detection in Micro-Enterprise Environments 144
Selahattin Hürol Türen, Rafiqul Islam, Kenneth Eustace and Geoffrey Fellows

From Poison to Antidote: Advancing Cybersecurity Education with AI Attack and Defense Training
Angelos Spyridon Kourtesis, Christian Leka, Konstantinos Lazaros, Aristidis G. Vrahatis and Christoforos Ntantogian 153

Analysing Multidisciplinary Approaches to Fight Large-Scale Digital Influence Operations
David Arroyo, Rafael Mata Milla, Marc Almeida Ros, Nikolaos Lykousas, Ivan Homoliak, Constantinos Patsakis and Fran Casino 161

Synthesising Attack Trees with Optimal Shape and Labelling 169
Olga Gadyatskaya, Sjouke Mauw, Rolando Trujillo-Rasua and Tim A. C. Willemse

SL1C3D: Slicer Library Injection for Covert 3D Data 177
Sai Gayatri Annamreddy, Paulo Costa and Matthew Jablonski

CARLE: Context Aware Recognition of maLicious Emails 185
Pedro Afonso, Eva Maia, Ivone Amorim and Isabel Praça

Malware Detection through System Call Vectorization and Neural Network Classification 193
Aleš Répáš, Simona Fornůsek and Róbert Lórencz

HEALTH-DP: A Framework for Health Data De-Anonymization Risk Assessment and Mitigation with Differential Privacy 201
Hamza Aguelal, Akasha Shafiq and Paolo Palmieri

Designing Secure Manufacturing-as-a-Service Platforms: Threat Modeling and Cybersecurity Risk Assessment 213
Kaspars Ābelnīca, Giacomo Leopizzi, Rūta Pirta, Jānis Grabis and Beāte Krauze

Cryptographic Vulnerability Detection in Code: A Hybrid Syntactic and Semantic Analysis Framework
Krishna Vellamchety, Maryam Abbasalizadeh, Areej Alnahdi, Pranathi Rayavaram, Vaishali Mohan Pajai and Sashank Narain 221

Exploring Factors of Organizational Culture that Promote Adherence to Security Rules 233
Yukiko Sawaya, Takamasa Isohara, Ayumu Kubota and Ayako Komatsu

Monitoring and Economic Sustainability: Preliminary Insights 241
Antonello Calabrò, Eda Marchetti and Albina Orlando

Design and First Evaluation of a Matrix-Based PUF Authentication Scheme for Blockchain-Based Tracking 249
Stefano Bistarelli, Ivan Mercanti, Igor Neri and Francesco Santini

On Addressing Isolation in Blockchain-Based Self-Sovereign Identity 257
Andreea Elena Drăgnoiu, Andrei Ciobanu and Ruxandra F. Olimid

Reflections of Social Engineering Awareness Negligence in Facilitating Cyber-Physical Attacks 265
Luís Filipe Gomes, Luís Miguel Batista and João Rafael Almeida

Evaluating the Effectiveness of Multi-Agent Large Language Models for Automated Vulnerable Code Repair 273
Martin Kilgi and Hayretdin Bahsi

Machine Learning-Based Security Solutions for Smart TVs: Mitigating Vulnerabilities and Enhancing Privacy in Smart Home Networks 284
Bilel Arfaoui, Hichem Mrabet and Abderrazak Jemai

STSRS: A New Dataset for Simulating Security Threats in Smart Railway Systems 292
Mays Abukeshek, Mohammed Al-Mhiqani and Simon Parkinson

A Lightweight Static Analysis Method for Identifying Hardcoded Vulnerabilities in Android Applications 300
Akira Kanaoka

A Tool for the Verification and Visualization of GDPR Compliance 308
Yassine Abich, Chebrine Ghiles and Clara Bertolissi

An Analysis of Modern Web Security Vulnerabilities Inside WebAssembly Applications 317
Lorenzo Corrias, Lorenzo Pisu, Davide Maiorca and Giorgio Giacinto

Similarity Is Not Enough: Issues with Adversarial Perturbations of Traffic Features against Intrusion Detection Systems 325
Marta Catillo, Antonio Pecchia and Umberto Villano

Cybersecurity Exercise Generation System Using LLMs with Real Attack Datasets 333
Hirokazu Hasegawa and Hiroki Takakura

Evolution and Perspectives of the Keep IT Secure Ecosystem: A Six-Year Analysis of Cybersecurity Experts Supporting Belgian SMEs 340
Christophe Ponsard, Jean-François Daune, Denis Darquennes, Malik Bouhou and Nicolas Point

A Tandem Approach to CPS Threat Modeling 348
Dallas Elleman and John Hale

A Contextualized Cybersecurity Incident Remediation Ontology 358
Rayan Kanawati, Nadira Lammari and Nada Mimouni

Detecting and Explaining Malware Family Evolution Using Rule-Based Drift Analysis 366
Olha Jurečková and Martin Jureček

Securing Critical Electric Vehicle Charging Infrastructure: Risk Assessment and Mitigation Using MITRE TARA 375
Xuemeng Yao, Elias Seid and Fredrik Blix

APPLICATIONS AND SERVICES

FULL PAPERS

Video Traffic Detection in VPN Network Using Lightweight Machine Learning Models 387
Ludovic Chavalarias, Johann Laurent, Nicolas Bohelay and Dominique Heller

VESPA: Vulnerability-Enhanced Selective Privacy Preservation Adaptation against Nucleotide Inference for Genomic Embeddings in Large Language Models 396
Reem Al-Saidi, Erman Ayday and Ziad Kobti

A Systematic Review of Artificial Intelligence in Air and Missile Defence 410
Gabriel Guerrero-Contreras, Sara Balderas-Díaz, Leopoldo Gutiérrez-Galeano, Germán Fuentes Landi and Juan José Domínguez-Jiménez

Breaking TEMPEST: Low-Frequency Bidirectional Covert Channel on Power Lines 422
Thien Dan Balsdon, Arthur Grisel-Davy and Sebastian Fischmeister

Advancing Security Incident Analysis with LLMs: A Study Using a Novel Security Log Dataset 434
Artur Nikitchuk and Hayretdin Bahsi

Can Knowledge of Demographics and Privacy Parameters Break Location Privacy? 448
Maja Schneider, Charini Nanayakkara, Peter Christen, Erik Buchmann and Erhard Rahm

Investigating the Influence of Black-Box Adversarial Machine Learning Attacks in Live Network Environments 462
Udaya Bhaskar Guntupalli, Medha Pujari, Jalal Abdel Halim and Weiqing Sun

Enhancing Continual Learning for Software Vulnerability Prediction: Addressing Catastrophic Forgetting via Hybrid@x -Confidence@x -Aware Selective Replay for Temporal LLM Fine-Tuning 474
Xuhui Dou, Hayretdin Bahsi and Alejandro Guerra-Manzanares

SHORT PAPERS

ML-Based Intrusion Detection in IoT/IIoT with Privacy-Aware Offloading to Cloud SIEM 489
Emmanuel Tuyishime, Petru A. Cotfas, Titus C. Balan, Alexandre Rekeraho, Daniel T. Cotfas and Vlad Popescu

A Modular GDPR Compliance Framework for Content Management Systems: Architectural Coordination and Performance Optimization in Plugin-Based Environments 497
Panagiotis Nikolaidis and Costas Iordanou

Uncertainty-Aware Reinforcement Learning for Zero Trust: An Empirical Evaluation of PPO, MC Dropout, and Bayesian Neural Networks 505
Vikram Kalekar

Emergency Traffic Control with Capability-Based Access Control for the V2X Communication Environment 515
Ryu Watanabe, Jun Kurihara, Toshiaki Tanaka and Kouichi Sakurai

Detecting Attack Patterns in Windows Registry Using CTI: A BERT-Based Approach 524
Leanne Briffa, Claudia Borg and Mark Vella

BetChain: Reinventing e-Betting with Trustless NFT-Driven Bets 533
Alexios Lymperis, Harald Gjermundrød and Ioanna Dionysiou

Boosting Phishing Detection with Graph Neural Networks 541
Dominique Portenier, Noah Lichtenecker and Ariane Trammell

MAWIFlow Benchmark: Realistic Flow-Based Evaluation for Network Intrusion Detection 549
Joshua Schraven, Alexander Windmann and Oliver Niggemann

Enhanced Malicious URL Filtering in Big Data Systems Using Machine Learning and Bloom Filters 557
Abdeslam El-yahyaoui, Ahmed Lbouchouari and Mohammed Erradi

Utilising Cloud Services in Local Governments as Digital Transformation Booster by Mastering Information Security Duties 565
Michael Diener and Thomas Meuche

A Scrutiny of SLMs' Performances for Mobile Malware Detection 577
Zhe Deng, Ants Torim, Hayretdin Bahsi and Sadok Ben Yahia

FIDELIS: Blockchain-Enabled Protection against Poisoning Attacks in Federated Learning 586
Jane Carney, Kushal Upreti, Gaby G. Dagher and Tim Andersen

ReDoS-M: A Dataset of Multi-Label Regrettable Disclosures on Social Media 595
Hervais Simo, Michael Kreutzer and Javor Nikolov

DRAPEbot: An AI Chatbot Assistant for the DRAPE Platform 604
Anna Sellani, Francisco Bischoff and Ana Ferreira

Explainable Risk Translation Layer for Cloud Cybersecurity: From Technical Vulnerability Signals to Economic Impact 612
Celia Cabello Collado, Víctor Adsuar Abaldea, Antonio Jimeno Morenilla and Higinio Mora Mora

Exploring Robust Intrusion Detection: A Benchmark Study of Feature Transferability in IoT Botnet Attack Detection 620
Alejandro Guerra-Manzanares and Jialin Huang

MI^{2}DAS: A Multi-Layer Intrusion Detection Framework with Incremental Learning for Securing Industrial IoT Networks 632
Wei Lian and Alejandro Guerra-Manzanares

AUTHOR INDEX 645