

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

Volume 1

Porto, Portugal
20-22 February 2025

Editors:

**Robert Di Pietro
Karen Renaud
Paolo Mori**

ISBN: 979-8-3313-1861-1

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© (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 <i>Wenjing Lou</i>	5
Securing Ultra-Large Scale Infrastructures: Challenges and Opportunities <i>Awais Rashid</i>	7
Turing's Echo on Deceptive Machines: The Challenge of Distinguishing Human and AI Creations <i>Ahmad-Reza Sadeghi</i>	9

MANAGEMENT AND OPERATIONS

FULL PAPERS

Cybersecurity Challenges in Critical Infrastructure: A Perspective on Regulations and Competence in Luxembourg <i>Maxime Naval, Erik Perjons and Simon Hacks</i>	15
Prioritization of Exploit Codes on GitHub for Better Vulnerability Triage <i>Kentaro Kita, Yuta Gempei, Tomoaki Mimoto, Takamasa Isohara, Shinsaku Kiyomoto and Toshiaki Tanaka</i>	27
Revisiting Permission Piggybacking of Third-Party Libraries in Android Apps <i>Kris Heid, Elena Julia Sonntag and Jens Heider</i>	39
Evaluating Explainable AI for Deep Learning-Based Network Intrusion Detection System Alert Classification <i>Rajesh Kalakoti, Risto Vaarandi, Hayretudin Bahşi and Sven Nõmm</i>	47
Robust Blockchain-Based Federated Learning <i>Aftab Akram, Clémentine Gritti, Mohd Hazali Mohamed Halip, Nur Diyana Kamarudin, Marini Mansor, Syarifah Bahiyah Rahayu and Melek Önen</i>	59
ConCERTS: An IoT Cybersecurity Research Range for Education, Experimentation, and Security Research <i>Dave McKay, Matthew Bush, Marko Kovacevic and Atefeh Mashatan</i>	71
CDAC: Content-Driven Access Control Architecture for Smart Farms <i>Ghadeer I. Yassin and Lakshmish M. Ramaswamy</i>	83
Enabling Trusted Data Sharing in Data Spaces: PROTON - A Privacy-by-Design Approach to Data Products <i>Laura Schuiki, Christoph Stach, Corinna Giebler, Eva Hoos and Bernhard Mitschang</i>	95
Characterising and Categorising Anonymization Techniques: A Literature-Based Approach <i>Andrea Fieschi, Pascal Hirmer, Christoph Stach and Bernhard Mitschang</i>	107

SHORT PAPERS

A Customizable Security Risk Assessment Framework Using Multi-Attribute Decision Making for IoT Systems <i>Mofareh Waqdan, Habib Louafi and Malek Mouhoub</i>	121
A Value-Driven Approach to the Online Consent Conundrum: A Study with the Unemployed <i>Paul van Schaik and Karen Renaud</i>	133
Got Ya!: Sensors for Identity Management Specific Security Situational Awareness <i>Daniela Pöhn and Heiner Lüken</i>	141
Qualitative In-Depth Analysis of GDPR Data Subject Access Requests and Responses from Major Online Services <i>Daniela Pöhn and Nils Gruschka</i>	149
Designing Data Trustees: A Prototype in the Building Sector <i>Michael Steinert, Anna Maria Schleimer, Marcel Altendeitering and David Hick</i>	157
Evaluating Keystroke Dynamics Performance in e-Commerce <i>Xiaofei Wang, Andy Meneely and Daqing Hou</i>	167
Analyzing a Concurrent Self-Modifying Program: Application to Malware Detection <i>Walid Messahel and Tayssir Touili</i>	176
To Be or Not to Be (in the EU): Measurement of Discrepancies Presented in Cookie Paywalls <i>Andreas Stenwreth, Simon Täng and Victor Morel</i>	183
Real-Time Detection of Multi-File DOM-Based XSS Vulnerabilities Using Static Analysis: A Developer-Oriented Approach for Securing Web Applications <i>Akira Kanaoka and Shu Hiura</i>	191
Managing a Ransomware Attack: The Resilience of a Swedish Municipality – A Case Study <i>Anton Holmström</i>	199
Assessing Sweden’s Current Cybersecurity Landscape: Implications of NATO Membership <i>Nike Henriksén, Isak Lexert, Jakob Bergquist Dahn and Simon Hacks</i>	209
PenQuestEnv: A Reinforcement Learning Environment for Cyber Security <i>Sebastian Eresheim, Simon Gmeiner, Alexander Piglmann, Thomas Petelin, Robert Luh, Paul Tavalato and Sebastian Schrittwieser</i>	217
A Novel Pairing-Free ECC-Based Ciphertext-Policy Attribute-Based Proxy Re-Encryption for Secure Cloud Storage <i>Shivangi Shukla and Sankita J. Patel</i>	225
Defending Against Phishing Attacks on Cloud-Systems: What Has Been Studied? <i>Carlos Eduardo Araújo Cardoso Cidrão, Oskar Hermansson and Simon Hacks</i>	234
A Reflection on Process-Oriented Industrial IoT Security Management <i>Markus Hornsteiner, Linda Koelbel, Daniel Oberhofer and Stefan Schoenig</i>	242
CampusQuest: Motivating Computer Science Students for Cybersecurity from Day One <i>Luca Pöhler, Marko Schuba, Tim Höner, Sacha Hack and Georg Neugebauer</i>	254

Knowledge Modelling for Automated Risk Assessment of Cybersecurity and Indirect Patient Harms in Medical Contexts <i>Samuel M. Senior, Laura Carmichael, Steve Taylor, Mike Surridge and Xavier Vilalta</i>	263
A Conceptual SOC Framework for Air Traffic Management Systems <i>Wesley Murisa and Marijke Coetzee</i>	275
CASTL: A Composable Source Code Query Language for Security and Vulnerability Analysis <i>Blake Johnson and Rahul Simha</i>	283
An Alternative Approach to Federated Learning for Model Security and Data Privacy <i>William Briguglio, Waleed A. Yousef, Issa Traoré, Mohammad Mamun and Sherif Saad</i>	291
USB-IDS-TC: A Flow-Based Intrusion Detection Dataset of DoS Attacks in Different Network Scenarios <i>Marta Catillo, Antonio Pecchia and Umberto Villano</i>	302
Design of an Intelligent Trust Management Architecture for 5G Service Deployment <i>Samra Bouakkaz, Luis Suárez, Nora Cuppens and Frédéric Cuppens</i>	310
Iterative Learning-Based Intrusion Detection System for Performance Enhancement in Imbalanced Data Environments <i>Yu-Ran Jeon and Il-Gu Lee</i>	318
Cyber Threat Modeling of an LLM-Based Healthcare System <i>Neha Nagaraja and Hayretdin Bahsi</i>	325
Systematisation of Security Risk Knowledge Across Different Domains: A Case Study of Security Implications of Medical Devices <i>Laura Carmichael, Steve Taylor, Samuel M. Senior, Mike Surridge, Gencer Erdogan and Simeon Tverdal</i>	337
Exploring the Accuracy and Privacy Tradeoff in AI-Driven Healthcare Through Differential Privacy <i>Surabhi Nayak and Sara Nayak</i>	349
Data Collection in Cyber Exercises Through Monitoring Points: Observing, Steering, and Scoring <i>Tobias Pfaller, Florian Skopik, Lenhard Reuter and Maria Leitner</i>	355
Compliance Standards and Frameworks and Its Implications on Cybersecurity: A NIS2 Study Within the Swedish Automotive Industries <i>Adenike Adesina, Elias Seid, Fredrik Blix and Oliver Popov</i>	367
SABEC: Secure and Adaptive Blockchain-Enabled Coordination Protocol for Unmanned Aerial Vehicles(UAVs) Network <i>Hulya Dogan and Anton Setzer</i>	377
Topology-Driven Defense: Detecting Model Poisoning in Federated Learning with Persistence Diagrams <i>Narges Alipourjeddi and Ali Miri</i>	389
Secure Opportunistic Routing Protocol in VANETs <i>Eqbal Darraji, Iain Phillips and Asma Adnane</i>	397
Current Research, Challenges, and Future Directions in Stalkerware Detection Techniques for Mobile Ecosystems <i>Mounika Bonam, Pranathi Rayavaram, Maryam Abbasalizadeh, Claire Seungeun Lee, April Pattavina and Sashank Narain</i>	405

CyberWise: Virtual Security Learning Platform <i>Payton Howard, Mark Ferraro and Sajal Bhatia</i>	416
GAI-Driven Offensive Cybersecurity: Transforming Pentesting for Proactive Defence <i>Mounia Zaydi and Yassine Maleh</i>	426
FEST: A Unified Framework for Evaluating Synthetic Tabular Data <i>Weijie Niu, Alberto Huertas Celdran, Karoline Siarsky and Burkhard Stiller</i>	434
AUTHOR INDEX	445