

21st International Conference on Security and Cryptography (SECRYPT 2024)

Dijon, France
8-10 July 2024

Editors:

**Sabrina De Capitani Di Vimercati
Pierangela Samarati**

ISBN: 979-8-3313-0551-2

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

- Explainability and Privacy-Preserving Data-Driven Models 5
Vicenc Torra
- Artificial Intelligence for Biometrics 7
Vincenzo Piuri

PAPERS

FULL PAPERS

- From Plant to Lab: Industrial Emulation Tools for Real-World Security Testing in Industrial Control Systems 13
Argiro Anagnostopoulou, Thomas Papaloukas, George Stergiopoulos and Dimitris Gritzalis
- Attribute Threat Analysis and Risk Assessment for ABAC and TBAC Systems 26
Leonard Bradatsch, Artur Hermann and Frank Kargl
- Fuzzy Vault Security Enhancement Avoid Statistical Biases 40
Sara Majbour, Morgan Barbier and Jean-Marie Le Bars
- UPCARE: User Privacy-Preserving Cancer Research Platform 52
Georg Bramm, Melek Önen, Martin Schanzenbach, Ilya Komarov, Frank Morgner, Christian Tiebel and Juan Cadavid
- Verifying Artifact Authenticity with Unclonable Optical Tags 64
Mónica P. Arenas, Gabriele Lenzini, Mohammadamin Rakeei, Peter Y. A. Ryan, Marjan Škrobot and Maria Zhekova
- A Composition Algebra for Decentralized Enforcement of Access Control Policies with an Application to Vehicular Networks 78
Peter Amthor and René Gorges
- DYNAMO: Towards Network Attack Campaign Attribution via Density-Aware Active Learning 91
Helene Orsini and Yufei Han
- Characterization of Consensus Correctness in Ripple (XRP) Networks 103
Rudrapana K. Shyamasundar
- A Secure and Privacy-Preserving Authentication Scheme with a Zero-Trust Approach to Vehicle Renting in VANETs 114
Mahdi Akil, Leonardo Martucci and Jaap-Henk Hoepman
- On Privacy of RFID-Based Authentication Protocols 128
Ferucio Laurențiu Țiplea
- Backdoor Attacks During Retraining of Machine Learning Models: A Mitigation Approach 140
Matthew Yudin, Achyut Reddy, Sridhar Venkatesan and Rauf Izmailov

Perception of Privacy Tools for Social Media: A Qualitative Analysis Among Japanese <i>Vanessa Bracamonte, Yohko Orito, Yasunori Fukuta, Kiyoshi Murata and Takamasa Isohara</i>	151
Violence Detection: A Serious-Gaming Approach <i>Derkjan Elzinga, Stan Ruessink, Giuseppe Cascavilla, Damian Tamburri, Francesco Leotta, Massimo Mecella and Willem-Jan Van Den Heuvel</i>	163
DISC: A Dataset for Information Security Classification <i>Elijah Bass, Massimiliano Albanese and Marcos Zampieri</i>	175
A White-Box Watermarking Modulation for Encrypted DNN in Homomorphic Federated Learning <i>Mohammed Lansari, Reda Bellafqira, Katarzyna Kapusta, Vincent Thouvenot, Olivier Bettan and Gouenou Coatrieux</i>	186
Formal Analysis of C-ITS PKI Protocols <i>Mounira Msahli, Pascal Lafourcade and Dhekra Mahmoud</i>	198
Balancing Patient Privacy and Health Data Security: The Role of Compliance in Protected Health Information (PHI) Sharing <i>Md Al Amin, Hemanth Tummala, Rushabh Shah and Indrajit Ray</i>	211
Enhancing Privacy in Machine Learning: A Robust Approach for Preventing Attribute Inference Attacks <i>Myria Bouhaddi and Kamel Adi</i>	224
Classifying Human-Generated and AI-Generated Election Claims in Social Media <i>Alphaeus Dmonte, Marcos Zampieri, Kevin Lybarger, Massimiliano Albanese and Genya Coulter</i>	237
Towards a Cryptographic Model for Wireless Communication <i>Frederik Armknecht and Christian Müller</i>	249
Cache Side-Channel Attacks Through Electromagnetic Emanations of DRAM Accesses <i>Julien Maillard, Thomas Hiscock, Maxime Lecomte and Christophe Clavier</i>	262
MATRaCAE: Time-Based Revocable Access Control in the IoT <i>Clémentine Gritti, Emanuel Regnath and Sebastian Steinhorst</i>	274
Large-Scale Analysis of GitHub and CVEs to Determine Prevalence of SQL Concatenations <i>Kevin Dennis, Bianca Dehaan, Parisa Momeni, Gabriel Laverghetta and Jay Ligatti</i>	286
QuDPas-FHA: Quantum-Defended Privacy-Preserved Fast Handover Authentication in Space Information Networks <i>Arijit Karati, Ting-Yu Chen and Kai-Yao Lin</i>	298
Imperceptible QR Watermarks in High-Resolution Videos <i>Tymoteusz Lindner, Tomasz Hawro and Piotr Syga</i>	310
Code Obfuscation Classification Using Singular Value Decomposition on Grayscale Image Representations <i>Sebastian Raubitzek, Sebastian Schrittwieser, Caroline Lawitschka, Kevin Mallinger, Andreas Ekelhart and Edgar Weippl</i>	323
An ASM-Based Approach for Security Assessment of Ethereum Smart Contracts <i>C. Braghin, E. Riccobene and Simone Valentini</i>	334

Towards a Secure and Intelligent Access Control Policy Adapter for Big Data Environment <i>El Mostapha Chakir, Marouane Hachimi and Mohammed Erradi</i>	345
TI-NERmerger: Semi-Automated Framework for Integrating NER Datasets in Cybersecurity <i>Inoussa Mouiche and Sherif Saad</i>	357
SHORT PAPERS	
Higher Order Leakage Assessment and Neural Network-based Attack on CRYSTALS-Kyber <i>Buvana Ganesh, Mosabbah Mushir Ahmed and Alieeldin Mady</i>	373
K-Resilient Public Key Authenticated Encryption with Keyword Search <i>Koon-Ming Chan, Swee-Huay Heng, Syh-Yuan Tan and Shing-Chiang Tan</i>	381
An Extended Method for Transmitting Secret Messages in Textual Documents Based on Paragraph Resizing <i>Benjamin Aziz, Estabraq Makiyah and Aysha Bukhelli</i>	389
High-Speed Pipelined FPGA Implementation of a Robust Steganographic Scheme for Secure Data Communication Systems <i>Salah Harb, M. Omair Ahmad and M. N. S. Swamy</i>	397
Security Analysis for BB84 Key Distillation <i>Sara Nikula, Anssi Lintulampi and Kimmo Halunen</i>	407
MultiVD: A Transformer-based Multitask Approach for Software Vulnerability Detection <i>Claudio Curto, Daniela Giordano, Simone Palazzo and Daniel Gustav Indelicato</i>	416
SCWAD: Automated Pentesting of Web Applications <i>Natan Talon, Valérie Viet Triem Tong, Gilles Guette, Yufei Han and Youssef Laarouchi</i>	424
Dvorak: A Browser Credential Dumping Malware <i>José Areia, Bruno Santos and Mário Antunes</i>	434
The Use of the DWARF Debugging Format for the Identification of Potentially Unwanted Applications (PUAs) in WebAssembly Binaries <i>Calebe Helpa, Tiago Heinrich, Marcus Botacin, Newton C. Will, Rafael R. Obelheiro and Carlos A. Maziero</i>	442
Automating Compliance for Improving TLS Security Postures: An Assessment of Public Administration Endpoints <i>Riccardo Geremia, Salvatore Manfredi, Matteo Rizzi, Giada Sciarretta, Alessandro Tomasi and Silvio Ranise</i>	450
Organizing Records for Retrieval in Multi-Dimensional Range Searchable Encryption <i>Mahdieh Heidaripour, Ladan Kian, Maryam Rezapour, Mark Holcomb, Benjamin Fuller, Gagan Agrawal and Hoda Maleki</i>	459
Autoencoder for Detecting Malicious Updates in Differentially Private Federated Learning <i>Lucia Alonso and Mina Alishahi</i>	467
The IoT Breaches Your Household Again <i>Davide Bonaventura, Sergio Esposito and Giampaolo Bella</i>	475
A Formal Analysis of CIE Level 2 Multi-Factor Authentication via SMS OTP <i>Roberto Van Eeden, Matteo Paier and Marino Miculan</i>	483

Solving Access Control Conflicts in Multi-User Systems <i>Alba Martinez Anton, Clara Bertolissi and Jean-Marc Talbot</i>	492
CVE2CWE: Automated Mapping of Software Vulnerabilities to Weaknesses Based on CVE Descriptions <i>Massimiliano Albanese, Olutola Adebisi and Frank Onovae</i>	500
Amun: Securing E-Voting Against Over-the-Shoulder Coercion <i>Riccardo Longo and Chiara Spadafora</i>	508
Simulating SASCA on Keccak: Security Implications for Post-Quantum Cryptographic Schemes <i>Julien Maillard, Thomas Hiscock, Maxime Lecomte and Christophe Clavier</i>	518
Kex-Filtering: A Proactive Approach to Filtering <i>Fabrizio Baiardi, Filippo Boni, Giovanni Braccini, Emanuele Briganti and Luca Deri</i>	528
Improving the Efficiency of Intrusion Detection Systems by Optimizing Rule Deployment Across Multiple IDSs <i>Arka Ghosh, Massimiliano Albanese, Preetam Mukherjee and Amir Alipour-Fanid</i>	536
Utilizing Machine Learning for Optimizing Cybersecurity Spending in Critical Infrastructures <i>George Stergiopoulos, Michalis Detsis, Sozon Leventopoulos and Dimitris Gritzalis</i>	544
Bringing Binary Exploitation at Port 80: Understanding C Vulnerabilities in WebAssembly <i>Emmanuele Massidda, Lorenzo Pisu, Davide Maiorca and Giorgio Giacinto</i>	552
Safe or Scam? An Empirical Simulation Study on Trust Indicators in Online Shopping <i>Sebastian Schrittwieser, Andreas Ekelhart, Esther Seidl and Edgar Weippl</i>	560
Do You Trust Your Device? Open Challenges in IoT Security Analysis <i>Lorenzo Binosi, Pietro Mazzini, Alessandro Sanna, Michele Carminati, Giorgio Giacinto, Riccardo Lazzaretti, Stefano Zanero, Mario Polino, Emilio Coppa and Davide Maiorca</i>	568
Comparison of Access Control Approaches for Graph-Structured Data <i>Aya Mohamed, Dagmar Auer, Daniel Hofer and Josef Küng</i>	576
Membership Inference Attacks Against Indoor Location Models <i>Vahideh Moghtadaiee, Amir Fathalizadeh and Mina Alishahi</i>	584
Enhancing Privacy and Utility in Federated Learning: A Hybrid P2P and Server-Based Approach with Differential Privacy Protection <i>Luca Corbucci, Anna Monreale and Roberto Pellungrini</i>	592
POSTERS	
Black Sheep Wall: Towards Multiple Vantage Point-Based Information Space Situational Awareness <i>Bernhards Blumbergs</i>	605
Evaluating Digital Forensic Readiness: A Honeypot Approach <i>Philip Zimmermann and Sebastian Obermeier</i>	615
HydroLab: A Versatile Hydroelectric Power Lab for Security Research and Education <i>Sebastian Obermeier, Giorgio Tresoldi, Bernhard Tellenbach and Vincent Lenders</i>	622
LAMA: Leakage Abuse Attacks Against Microsoft Always Encrypted <i>Ryan Seah, Daren Khu, Alexander Hoover and Ruth Ng</i>	628

chiku: Efficient Probabilistic Polynomial Approximations Library <i>Devharsh Trivedi, Nesrine Kaaniche, Aymen Boudguiga and Nikos Triandopoulos</i>	634
On the Implementation of a Lattice-Based DAA for Vanet System <i>Doryan Lesaignoux and Mikael Carmona</i>	642
Towards Privacy-Preserving Multi-Cloud Identity Management Using SOLID <i>Alfredo Cuzzocrea and Islam Belmerabet</i>	649
Linkage Between CVE and ATT&CK with Public Information <i>Tomoaki Mimoto, Yuta Gempei, Kentaro Kita, Takamasa Isohara, Shinsaku Kiyomoto and Toshiaki Tanaka</i>	655
A Framework for Federated Analysis of Health Data Using Multiparty Homomorphic Encryption <i>Miroslav Puskaric</i>	661
A Performant Quantum-Resistant KEM for Constrained Hardware: Optimized HQC <i>Ridwane Aissaoui, Jean-Christophe Deneuville, Christophe Guerber and Alain Pirovano</i>	668
OIPM: Access Control Method to Prevent ID/Session Token Abuse on OpenID Connect <i>Junki Yuasa, Taisho Sasada, Christophe Kiennert, Gregory Blanc, Yuzo Taenaka and Youki Kadobayashi</i>	674
Encrypted KNN Implementation on Distributed Edge Device Network <i>B. Pradeep Kumar Reddy, Ruchika Meel and Ayantika Chatterjee</i>	680
GAN-based Seed Generation for Efficient Fuzzing <i>Shyamili Toluchuri, Aishwarya Upadhyay, Smita Naval, Vijay Laxmi and Manoj Singh Gaur</i>	686
InspectorLog: A New Tool for Offline Attack Detection over Web Log Trace Files <i>Jesús E. Díaz-Verdejo, Javier Muñoz-Calle, Rafael Estepa Alonso and Antonio Estepa Alonso</i>	692
An Efficient Hash Function Construction for Sparse Data <i>Nir Soffer and Erez Waisbard</i>	698
Securing Patient Data in IoT Devices: A Blockchain-NFT Approach for Privacy, Security, and Authentication <i>Farha Masroor, Adarsh Gopalakrishnan and Neena Goveas</i>	704
Towards an Adaptive Trust Management Model Based on ANFIS in the SIoT <i>Hamdi Ouechtati and Nadia Ben Azzouna</i>	710
Secure Multi-Party Traversal Queries over Federated Graph Databases <i>Nouf Aljuaid, Alexei Lisitsa and Sven Schewe</i>	716
Leveraging Deep Learning for Intrusion Detection in IoT Through Visualized Network Data <i>Amine Hattak, Fabio Martinelli, Francesco Mercaldo and Antonella Santone</i>	722
FPGA Implementation of AES-Based on Optimized Dynamic s-Box <i>Calvo Mayaudón Haroldo, Nakojah Chris David, Mahdi Madani and El-Bay Bourennane</i>	730
Privacy-Preserving Anomaly Detection Through Sampled, Synthetic Data Generation <i>Fatema Rashid and Ali Miri</i>	738
Spellchecker Analysis for Behavioural Biometric of Typing Errors Scenario <i>Bartłomiej Marek and Wojciech Wodo</i>	748

Enhancing Adversarial Defense in Behavioral Authentication Systems Through Random Projections <i>Md Morshedul Islam and Md Khairul Anam</i>	758
Lightweight Cryptographic Algorithms: A Position Paper <i>Gabriela Mendes Corrêa de Miranda, José Antônio Moreira Xexéo and Renato Hidaka Torres</i>	764
An Uncertain Reasoning-Based Intrusion Detection System for DoS/DDoS Detection <i>Harpreet Singh, Habib Louafi and Yiyu Yao</i>	771
Manipulating Prompts and Retrieval-Augmented Generation for LLM Service Providers <i>Aditya Kuppaa, Jack Nicholls and Nhien-An Le-Khac</i>	777
Revolutionizing Blockchain Consensus: Towards Deliberative and Unanimous Agreement <i>Syed Badruddoja, Ram Dantu, Mark Dockendorf, Abiola Salau and Kritagya Upadhyay</i>	786
Compact Representation of Digital Camera's Fingerprint with Convolutional Autoencoder <i>Jarostaw Bernacki and Rafal Scherer</i>	792
On the Privacy Afforded by Opaque Identifiers in Traffic Monitoring <i>Marcus Gelderie</i>	798
QPTA: Quantum-Safe Privacy-Preserving Multi-Factor Authentication Scheme for Lightweight Devices <i>Basker Palaniswamy and Arijit Karati</i>	804
Toward the Foundation of Digital Identity Theory <i>Pierre Fobougong Saha, Mohamed Mejri and Kamel Adi</i>	812
Local Differential Privacy for Data Clustering <i>Lisa Bruder and Mina Alishahi</i>	820
Open-Source Post-Quantum Encryptor: Design, Implementation and Deployment <i>Petr Tuma, Jan Hajny, Petr Muzikant, Jan Havlin, Lukas Malina, Patrik Dobias and Jan Willemson</i>	826
Graph-Based Modelling of Maximum Period Property for Nonlinear Feedback Shift Registers <i>Eric Filiol and Pierre Filiol</i>	832
BlueDoS: A Novel Approach to Perform and Analyse DoS Attacks on Bluetooth Devices <i>Poonam Namdeo Shelke, Saurav Gupta and Sukumar Nandi</i>	838
Enhancing OpenID Connect for Verifiable Credentials with DIDComm <i>Roberto De Prisco, Sergiy Shevchenko and Pompeo Faruolo</i>	844
Balancing Act: Navigating the Privacy-Utility Spectrum in Principal Component Analysis <i>Saloni Kwatra, Anna Monreale and Francesca Naretto</i>	850
Malware Analysis Using Transformer Based Models: An Empirical Study <i>Abhishek Joshi, Divyateja Pasupuleti, P. Nischith, Sarvesh Sutaone, Soumil Ray, Soumyadeep Dey and Barsha Mitra</i>	858
Virtually Free Randomisations of NTT in RLWE Cryptosystem to Counteract Side Channel Attack Based on Belief Propagation <i>Christophe Negre and Mbaye Ngom</i>	866
Property Inference as a Regression Problem: Attacks and Defense <i>Joshua Stock, Lucas Lange, Erhard Rahm and Hannes Federrath</i>	876

