2024 21st Annual International Conference on Privacy, Security and Trust (PST 2024)

Sydney, Australia
28-30 August 2024

IEEE Catalog Number: CFP2404F-POD
ISBN: 979-8-3503-6710-2

**Copyright © 2024 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

***** *This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP2404F-POD
ISBN (Print-On-Demand):	979-8-3503-6710-2
ISBN (Online):	979-8-3503-6709-6
ISSN:	2574-139X

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
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

Table of Contents

Visualizing Differential Privacy: Assessing Infographics' Impact on Layperson Data-sharing Decisions and Comprehension 1
Mst Mahamuda Sarkar Mithila, Fangyi Yu, Miguel Vargas Martin and Shengqian Wang

"I was diagnosed with...": sensitivity detection and rephrasing of Amazon reviews with ChatGPT 14
Costanza Alfieri, Suryia Ganesh, Limin Ge, Jingxin Shi and Norman Sadeh

Efficient Integration of Exchange Chains in Privacy-Preserving Kidney Exchange 26
Malte Breuer, Ulrike Meyer and Susanne Wetzel

Synthetic Trajectory Generation Through Convolutional Neural Networks 36
Jesse Merhi, Erik Buchholz and Salil S. Kanhere

Quantifying Privacy in Cooperative Awareness Services Through Trajectory Reconstruction 48
Atthapan Daramas, Vimal Kumar and Marinho Barcellos

Effectiveness of Privacy-Preserving Algorithms for Large Language Models: A Benchmark Analysis 58
Jinglin Sun, Basem Suleiman and Imdad Ullah

Pk-Anonymization Meets Differential Privacy 66
Masaya Kobayashi, Atsushi Fujioka, Koji Chida, Akira Nagai and Kan Yasuda

Malicious Unlearning in Ensemble Models 77
Huanyi Ye, Ziyao Liu, Yu Jiang, Jiale Guo and Kwok-Yan Lam

Group Signatures with Designated Traceability over Openers' Attributes from Symmetric-Key Primitives 83
Hiroaki Anada, Masayuki Fukumitsu and Shingo Hasegawa

PEL: Privacy Embedded Learning in Smart Healthcare Systems 92
Mahmuda Akter, Nour Moustafa and Benjamin Turnbull

Post-Quantum Authentication and Integrity in 3-Layer IoT Architectures 102
Juliet Samandari and Clémentine Gritti

An Efficient Method for Accelerating Kyber and Dilithium Post-Quantum Cryptography . 113
Duc-Thuan Dam, Trong-Hung Nguyen, Thai-Ha Tran, Binh Kieu-Do-Nguyen, Trong-Thuc Hoang and Cong-Kha Pham

DID Link: Authentication in TLS with Decentralized Identifiers and Verifiable Credentials 118
Sandro Rodriguez Garzon, Dennis Natusch, Artur Philipp, Axel Küpper, Hans Joachim Einsiedler and Daniela Schneider

Mobile Login Bridge: Subverting 2FA and Passwordless Authentication via Android Debug Bridge 129
Ahmed Tanvir Mahdad and Nitesh Saxena

PrivBench: A Benchmark Capturing Privilege Escalation Vulnerabilities in Android 141
Mohammed-El-Amin Tebib, Oum-El-Kheir Aktouf, Pascal André and Mariem Graa

Model-Based Security Analysis of Interconnected Subsystems: A Methodology for Security Compatibility Evaluation 153
Mohamed Abdelsalam, Isaac Mpidi Bita, Simon Greiner, Oum-El-Kheir Aktouf and Annabelle Mercier

Efficient Data Security Using Predictions of File Availability on the Web 164
Kevin Saric, Gowri Sankar Ramachandran, Raja Jurdak and Surya Nepal

DevilDiffusion: Embedding Hidden Noise Backdoors into Diffusion Models 176
William Aiken, Paula Branco and Guy-Vincent Jourdan

Disease Detector: A Disease Inference Attack Using Brainwave Signals Associated with Body Postures 187
Anuradha Mandal and Nitesh Saxena

DEFD: Dual-Entity Fuzzy Deduplication for Untrusted Environments 199
Zehui Tang, Shengke Zeng, Song Han, Qi Yu, Shihai Jiang and Peng Chen

Extending ISO 15118-20 EV Charging: Preventing Downgrade Attacks and Enabling New Security Capabilities 210
Ross Porter, Morteza Biglari-Abhari, Duleepa Thrimawithana and Benjamin Tan

Poisoning and Evasion: Deep Learning-Based NIDS under Adversarial Attacks 219
Hesamodin Mohammadian, Arash Habibi Lashkari and Ali Ghorbani

Hardware Implementation of a Hybrid Dynamic Gold Code-Based Countermeasure Against Side-Channel Attacks 228
Thai-Ha Tran, Duc-Thuan Dam, Binh Kieu-Do-Nguyen, Van-Phuc Hoang, Trong-Thuc Hoang and Cong-Kha Pham

CompFreeze : Combining Compacters and Layer Freezing for Enhanced Pre-Trained Language Model 233
Saurabh Anand, Shubham Malaviya, Manish Shukla and Sachin Lodha

Enhancing Network Intrusion Detection Systems: A Review of Feature Selection Algorithms for Streaming Data Processing 242
Abdelfattah Amamra, Rym Khettab and Raissa Mezine

Experimental Demonstration of Risks and Influences of Cyber Attacks on Wireless Communication in Microgrids 252
Zhibo Zhang, Jiankun Hu, Hemanshu Pota, Shabnam Kasra, Benjamin Turnbull, Ernesto Damiani and Chan Yeob Yeun

can-fp: An attack-aware analysis of false alarms in automotive intrusion detection models 257
Brooke Kidmose and Weizhi Meng

A Comprehensive Study on Multi-Task Learning for Domain Generation Algorithm (DGA) Detection 269
Arthur Drichel and Ulrike Meyer

Stake-Driven Rewards and Log-Based Free Rider Detection in Federated Learning 279
Huong Nguyen, Hong-Tri Nguyen, Lauri Loven and Susanna Pirttikangas

Proactive Audio Authentication using Speaker Identity Watermarking 289
Qi Li and Xiaodong Lin

MIKA: A Minimalist Approach to Hybrid Key Exchange 299
Raymond K. Zhao, Nazatul H. Sultan, Phillip Yialeloglou, Dongxi Liu, David Liebowitz and Josef Pieprzyk

Towards SAR Automatic Target Recognition Multi- Category SAR Image Classification Based on Light Weight Vision Transformer 310
Guibin Zhao, Pengfei Li, Zhibo Zhang, Fusen Guo, Xueting Huang, Wei Xu, Jinyin Wang and Jianlong Chen

Lack of Systematic Approach to Security of IoT Context Sharing Platforms 316
Mohammad Goudarzi, Arash Shaghaghi, Simon Finn and Sanjay Jha

AI Efficiency in Cybersecurity: Estimating Token Consumption for Optimal Operations . . 320
Emma Romanous and Jeremy Ginger

Cybersecurity in Industry 5.0: Open Challenges and Future Directions 325
Bruno Santos, Rogério Costa and Leonel Santos

Privacy Preservation in Service Operations by Minimizing Sensitive Data Exposure 331
Rishabh Kumar, Rohit Gupta, Sutapa Mondal, Mangesh Gharote, Praveen Gauravaram and Sachin Lodha

The Value of Strong Identity and Access Management for ICS/OT Security 336
Mohammad Reza Nosouhi, Zubair Baig, Robin Doss, Praveen Gauravaram, Debi Prasad Pati, Divyans Mahansaria, Keshav Sood and Lei Pan

Towards a Portability Scheme for Decentralized Identifiers in Self-Sovereign Identities 341
Joao Pedro Alonso Almeida, Gowri Ramachandran, Paul Ashley, Raja Jurdak, Steven McCown and Jo Ueyama

Insource vs Outsourcing Offensive Security Operations 345
Jason Ford and Caleb House