

20th International Conference on Security and Cryptography (SECRYPT 2023)

Rome, Italy
10-12 July 2023

Editors:

**Sabrina De Capitani di Vimercati
Pierangela Samarati**

ISBN: 978-1-7138-7649-6

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© (2023) by SCITEPRESS – Science and Technology Publications, Lda.
All rights reserved.

Printed with permission by Curran Associates, Inc. (2023)

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

The Certification Panacea
Rigo Wenning 5

Large Language Models for Code Obfuscation Evaluation of the Obfuscation Capabilities of OpenAI's GPT-3.5 on C Source Code
Patrick Kochberger, Maximilian Gramberger, Sebastian Schrittwieser, Caroline Lawitschka and Edgar R. Weippl 7

PAPERS

FULL PAPERS

MEMES: Memory Encryption-Based Memory Safety on Commodity Hardware
David Schrammel, Salmin Sultana, Karanvir Grewal, Michael LeMay, David M. Durham, Martin Unterguggenberger, Pascal Nasahl and Stefan Mangard 25

K-Anonymous Privacy Preserving Manifold Learning
Sonakshi Garg and Vıcenç Torra 37

AIS Authentication Using Certificateless Cryptography
Axel Rousselot, Nora Cuppens and Samra Bouakkaz 49

CAPoW: Context-Aware AI-Assisted Proof of Work Based DDoS Defense
Trisha Chakraborty, Shaswata Mitra and Sudip Mittal 62

Adapting P2P Mixnets to Provide Anonymity for Uplink-Intensive Applications
Francesco Buccafurri, Vincenzo De Angelis and Sara Lazzaro 73

Classical to Post-Quantum Secure ABE-IBE Proxy Re-Encryption Scheme
Muhammad Nauman Khan, Asha Rao, Seyit Camtepe and Josef Pieprzyk 85

ZT-NIDS: Zero Trust, Network Intrusion Detection System
Abeer Z. Alalmaie, Priyadarsi Nanda and Xiangjian He 99

On the Effectiveness of Re-Identification Attacks and Local Differential Privacy-Based Solutions for Smart Meter Data
Zeynep Sila Kaya and M. Emre Gursoy 111

A First Appraisal of Cryptographic Mechanisms for the Selective Disclosure of Verifiable Credentials
Andrea Flamini, Silvio Ranise, Giada Sciarretta, Mario Scuro, Amir Sharif and Alessandro Tomasi 123

BeeHIVE: Behavioral Biometric System Based on Object Interactions in Smart Environments
Klaudia Krawiecka, Simon Birnbach, Simon Eberz and Ivan Martinovic 135

Griffin: Towards Mixed Multi-Key Homomorphic Encryption
Thomas Schneider, Hossein Yalame and Michael Yonli 147

Informed Consent as Patient Driven Policy for Clinical Diagnosis and Treatment: A Smart Contract Based Approach <i>Md Al Amin, Amani Altarawneh and Indrajit Ray</i>	159
Using Untrusted and Unreliable Cloud Providers to Obtain Private Email <i>Nicolas Chiapputo, Yvo Desmedt and Kirill Morozov</i>	171
Towards Usable Scoring of Common Weaknesses <i>Olutola Adebiyi and Massimiliano Albanese</i>	183
Heterogeneous Graph Storage and Leakage Prevention for Data Cooperatives <i>Mark Dockendorf and Ram Dantu</i>	192
Generic Blockchain on Generic Human Behavior <i>Clémentine Gritti, Frédéric A. Hayek and Pascal Lafourcade</i>	206
Smart Bulbs Can Be Hacked to Hack into Your Household <i>Davide Bonaventura, Sergio Esposito and Giampaolo Bella</i>	218
Optimizing Attribute-Based Encryption for Circuits Using Compartmented Access Structures <i>Alexandru Ioniță</i>	230
RSSI-Based Fingerprinting of Bluetooth Low Energy Devices <i>Guillaume Gagnon, Sébastien Gambs and Mathieu Cunche</i>	242
Receipt-Free Electronic Voting from zk-SNARK <i>Maryam Sheikhi, Rosario Giustolisi and Carsten Schuermann</i>	254
Anomaly-Based Intrusion Detection System for DDoS Attack with Deep Learning Techniques <i>Davide Agostinello, Angelo Genovese and Vincenzo Piuri</i>	267
SHORT PAPERS	
Privacy Protection of Synthetic Smart Grid Data Simulated via Generative Adversarial Networks <i>Kayode S. Adewole and Vicenç Torra</i>	279
JShelter: Give Me My Browser Back <i>Libor Polčák, Marek Saloň, Giorgio Maone, Radek Hranický and Michael McMahon</i>	287
Threshold Cryptosystems Based on 2^k -th Power Residue Symbols <i>George Teşeleanu</i>	295
Improvement of Winternitz OTS with a Novel Fingerprinting Function <i>Motonari Honda and Yuichi Kaji</i>	303
Lessons Learned: Defending Against Property Inference Attacks <i>Joshua Stock, Jens Wettlaufer, Daniel Demmler and Hannes Federrath</i>	312
When the Few Outweigh the Many: Illicit Content Recognition with Few-Shot Learning <i>G. Cascavilla, G. Catolino, M. Conti, D. Mellios and D. A. Tamburri</i>	324
Context-Aware Behavioral Fingerprinting of IoT Devices via Network Traffic Analysis <i>Arjun Prasad, Kevin Kanichery Biju, Soumya Somani and Barsha Mitra</i>	335
One to Bind Them: Binding Verifiable Credentials to User Attributes <i>Alexander Mühle, Katja Assaf and Christoph Meinel</i>	345

A Note on a CBC-Type Mode of Operation <i>George Teșeleanu</i>	353
On the Security of the Novel Authentication Scheme for UAV-Ground Station and UAV-UAV Communication <i>Mustapha Benssalah and Karim Drouiche</i>	361
SEBDA: A Secure and Efficient Blockchain Based Data Aggregation Scheme <i>Sehrish Shafeeq and Mathias Fischer</i>	369
Risk-Based Illegal Information Flow Detection in the IIoT <i>Argiro Anagnostopoulou, Ioannis Mavridis and Dimitris Gritzalis</i>	377
A Method for Robust and Explainable Image-Based Network Traffic Classification with Deep Learning <i>Amine Hattak, Giacomo Iadarola, Fabio Martinelli, Francesco Mercaldo and Antonella Santone</i>	385
Towards a Geometric Deep Learning-Based Cyber Security: Network System Intrusion Detection Using Graph Neural Networks <i>Rocco Zaccagnino, Antonio Cirillo, Alfonso Guarino, Nicola Lettieri, Delfina Malandrino and Gianluca Zaccagnino</i>	394
Trans-IDS: A Transformer-Based Intrusion Detection System <i>El Mahdi Mercha, El Mostapha Chakir and Mohammed Erradi</i>	402
Regulating Cyber Incidents: A Review of Recent Reporting Requirements <i>Angelica Marotta and Stuart Madnick</i>	410
BAGUETTE: Hunting for Evidence of Malicious Behavior in Dynamic Analysis Reports <i>Vincent Raulin, Pierre-François Gimenez, Yufei Han and Valérie Viet Triem Tong</i>	417
PIUDI: Private Information Update for Distributed Infrastructure <i>Shubham Raj, Snehil Joshi and Kannan Srinathan</i>	425
OCScraper: Automated Analysis of the Fingerprintability of the iOS API <i>Gerald Palfinger</i>	433
XACML Extension for Graphs: Flexible Authorization Policy Specification and Datastore-Independent Enforcement <i>Aya Mohamed, Dagmar Auer, Daniel Hofer and Josef Küng</i>	442
Automated Feature Engineering for AutoML Using Genetic Algorithms <i>Kevin Shi and Sherif Saad</i>	450
Smoothing the Ride: Providing a Seamless Upgrade Path from Established Cross-Border eID Workflows Towards eID Wallet Systems <i>Roland Czerny, Christian Kollmann, Blaž Podgorelec, Bernd Prünster and Thomas Zefferer</i>	460
Unclonable Cryptography: A Tale of Two No-Cloning Paradigms <i>Ghada Almashaqbeh and Rohit Chatterjee</i>	469
Design of a New Hardware IP-HLS for Real-Time Image Chaos-Based Encryption <i>Mohamed Salah Azzaz, Redouane Kaibou, Hamdane Kamelia, Abdenour Kifouche and Djamel Tegui</i>	478
Virtual Private Networks in the Quantum Era: A Security in Depth Approach <i>David Schatz, Friedrich Altheide, Hedwig Koerfgen, Michael Rossberg and Guenter Schaefer</i>	486

Secure E-Commerce Protocol with Complex Trading Capabilities of Intermediaries <i>Cătălin V. Bîrjoveanu and Mirela Bîrjoveanu</i>	495
5G Handover: When Forward Security Breaks <i>Navya Sivaraman and Simin Nadjm-Tehrani</i>	503
The Explainability-Privacy-Utility Trade-Off for Machine Learning-Based Tabular Data Analysis <i>Wisam Abbasi, Paolo Mori and Andrea Saracino</i>	511
VerifMSI: Practical Verification of Hardware and Software Masking Schemes Implementations <i>Quentin L. Meunier and Abdul Rahman Taleb</i>	520
A Lightweight Access Control Scheme with Attribute Policy for Blockchain-Enabled Internet of Things <i>Syed Sajid Ullah, Vladimir Oleshchuk and Harsha S. Gardiyawasam Pussewalage</i>	528
On Single-Server Delegation Without Precomputation <i>Matluba Khodjaeva and Giovanni Di Crescenzo</i>	540
WEBAPPAUTH: An Architecture to Protect from Compromised First-Party Web Servers <i>Pascal Wichmann, Sam Ansari, Hannes Federrath and Jens Lindemann</i>	548
ERC20: Correctness via Linearizability and Interference Freedom of the Underlying Smart Contract <i>Rudrapatna K. Shyamasundar</i>	557
A Rand Index-Based Analysis of Consensus Protocols <i>Sangita Roy and Rudrapatna K. Shyamasundar</i>	567
Δ SFL: (Decoupled Server Federated Learning) to Utilize DLG Attacks in Federated Learning by Decoupling the Server <i>Sudipta Paul and Vicenç Torra</i>	577
POSTERS	
Light Quantum Key Distribution Network Security Estimation Tool <i>Sara Nikula, Pekka Koskela, Outi-Marja Latvala and Sami Lehtonen</i>	587
Evaluating Label Flipping Attack in Deep Learning-Based NIDS <i>Hesamodin Mohammadian, Arash Habibi Lashkari and Ali A. Ghorbani</i>	597
Security for Next-Gen Analytics for Cross-Organisation Collaboration <i>Laurent Gomez, Francesco Capano and Patrick Duverger</i>	604
Leveraging Hardware Reverse Engineering to Improve the Cyber Security and Resilience of the Smart Grid <i>Arne Roar Nygård and Sokratis Katsikas</i>	610
On the Implementation of a Lattice-Based Revocable Hierarchical Ibe <i>Mikael Carmona, Doryan Lesaignoux and Antoine Loiseau</i>	617
Privacy in Practice: Private COVID-19 Detection in X-Ray Images <i>Lucas Lange, Maja Schneider, Peter Christen and Erhard Rahm</i>	624
ArmorDroid: A Rule-Set Customizable Plugin for Secure Android Application Development <i>Cong-Binh Le, Bao-Thi Nguyen-Le, Phuoc-Loc Truong, Minh-Triet Tran and Anh-Duy Tran</i>	634

SQLi Detection with ML: A Data-Source Perspective <i>Balázs Pejó and Nikolett Kapui</i>	642
Guidelines and a Framework to Improve the Delivery of Network Intrusion Detection Datasets <i>Brian Lewandowski</i>	649
Labelled Vulnerability Dataset on Android Source Code (LVDAndro) to Develop AI-Based Code Vulnerability Detection Models <i>Janaka Senanayake, Harsha Kalutarage, Mhd Omar Al-Kadri, Luca Piras and Andrei Petrovski</i>	659
A Comprehensive Risk Assessment Framework for IoT-Enabled Healthcare Environment <i>Mofareh Waqdan, Habib Louafi and Malek Mouhoub</i>	667
Robust Three-Factor Lightweight Authentication Based on Extended Chaotic Maps for Portable Resource-Constrained Devices <i>Arijit Karati, Yu-Sheng Chang and Ting-Yu Chen</i>	673
Data Protection and Security Issues with Network Error Logging <i>Libor Polčák and Kamil Jeřábek</i>	683
Defeating MageCart Attacks in a NAISS Way <i>Cătălin Rus, Dipti Kapoor Sarmah and Mohammed El-Hajj</i>	691
Fidelis: Verifiable Keyword Search with No Trust Assumption <i>Laltu Sardar and Subhra Mazumdar</i>	698
Lightweight FHE-based Protocols Achieving Results Consistency for Data Encrypted Under Different Keys <i>Marina Checri, Jean-Paul Bultel, Renaud Sirdey and Aymen Boudguiga</i>	704
Approximate Homomorphic Pre-Processing for CNNs <i>Shabnam Khanna and Ciara Rafferty</i>	710
A 10-Layer Model for Service Availability Risk Management <i>Jan Marius Evang</i>	716
Lattice-Based Threshold Signature Implementation for Constrained Devices <i>Patrik Dobias, Sara Ricci, Petr Dzurenda, Lukas Malina and Nikita Snetkov</i>	724
How to Plausibly Deny Steganographic Secrets <i>Shahzad Ahmad and Stefan Rass</i>	731
Proctoring Online Exam Using Eye Tracking <i>Waheeb Yaqub, Manoranjan Mohanty and Basem Suleiman</i>	738
Blockchain Data Replication <i>Roberto De Prisco, Sergiy Shevchenko and Pompeo Faruolo</i>	746
Toward a Compliant Token-Based e-Voting System with SSI-Granted Eligibility <i>Dario Castellano, Roberto De Prisco and Pompeo Faruolo</i>	752
Self-Sovereign Identity (SSI) Attribute-Based Web Authentication <i>Biagio Boi, Marco De Santis and Christian Esposito</i>	758

International Mutual Recognition: A Description of Trust Services in US, UK, EU and JP and the Testbed “Hakoniwa” <i>Satoshi Kai, Takao Kondo, Naghmeh Karimi, Konstantinos Mersinas, Marc Sel, Roberto Yus and Satoru Tezuka</i>	764
Improving Intrusion Detection Systems with Multi-Agent Deep Reinforcement Learning: Enhanced Centralized and Decentralized Approaches <i>Amani Bacha, Farah Barika Ktata and Faten Louati</i>	772
Combining Generators of Adversarial Malware Examples to Increase Evasion Rate <i>Matouš Kozák and Martin Jureček</i>	778
Detecting BrakTooth Attacks <i>Achyuth Nandikotkur, Issa Traore and Mohammad Mamun</i>	787
SoK: Towards CCA Secure Fully Homomorphic Encryption <i>Hiroki Okada and Kazuhide Fukushima</i>	793
IMAGINE Dataset: Digital Camera Identification Image Benchmarking Dataset <i>Jarosław Bernacki and Rafał Scherer</i>	799
Remote Security Assessment for Cyber-Physical Systems: Adapting Design Patterns for Enhanced Diagnosis <i>Kazutaka Matsuzaki, Kenji Sawada and Shinich Honiden</i>	805
Uncovering Flaws in Anti-Phishing Blacklists for Phishing Websites Using Novel Cloaking Techniques <i>Wenhao Li, Yongqing He, Zhimin Wang, Saleh Mansor Alqahtani and Priyadarsi Nanda</i>	813
CNN-HMM Model for Real Time DGA Categorization <i>Aimen Mahmood, Haider Abbas and Faisal Amjad</i>	822
Anomaly Detection in Smart Grid Networks Using Power Consumption Data <i>Hasina Rahman, Priyadarsi Nanda, Manoranjan Mohanty and Nazim Uddin Sheikh</i>	830
Security for Distributed Machine Learning <i>Laurent Gomez, Tianchi Yu and Patrick Duverger</i>	838
A Secure Emergency Framework in an IoT Based Patient Monitoring System <i>Neila Mekki, Mohamed Hamdi, Taoufik Aguilu and Tai-hoon Kim</i>	844
A Two-Party Hierarchical Deterministic Wallets in Practice <i>ChihYun Chuang, Ihung Hsu and TingFang Lee</i>	850
Migrating Applications to Post-Quantum Cryptography: Beyond Algorithm Replacement <i>Alexandre Augusto Giron</i>	857
Analyzing Image Based Strategies for Android Malware Detection and Classification: An Empirical Exploration <i>Chirag Jaju, Dhairya Agrawal, Rishi Poddar, Shubh Badjate, Sidharth Anand, Barsha Mitra and Soumyadeep Dey</i>	863
Multi-Environment Training Against Reward Poisoning Attacks on Deep Reinforcement Learning <i>Myria Bouhaddi and Kamel Adi</i>	870

Privacy-Preserving Algorithms for Data Cooperatives with Directed Graphs <i>Mark Dockendorf and Ram Dantu</i>	876
AUTHOR INDEX	885