19th International Conference on Security and Cryptography (SECRYPT 2022)

Lisbon, Portugal
11 – 13 July 2022

Editors:

Sabrina De Capitani di Vimercati
Pierangela Samarati

ISBN: 978-1-7138-6394-6

Printed from e-media with permission by:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571

CURRAN ASSOCIATES INC.
proceedings
.com

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

Cyber Security When IT Meets OT 5
Sokratis K. Katsikas

Don't Tell Me The Cybersecurity Moon Is Shining… (Cybersecurity Show and Tell) 7
Luca Vigano

PAPERS

Full Papers

SEVIL: @*underline*S@ecure and @*underline*E@fficient @*underline*V@erif@*underline*I@cation over Massive Proofs of Know@*underline*L@edge 13
Souha Masmoudi, Maryline Laurent and Nesrine Kaaniche

Blind Side Channel on the Elephant LFSR 25
Awaleh Houssein Meraneh, Christophe Clavier, Hélène Le Bouder, Julien Maillard and Gaël Thomas

Towards an Automated Business Process Model Risk Assessment: A Process Mining Approach 35
Panagiotis Dedousis, Melina Raptaki, George Stergiopoulos and Dimitris Gritzalis

Metering Homes: Do Energy Efficiency and Privacy Need to Be in Conflict? 47
Libor Polčák and Petr Matoušek

Stacked Ensemble Model for Enhancing the DL based SCA 59
Anh Tuan Hoang, Neil Hanley, Ayesha Khalid, Dur-e-Shahwar Kundi and Maire O'Neill

Comparison-based MPC in Star Topology 69
Gowri R. Chandran, Carmit Hazay, Robin Hundt and Thomas Schneider

CRGC: A Practical Framework for Constructing Reusable Garbled Circuits 83
Christopher Harth-Kitzerow, Georg Carle, Fan Fei, Andre Luckow and Johannes Klepsch

An Adaptive Web Application Firewall 96
Miguel Calvo and Marta Beltrán

FAPRIL: Towards Faster Privacy-preserving Fingerprint-based Localization 108
Christopher van der Beets, Raine Nieminen and Thomas Schneider

A Longitudinal Study of Cryptographic API: A Decade of Android Malware 121
Adam Janovsky, Davide Maiorca, Dominik Macko, Vashek Matyas and Giorgio Giacinto

Large-scale Randomness Study of Security Margins for 100+ Cryptographic Functions 134
Dušan Klinec, Marek Sýs, Karel Kubíček, Petr Švenda and Vashek Matyáš

PAMMELA: Policy Administration Methodology using Machine Learning 147
Varun Gumma, Barsha Mitra, Soumyadeep Dey, Pratik Shashikantbhai Patel, Sourabh Suman, Saptarshi Das and Jaideep Vaidya

Partially Oblivious Neural Network Inference
Panagiotis Rizomiliotis, Christos Diou, Aikaterini Triakosia, Ilias Kyrannas and Konstantinos Tserpes 158

Federated Naive Bayes under Differential Privacy
Thomas Marchioro, Lodovico Giaretta, Evangelos Markatos and Šarūnas Girdzijauskas 170

Effectiveness of Adversarial Component Recovery in Protected Netlist Circuit Designs
Jeffrey T. Mcdonald, Jennifer Parnell, Todd R. Andel and Samuel H. Russ 181

Membership Inference Attacks on Aggregated Time Series with Linear Programming
Antonin Voyez, Tristan Allard, Gildas Avoine, Pierre Cauchois, Elisa Fromont and Matthieu Simonin 193

Graph Algorithms over Homomorphic Encryption for Data Cooperatives
Mark Dockendorf, Ram Dantu and John Long 205

Mason Vulnerability Scoring Framework: A Customizable Framework for Scoring Common Vulnerabilities and Weaknesses
Ibifubara Iganibo, Massimiliano Albanese, Kaan Turkmen, Thomas R. Campbell and Marc Mosko 215

Threats to Adversarial Training for IDSs and Mitigation
Hassan Chaitou, Thomas Robert, Jean Leneutre and Laurent Pautet 226

CatNap: Leveraging Generic MPC for Actively Secure Privacy-enhancing Proximity Testing with a Napping Party
Ivan Oleynikov, Elena Pagnin and Andrei Sabelfeld 237

Real-time Crowd Counting based on Wearable Ephemeral IDs
Daniel Morales, Isaac Agudo and Javier Lopez 249

HTTPFuzz: Web Server Fingerprinting with HTTP Request Fuzzing
Animesh Kar, Andrei Natadze, Enrico Branca and Natalia Stakhanova 261

SHORT PAPERS

A Region-based Training Data Segmentation Strategy to Credit Scoring
Roberto Saia, Salvatore Carta, Gianni Fenu and Livio Pompianu 275

A Spendable Cold Wallet from QR Video
Rafael Dowsley, Mylène C. Q. Farias, Mario Larangeira, Anderson Nascimento and Jot Virdee 283

Collusion-resistant Broadcast Encryption based on Hidden RSA Subgroups
Sigurd Eskeland 291

Cryptanalysis of a Privacy-preserving Behavior-oriented Authentication Scheme
Sigurd Eskeland and Ahmed Fraz Baig 299

SHINE: Resilience via Practical Interoperability of Multi-party Schnorr Signature Schemes
Antonin Dufka, Vladimir Sedlacek and Petr Svenda 305

Application Sandboxing for Linux Desktops: A User-friendly Approach
Lukas Brodschelm and Marcus Gelderie 317

A Local Differential Privacy based Hybrid Recommendation Model with BERT and Matrix Factorization
Jeyamohan Neera, Xiaomin Chen, Nauman Aslam, Biju Issac and Eve O'Brien 325

Behavior Modeling of a Distributed Application for Anomaly Detection
Amanda Viescinski, Tiago Heinrich, Newton C. Will and Carlos Maziero 333

What your Fitbit Says about You: De-anonymizing Users in Lifelogging Datasets
Andrei Kazlouski, Thomas Marchioro and Evangelos Markatos 341

Key Encapsulation Mechanism in Ciphertext-policy Attribute based Setting Featuring Revocation and Key-homomorphic Property
Anushree Belel, Ratna Dutta and Sourav Mukhopadhyay 349

Tick Tock Break the Clock: Breaking CAPTCHAs on the Darkweb
David Holm Audran, Marcus Braunschweig Andersen, Mark Højer Hansen, Mikkel Møller Andersen, Thomas B. Frederiksen, Kasper H. Hansen, Dimitrios Georgoulias and Emmanouil Vasilomanolakis 357

A New Leakage Resilient Symmetric Searchable Encryption Scheme for Phrase Search
Samiran Bag, Indranil Ghosh Ray and Feng Hao 366

Code-based Key Encapsulation Mechanism Preserving Short Ciphertext and Secret Key
Jayashree Dey and Ratna Dutta 374

Near-collisions and Their Impact on Biometric Security
Axel Durbet, Paul-Marie Grollemund, Pascal Lafourcade and Kevin Thiry-Atighehchi 382

Resilience of GANs against Adversarial Attacks
Kyrylo Rudavskyy and Ali Miri 390

Implementation of a Stateful Network Protocol Intrusion Detection Systems
S. Seng, J. Garcia-Alfaro and Y. Laarouci 398

zkBeacon: Proven Randomness Beacon based on Zero-knowledge Verifiable Computation
Lavaur Thomas and Lacan Jérôme 406

Yet Another Algebraic Cryptanalysis of Small Scale Variants of AES
Marek Bielik, Martin Jureček, Olha Jurečková and Róbert Lórencz 415

PhishGNN: A Phishing Website Detection Framework using Graph Neural Networks
Tristan Bilot, Grégoire Geis and Badis Hammi 428

Are Clouds making Our Research Irrelevant and Who Is at Fault? (Position Paper)
Yvo Desmedt 436

PASS-P: Performance and Security Sensitive Dynamic Cache Partitioning
Nirmal Kumar Boran, Pranil Joshi and Virendra Singh 443

GAN-based Approach to Crafting Adversarial Malware Examples against a Heterogeneous Ensemble Classifier
Saad Al-Ahmadi and Saud Al-Eyead 451

Reverse Engineering for Thwarting Digital Supply Chain Attacks in Critical Infrastructures: Ethical Considerations
Arne Roar Nygård, Arvind Sharma and Sokratis Katsikas 461

A Decentralised Real Estate Transfer Verification based on Self-Sovereign Identity and Smart Contracts
Abubakar-Sadiq Shehu, António Pinto and Manuel E. Correia 469

Posters

Irreversible Applications for Windows NT Systems
Rahul Sankalana Gunawardhana and Kavinga Yapa Abeywardena 479

Bypassing Current Limitations for Implementing a Credential Delegation for the Industry 4.0
Santiago de Diego, Óscar Lage, Cristina Regueiro, Sergio Anguita and Gabriel Maciá-Fernández 485

A Generic Privacy-preserving Protocol for Keystroke Dynamics-based Continuous Authentication
Ahmed Fraz Baig and Sigurd Eskeland 491

Risk-driven Model-based Architecture Design for Secure Information Flows in Manufacturing Infrastructures
Loris Dal Lago, Fabio Federici, Davide Martintoni and Valerio Senni 499

Seccomp Filters from Fuzzing
Marcus Gelderie, Valentin Barth, Maximilian Luff and Julian Birami 507

A Method for Road Accident Prevention in Smart Cities based on Deep Reinforcement Learning
Giuseppe Crincoli, Fabiana Fierro, Giacomo Iadarola, Piera Elena La Rocca, Fabio Martinelli, Francesco Mercaldo and Antonella Santone 513

TrustLend: Using Borrower Trustworthiness for Lending on Ethereum
Wisnu Uriawan, Youakim Badr, Omar Hasan and Lionel Brunie 519

Efficient IoT Device Fingerprinting Approach using Machine Learning
Richmond Osei, Habib Louafi, Malek Mouhoub and Zhongwen Zhu 525

A Real-time Method for CAN Bus Intrusion Detection by Means of Supervised Machine Learning
Francesco Mercaldo, Rosangela Casolare, Giovanni Ciaramella, Giacomo Iadarola, Fabio Martinelli, Francesco Ranieri and Antonella Santone 534

Parallel and Distributed Implementations of the Wiedemann and the Block-Wiedemann Methods over GF(2)
Rahul Roy, Abhijit Das and Dipanwita Roy Chowdhury 540

Discovering How to Attack a System
Fabrizio Baiardi, Daria Maggi and Mauro Passacantando 548

Decentralized Public Key Infrastructure with Identity Management using Hyperledger Fabric
Amisha Sinha and Debanjan Sadhya 554

The Weakest Link: On Breaking the Association between Usernames and Passwords in Authentication Systems
Eva Anastasiadi, Elias Athanasopoulos and Evangelos Markatos 560

Authentication Attacks on Projection-based Cancelable Biometric Schemes
Axel Durbet, Paul-Marie Grollemund, Pascal Lafourcade, Denis Migdal and Kevin Thiry-Atighehchi 568

Weighted Attribute-based Encryption with Parallelized Decryption
Alexandru Ioniţă 574

Evaluation of AI-based Malware Detection in IoT Network Traffic
Nuno Prazeres, Rogério Luís de C. Costa, Leonel Santos and Carlos Rabadão 580

Towards Heterogeneous Remote Attestation Protocols
Paul Georg Wagner and Jürgen Beyerer 586

Identifying Organizations Receiving Personal Data in Android Apps
David Rodriguez, Miguel Cozar and Jose M. Del Alamo 592

JCAlgTest: Robust Identification Metadata for Certified Smartcards
Petr Svenda, Rudolf Kvasnovsky, Imrich Nagy and Antonin Dufka 597

On the Efficiency and Security of Quantum-resistant Key Establishment Mechanisms on FPGA Platforms
Lukas Malina, Sara Ricci, Patrik Dobias, Petr Jedlicka, Jan Hajny and Kim-Kwang Raymond Choo 605

Brain Waves and Evoked Potentials as Biometric User Identification Strategy: An Affordable Low-cost Approach
Roberto Saia, Salvatore Carta, Gianni Fenu and Livio Pompianu 614

Illicit Darkweb Classification via Natural-language Processing: Classifying Illicit Content of Webpages based on Textual Information
Giuseppe Cascavilla, Gemma Catolino and Mirella Sangiovanni 620

Verification of PUF-based IoT Protocols with AVISPA and Scyther
Tomáš Rabas, Róbert Lórencz and Jiří Buček 627

PE-AONT: Partial Encryption All or Nothing Transform
Katarzyna Kapusta and Gerard Memmi 636

From GDPR to Privacy Design Patterns: The MATERIALIST Framework
Vita Barletta, Giuseppe Desolda, Domenico Gigante, Rosa Lanzilotti and Marco Saltarella 642

Moving Target Defense Router: MaTaDoR
Berkan Ufuk and Mehmet Tahir Sandikkaya 649

Transient State Signaling for Spectre/Meltdown Transient Cache Side-channel Prevention
Zelong Li and Akhilesh Tyagi 655

On the Practicality of Relying on Simulations in Different Abstraction Levels for Pre-silicon Side-Channel Analysis
Javad Bahrami, Mohammad Ebrahimabadi, Sofiane Takarabt, Jean-luc Danger, Sylvain Guilley and Naghmeh Karimi 661

A Secure Federated Learning: Analysis of Different Cryptographic Tools
Oana Stan, Vincent Thouvenot, Aymen Boudguiga, Katarzyna Kapusta, Martin Zuber and Renaud Sirdey 669

Novel Design for IE-Cache to Mitigate Conflict-based Cache-side Channel Attacks with Reduced Energy Consumption
Saqib Javed, Muhammad Asim Mukhtar, Muhammad Khurram Bhatti and Guy Gogniat 675

Switched-based Control Testbed to Assure Cyber-physical Resilience by Design
Mariana Segovia, Jose Rubio-Hernan, Ana R. Cavalli and Joaquin Garcia-Alfaro 681

Offline-verifiable Data from Distributed Ledger-based Registries
Stefan More, Jakob Heher and Clemens Walluschek 687

Efficient Hybrid Model for Intrusion Detection Systems
Nesrine Kaaniche, Aymen Boudguiga and Gustavo Gonzalez-Granadillo 694

Side-channel Analysis and Countermeasure for Implementation of Lattice-based Signature
Kazuhide Fukushima, Hiroki Okada, Sofiane Takarabt, Amina Korchi, Meziane Hamoud, Khaled Karray, Youssef Souissy and Sylvain Guilley 701

Towards a Threat Model and Security Analysis for Data Cooperatives
Abiola Salau, Ram Dantu, Kirill Morozov, Kritagya Upadhyay and Syed Badruddoja 707

A Novel Method for Embedding and Extracting Secret Messages in Textual Documents based on Paragraph Resizing
Benjamin Aziz, Aysha Bukhelli, Rinat Khusainov and Alaa Mohasseb 714

AUTHOR INDEX 721