18th International Conference on Security and Cryptography (SECRYPT 2021)

Online
6 – 8 July 2021

Editors:
Sabrina De Capitani di Vimercati
Pierangela Samarati

ISBN: 978-1-7138-3998-9
CONTENTS

INVITED SPEAKERS

KEYNOTE SPEAKERS
Privacy-Preserving Analytics in the Big Data Environment  
Jaideep Vaidya  
5

VEST: An Early Warning System for Future Cyber-Attacks  
V. S. Subrahmanian  
7

Access Control Convergence: Challenges and Opportunities  
Ravi Sandhu  
9

PAPERS

FULL PAPERS
An Upcycling Tokenization Method for Credit Card Numbers  
Cyrius Nugier, Diane Leblanc-Albarel, Agathe Blaise, Simon Masson, Paul Huynh and Yris Brice Wandji Piugie  
15

A Unified Model to Detect Information Flow and Access Control Violations in Software Architectures  
Stephan Seifermann, Robert Heinrich, Dominik Werle and Ralf Reussner  
26

Can a TLS Certificate Be Phishy?  
Kaspar Hageman, Egon Kidmose, René Rydhoif Hansen and Jens Myrup Pedersen  
38

Comparing Classifiers’ Performance under Differential Privacy  
Milan Lopuhaä-Zwakenberg, Mina Alishahi, Jeroen Kivits, Jordi Klarenbeek, Gert-Jan van der Velde and Nicola Zannone  
50

Hashing to Prime in Zero-Knowledge  
Thomas Groß  
62

BLT+L: Efficient Signatures from Timestamping and Endorsements  
Denis Firsov, Henri Lakk, Sven Laur and Ahto Truu  
75

Scalable k-anonymous Microaggregation: Exploiting the Tradeoff between Computational Complexity and Information Loss  
Florian Thaeter and Rüdiger Reischuk  
87

Statically Identifying XSS using Deep Learning  
Heloise Maurel, Santiago Vidal and Tamara Rezk  
99

Are You There, Moriarty? Feasibility Study of Internet-based Location for Location-based Access Control Systems  
Muhammad I. H. Sukmana, Kai-Oliver Kohlen, Carl Gödecke, Pascal Schulze and Christoph Meinel  
111

Python and Malware: Developing Stealth and Evasive Malware without Obfuscation  
Vasilios Koutskokostas and Constantinos Patsakis  
125
SSI Strong Authentication using a Mobile-phone based Identity Wallet Reaching a High Level of Assurance
Andreas Abraham, Christopher Schinnerl and Stefan More

Armored Twins: Flexible Privacy Protection for Digital Twins through Conditional Proxy Re-Encryption and Multi-Party Computation
Felix Hörandner and Bernd Prünster

Towards Integrating Security in Industrial Engineering Design Practices
Panagiotis Dedousis, George Stergiopoulos, George Arampatzis and Dimitris Gritzalis

Balancing Quality and Efficiency in Private Clustering with Affinity Propagation
Hannah Keller, Helen Möllering, Thomas Schneider and Hossein Yalame

Automated Symbolic Verification of Telegram’s MTProto 2.0
Marino Miculan and Nicola Vitacolonna

Formal Proof of a Vulnerability in Z-Wave IoT Protocol
Mario Lilli, Chiara Braghin and Elvinia Riccobene

Formal Analysis of EDHOC Key Establishment for Constrained IoT Devices
Karl Norrman, Vaishnavi Sundararajan and Alessandro Bruni

A Framework for Security and Risk Analysis of Enrollment Procedures: Application to Fully-remote Solutions based on eDocuments
Marco Pernpruner, Giada Sciarretta and Silvio Ranise

The Missing Piece of the ABAC Puzzle: A Modeling Scheme for Dynamic Analysis
Marius Schlegel and Peter Amthor

Program Protection through Software-based Hardware Abstraction
J. Todd McDonald, Ramya K. Manikyam, Sébastien Bardin, Richard Bonichon and Todd R. Andel

Vulnerability Metrics for Graph-based Configuration Security
Ibifubara Iganibo, Massimiliano Albanese, Marc Mosko, Eric Bier and Alejandro E. Brito

Model Inversion for Impersonation in Behavioral Authentication Systems
Md Morshedul Islam and Reihaneh Safavi-Naini

Trace Recovery: Inferring Fine-grained Trace of Energy Data from Aggregates
Nazim Uddin Sheikh, Zhigang Lu, Hassan Jameel Asghar and Mohamed Ali Kaafar

Preventing Watermark Forging Attacks in a MLaaS Environment
Softane Lounici, Mohamed Njieh, Orhan Ermis, Melek Önen and Slim Trabelsi

Systematic Evaluation of Probabilistic k-Anonymity for Privacy Preserving Micro-data Publishing and Analysis
Navoda Senavirathne and Vicenç Torra

Boolean Exponent Splitting
Michael Tunstall, Louiza Papachristodoulou and Kostas Papagiannopoulos

Proof-of-Forgery for Hash-based Signatures
Evgeniy Kiktenko, Mikhail Kudinov, Andrey Bulychev and Aleksey Fedorov

XII
Trusted Enforcement of Application-specific Security Policies
Marius Schlegel 343

Responding to Living-Off-the-Land Tactics using Just-In-Time Memory Forensics (JIT-MF) for Android
Jennifer Bellizzi, Mark Vella, Christian Colombo and Julio Hernandez-Castro 356

Cryptographic Enforcement of Access Control Policies in the Cloud: Implementation and Experimental Assessment
Stefano Berlato, Roberto Carbone and Silvio Ranise 370

SHORT PAPERS

Supporting Cyber Threat Analysis with Service-Oriented Enterprise Modeling
Kees Leune and Sung Kim 385

Signer and Message Ambiguity from a Variety of Keys
George Teșeleanu 395

Ransomware Detection using Markov Chain Models over File Headers
Nicolas Bailluet, Hélène Le Bouder and David Lubiczc 403

Proof-of-Useful-Randomness: Mitigating the Energy Waste in Blockchain Proof-of-Work
Efe Ulas Akay Seyitoglu, Artila Ayat Yavuz and Thang Hoang 412

A New MILP Model for Matrix Multiplications with Applications to KLEIN and PRINCE
Murat Burhan İlter and Ali Aydın Selçuk 420

Protecting End User’s Privacy When using Social Login through GDPR Compliance
Carlos Villardán and Marta Beltrán 428

Efficient Joint Random Number Generation for Secure Multi-party Computation
Erwin Hoogerwerf, Daphne van Tetering, Aslí Bay and Zekeriya Erkin 436

Improved Circuit Compilation for Hybrid MPC via Compiler Intermediate Representation
Daniel Demmler, Stefan Katzenbeisser, Thomas Schneider, Tom Schuster and Christian Weinert 444

A Novel Security Framework for Minimization of False Information Dissemination in VANETs: Bayesian Game Formulation
Basant Subba and Ayushi Singh 452

An Extension of the Avalanche Criterion in the Context of c-Differentials
Pål Ellingsen, Constanza Riera, Pantelimon Stănića and Anton Tkachenko 460

A New Delegated Authentication Protocol based on PRE
Anass Sbai, Cyril Drocourt and Gilles Dequen 468

Mobile Family Detection through Audio Signals Classification
Rosangela Casolare, Giacomo Iadarola, Fabio Martinelli, Francesco Mercaldo and Antonella Santone 479

Accurate Measurement of the Energy Consumption of Security Functions
Benoît Fournier, Valérie Viet Triem Tong and Gilles Guette 487

 Practically Efficient RFID Scheme with Constant-time Identification
Ferucio Laurențiu Țiplea and Cristian Hristea 495

XIII
A Comparison of GKE Protocols based on SIDH
Hiroki Okada, Shinsaku Kiyomoto and Carlos Cid 507

Multi-Party Private Set Intersection Protocols for Practical Applications
Asli Bay, Zeki Erkin, Mina Alishahi and Jelle Vos 515

Using Program Analysis to Identify the Use of Vulnerable Functions
Rasmus Hagberg, Martin Hell and Christoph Reichenbach 523

Compact Variable-base ECC Scalar Multiplication using Euclidean Addition Chains
Fabien Herbaut, Nicolas Méloni and Pascal Véron 531

Secure Computation by Secret Sharing using Input Encrypted with Random Number
Keiichi Iwamura and Ahmad Akmal Aminuddin Mohd Kamal 540

A Scalable Bitcoin-based Public Key Certificate Management System
Chloe Tartan, Craig Wright, Michaella Pettit and Wei Zhang 548

Cloud Key Management using Trusted Execution Environment
Jaouhara Bouamama, Mustapha Hedabou and Mohammed Erradi 560

An Improved Live Anomaly Detection System (I-LADS) based on Deep Learning Algorithms
Gustavo Gonzalez-Granadillo, Alejandro G. Bedoya and Rodrigo Diaz 568

Inferring Flow Table State through Active Fingerprinting in SDN Environments: A Practical Approach
Marcin Gregorczyk and Wojciech Mazurczyk 576

SecSDN: A Novel Architecture for a Secure SDN
Parjanya Vyas and R. K. Shyamasundar 587

Storage Friendly Provably Secure Multivariate Identity-Based Signature from Isomorphism of Polynomials Problem
Ratna Dutta, Sumit Kumar Debnath and Chinmoy Biswas 595

Formal Security Verification of the Station-to-Station based Cell-attachment Procedure of LDACS
Nils Mäurer, Christoph Gentsch, Thomas Gräupl and Corinna Schmitt 603

Side Channel Counter-measures based on Randomized AMNS Modular Multiplication
Christophe Negre 611

Selective Owner-side Encryption in Digital Data Markets: Strategies for Key Derivation
Sara Foresti and Giovanni Livraga 620

POSTERS

Security Issues of Electronic and Mobile Banking
Wojciech Wodo, Damian Stygar and Przemyslaw Błaskiewicz 631

Enforcing Cardinality Constraint in Temporal RBAC
Sohail Rajdev and Barsha Mitra 639

Dynamic Access Control Framework for Enterprise Content Management Systems
Nadia Hocine and Ismail Bokhari 647

AVX-512-based Parallelization of Block Sieving and Bucket Sieving for the General Number Field Sieve Method
Pritam Pallab and Abhijit Das 653

XIV
Involving Humans in the Cryptographic Loop: Introduction and Threat Analysis of EEVEHAC
Julius Hekkala, Sara Nikula, Outi-Marja Latvala and Kimmo Halunen
659

Empirical Security and Privacy Analysis of Mobile Symptom Checking Apps on Google Play
I. Wayan Budi Sentana, Muhammad Ikram, Mohamed Ali Kaafar and Shlomo Berkovsky
665

BlockJack: Towards Improved Prevention of IP Prefix Hijacking Attacks in Inter-domain Routing via Blockchain
I. Wayan Budi Sentana, Muhammad Ikram and Mohamed Ali Kaafar
674

Private Set Intersection: Past, Present and Future
Ionita Andreea
680

MMU-based Access Control for Libraries
Marinos Tsantekidis and Vassilis Prevelakis
686

Exposure Resilient Public-key Encryption with Keyword Search against Keyword Guessing Attack
Kaito Uemura and Satoshi Obana
692

PUF based Lightweight Authentication and Key Exchange Protocol for IoT
Sourav Roy, Dipnarayan Das, Anindan Mondal, Mahabub Hasan Mahalat, Suchismita Roy and Bibhash Sen
698

On Chameleon Pseudonymisation and Attribute Compartmentation-as-a-Service
Anne V. D. M. Kayem, Nikolai J. Podlesny, Christoph Meinel and Anja Lehmann
704

Property Inference Attacks on Convolutional Neural Networks: Influence and Implications of Target Model’s Complexity
Mathias Parisot, Balázs Pejó and Dayana Spagnuelo
715

RMCCS: RSSI-based Message Consistency Checking Scheme for V2V Communications
Mujahid Muhammad, Paul Kearney, Adel Aneiba, Junaid Arshad and Andreas Kunz
722

A New Method of Testing Machine Learning Models of Detection for Targeted DDoS Attacks
Mateusz Kozłowski and Bogdan Ksie żopolski
728

Comparing Support Vector Machine and Neural Network Classifiers of CVE Vulnerabilities
Grzegorz J. Blinowski, Paweł Piotrowski and Michał Wiśniewski
734

Privacy Aura for Transparent Authentication on Multiple Smart Devices
Takoua Guiga, Jean-Jacques Schwartzmann and Christophe Rosenberger
741

Classifying Biometric Systems Users among the Doddington Zoo: Application to Keystroke Dynamics
Denis Migdal, Ilaria Magotti and Christophe Rosenberger
747

Fair Mutual Authentication
Jacek Cichoń, Krzysztof Majcher and Mirosław Kutylowski
754

Towards CRYSTALS-Kyber VHDL Implementation
Sara Ricci, Petr Jedlicka, Peter Cibík, Petr Dzurenda, Lukas Malina and Jan Hajny
760

Fast Cramer-Shoup Cryptosystem
Pascal Lafourcade, Léo Robert and Demba Sow
766

Yosra Fraiji, Lamia ben Azzouz, Wassim Trojet, Ghaleb Hoblos and Leila Azouz Saidane
772
Verify It Yourself: A Note on Activation Functions’ Influence on Fast DeepFake Detection
Piotr Kawa and Piotr Syga

GRANEF: Utilization of a Graph Database for Network Forensics
Milan Cermak and Denisa Sramkova

Anonymous Attribute-based Credentials in Collaborative Indoor Positioning Systems
Raúl Casanova-Marqués, Pavel Pascacio, Jan Hajny and Joaquín Torres-Sospedra

HIJaX: Human Intent JavaScript XSS Generator
Yaw Frempong, Yates Snyder, Erfan Al-Hossami, Meera Sridhar and Samira Shaikh

User Identification from Time Series of Fitness Data
Thomas Marchioro, Andrei Kazlouski and Evangelos Markatos

Privacy Preserving Scalable Authentication Protocol with Partially Trusted Third Party for Distributed Internet-of-Things
Hiral S. Trivedi and Sankita J. Patel

C2RBAC: An Extended Capability-Role-Based Access Control with Context Awareness for Dynamic Environments
Mitsuhiro Mabuchi and Koji Hasebe

Can Data Subject Perception of Privacy Risks Be Useful in a Data Protection Impact Assessment?
Salimeh Dashti, Anderson Santana de Oliveira, Caelin Kaplan, Manuel Dalcastagnè and Silvio Ranise

Goal and Threat Modelling for Driving Automotive Cybersecurity Risk Analysis Conforming to ISO/SAE 21434
Christophe Ponsard, Valéry Ramon and Jean-Christophe Deprez

Collateral-Free Trustworthiness-based Personal Lending on a Decentralized Application (DApp)
Wisnu Uriawan, Omar Hasan, Youakim Badr and Lionel Brunie

Investing Data with Untrusted Parties using HE
Mark Dockendorf, Ram Dantu, Kirill Morozov and Sanjukta Bhownick

Machine Learning Classification of Obfuscation using Image Visualization
Colby B. Parker, J. Todd McDonald and Dimitrios Damopoulos

AUTHOR INDEX