

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

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© (2021) by SCITEPRESS – Science and Technology Publications, Lda.
All rights reserved.

Printed with permission by Curran Associates, Inc. (2021)

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

Privacy-Preserving Analytics in the Big Data Environment <i>Jaideep Vaidya</i>	5
VEST: An Early Warning System for Future Cyber-Attacks <i>V. S. Subrahmanian</i>	7
Access Control Convergence: Challenges and Opportunities <i>Ravi Sandhu</i>	9

PAPERS

FULL PAPERS

An Upcycling Tokenization Method for Credit Card Numbers <i>Cyrius Nugier, Diane Leblanc-Albarel, Agathe Blaise, Simon Masson, Paul Huynh and Yris Brice Wandji Piugie</i>	15
A Unified Model to Detect Information Flow and Access Control Violations in Software Architectures <i>Stephan Seifermann, Robert Heinrich, Dominik Werle and Ralf Reussner</i>	26
Can a TLS Certificate Be Phishy? <i>Kaspar Hageman, Egon Kidmose, René Rydhof Hansen and Jens Myrup Pedersen</i>	38
Comparing Classifiers' Performance under Differential Privacy <i>Milan Lopuhaä-Zwakenberg, Mina Alishahi, Jeroen Kivits, Jordi Klarenbeek, Gert-Jan van der Velde and Nicola Zannone</i>	50
Hashing to Prime in Zero-Knowledge <i>Thomas Groß</i>	62
BLT+L: Efficient Signatures from Timestamping and Endorsements <i>Denis Firsov, Henri Lakk, Sven Laur and Ahto Truu</i>	75
Scalable k -anonymous Microaggregation: Exploiting the Tradeoff between Computational Complexity and Information Loss <i>Florian Thaefer and Rüdiger Reischuk</i>	87
Statically Identifying XSS using Deep Learning <i>Heloise Maurel, Santiago Vidal and Tamara Rezk</i>	99
Are You There, Moriarty? Feasibility Study of Internet-based Location for Location-based Access Control Systems <i>Muhammad I. H. Sukmana, Kai-Oliver Kohlen, Carl Gödecken, Pascal Schulze and Christoph Meinel</i>	111
Python and Malware: Developing Stealth and Evasive Malware without Obfuscation <i>Vasilios Koutsokostas and Constantinos Patsakis</i>	125

SSI Strong Authentication using a Mobile-phone based Identity Wallet Reaching a High Level of Assurance <i>Andreas Abraham, Christopher Schinnerl and Stefan More</i>	137
Armored Twins: Flexible Privacy Protection for Digital Twins through Conditional Proxy Re-Encryption and Multi-Party Computation <i>Felix Hörandner and Bernd Prünster</i>	149
Towards Integrating Security in Industrial Engineering Design Practices <i>Panagiotis Dedousis, George Stergiopoulos, George Arampatzis and Dimitris Gritzalis</i>	161
Balancing Quality and Efficiency in Private Clustering with Affinity Propagation <i>Hannah Keller, Helen Möllering, Thomas Schneider and Hossein Yalame</i>	173
Automated Symbolic Verification of Telegram’s MTPROTO 2.0 <i>Marino Miculan and Nicola Vitacolonna</i>	185
Formal Proof of a Vulnerability in Z-Wave IoT Protocol <i>Mario Lilli, Chiara Braghin and Elvinia Riccobene</i>	198
Formal Analysis of EDHOC Key Establishment for Constrained IoT Devices <i>Karl Norrman, Vaishnavi Sundararajan and Alessandro Bruni</i>	210
A Framework for Security and Risk Analysis of Enrollment Procedures: Application to Fully-remote Solutions based on eDocuments <i>Marco Pernpruner, Giada Sciarretta and Silvio Ranise</i>	222
The Missing Piece of the ABAC Puzzle: A Modeling Scheme for Dynamic Analysis <i>Marius Schlegel and Peter Amthor</i>	234
Program Protection through Software-based Hardware Abstraction <i>J. Todd McDonald, Ramya K. Manikyam, Sébastien Bardin, Richard Bonichon and Todd R. Andel</i>	247
Vulnerability Metrics for Graph-based Configuration Security <i>Ibifubara Iganibo, Massimiliano Albanese, Marc Mosko, Eric Bier and Alejandro E. Brito</i>	259
Model Inversion for Impersonation in Behavioral Authentication Systems <i>Md Morshedul Islam and Reihaneh Safavi-Naini</i>	271
Trace Recovery: Inferring Fine-grained Trace of Energy Data from Aggregates <i>Nazim Uddin Sheikh, Zhigang Lu, Hassan Jameel Asghar and Mohamed Ali Kaafar</i>	283
Preventing Watermark Forging Attacks in a MLaaS Environment <i>Sofiane Lounici, Mohamed Njeh, Orhan Ermis, Melek Önen and Slim Trabelsi</i>	295
Systematic Evaluation of Probabilistic k-Anonymity for Privacy Preserving Micro-data Publishing and Analysis <i>Navoda Senavirathne and Vicenç Torra</i>	307
Boolean Exponent Splitting <i>Michael Tunstall, Louiza Papachristodoulou and Kostas Papagiannopoulos</i>	321
Proof-of-Forgery for Hash-based Signatures <i>Evgeniy Kiktenko, Mikhail Kudinov, Andrey Bulychev and Aleksey Fedorov</i>	333

Trusted Enforcement of Application-specific Security Policies <i>Marius Schlegel</i>	343
Responding to Living-Off-the-Land Tactics using Just-In-Time Memory Forensics (JIT-MF) for Android <i>Jennifer Bellizzi, Mark Vella, Christian Colombo and Julio Hernandez-Castro</i>	356
Cryptographic Enforcement of Access Control Policies in the Cloud: Implementation and Experimental Assessment <i>Stefano Berlato, Roberto Carbone and Silvio Ranise</i>	370
SHORT PAPERS	
Supporting Cyber Threat Analysis with Service-Oriented Enterprise Modeling <i>Kees Leune and Sung Kim</i>	385
Signer and Message Ambiguity from a Variety of Keys <i>George Teşeleanu</i>	395
Ransomware Detection using Markov Chain Models over File Headers <i>Nicolas Bailluet, H�el�ene Le Bouder and David Lubicz</i>	403
Proof-of-Useful-Randomness: Mitigating the Energy Waste in Blockchain Proof-of-Work <i>Efe Ulas Akay Seyitoglu, Attila Altay Yavuz and Thang Hoang</i>	412
A New MILP Model for Matrix Multiplications with Applications to KLEIN and PRINCE <i>Murat Burhan �lter and Ali Ayd�n Sel�uk</i>	420
Protecting End User’s Privacy When using Social Login through GDPR Compliance <i>Carlos Villar�n and Marta Beltr�n</i>	428
Efficient Joint Random Number Generation for Secure Multi-party Computation <i>Erwin Hoogerwerf, Daphne van Tetering, Asl� Bay and Zekeriya Erkin</i>	436
Improved Circuit Compilation for Hybrid MPC via Compiler Intermediate Representation <i>Daniel Demmler, Stefan Katzenbeisser, Thomas Schneider, Tom Schuster and Christian Weinert</i>	444
A Novel Security Framework for Minimization of False Information Dissemination in VANETs: Bayesian Game Formulation <i>Basant Subba and Ayushi Singh</i>	452
An Extension of the Avalanche Criterion in the Context of c-Differentials <i>P�l Ellingsen, Constanza Riera, Pantelimon St�nic� and Anton Tkachenko</i>	460
A New Delegated Authentication Protocol based on PRE <i>Anass Sbai, Cyril Drocourt and Gilles Dequen</i>	468
Mobile Family Detection through Audio Signals Classification <i>Rosangela Casolare, Giacomo Iadarola, Fabio Martinelli, Francesco Mercaldo and Antonella Santone</i>	479
Accurate Measurement of the Energy Consumption of Security Functions <i>Beno�t Fournier, Val�rie Viet Triem Tong and Gilles Guette</i>	487
Practically Efficient RFID Scheme with Constant-time Identification <i>Ferucio Lauren�iu �iplea and Cristian Hristea</i>	495

A Comparison of GKE Protocols based on SIDH <i>Hiroki Okada, Shinsaku Kiyomoto and Carlos Cid</i>	507
Multi-Party Private Set Intersection Protocols for Practical Applications <i>Asli Bay, Zeki Erkin, Mina Alishahi and Jelle Vos</i>	515
Using Program Analysis to Identify the Use of Vulnerable Functions <i>Rasmus Hagberg, Martin Hell and Christoph Reichenbach</i>	523
Compact Variable-base ECC Scalar Multiplication using Euclidean Addition Chains <i>Fabien Herbaut, Nicolas Méloni and Pascal Véron</i>	531
Secure Computation by Secret Sharing using Input Encrypted with Random Number <i>Keiichi Iwamura and Ahmad Akmal Aminuddin Mohd Kamal</i>	540
A Scalable Bitcoin-based Public Key Certificate Management System <i>Chloe Tartan, Craig Wright, Michaella Pettit and Wei Zhang</i>	548
Cloud Key Management using Trusted Execution Environment <i>Jaouhara Bouamama, Mustapha Hedabou and Mohammed Erradi</i>	560
An Improved Live Anomaly Detection System (I-LADS) based on Deep Learning Algorithms <i>Gustavo Gonzalez-Granadillo, Alejandro G. Bedoya and Rodrigo Diaz</i>	568
Inferring Flow Table State through Active Fingerprinting in SDN Environments: A Practical Approach <i>Marcin Gregorzcyk and Wojciech Mazurczyk</i>	576
SecSDN: A Novel Architecture for a Secure SDN <i>Parjanya Vyas and R. K. Shyamasundar</i>	587
Storage Friendly Provably Secure Multivariate Identity-Based Signature from Isomorphism of Polynomials Problem <i>Ratna Dutta, Sumit Kumar Debnath and Chinmoy Biswas</i>	595
Formal Security Verification of the Station-to-Station based Cell-attachment Procedure of LDACS <i>Nils Mäurer, Christoph Gentsch, Thomas Gräupl and Corinna Schmitt</i>	603
Side Channel Counter-measures based on Randomized AMNS Modular Multiplication <i>Christophe Negre</i>	611
Selective Owner-side Encryption in Digital Data Markets: Strategies for Key Derivation <i>Sara Foresti and Giovanni Livraga</i>	620
POSTERS	
Security Issues of Electronic and Mobile Banking <i>Wojciech Wodo, Damian Stygar and Przemysław Błażkiewicz</i>	631
Enforcing Cardinality Constraint in Temporal RBAC <i>Sohail Rajdev and Barsha Mitra</i>	639
Dynamic Access Control Framework for Enterprise Content Management Systems <i>Nadia Hocine and Ismail Bokhari</i>	647
AVX-512-based Parallelization of Block Sieving and Bucket Sieving for the General Number Field Sieve Method <i>Pritam Pallab and Abhijit Das</i>	653

Involving Humans in the Cryptographic Loop: Introduction and Threat Analysis of EEVEHAC <i>Julius Hekkala, Sara Nikula, Outi-Marja Latvala and Kimmo Halunen</i>	659
Empirical Security and Privacy Analysis of Mobile Symptom Checking Apps on Google Play <i>I. Wayan Budi Sentana, Muhammad Ikram, Mohamed Ali Kaafar and Shlomo Berkovsky</i>	665
BlockJack: Towards Improved Prevention of IP Prefix Hijacking Attacks in Inter-domain Routing via Blockchain <i>I. Wayan Budi Sentana, Muhammad Ikram and Mohamed Ali Kaafar</i>	674
Private Set Intersection: Past, Present and Future <i>Ionita Andreea</i>	680
MMU-based Access Control for Libraries <i>Marinos Tsantekidis and Vassilis Prevelakis</i>	686
Exposure Resilient Public-key Encryption with Keyword Search against Keyword Guessing Attack <i>Kaito Uemura and Satoshi Obana</i>	692
PUF based Lightweight Authentication and Key Exchange Protocol for IoT <i>Sourav Roy, Dipnarayan Das, Anindan Mondal, Mahabub Hasan Mahalat, Suchismita Roy and Bibhash Sen</i>	698
On Chameleon Pseudonymisation and Attribute Compartmentation-as-a-Service <i>Anne V. D. M. Kayem, Nikolai J. Podlesny, Christoph Meinel and Anja Lehmann</i>	704
Property Inference Attacks on Convolutional Neural Networks: Influence and Implications of Target Model's Complexity <i>Mathias Parisot, Balázs Pejó and Dayana Spagnuolo</i>	715
RMCCS: RSSI-based Message Consistency Checking Scheme for V2V Communications <i>Mujahid Muhammad, Paul Kearney, Adel Aneiba, Junaid Arshad and Andreas Kunz</i>	722
A New Method of Testing Machine Learning Models of Detection for Targeted DDoS Attacks <i>Mateusz Kozłowski and Bogdan Ksiezopolski</i>	728
Comparing Support Vector Machine and Neural Network Classifiers of CVE Vulnerabilities <i>Grzegorz J. Blinowski, Paweł Piotrowski and Michał Wiśniewski</i>	734
Privacy Aura for Transparent Authentication on Multiple Smart Devices <i>Takoua Guiga, Jean-Jacques Schwartzmann and Christophe Rosenberger</i>	741
Classifying Biometric Systems Users among the Doddington Zoo: Application to Keystroke Dynamics <i>Denis Migdal, Ilaria Magotti and Christophe Rosenberger</i>	747
Fair Mutual Authentication <i>Jacek Cichoń, Krzysztof Majcher and Mirosław Kutyłowski</i>	754
Towards CRYSTALS-Kyber VHDL Implementation <i>Sara Ricci, Petr Jedlicka, Peter Cibik, Petr Dzurenda, Lukas Malina and Jan Hajny</i>	760
Fast Cramer-Shoup Cryptosystem <i>Pascal Lafourcade, Léo Robert and Demba Sow</i>	766
RICAV: RiSk based Context-Aware Security Solution for the Intra-Electric Vehicle Network <i>Yosra Fraiji, Lamia ben Azzouz, Wassim Trojet, Ghaleb Hoblos and Leila Azouz Saidane</i>	772

Verify It Yourself: A Note on Activation Functions' Influence on Fast DeepFake Detection <i>Piotr Kawa and Piotr Syga</i>	779
GRANEF: Utilization of a Graph Database for Network Forensics <i>Milan Cermak and Denisa Sramkova</i>	785
Anonymous Attribute-based Credentials in Collaborative Indoor Positioning Systems <i>Raúl Casanova-Marqués, Pavel Pascacio, Jan Hajny and Joaquín Torres-Sospedra</i>	791
HIJaX: Human Intent JavaScript XSS Generator <i>Yaw Frempong, Yates Snyder, Erfan Al-Hossami, Meera Sridhar and Samira Shaikh</i>	798
User Identification from Time Series of Fitness Data <i>Thomas Marchioro, Andrei Kazlouski and Evangelos Markatos</i>	806
Privacy Preserving Scalable Authentication Protocol with Partially Trusted Third Party for Distributed Internet-of-Things <i>Hiral S. Trivedi and Sankita J. Patel</i>	812
C2RBAC: An Extended Capability-Role-Based Access Control with Context Awareness for Dynamic Environments <i>Mitsuhiro Mabuchi and Koji Hasebe</i>	819
Can Data Subject Perception of Privacy Risks Be Useful in a Data Protection Impact Assessment? <i>Salimeh Dashti, Anderson Santana de Oliveria, Caelin Kaplan, Manuel Dalcastagnè and Silvio Ranise</i>	827
Goal and Threat Modelling for Driving Automotive Cybersecurity Risk Analysis Conforming to ISO/SAE 21434 <i>Christophe Ponsard, Valery Ramon and Jean-Christophe Deprez</i>	833
Collateral-Free Trustworthiness-based Personal Lending on a Decentralized Application (DApp) <i>Wisnu Uriawan, Omar Hasan, Youakim Badr and Lionel Brunie</i>	839
Investing Data with Untrusted Parties using HE <i>Mark Dockendorf, Ram Dantu, Kirill Morozov and Sanjukta Bhowmick</i>	845
Machine Learning Classification of Obfuscation using Image Visualization <i>Colby B. Parker, J. Todd McDonald and Dimitrios Damopoulos</i>	854
AUTHOR INDEX	861