2014 11th International Conference on Security and Cryptography (SECRYPT 2014)

Vienna, Austria
28-30 August 2014

IEEE Catalog Number: CFP1482N-POD
ISBN: 978-1-4673-9240-2

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

IEEE Catalog Number: CFP1482N-POD
ISBN (Print-On-Demand): 978-1-4673-9240-2
ISBN (Online): 978-989-8565-95-2

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

CONTENTS

INVITED SPEAKERS

KEYNOTE SPEAKERS

A Need-based Assessment for Building a National Cyber Security Workforce
Seymour Goodman IS-5

Democratization in Science and Technology through Cloud Computing
Ivona Brandić IS-7

Model-driven Development of Multi-View Modelling Tools - The MUVIEMOT Approach
Dimitris Karagiannis IS-9

Social Business Intelligence - OLAP Applied to User Generated Contents
Matteo Golfarelli IS-11

Advanced Persistent Threats & Social Engineering
Edgar Weippl IS-13

PAPERS

FULL PAPERS

CloudaSec: A Novel Public-key Based Framework to Handle Data Sharing Security in Clouds
Nesrine Kaaniche, Maryline Laurent and Mohammed El Barbori 5

Keeping Intruders at Large - A Graph-theoretic Approach to Reducing the Probability of Successful Network Intrusions
Paulo Shakarian, Damon Paulo, Massimiliano Albanese and Sushil Jajodia 19

Certificateless Non-Interactive Key Exchange Protocol without Pairings
Yun Wei, Fushan Wei and Chuangui Ma 31

Adaptive Oblivious Transfer with Hidden Access Policy Realizing Disjunction
Vandana Guleria and Ratna Dutta 43

A Secure Anonymous Proxy Multi-signature Scheme
Vishal Saraswat and Rajeev Anand Sahu 55

Pairing-free Single Round Certificateless and Identity Based Authenticated Key Exchange Protocols
Saikrishna Badrinarayanan and C. Pandu Rangan 67

Mobile Devices - A Phisher's Paradise
Nikos Virvilis, Nikolaos Tsalis, Alexios Mylonas and Dimitris Gritzalis 79

Dynamic Analysis of Usage Control Policies
Yehia Elrakaiby and Jun Pang 88

Formal Analysis of Electronic Exams
Jannik Dreier, Rosario Giustolisi, Ali Kassem, Pascal Lafourcade, Gabriele Lenzini and Peter Y. A. Ryan 101

Towards a Framework for Assessing the Feasibility of Side-channel Attacks in Virtualized Environments
Tsvetoslava Vateva-Gurova, Jesus Luna, Giancarlo Pellegrino and Neeraj Suri 113

FORCE - Fully Off-line secuRe CrEdits for Mobile Micro Payments
Vanesa Daza, Roberto Di Pietro, Flavio Lombardi and Matteo Signorini 125

Privacy Preserving Delegated Word Search in the Cloud
Kaoutar Elkhiyaoui, Melek Önen and Refik Molva 137

Identifying Cryptographic Functionality in Android Applications
Alexander Oprisnik, Daniel Hein and Peter Teufl 151

SHORT PAPERS

A Formal Model for Forensic Storage Media Preparation Tools
Benjamin Aziz, Philippe Massonet and Christophe Ponsard 165

An Efficient Lightweight Security Algorithm for Random Linear Network Coding
Hassan Noura, Steven Martin and Khaldoun Al Agha 171

A Steganographic Protocol Based on Linear Error-Block Codes
Rabiî Dariti and El Mamoun Souidi 178

Enhanced Intrusion Detection System Based on Bat Algorithm-support Vector Machine
Adriana-Cristina Enache and Valentin Sgârciu 184

Robust Multispectral Palmprint Identification System by Jointly Using Contourlet Decomposition & Gabor Filter Response
Abdallah Meraoumia, Salim Chitroub and Ahmed Bouridane 190

Shellcode Detection in IPv6 Networks with HoneydV6
Sven Schindler, Oliver Eggert, Bettina Schnor and Thomas Scheffler 198

Signaling Attacks in Mobile Telephony
Mihajlo Pavloski and Erol Gelenbe 206

Efficient Construction of Infinite Length Hash Chains with Perfect Forward Secrecy Using Two Independent Hash Functions
Sebastian Bittl 213

SMS Spam - A Holistic View
Lamine Aouad, Alejandro Mosquera, Slawomir Grzonkowski and Dylan Morss 221

Constructing Empirical Tests of Randomness
Marek Sýs, Petr Švenda, Martin Ukrop and Vashek Matyáš 229

Hybrid-Style Personal Key Management in Ubiquitous Computing
Byoungcheon Lee 238

Using the Juliet Test Suite to Compare Static Security Scanners
Andreas Wagner and Johannes Sametinger 244

Secure Video Player for Mobile Devices Integrating a Watermarking-based Tracing Mechanism
Pablo Antón del Pino, Antoine Monsifrot, Charles Salmon-Legagneur and Gwenaël Doërr 253

On Privacy Protection in the Internet Surveillance Era
Dijana Vukovic, Danilo Gligoroski and Zoran Djuric 261

Framework for Securing Data in Cloud Storage Services
Mai Dahshan and Sherif Elkassas 267

Partial Fingerprint Identification Through Correlation-based Approach 275
Omid Zanganeh, Nandita Bhattacharjee and Bala Srinivasan

Framework Implementation Based on Grid of Smartcards to Authenticate Users and Virtual Machines 285
Hassane Aissaoui-Mehrez, Pascal Urien and Guy Pujolle

On Reliability of Clock-skew-based Remote Computer Identification 291
Libor Polčák and Barbora Franková

KDM-CCA Security of the Cramer-Shoup Cryptosystem, Revisited 299
Jinyong Chang and Rui Xue

A Multiple-server Efficient Reusable Proof of Data Possesion from Private Information Retrieval Techniques 307
Juan Camilo Corena, Anirban Basu, Yuto Nakano, Shinsaku Kiyomoto and Yutaka Miyake

Modeling Requirements for Security-enhanced Design of Embedded Systems **N/A**
Alberto Ferrante, Igor Kaitovic and Jelena Milosevic

A Novel Pseudo Random Number Generator Based on L'Ecuyer's Scheme 321
Francesco Buccafurri and Gianluca Lax

Verifying Conformance of Security Implementation with Organizational Access Policies in Community Cloud - A Formal Approach 329
Nirnay Ghosh, Triparna Mondal, Debangshu Chatterjee and Soumya K. Ghosh

NFC Based Mobile Single Sign-On Solution as a Chrome Extension 337
Ufuk Celikkan and Can Gelis

Secure Virtual Machine Migration (SV2M) in Cloud Federation 344
Muhammad Awais Shibli, Naveed Ahmad, Ayesha Kanwal and Abdul Ghafoor

Randomized Addition of Sensitive Attributes for l-diversity 350
Yuichi Sei and Akihiko Ohsuga

Optimizing Elliptic Curve Scalar Multiplication with Near-Factorization 361
Pratik Poddar, Achin Bansal and Bernard Menezes

A Hybrid Approach for Content Based Image Authentication 371
Jinse Shin and Christoph Ruland

Revisiting a Recent Resource-efficient Technique for Increasing the Throughput of Stream Ciphers 379
Frederik Armknecht and Vasily Mikhalev

Secure Protocol for Financial Transactions Using Smartphones - SPFT - Formally Proved by AVISPA 387
Shizra Sultan, Abdul Ghafoor Abbasi, Awais Shibli and Ali Nasir

A Cryptographic Study of Tokenization Systems 393
Sandra Díaz-Santiago, Lil Maria Rodriguez-Henriquez and Debrup Chakraborty

Combined Algebraic and Truncated Differential Cryptanalysis on Reduced-round Simon 399
Nicolas Courtois, Theodosis Mourouzis, Guangyan Song, Pouyan Sepehrdad and Petr Susil

Software and Hardware Certification Techniques in a Combined Certification Model 405
Antonio Muñoz and Antonio Maña

Experimental Study of Performance and Security Constraints on Wireless Key Distribution Using Random Phase of Multipath Radio Signal 411
Amir I. Sulimov, Alexey D. Smolyakov, Arkadij V. Karpov and Oleg N. Sherstyukov

Network-based Intrusion Prevention System Prototype with Multi-Detection - A Position Paper 417
Daniel Kavan, Klára Škodová and Martin Klíma

Could Bitcoin Transactions Be 100x Faster? 426
Nicolas T. Courtois, Pinar Emirdag and Daniel A. Nagy

Using Bitmaps for Executing Range Queries in Encrypted Databases 432
Lil María Rodríguez-Henríquez and Debrup Chakraborty

Differential Fault Attacks against AES Tampering with the Instruction Flow 439
Silvia Mella, Filippo Melzani and Andrea Visconti

Secure Key Distribution based on Meteor Burst Communications 445
Amir Sulimov and Arkadij Karpov

COGITO: Code Polymorphism to Secure Devices 451
Damien Couroussé, Bruno Robisson, Jean-Louis Lanet, Thierno Barry, Hassan Noura, Philippe Jaillon and Philippe Lalevée

Using Abductive and Inductive Inference to Generate Policy Explanations 457
Fabio Marfia

Towards a Legislation Driven Framework for Access Control and Privacy Protection in Public Cloud 463
Maherzia Belaazi, Hanen Boussi Rahmouni and Adel Bouhoula

Pseudorandom Number Generators with Balanced Gray Codes 469
J.-F. Couchot, P.-C. Heam, C. Guyeux, Q. Wang and J. M. Bahi

Keeping an Eye on Your Security Through Assurance Indicators 476
Moussa Ouedraogo, Chien-Ting Kuo, Simon Tjoa, David Preston, Eric Dubois, Paulo Simoes and Tiago Cruz

QR Steganography - A Threat to New Generation Electronic Voting Systems 484
Jordi Cucurull, Sandra Guasch, Alex Escala, Guillermo Navarro-Arribas and Víctor Acín

On the Security of Partially Masked Software Implementations 492
Alessandro Barenghi and Gerardo Pelosi

RBAC with ABS - Implementation Practicalities for RBAC Integrity Policies 500
Mikko Kiviharju

AUTHOR INDEX 511