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

Vienna, Austria
28-30 August 2014
CONTENTS

INVITED SPEAKERS

KEYNOTE SPEAKERS
A Need-based Assessment for Building a National Cyber Security Workforce
Seymour Goodman

Democratization in Science and Technology through Cloud Computing
Ivona Brandić

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

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

Advanced Persistent Threats & Social Engineering
Edgar Weippl

PAPERS

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

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

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

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

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

Pairing-free Single Round Certificateless and Identity Based Authenticated Key Exchange Protocols
SaiKrishna Badrinarayanan and C. Panda Rangan

Mobile Devices - A Phisher’s Paradise
Nikos Virvilis, Nikolaos Tsalis, Alexios Mylonas and Dimitris Grizalis

Dynamic Analysis of Usage Control Policies
Yehia Elrakaby and Jun Pang

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

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

XII
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
Koautar Elkhyaoui, Melek Onen and Refik Molva 137

Identifying Cryptographic Functionality in Android Applications
Alexander Oprisnik, Daniel Hein and Peter Teuff 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 Khalidoun Al Agha 171

A Steganographic Protocol Based on Linear Error-Block Codes
Rabih Darit and El Manouni Soudi 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

Shellecode 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 Morris 221

Constructing Empirical Tests of Randomness
Marek Syś, Petr Švenda, Martin Ukrop and Vashek Matyaš 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 Environment
Dijana Vukovic, Danilo Gligorosi 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
Omid Zanganee, Nandita Bhattacharjee and Bala Srinivasan 275

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

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

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

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

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

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

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

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

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

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

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

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

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

Secure Protocol for Financial Transactions Using Smartphones - SPFT - Formally Proved by AVISPA
Shuzra Sultani, Abdul Ghafoor Abbasi, Awaiz Shibli and Ali Nasir 387

A Cryptographic Study of Tokenization Systems
Sandra Díaz-Santiago, Lil María Rodríguez-Henríquez and Debrup Chakraborty 393

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

Software and Hardware Certification Techniques in a Combined Certification Model
Antonio Muñoz and Antonio María 405
Experimental Study of Performance and Security Constraints on Wireless Key Distribution Using Random Phase of Multipath Radio Signal
Amir I. Salimov, Alexey D. Smolyakov, Arkadij V. Karpov and Oleg N. Sherstyukov
411

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

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

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

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

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

COGITO: Code Polymorphism to Secure Devices
Damien Courroux, Bruno Robisson, Jean-Louis Lanet, Therno Barry, Hassan Noura, Philippe Jaillot and Philippe Lalévé
451

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

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

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

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

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

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

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

AUTHOR INDEX
511