Contents – Part I

Networks and Web Security

Towards Security of Internet Naming Infrastructure
Haya Shulman and Michael Waidner 3

Waiting for CSP – Securing Legacy Web Applications with JSAgents
Mario Heiderich, Marcus Niemietz, and Jörg Schwenk 23

Analyzing the BrowserID SSO System with Primary Identity Providers
Using an Expressive Model of the Web
Daniel Fett, Ralf Küsters, and Guido Schmitz 43

System Security

A Practical Approach for Adaptive Data Structure Layout Randomization
Ping Chen, Jun Xu, Zhiqiang Lin, Dongyan Xu, Bing Mao, and Peng Liu 69

Trustworthy Prevention of Code Injection in Linux on Embedded Devices
Hind Chfouka, Hamed Nemati, Roberto Guanciale, Mads Dam,
and Patrik Ekdahl 90

Practical Memory Deduplication Attacks in Sandboxed Javascript
Daniel Gruss, David Bidner, and Stefan Mangard 108

Cryptography

Computational Soundness for Interactive Primitives
Michael Backes, Esfandiar Mohammadi, and Tim Ruffing 125

Verifiably Encrypted Signatures: Security Revisited and a New
Construction
Christian Hanser, Max Rabkin, and Dominique Schröder 146

Interleaving Cryptanalytic Time-Memory Trade-Offs on Non-uniform
Distributions
Gildas Avoine, Xavier Carpent, and Cédric Lauradoux 165

Efficient Message Authentication Codes with Combinatorial Group Testing
Kazuhiko Minematsu 185
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symmetric-Key Based Proofs of Retrievability Supporting Public</td>
<td>203</td>
</tr>
<tr>
<td>Verification</td>
<td></td>
</tr>
<tr>
<td>Chaowen Guan, Kui Ren, Fangguo Zhang, Florian Kerschbaum, and Jia Yu</td>
<td></td>
</tr>
<tr>
<td>DTLS-HIMMO: Achieving DTLS Certificate Security with Symmetric Key</td>
<td>224</td>
</tr>
<tr>
<td>Overhead</td>
<td></td>
</tr>
<tr>
<td>Oscar Garcia-Morchon, Ronald Rietman, Sahil Sharma, Ludo Tolhuizen,</td>
<td></td>
</tr>
<tr>
<td>and Jose Luis Torre-Arce</td>
<td></td>
</tr>
<tr>
<td>Short Accountable Ring Signatures Based on DDH</td>
<td>243</td>
</tr>
<tr>
<td>Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi,</td>
<td></td>
</tr>
<tr>
<td>Jens Groth, and Christophe Petit</td>
<td></td>
</tr>
<tr>
<td>Updatable Hash Proof System and Its Applications</td>
<td>266</td>
</tr>
<tr>
<td>Rupeng Yang, Qiuliang Xu, Yongbin Zhou, Rui Zhang, Chengyu Hu,</td>
<td></td>
</tr>
<tr>
<td>and Zuoxia Yu</td>
<td></td>
</tr>
<tr>
<td>Server-Aided Revocable Identity-Based Encryption</td>
<td>286</td>
</tr>
<tr>
<td>Baodong Qin, Robert H. Deng, Yingjiu Li, and Shengli Liu</td>
<td></td>
</tr>
<tr>
<td>Efficient Zero-Knowledge Proofs for Commitments from Learning</td>
<td>305</td>
</tr>
<tr>
<td>with Errors over Rings</td>
<td></td>
</tr>
<tr>
<td>Fabrice Benhamouda, Stephan Krenn, Vadim Lyubashevsky, and Krzysztof</td>
<td></td>
</tr>
<tr>
<td>Pietrzak</td>
<td></td>
</tr>
<tr>
<td>Making Any Identity-Based Encryption Accountable, Efficiently</td>
<td>326</td>
</tr>
<tr>
<td>Aggelos Kiayias and Qiang Tang</td>
<td></td>
</tr>
<tr>
<td>Practical Threshold Password-Authenticated Secret Sharing Protocol</td>
<td>347</td>
</tr>
<tr>
<td>Xun Yi, Feng Hao, Liqun Chen, and Joseph K. Liu</td>
<td></td>
</tr>
<tr>
<td>On Security of Content-Based Video Stream Authentication</td>
<td>366</td>
</tr>
<tr>
<td>Swee-Won Lo, Zhuo Wei, Robert H. Deng, and Xuhua Ding</td>
<td></td>
</tr>
<tr>
<td>Oblivious Maximum Bipartite Matching Size Algorithm with Applications</td>
<td>384</td>
</tr>
<tr>
<td>to Secure Fingerprint Identification</td>
<td></td>
</tr>
<tr>
<td>Marina Blanton and Siddharth Saraph</td>
<td></td>
</tr>
<tr>
<td>Practical Invalid Curve Attacks on TLS-ECDH</td>
<td>407</td>
</tr>
<tr>
<td>Tibor Jager, Jörg Schwenk, and Juraj Somorovsky</td>
<td></td>
</tr>
<tr>
<td><strong>Crypto Applications and Attacks</strong></td>
<td></td>
</tr>
<tr>
<td>Challenging the Trustworthiness of PGP: Is the Web-of-Trust Tear-</td>
<td>429</td>
</tr>
<tr>
<td>Proof?</td>
<td></td>
</tr>
<tr>
<td>Alessandro Barenghi, Alessandro Di Federico, Gerardo Pelosi,</td>
<td></td>
</tr>
<tr>
<td>and Stefano Sanfilippo</td>
<td></td>
</tr>
</tbody>
</table>
Transforming Out Timing Leaks, More or Less ............... 447
Heiko Mantel and Artem Starostin

Small Tweaks Do Not Help: Differential Power Analysis of MILENAGE Implementations in 3G/4G USIM Cards ......................... 468
Junrong Liu, Yu Yu, François-Xavier Standaert, Zheng Guo, Dawu Gu, Wei Sun, Yijie Ge, and Xinjun Xie

Risk Analysis

Aron Laszka and Jens Grossklags

Lightweight and Flexible Trust Assessment Modules for the Internet of Things .................................................. 503
Jan Tobias Mühlberg, Job Noorman, and Frank Piessens

Confidence Analysis for Nuclear Arms Control: SMT Abstractions of Bayesian Belief Networks ............................ 521
Paul Beaumont, Neil Evans, Michael Huth, and Tom Plant

Author Index ................................................. 541

Contents – Part I XIII
## Contents – Part II

### Privacy

**FP-Block: Usable Web Privacy by Controlling Browser Fingerprinting** ........................................... 3  
Christof Ferreira Torres, Hugo Jonker, and Sjouke Mauw

**Mind-Reading: Privacy Attacks Exploiting Cross-App KeyEvent Injections** ......................... 20  
Wenrui Diao, Xiangyu Liu, Zhe Zhou, Kehuan Zhang, and Zhou Li

**Enabling Privacy-Assured Similarity Retrieval over Millions of Encrypted Records** ........ 40  
Xingliang Yuan, Helei Cui, Xinyu Wang, and Cong Wang

**Privacy-Preserving Link Prediction in Decentralized Online Social Networks** ..................... 61  
Yao Zheng, Bing Wang, Wenjing Lou, and Y. Thomas Hou

**Privacy-Preserving Observation in Public Spaces** ................................................................. 81  
Florian Kerschbaum and Hoon Wei Lim

**Privacy-Preserving Context-Aware Recommender Systems: Analysis and New Solutions** .... 101  
Qiang Tang and Jun Wang

### Cloud Security

**Rich Queries on Encrypted Data: Beyond Exact Matches** ....................................................... 123  
Sky Faber, Stanislaw Jarecki, Hugo Krawczyk, Quan Nguyen, Marcel Rosu, and Michael Steiner

**Extended Proxy-Assisted Approach: Achieving Revocable Fine-Grained Encryption of Cloud Data** 146  
Yanjiang Yang, Joseph K. Liu, Kaitai Liang, Kim-Kwang Raymond Choo, and Jianying Zhou

**Batch Verifiable Computation of Polynomials on Outsourced Data** ................................ 167  
Liang Feng Zhang and Reihaneh Safavi-Naini

**CloudBI: Practical Privacy-Preserving Outsourcing of Biometric Identification in the Cloud** ...... 186  
Qian Wang, Shengshan Hu, Kui Ren, Meiqi He, Minxin Du, and Zhibo Wang
Protocols and Attribute-Based Encryption

Typing and Compositionality for Security Protocols: A Generalization to the Geometric Fragment

Omar Almousa, Sebastian Mödersheim, Paolo Modesti, and Luca Viganò

Checking Trace Equivalence: How to Get Rid of Nonces?

Rémy Chrétien, Véronique Cortier, and Stéphanie Delaune

Attribute Based Broadcast Encryption with Short Ciphertext and Decryption Key

Tran Viet Xuan Phuong, Guomin Yang, Willy Susilo, and Xiaofeng Chen

Accountable Authority Ciphertext-Policy Attribute-Based Encryption with White-Box Traceability and Public Auditing in the Cloud

Jianting Ning, Xiaolei Dong, Zhenfu Cao, and Lifei Wei

Code Analysis and Side-Channels

DexHunter: Toward Extracting Hidden Code from Packed Android Applications

Yueqian Zhang, Xiapu Luo, and Haoyang Yin

Identifying Arbitrary Memory Access Vulnerabilities in Privilege-Separated Software

Hong Hu, Zheng Leong Chua, Zhenkai Liang, and Prateek Saxena

vBox: Proactively Establishing Secure Channels Between Wireless Devices Without Prior Knowledge

Wei Wang, Jingqiang Lin, Zhan Wang, Ze Wang, and Luning Xia

Detection and Monitoring

Accurate Specification for Robust Detection of Malicious Behavior in Mobile Environments

Sufatrio, Tong-Wei Chua, Darell J.J. Tan, and Vrizlynn L.L. Thing

A Bytecode Interpreter for Secure Program Execution in Untrusted Main Memory

Maximilian Seitzer, Michael Gruhn, and Tilo Müller

Learning from Others: User Anomaly Detection Using Anomalous Samples from Other Users

Youngja Park, Ian M. Molloy, Suresh N. Chari, Zenglin Xu, Chris Gates, and Ninghi Li
## Authentication

Towards Attack-Resistant Peer-Assisted Indoor Localization .......................... Jingyu Hua, Shaoyong Du, and Sheng Zhong


The Emperor’s New Password Creation Policies:: An Evaluation of Leading Web Services and the Effect of Role in Resisting Against Online Guessing ................................................... Ding Wang and Ping Wang

## Policies

A Theory of Gray Security Policies ............................................................ Donald Ray and Jay Ligatti

Factorization of Behavioral Integrity ...................................................... Ximeng Li, Flemming Nielson, and Hanne Riis Nielson

Checking Interaction-Based Declassification Policies for Android Using Symbolic Execution .................................................. Kristopher Micinski, Jonathan Fetter-Degges, Jinseong Jeon, Jeffrey S. Foster, and Michael R. Clarkson

## Applied Security

Enhancing Java Runtime Environment for Smart Cards Against Runtime Attacks .................................................. Raja Naeem Akram, Konstantinos Markantonakis, and Keith Mayes

Making Bitcoin Exchanges Transparent .................................................. Christian Decker, James Guthrie, Jochen Seidel, and Roger Wattenhofer

Web-to-Application Injection Attacks on Android: Characterization and Detection .................................................. Behnaz Hassanshahi, Yaoqi Jia, Roland H.C. Yap, Prateek Saxena, and Zhenkai Liang

All Your Voices are Belong to Us: Stealing Voices to Fool Humans and Machines .................................................. Dibya Mukhopadhyay, Maliheh Shirvanian, and Nitesh Saxena

Balloon: A Forward-Secure Append-Only Persistent Authenticated Data Structure .................................................. Tobias Pulls and Roel Peeters
On the Fly Design and Co-simulation of Responses Against Simultaneous Attacks .......................... 642

Léa Samarji, Nora Cuppens-Boulahia, Frédéric Cuppens, Serge Papillon, Waël Kanoun, and Samuel Dubus

Author Index ................................................................. 663
Computer Security -- ESORICS 2015
20th European Symposium on Research in Computer
Security, Vienna, Austria, September 21-25, 2015,
Proceedings, Part I
Pernul, G.; Y A Ryan, P.; Weippl, E. (Eds.)
2015, XVIII, 543 p. 114 illus. in color., Softcover
ISBN: 978-3-319-24173-9