

## Contents – Part II

### Privacy

<i>FP-Block: Usable Web Privacy by Controlling Browser Fingerprinting . . . . .</i>	<i>3</i>
<i>Christof Ferreira Torres, Hugo Jonker, and Sjouke Mauw</i>	
<i>Mind-Reading: Privacy Attacks Exploiting Cross-App KeyEvent Injections. . . . .</i>	<i>20</i>
<i>Wenrui Diao, Xiangyu Liu, Zhe Zhou, Kehuan Zhang, and Zhou Li</i>	
<i>Enabling Privacy-Assured Similarity Retrieval over Millions of Encrypted Records . . . . .</i>	<i>40</i>
<i>Xingliang Yuan, Helei Cui, Xinyu Wang, and Cong Wang</i>	
<i>Privacy-Preserving Link Prediction in Decentralized Online Social Networks . . . . .</i>	<i>61</i>
<i>Yao Zheng, Bing Wang, Wenjing Lou, and Y. Thomas Hou</i>	
<i>Privacy-Preserving Observation in Public Spaces. . . . .</i>	<i>81</i>
<i>Florian Kerschbaum and Hoon Wei Lim</i>	
<i>Privacy-Preserving Context-Aware Recommender Systems: Analysis and New Solutions . . . . .</i>	<i>101</i>
<i>Qiang Tang and Jun Wang</i>	

### Cloud Security

<i>Rich Queries on Encrypted Data: Beyond Exact Matches. . . . .</i>	<i>123</i>
<i>Sky Faber, Stanislaw Jarecki, Hugo Krawczyk, Quan Nguyen, Marcel Rosu, and Michael Steiner</i>	
<i>Extended Proxy-Assisted Approach: Achieving Revocable Fine-Grained Encryption of Cloud Data . . . . .</i>	<i>146</i>
<i>Yanjiang Yang, Joseph K. Liu, Kaitai Liang, Kim-Kwang Raymond Choo, and Jianying Zhou</i>	
<i>Batch Verifiable Computation of Polynomials on Outsourced Data . . . . .</i>	<i>167</i>
<i>Liang Feng Zhang and Reihaneh Safavi-Naini</i>	
<i>CloudBI: Practical Privacy-Preserving Outsourcing of Biometric Identification in the Cloud . . . . .</i>	<i>186</i>
<i>Qian Wang, Shengshan Hu, Kui Ren, Meiqi He, Minxin Du, and Zhibo Wang</i>	

**Protocols and Attribute-Based Encryption**

Typing and Compositionality for Security Protocols: A Generalization to the Geometric Fragment. . . . .	209
<i>Omar Almousa, Sebastian Mödersheim, Paolo Modesti, and Luca Viganò</i>	
Checking Trace Equivalence: How to Get Rid of Nonces? . . . . .	230
<i>Rémy Chrétien, Véronique Cortier, and Stéphanie Delaune</i>	
Attribute Based Broadcast Encryption with Short Ciphertext and Decryption Key . . . . .	252
<i>Tran Viet Xuan Phuong, Guomin Yang, Willy Susilo, and Xiaofeng Chen</i>	
Accountable Authority Ciphertext-Policy Attribute-Based Encryption with White-Box Traceability and Public Auditing in the Cloud. . . . .	270
<i>Jianting Ning, Xiaolei Dong, Zhenfu Cao, and Lifei Wei</i>	

**Code Analysis and Side-Channels**

DexHunter: Toward Extracting Hidden Code from Packed Android Applications. . . . .	293
<i>Yueqian Zhang, Xiapu Luo, and Haoyang Yin</i>	
Identifying Arbitrary Memory Access Vulnerabilities in Privilege-Separated Software . . . . .	312
<i>Hong Hu, Zheng Leong Chua, Zhenkai Liang, and Prateek Saxena</i>	
vBox: Proactively Establishing Secure Channels Between Wireless Devices Without Prior Knowledge. . . . .	332
<i>Wei Wang, Jingqiang Lin, Zhan Wang, Ze Wang, and Luning Xia</i>	

**Detection and Monitoring**

Accurate Specification for Robust Detection of Malicious Behavior in Mobile Environments. . . . .	355
<i>Sufatrio, Tong-Wei Chua, Darell J.J. Tan, and Vrizlynn L.L. Thing</i>	
A Bytecode Interpreter for Secure Program Execution in Untrusted Main Memory . . . . .	376
<i>Maximilian Seitzer, Michael Gruhn, and Tilo Müller</i>	
Learning from Others: User Anomaly Detection Using Anomalous Samples from Other Users . . . . .	396
<i>Youngja Park, Ian M. Molloy, Suresh N. Chari, Zenglin Xu, Chris Gates, and Ninghi Li</i>	

**Authentication**

Towards Attack-Resistant Peer-Assisted Indoor Localization. . . . .	417
<i>Jingyu Hua, Shaoyong Du, and Sheng Zhong</i>	
Leveraging Real-Life Facts to Make Random Passwords More Memorable. . . .	438
<i>Mahdi Nasrullah Al-Ameen, Kanis Fatema, Matthew Wright, and Shannon Scielzo</i>	
The Emperor’s New Password Creation Policies:: An Evaluation of Leading Web Services and the Effect of Role in Resisting Against Online Guessing . . . . .	456
<i>Ding Wang and Ping Wang</i>	

**Policies**

A Theory of Gray Security Policies. . . . .	481
<i>Donald Ray and Jay Ligatti</i>	
Factorization of Behavioral Integrity . . . . .	500
<i>Ximeng Li, Flemming Nielson, and Hanne Riis Nielson</i>	
Checking Interaction-Based Declassification Policies for Android Using Symbolic Execution . . . . .	520
<i>Kristopher Micinski, Jonathan Fetter-Degges, Jinseong Jeon, Jeffrey S. Foster, and Michael R. Clarkson</i>	

**Applied Security**

Enhancing Java Runtime Environment for Smart Cards Against Runtime Attacks . . . . .	541
<i>Raja Naeem Akram, Konstantinos Markantonakis, and Keith Mayes</i>	
Making Bitcoin Exchanges Transparent . . . . .	561
<i>Christian Decker, James Guthrie, Jochen Seidel, and Roger Wattenhofer</i>	
Web-to-Application Injection Attacks on Android: Characterization and Detection . . . . .	577
<i>Behnaz Hassanshahi, Yaoqi Jia, Roland H.C. Yap, Prateek Saxena, and Zhenkai Liang</i>	
All Your Voices are Belong to Us: Stealing Voices to Fool Humans and Machines . . . . .	599
<i>Dibya Mukhopadhyay, Maliheh Shirvanian, and Nitesh Saxena</i>	
Balloon: A Forward-Secure Append-Only Persistent Authenticated Data Structure. . . . .	622
<i>Tobias Pulls and Roel Peeters</i>	

On the Fly Design and Co-simulation of Responses Against Simultaneous Attacks . . . . .	642
<i>Léa Samarji, Nora Cuppens-Boulahia, Frédéric Cuppens, Serge Papillon, Waël Kanoun, and Samuel Dubus</i>	
<b>Author Index</b> . . . . .	663

# Contents – Part I

## Networks and Web Security

Towards Security of Internet Naming Infrastructure . . . . .	3
<i>Haya Shulman and Michael Waidner</i>	
Waiting for CSP – Securing Legacy Web Applications with JSAgents . . . . .	23
<i>Mario Heiderich, Marcus Niemietz, and Jörg Schwenk</i>	
Analyzing the BrowserID SSO System with Primary Identity Providers Using an Expressive Model of the Web . . . . .	43
<i>Daniel Fett, Ralf Küsters, and Guido Schmitz</i>	

## System Security

A Practical Approach for Adaptive Data Structure Layout Randomization . . .	69
<i>Ping Chen, Jun Xu, Zhiqiang Lin, Dongyan Xu, Bing Mao, and Peng Liu</i>	
Trustworthy Prevention of Code Injection in Linux on Embedded Devices . . .	90
<i>Hind Chfouka, Hamed Nemati, Roberto Guanciale, Mads Dam, and Patrik Ekdahl</i>	
Practical Memory Deduplication Attacks in Sandboxed Javascript . . . . .	108
<i>Daniel Gruss, David Bidner, and Stefan Mangard</i>	

## Cryptography

Computational Soundness for Interactive Primitives . . . . .	125
<i>Michael Backes, Esfandiar Mohammadi, and Tim Ruffing</i>	
Verifiably Encrypted Signatures: Security Revisited and a New Construction . . . . .	146
<i>Christian Hanser, Max Rabkin, and Dominique Schröder</i>	
Interleaving Cryptanalytic Time-Memory Trade-Offs on Non-uniform Distributions . . . . .	165
<i>Gildas Avoine, Xavier Carpent, and Cédric Lauradoux</i>	
Efficient Message Authentication Codes with Combinatorial Group Testing . . .	185
<i>Kazuhiko Minematsu</i>	

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

Transforming Out Timing Leaks, More or Less . . . . .	447
<i>Heiko Mantel and Artem Starostin</i>	
Small Tweaks Do Not Help: Differential Power Analysis of MILENAGE Implementations in 3G/4G USIM Cards. . . . .	468
<i>Junrong Liu, Yu Yu, François-Xavier Standaert, Zheng Guo, Dawu Gu, Wei Sun, Yijie Ge, and Xinjun Xie</i>	
<b>Risk Analysis</b>	
Should Cyber-Insurance Providers Invest in Software Security? . . . . .	483
<i>Aron Laszka and Jens Grossklags</i>	
Lightweight and Flexible Trust Assessment Modules for the Internet of Things. . . . .	503
<i>Jan Tobias Mühlberg, Job Noorman, and Frank Piessens</i>	
Confidence Analysis for Nuclear Arms Control: SMT Abstractions of Bayesian Belief Networks . . . . .	521
<i>Paul Beaumont, Neil Evans, Michael Huth, and Tom Plant</i>	
<b>Author Index</b> . . . . .	541

Computer Security -- ESORICS 2015

20th European Symposium on Research in Computer  
Security, Vienna, Austria, September 21-25, 2015,  
Proceedings, Part II

Pernul, G.; Y A Ryan, P.; Weippl, E.R. (Eds.)

2015, XVII, 665 p. 124 illus., Softcover

ISBN: 978-3-319-24176-0