### Contents – Part I

#### Networks and Web Security

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

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

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

#### System Security

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

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

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

#### Cryptography

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

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

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

- **Efficient Message Authentication Codes with Combinatorial Group Testing** .... 185  
  *Kazuhiko Minematsu*
Symmetric-Key Based Proofs of Retrievability Supporting Public Verification ............................................................... 203
Chaowen Guan, Kui Ren, Fangguo Zhang, Florian Kerschbaum, and Jia Yu

DTLS-HIMMO: Achieving DTLS Certificate Security with Symmetric Key Overhead ......................................................... 224
Oscar Garcia-Morchon, Ronald Rietman, Sahil Sharma, Ludo Tolhuizen, and Jose Luis Torre-Arce

Short Accountable Ring Signatures Based on DDH .......................................................... 243
Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, Jens Groth, and Christophe Petit

Updatable Hash Proof System and Its Applications .................................................. 266
Rupeng Yang, Qiuliang Xu, Yongbin Zhou, Rui Zhang, Chengyu Hu, and Zuoxia Yu

Server-Aided Revocable Identity-Based Encryption .................................................. 286
Baodong Qin, Robert H. Deng, Yingjiu Li, and Shengli Liu

Efficient Zero-Knowledge Proofs for Commitments from Learning with Errors over Rings .................................................. 305
Fabrice Benhamouda, Stephan Krenn, Vadim Lyubashevsky, and Krzysztof Pietrzak

Making Any Identity-Based Encryption Accountable, Efficiently ................................ 326
Aggelos Kiayias and Qiang Tang

Practical Threshold Password-Authenticated Secret Sharing Protocol ................... 347
Xun Yi, Feng Hao, Liqun Chen, and Joseph K. Liu

On Security of Content-Based Video Stream Authentication ..................................... 366
Swee-Won Lo, Zhuo Wei, Robert H. Deng, and Xuhua Ding

Oblivious Maximum Bipartite Matching Size Algorithm with Applications to Secure Fingerprint Identification .................................................. 384
Marina Blanton and Siddharth Saraph

Practical Invalid Curve Attacks on TLS-ECDH .............................................................. 407
Tibor Jager, Jörg Schwenk, and Juraj Somorovsky

Crypto Applications and Attacks

Challenging the Trustworthiness of PGP: Is the Web-of-Trust Tear-Proof? .......... 429
Alessandro Barenghi, Alessandro Di Federico, Gerardo Pelosi, and Stefano Sanfilippo
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 II

### Privacy

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

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

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

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

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

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

### Cloud Security

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

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

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

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

Typing and Compositionality for Security Protocols: A Generalization to the Geometric Fragment ........................................ 209
  Omar Almousa, Sebastian Mödersheim, Paolo Modesti, and Luca Viganò

Checking Trace Equivalence: How to Get Rid of Nonces? .......... 230
  Rémy Chrétien, Véronique Cortier, and Stéphanie Delaune

Attribute Based Broadcast Encryption with Short Ciphertext and Decryption Key ........................................ 252
  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 .......... 270
  Jianting Ning, Xiaolei Dong, Zhenfu Cao, and Lifei Wei

Code Analysis and Side-Channels

DexHunter: Toward Extracting Hidden Code from Packed Android Applications ........................................ 293
  Yueqian Zhang, Xiapu Luo, and Haoyang Yin

Identifying Arbitrary Memory Access Vulnerabilities in Privilege-Separated Software ........................................ 312
  Hong Hu, Zheng Leong Chua, Zhenkai Liang, and Prateek Saxena

vBox: Proactively Establishing Secure Channels Between Wireless Devices Without Prior Knowledge ........................................ 332
  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 ........................................ 355
  Sufatrio, Tong-Wei Chua, Darell J.J. Tan, and Vrizlynn L.L. Thing

A Bytecode Interpreter for Secure Program Execution in Untrusted Main Memory ........................................ 376
  Maximilian Seitzer, Michael Gruhn, and Tilo Müller

Learning from Others: User Anomaly Detection Using Anomalous Samples from Other Users ........................................ 396
  Youngja Park, Ian M. Molloy, Suresh N. Chari, Zenglin Xu, Chris Gates, and Ninghi Li
Authentication

Towards Attack-Resistant Peer-Assisted Indoor Localization. . . . . . . . . . . . . 417
   Jingyu Hua, Shaoyong Du, and Sheng Zhong

Leveraging Real-Life Facts to Make Random Passwords More Memorable. . . 438
   Mahdi Nasrullah Al-Ameen, Kanis Fatema, Matthew Wright,
   and Shannon Scielzo

The Emperor’s New Password Creation Policies:: An Evaluation
of Leading Web Services and the Effect of Role in Resisting Against
Online Guessing . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 456
   Ding Wang and Ping Wang

Policies

A Theory of Gray Security Policies. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 481
   Donald Ray and Jay Ligatti

Factorization of Behavioral Integrity . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 500
   Ximeng Li, Flemming Nielson, and Hanne Riis Nielson

Checking Interaction-Based Declassification Policies for Android
Using Symbolic Execution . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 520
   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 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 541
   Raja Naeem Akram, Konstantinos Markantonakis, and Keith Mayes

Making Bitcoin Exchanges Transparent . . . . . . . . . . . . . . . . . . . . . . . . . . . 561
   Christian Decker, James Guthrie, Jochen Seidel, and Roger Wattenhofer

Web-to-Application Injection Attacks on Android: Characterization
and Detection . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 577
   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 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 599
   Dibya Mukhopadhyay, Maliheh Shirvanian, and Nitesh Saxena

Balloon: A Forward-Secure Append-Only Persistent Authenticated
Data Structure. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 622
   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, Wael 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