

Contents

Security of Operating Systems

Integrity Checking of Function Pointers in Kernel Pools via Virtual Machine Introspection	3
<i>Irfan Ahmed, Golden G. Richard III, Aleksandar Zoranic, and Vassil Roussev</i>	
Lightweight Attestation and Secure Code Update for Multiple Separated Microkernel Tasks.	20
<i>Steffen Wagner, Christoph Krauß, and Claudia Eckert</i>	

Secret Sharing

The Security Defect of a Multi-pixel Encoding Method	39
<i>Teng Guo, Feng Liu, ChuanKun Wu, YoungChang Hou, YaWei Ren, and Wen Wang</i>	
Encrypted Secret Sharing and Analysis by Plaintext Randomization	49
<i>Stephen R. Tate, Roopa Vishwanathan, and Scott Weeks</i>	

Encryption

Round-Efficient Private Stable Matching from Additive Homomorphic Encryption	69
<i>Tadanori Teruya and Jun Sakuma</i>	
Efficient and Fully Secure Forward Secure Ciphertext-Policy Attribute-Based Encryption.	87
<i>Takashi Kitagawa, Hiroki Kojima, Nuttapong Attrapadung, and Hideki Imai</i>	
Reducing Public Key Sizes in Bounded CCA-Secure KEMs with Optimal Ciphertext Length	100
<i>Takashi Yamakawa, Shota Yamada, Takahiro Matsuda, Goichiro Hanaoka, and Noboru Kunihiro</i>	

Malware and Critical Infrastructures

4GMOP: Mopping Malware Initiated SMS Traffic in Mobile Networks	113
<i>Marián Kühnel and Ulrike Meyer</i>	

Design and Analysis of a Sophisticated Malware Attack Against Smart Grid . . .	130
<i>Byungho Min and Vijay Varadharajan</i>	
Multi-round Attacks on Structural Controllability Properties for Non-complete Random Graphs	140
<i>Cristina Alcaraz, Estefanía Etchev��s Mic��olino, and Stephen Wolthusen</i>	
Cryptanalysis	
Improved Meet-in-the-Middle Attacks on Round-Reduced ARIA	155
<i>Dongxia Bai and Hongbo Yu</i>	
Establishing Equations: The Complexity of Algebraic and Fast Algebraic Attacks Revisited	169
<i>Lin Jiao, Bin Zhang, and Mingsheng Wang</i>	
Factoring a Multiprime Modulus N with Random Bits	185
<i>Routo Terada and Reynaldo C��ceres Villena</i>	
Block Ciphers and Stream Ciphers	
Faster 128-EEA3 and 128-EIA3 Software	199
<i>Roberto Avanzi and Billy Bob Brumley</i>	
Merging the Camellia, SMS4 and AES S-Boxes in a Single S-Box with Composite Bases.	209
<i>Alberto F. Mart��nez-Herrera, Carlos Mex-Perera, and Juan Nolasco-Flores</i>	
Entity Authentication	
Offline Dictionary Attack on Password Authentication Schemes Using Smart Cards	221
<i>Ding Wang and Ping Wang</i>	
Self-blindable Credential: Towards Anonymous Entity Authentication Upon Resource Constrained Devices	238
<i>Yanjiang Yang, Xuhua Ding, Haibing Lu, Jian Weng, and Jianying Zhou</i>	
Practical and Provably Secure Distance-Bounding	248
<i>Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay</i>	

Usability and Risk Perception

- On the Viability of CAPTCHAs for use in Telephony Systems: A Usability Field Study 261
Niharika Sachdeva, Nitesh Saxena, and Ponnuram Kumaraguru
- Cars, Condoms, and Facebook 280
Vaibhav Garg and L. Jean Camp

Access Control

- Achieving Revocable Fine-Grained Cryptographic Access Control over Cloud Data. 293
Yanjiang Yang, Xuhua Ding, Haibing Lu, Zhiguo Wan, and Jianying Zhou
- Fine-Grained Access Control for HTML5-Based Mobile Applications in Android 309
Xing Jin, Lusha Wang, Tongbo Luo, and Wenliang Du

Computer Security

- CrowdFlow: Efficient Information Flow Security 321
Christoph Kerschbaumer, Eric Hennigan, Per Larsen, Stefan Brunthaler, and Michael Franz

Privacy Attacks

- DroidTest: Testing Android Applications for Leakage of Private Information 341
Sarker T. Ahmed Rumeen and Donggang Liu
- A Dangerous Mix: Large-Scale Analysis of Mixed-Content Websites 354
Ping Chen, Nick Nikiforakis, Christophe Huygens, and Lieven Desmet

Cryptography

- An Ordered Multisignature Scheme Under the CDH Assumption Without Random Oracles 367
Naoto Yanai, Masahiro Mambo, and Eiji Okamoto
- Human Assisted Randomness Generation Using Video Games 378
Mohsen Alimomeni and Reihaneh Safavi-Naini
- Security Ranking Among Assumptions Within the *Uber Assumption* Framework. 391
Antoine Joux and Antoine Rojat

A Secure and Efficient Method for Scalar Multiplication on Supersingular Elliptic Curves over Binary Fields.	407
<i>Matheus F. de Oliveira and Marco Aurélio Amaral Henriques</i>	
Author Index	417



<http://www.springer.com/978-3-319-27658-8>

Information Security

16th International Conference, ISC 2013, Dallas, Texas,

November 13-15, 2013, Proceedings

Desmedt, Y. (Ed.)

2015, XIV, 418 p. 52 illus. in color., Softcover

ISBN: 978-3-319-27658-8