

Contents

Keynote Talks

- Optimization Problems in Infrastructure Security 3
Evangelos Kranakis and Danny Krizanc
- Secure Distributed Computation on Private Inputs 14
Geoffroy Couteau, Thomas Peters, and David Pointcheval

RFID, Sensors and Secure Computation

- Survey of Distance Bounding Protocols and Threats 29
Agnès Brelurut, David Gerault, and Pascal Lafourcade
- Inferring Touch from Motion in Real World Data 50
Pascal Bissig, Philipp Brandes, Jonas Passerini, and Roger Wattenhofer
- Point-Counting Method for Embarrassingly Parallel Evaluation in Secure Computation. 66
Toomas Krips and Jan Willemson

Security Policies and Biometrics

- Security Mechanisms Planning to Enforce Security Policies 85
Anis Bkakria, Frédéric Cuppens, Nora Cuppens-Boulahia, and David Gross-Amblard
- Runtime Enforcement with Partial Control 102
Raphaël Khoury and Sylvain Hallé
- Privacy-Preserving Fuzzy Commitment for Biometrics via Layered Error-Correcting Codes 117
Masaya Yasuda, Takeshi Shimoyama, Narishige Abe, Shigefumi Yamada, Takashi Shinzaki, and Takeshi Koshiba

Evaluation of Protocols and Obfuscation Security

- Performance Evaluations of Cryptographic Protocols Verification Tools Dealing with Algebraic Properties 137
Pascal Lafourcade and Maxime Puy
- AnBx: Automatic Generation and Verification of Security Protocols Implementations 156
Paolo Modesti

Evaluating Obfuscation Security: A Quantitative Approach. 174
Rabih Mohsen and Alexandre Miranda Pinto

Spam Emails, Botnets and Malware

Fast and Effective Clustering of Spam Emails Based on Structural Similarity. 195
Mina Sheikhalishahi, Andrea Saracino, Mohamed Mejri, Nadia Tawbi, and Fabio Martinelli

A Closer Look at the HTTP and P2P Based Botnets from a Detector’s Perspective. 212
Fariba Haddadi and A. Nur Zincir-Heywood

Obfuscation Code Localization Based on CFG Generation of Malware 229
Nguyen Minh Hai, Mizuhito Ogawa, and Quan Thanh Tho

Short Papers

Runtime Monitoring of Stream Logic Formulae 251
Sylvain Hallé and Raphaël Khoury

MIME: A Formal Approach to (Android) Emulation Malware Analysis 259
Fabio Bellini, Roberto Chiodi, and Isabella Mastroeni

Information Classification Enablers 268
Erik Bergström and Rose-Mharie Åhlfeldt

Information Flow Control on a Multi-paradigm Web Application for SQL Injection Prevention. 277
Meriam Ben-Ghorbel-Talbi, François Lesueur, and Gaetan Perrin

Searchable Encryption in Apache Cassandra. 286
Tim Waage, Ramaninder Singh Jhaji, and Lena Wiese

AndroSSL: A Platform to Test Android Applications Connection Security . . . 294
François Gagnon, Marc-Antoine Ferland, Marc-Antoine Fortier, Simon Desloges, Jonathan Ouellet, and Catherine Boileau

Onion Routing in Deterministic Delay Tolerant Networks 303
Adrian Antunez-Veas and Guillermo Navarro-Arribas

Security Enforcement by Rewriting: An Algebraic Approach 311
Guangye Sui and Mohamed Mejri

Author Index 323



<http://www.springer.com/978-3-319-30302-4>

Foundations and Practice of Security
8th International Symposium, FPS 2015,
Clermont-Ferrand, France, October 26-28, 2015,
Revised Selected Papers
Garcia-Alfaro, J.; Kranakis, E.; Bonfante, G. (Eds.)
2016, XII, 323 p. 51 illus. in color., Softcover
ISBN: 978-3-319-30302-4