

# Contents

## Authentication and Key Management

- Securing Transactions with the eIDAS Protocols . . . . . 3  
*Frank Morgner, Paul Bastian, and Marc Fischlin*
- Novel Lightweight Signcryption-Based Key Distribution Mechanisms  
for MIKEY . . . . . 19  
*Kim Thuat Nguyen, Nouha Oualha, and Maryline Laurent*
- Codes v. People: A Comparative Usability Study of Two Password  
Recovery Mechanisms . . . . . 35  
*Vlasta Stavova, Vashek Matyas, and Mike Just*

## Secure Hardware Systems

- An Implementation of a High Assurance Smart Meter Using Protected  
Module Architectures. . . . . 53  
*Jan Tobias Mühlberg, Sara Cleemput, Mustafa A. Mustafa,  
Jo Van Bulck, Bart Preneel, and Frank Piessens*
- Security Challenges of Small Cell as a Service in Virtualized Mobile  
Edge Computing Environments. . . . . 70  
*Vassilios Vassilakis, Emmanouil Panaousis, and Haralambos Mouratidis*
- An HMM-Based Anomaly Detection Approach for SCADA Systems . . . . . 85  
*Kyriakos Stefanidis and Artemios G. Voyiatzis*

## Attacks to Software and Network Systems

- Attacking and Defending Dynamic Analysis System-Calls Based IDS . . . . . 103  
*Ishai Rosenberg and Ehud Gudes*
- Towards Automatic Risk Analysis and Mitigation of Software Applications . . . 120  
*Leonardo Regano, Daniele Canavese, Cataldo Basile, Alessio Viticchié,  
and Antonio Lioy*
- Runtime Code Polymorphism as a Protection Against Side Channel Attacks. . . 136  
*Damien Couroussé, Thierno Barry, Bruno Robisson, Philippe Jaillon,  
Olivier Potin, and Jean-Louis Lanet*
- Analysis of a Code-Based Countermeasure Against Side-Channel  
and Fault Attacks . . . . . 153  
*Guillaume Barbu and Alberto Battistello*

**Access Control and Data Protection**

LAMP - Label-Based Access-Control for More Privacy  
in Online Social Networks . . . . . 171  
*Leila Bahri, Barbara Carminati, Elena Ferrari, and William Lucia*

Privacy-Preserving Two-Party Skyline Queries Over Horizontally  
Partitioned Data . . . . . 187  
*Ling Chen, Ting Yu, and Rada Chirkova*

Fault-Channel Watermarks . . . . . 204  
*Peter Samarin, Alexander Skripnik, and Kerstin Lemke-Rust*

**Short Papers**

The Effect of Semantic Elaboration on the Perceived Security  
and Privacy Risk of Privacy-ABCs — An Empirical Experiment . . . . . 223  
*Ahmad Sabouri*

Delegating Biometric Authentication with the Sumcheck Protocol . . . . . 236  
*Hervé Chabanne, Julien Keuffer, and Roch Lescuyer*

Password Generators: Old Ideas and New . . . . . 245  
*Fatma Al Maqbali and Chris J. Mitchell*

Provable Network Activity for Protecting Users Against False Accusation . . . 254  
*Panagiotis Papadopoulos, Elias Athanasopoulos, Eleni Kosta,  
George Siganos, Angelos D. Keromytis, and Evangelos P. Markatos*

Combining Third Party Components Securely in Automotive Systems . . . . . 262  
*Madeline Cheah, Siraj A. Shaikh, Jeremy Bryans,  
and Hoang Nga Nguyen*

**Author Index** . . . . . 271



<http://www.springer.com/978-3-319-45930-1>

Information Security Theory and Practice  
10th IFIP WG 11.2 International Conference, WISTP  
2016, Heraklion, Crete, Greece, September 26-27,  
2016, Proceedings  
Foresti, S.; Lopez, J. (Eds.)  
2016, X, 271 p. 59 illus., Softcover  
ISBN: 978-3-319-45930-1