

# Contents

## Internet of Things and Privacy

PUDA – Privacy and Unforgeability for Data Aggregation. . . . .	3
<i>Iraklis Leontiadis, Kaoutar Elkhiyaoui, Melek Önen, and Refik Molva</i>	
A Security Framework for Internet of Things . . . . .	19
<i>Imane Bouij-Pasquier, Anas Abou El Kalam, Abdellah Ait Ouahman, and Mina De Montfort</i>	
Privacy-Aware Authentication in the Internet of Things . . . . .	32
<i>Hannes Gross, Marko Hölbl, Daniel Slamanig, and Raphael Spreitzer</i>	

## Password-Based Authentication

Security of Linear Secret-Sharing Schemes Against Mass Surveillance. . . . .	43
<i>Irene Giacomelli, Ruxandra F. Olimid, and Samuel Ranellucci</i>	
Secure Set-Based Policy Checking and Its Application to Password Registration . . . . .	59
<i>Changyu Dong and Franziskus Kiefer</i>	
SEPM: Efficient Partial Keyword Search on Encrypted Data . . . . .	75
<i>Yutaka Kawai, Takato Hirano, Yoshihiro Koseki, and Tatsuji Munaka</i>	

## Attacks and Malicious Code

Bad Sounds Good Sounds: Attacking and Defending Tap-Based Rhythmic Passwords Using Acoustic Signals . . . . .	95
<i>S. Abhishek Anand, Prakash Shrestha, and Nitesh Saxena</i>	
iDeFEND: Intrusion Detection Framework for Encrypted Network Data . . . .	111
<i>Fatih Kilic and Claudia Eckert</i>	
On the Weaknesses of PBKDF2 . . . . .	119
<i>Andrea Visconti, Simone Bossi, Hany Ragab, and Alexandro Calò</i>	

## Security Modeling and Verification

Verifiable Random Functions from (Leveled) Multilinear Maps . . . . .	129
<i>Bei Liang, Hongda Li, and Jinyong Chang</i>	

A Formal Environment for MANET Organization and Security . . . . .	144
<i>Aida Ben Chehida Douss, Ryma Abassi, Nihel Ben Youssef, and Sihem Guemara El Fatmi</i>	
Analysis and Implementation of an Efficient Ring-LPN Based Commitment Scheme. . . . .	160
<i>Helger Lipmaa and Kateryna Pavlyk</i>	
<b>Secure Multi-party Computation</b>	
Practical Password-Based Authentication Protocol for Secret Sharing Based Multiparty Computation . . . . .	179
<i>Ryo Kikuchi, Koji Chida, Dai Ikarashi, and Koki Hamada</i>	
Bandwidth-Optimized Secure Two-Party Computation of Minima . . . . .	197
<i>Jan Henrik Ziegeldorf, Jens Hiller, Martin Henze, Hanno Wirtz, and Klaus Wehrle</i>	
Outsourcing Secure Two-Party Computation as a Black Box . . . . .	214
<i>Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler</i>	
<b>Cryptography and VPNs</b>	
What Users Should Know About Full Disk Encryption Based on LUKS . . . .	225
<i>Simone Bossi and Andrea Visconti</i>	
Q-OpenVPN: A New Extension of OpenVPN Based on a Quantum Scheme for Authentication and Key Distribution. . . . .	238
<i>Aymen Ghilen, Mostafa Azizi, and Ridha Bouallegue</i>	
An LTE-Based VPN for Enhancing QoS and Authentication in Smallcell Enterprise Networks . . . . .	248
<i>Maroua Gharam, Meriem Salhi, and Noureddine Boudriga</i>	
<b>Author Index</b> . . . . .	257

Cryptology and Network Security  
14th International Conference, CANS 2015, Marrakesh,  
Morocco, December 10-12, 2015, Proceedings  
Reiter, M.; Naccache, D. (Eds.)  
2015, X, 257 p. 41 illus. in color., Softcover  
ISBN: 978-3-319-26822-4