

Raja Naeem Akram · Sushil Jajodia (Eds.)

Information Security Theory and Practice

9th IFIP WG 11.2 International Conference, WISTP 2015
Heraklion, Crete, Greece, August 24–25, 2015
Proceedings

Contents

Security and Privacy Services

On Secrecy Amplification Protocols	3
<i>Radim Ošťádal, Petr Švenda, and Vashek Matyáš</i>	
Privacy-Respecting Auctions as Incentive Mechanisms in Mobile Crowd Sensing	20
<i>Tassos Dimitriou and Ioannis Krontiris</i>	
Electrical Heart Signals can be Monitored from the Moon: Security Implications for IPI-Based Protocols	36
<i>Alejandro Calleja, Pedro Peris-Lopez, and Juan E. Tapiador</i>	
Private Minutia-Based Fingerprint Matching	52
<i>Neyire Deniz Sarier</i>	

Secure Resource Sharing and Access Control

Secure Resource Sharing for Embedded Protected Module Architectures	71
<i>Jo Van Bulck, Job Noorman, Jan Tobias Mühlberg, and Frank Piessens</i>	
Secure Obfuscation of Authoring Style	88
<i>Hoi Le, Reihaneh Safavi-Naini, and Asadullah Galib</i>	
DET-ABE: A Java API for Data Confidentiality and Fine-Grained Access Control from Attribute Based Encryption	104
<i>Miguel Morales-Sandoval and Arturo Diaz-Perez</i>	
WSACd - A Usable Access Control Framework for Smart Home Devices . . .	120
<i>Konstantinos Fysarakis, Charalampos Konstantourakis, Konstantinos Rantos, Charalampos Manifavas, and Ioannis Papaefstathiou</i>	

Secure Devices and Execution Environment

Automatic Top-Down Role Engineering Framework Using Natural Language Processing Techniques	137
<i>Masoud Narouei and Hassan Takabi</i>	
Practical and Privacy-Preserving TEE Migration	153
<i>Ghada Arfaoui, Saïd Gharout, Jean-François Lalande, and Jacques Traoré</i>	

Randomizing the Montgomery Powering Ladder 169
Duc-Phong Le, Chik How Tan, and Michael Tunstall

Challenges of Security and Reliability

How Current Android Malware Seeks to Evade Automated Code Analysis. 187
Siegfried Rasthofer, Irfan Asrar, Stephan Huber, and Eric Bodden

On Linkability and Malleability in Self-blindable Credentials 203
Jaap-Henk Hoepman, Wouter Lueks, and Sietse Ringers

Device Synchronisation: A Practical Limitation on Reader Assisted
Jamming Methods for RFID Confidentiality 219
Qiao Hu, Lavinia Mihaela Dinca, and Gerhard Hancke

Short Papers

Normalizing Security Events with a Hierarchical Knowledge Base 237
David Jaeger, Amir Azodi, Feng Cheng, and Christoph Meinel

Attack Tree Generation by Policy Invalidation 249
*Marieta Georgieva Ivanova, Christian W. Probst, René Rydhof Hansen,
and Florian Kammüller*

Lightweight Password Hashing Scheme for Embedded Systems 260
*George Hatzivasilis, Ioannis Papaefstathiou, Charalampos Manifavas,
and Ioannis Askoxylakis*

Secure and Authenticated Access to LLN Resources Through Policy
Constraints 271
*Konstantinos Rantos, Konstantinos Fysarakis, Othonas Soultatos,
and Ioannis Askoxylakis*

Author Index 281