

Lidong Chen · David McGrew
Chris Mitchell (Eds.)

Security Standardisation Research

Third International Conference, SSR 2016
Gaithersburg, MD, USA, December 5–6, 2016
Proceedings

Contents

Analyzing and Fixing the QACCE Security of QUIC	1
<i>Hideki Sakurada, Kazuki Yoneyama, Yoshikazu Hanatani, and Maki Yoshida</i>	
Cross-Tool Semantics for Protocol Security Goals	32
<i>Joshua D. Guttman, John D. Ramsdell, and Paul D. Rowe</i>	
Cryptanalysis of GlobalPlatform Secure Channel Protocols	62
<i>Mohamed Sabt and Jacques Traoré</i>	
NFC Payment Spy: A Privacy Attack on Contactless Payments	92
<i>Maryam Mehrnezhad, Mohammed Aamir Ali, Feng Hao, and Aad van Moorsel</i>	
Security Analysis of the W3C Web Cryptography API	112
<i>Kelsey Cairns, Harry Halpin, and Graham Steel</i>	
Algorithm Agility – Discussion on TPM 2.0 ECC Functionalities	141
<i>Liqun Chen and Rainer Urian</i>	
Reactive and Proactive Standardisation of TLS	160
<i>Kenneth G. Paterson and Thyla van der Merwe</i>	
Extending the UML Standards to Model Tree-Structured Data and Their Access Control Requirements	187
<i>Alberto De la Rosa Algarín and Steven A. Demurjian</i>	
Attribute-Based Access Control Architectures with the eIDAS Protocols	205
<i>Frank Morgner, Paul Bastian, and Marc Fischlin</i>	
Secure Multicast Group Management and Key Distribution in IEEE 802.21	227
<i>Yoshikazu Hanatani, Naoki Ogura, Yoshihiro Ohba, Lidong Chen, and Subir Das</i>	
State Management for Hash-Based Signatures	244
<i>David McGrew, Panos Kampanakis, Scott Fluhrer, Stefan-Lukas Gazdag, Denis Butin, and Johannes Buchmann</i>	
Analysis of a Proposed Hash-Based Signature Standard	261
<i>Jonathan Katz</i>	
Author Index	275