

Table of Contents

Protocols.

Trust in Peer-to-Peer content distribution protocols	1
<i>Nicolai Kuntze, Carsten Rudolph, Andreas Fuchs</i>	
Exploiting Node Mobility for Coordinating Data Usage in Crisis Scenarios	2
<i>Giovanni Russello, Enrico Scalavino</i>	
Generic Constructions of Biometric Identity Based Encryption Systems . .	3
<i>Neyire Deniz Sarier</i>	

Protocols for Smart Devices.

Efficient Mutual Authentication for Multi-Domain RFID Systems Using Distributed Signatures	6
<i>Michael Braun, Ulrike Meyer, Susanne Wetzel</i>	
Practical Schemes For Privacy & Security Enhanced RFID	7
<i>Jaap-Henk Hoepman, Rieks Joosten</i>	
Design and Analysis of a Generalized Canvas Protocol	8
<i>Marian Novotny</i>	

Embedded Software.

A Probabilistic Diffusion Scheme for Anomaly Detection on Smartphones	9
<i>Christian Bauckhage, Tansu Alpcan, Aubrey-Derrick Schmidt</i>	
Efficient and Effective Buffer Overflow Protection on ARM Processors . . .	10
<i>Raoul Strackx, Yves Younan, Pieter Philippaerts, Frank Piessens</i>	
A Smart Card Implementation of the McEliece PKC	11
<i>Falko Strenzke</i>	

Hardware Implementations.

Novel FPGA-Based Signature Matching for Deep Packet Inspection	12
<i>Nitesh Guinde, Sotirios Ziavras</i>	
Towards Electrical, Integrated Implementations of SIMPL Systems	13
<i>Ulrich Rührmair, Qingqing Chen, Martin Stutzmann, Paolo Lugli, Ulf Schlichtmann, György Csaba</i>	
A Very Compact Hardware Implementation of the KASUMI Block Cipher	14
<i>Dai Yamamoto, Kowichi Itoh, Jun Yajima</i>	

Database Security.

The Market Failure of Anonymity Services	4
<i>Heiko Roßnagel</i>	
Predicting and Preventing Insider Threat in Relational Database Systems	16
<i>Qussai Yaseen, Brajendra Panda</i>	
Security Analysis of Anonymity Protocols	5
<i>Sami Zhioua</i>	

Network Security.

MoteAODV - An AODV Implementation for TinyOS 2.0	17
<i>Werner Backes, Jared Cordasco</i>	
Improvements of pan-European IDM Architecture to Enable Identity Delegation Based on X.509 Proxy Certificates and SAML	15
<i>Sergio Sánchez, Ana Gómez</i>	
Fraud Detection for Voice over IP services on Next-Generation Networks	18
<i>Igor Ruiz-Agundez, Yoseba K. Penya, Pablo García Bringas</i>	

Security of Cryptographic Devices.

Random Number Generation Based on Fingerprints	19
<i>Shkodran Gerguri, Václav Matyáš, Zdeněk Říha, Luděk Smolék</i>	
Evaluation Metrics of Physical Non-Invasive Security for Cryptographic Modules	20
<i>Huiyun Li, Fengqi Yu, Hai Yuan</i>	
Efficient Entropy Estimation for Mutual Information Analysis using B-splines	21
<i>Alexandre Venelli</i>	

Short Papers — Security.

Proxy Smart Card Systems	23
<i>Giuseppe Cattaneo, Pompeo Faruolo, Ivan Visconti, Vincenzo Palazzo</i>	
Supporting Applications' Evolution in Multi-Application Smart Cards by Security-by-Contract	26
<i>Nicola Dragoni, Olga Gadyatskaya, Fabio Massacci</i>	
Website Credential Storage and Two Factor Web Authentication with a Java SIM	27
<i>Jon Hart, Konstantinos Markantonakis, Keith Mayes</i>	

Secure and Usable Out Of Band Channels for Ad hoc Mobile Device Interactions	28
<i>Ronald Kainda, Bill Roscoe, Ivan Flechais</i>	
Identification and Verification of Security Relevant Functions in Embedded Systems Based on Source Code Annotations and Assertions ..	29
<i>Johannes Loinig, Christian Steger, Reinhold Weiss, Ernst Haselsteiner</i>	
Short Papers — Cryptography.	
Attribute-based Encryption with Break-glass	22
<i>Achim D. Brucker, Helmut Petritsch, Stefan G. Weber</i>	
On the Security of a Two-Factor Authentication Scheme	24
<i>Luigi Catuogno, Clemente Galdi</i>	
An Energy-Efficient Symmetric Cryptography Based Authentication Scheme for Wireless Sensor Networks	25
<i>Oscar Delgado-Mohatar, José M. Sierra, Ljiljana Brankovic, Amparo Fuster-Sabater</i>	
Security Analysis of Mobile Phones Used as OTP Generators	30
<i>Håvard Raddum, Lars Hopland Nestås, Kjell Jørgen Hole</i>	
The Design of Secure and Efficient P2PSIP Communication Systems	31
<i>Xianghan Zheng, Vladimir Oleshchuk</i>	