

Table of Contents

Embedded Security

Efficient and Effective Buffer Overflow Protection on ARM Processors	1
<i>Raoul Strackx, Yves Younan, Pieter Philippaerts, and Frank Piessens</i>	
Efficient Entropy Estimation for Mutual Information Analysis Using B-Splines	17
<i>Alexandre Venelli</i>	
A Probabilistic Diffusion Scheme for Anomaly Detection on Smartphones	31
<i>Tansu Alpcan, Christian Bauckhage, and Aubrey-Derrick Schmidt</i>	
A Smart Card Implementation of the McEliece PKC	47
<i>Falko Strenzke</i>	
Evaluation Metrics of Physical Non-invasive Security	60
<i>Huiyun Li, Keke Wu, Fengqi Yu, and Hai Yuan</i>	

Protocols

Trust in Peer-to-Peer Content Distribution Protocols	76
<i>Nicolai Kuntze, Carsten Rudolph, and Andreas Fuchs</i>	
Generic Constructions of Biometric Identity Based Encryption Systems	90
<i>Neyire Deniz Sarier</i>	
Design and Analysis of a Generalized Canvas Protocol	106
<i>Marián Novotný</i>	

Highly Constrained Embedded Systems

Efficient Mutual Authentication for Multi-domain RFID Systems Using Distributed Signatures	122
<i>Michael Braun, Ulrike Meyer, and Susanne Wetzel</i>	
Practical Schemes for Privacy and Security Enhanced RFID (Extended Abstract)	138
<i>Jaap-Henk Hoepman and Rieks Joosten</i>	
MoteAODV – An AODV Implementation for TinyOS 2.0	154
<i>Werner Backes and Jared Cordasco</i>	

Security

Random Number Generation Based on Fingerprints	170
<i>Shkodran Gerguri, Václav Matyáš, Zdeněk Říha, and Luděk Smolík</i>	
Improvements of pan-European IDM Architecture to Enable Identity Delegation Based on X.509 Proxy Certificates and SAML	183
<i>Sergio Sánchez García and Ana Gómez Oliva</i>	
Fraud Detection for Voice over IP Services on Next-Generation Networks	199
<i>Igor Ruiz-Agundez, Yoseba K. Penya, and Pablo Garcia Bringas</i>	

Smart Card Security

Proxy Smart Card Systems	213
<i>Giuseppe Cattaneo, Pompeo Faruolo, Vincenzo Palazzo, and Ivan Visconti</i>	
Can We Support Applications' Evolution in Multi-application Smart Cards by Security-by-Contract?	221
<i>Nicola Dragoni, Olga Gadyatskaya, and Fabio Massacci</i>	
Website Credential Storage and Two-Factor Web Authentication with a Java SIM	229
<i>Jonathan Hart, Konstantinos Markantonakis, and Keith Mayes</i>	

Algorithms

Attribute-Based Encryption with Break-Glass	237
<i>Achim D. Brucker, Helmut Petritsch, and Stefan G. Weber</i>	
On the Security of a Two-Factor Authentication Scheme	245
<i>Luigi Catuogno and Clemente Galdi</i>	
The Design of Secure and Efficient P2PSIP Communication Systems ...	253
<i>Xianghan Zheng and Vladimir Oleshchuk</i>	

Hardware Implementations

Novel FPGA-Based Signature Matching for Deep Packet Inspection	261
<i>Nitesh B. Guinde and Sotirios G. Ziavras</i>	
Towards Electrical, Integrated Implementations of SIMPL Systems	277
<i>Ulrich Rührmair, Qingqing Chen, Martin Stutzmann, Paolo Lugli, Ulf Schlichtmann, and György Csaba</i>	

A Very Compact Hardware Implementation of the KASUMI Block Cipher	293
<i>Dai Yamamoto, Kouichi Itoh, and Jun Yajima</i>	

Embedded Systems

Secure and Usable Out-Of-Band Channels for <i>Ad Hoc</i> Mobile Device Interactions	308
<i>Ronald Kainda, Ivan Flechais, and A.W. Roscoe</i>	
Identification and Verification of Security Relevant Functions in Embedded Systems Based on Source Code Annotations and Assertions	316
<i>Johannes Loinig, Christian Steger, Reinhold Weiss, and Ernst Haselsteiner</i>	
Security Analysis of Mobile Phones Used as OTP Generators	324
<i>Håvard Raddum, Lars Hopland Nestås, and Kjell Jørgen Hole</i>	
An Energy-Efficient Symmetric Cryptography Based Authentication Scheme for Wireless Sensor Networks	332
<i>Oscar Delgado-Mohatar, José M. Sierra, Ljiljana Brankovic, and Amparo Fúster-Sabater</i>	

Anonymity/Database Security

The Market Failure of Anonymity Services	340
<i>Heiko Rossnagel</i>	
Exploiting Node Mobility for Coordinating Data Usage in Crisis Scenarios	355
<i>Giovanni Russello and Enrico Scalavino</i>	
Predicting and Preventing Insider Threat in Relational Database Systems	368
<i>Qussai Yaseen and Brajendra Panda</i>	

Author Index	385
---------------------------	-----