

Contents

Keynote Address

On the Efficiency of Mathematics in Intrusion Detection: The NetEntropy Case	3
<i>Jean Goubault-Larrecq and Julien Olivain</i>	

Security Protocols

On the Feasibility of a Censorship Resistant Decentralized Name System . . .	19
<i>Matthias Wachs, Martin Schanzenbach, and Christian Grothoff</i>	
A General Framework for Group Authentication and Key Exchange Protocols	31
<i>Huihui Yang, Lei Jiao, and Vladimir A. Oleshchuk</i>	
Modelling Simultaneous Mutual Authentication for Authenticated Key Exchange	46
<i>Zheng Yang</i>	

Formal Methods

Model-Based Specification and Validation of Security and Dependability Patterns.	65
<i>Brahim Hamid and Christian Percebois</i>	
Enforcing Information Flow by Combining Static and Dynamic Analysis . . .	83
<i>Andrew Bedford, Josée Desharnais, Théophane G. Godonou, and Nadia Tawbi</i>	

Physical Security

Fault Injection to Reverse Engineer DES-Like Cryptosystems	105
<i>Hélène Le Boudier, Sylvain Guilley, Bruno Robisson, and Assia Tria</i>	
Software Camouflage	122
<i>Sylvain Guilley, Damien Marion, Zakaria Najm, Youssef Souissi, and Antoine Wurcker</i>	
Investigation of Parameters Influencing the Success of Optical Fault Attacks . . .	140
<i>Thomas Korak</i>	

Attack Classification and Assessment

ONTIDS: A Highly Flexible Context-Aware and Ontology-Based Alert Correlation Framework	161
<i>Alireza Sadighian, José M. Fernandez, Antoine Lemay, and Saman T. Zargar</i>	
Quantitative Evaluation of Enforcement Strategies	178
<i>Vincenzo Ciancia, Fabio Martinelli, Matteucci Ilaria, and Charles Morisset</i>	

Access Control

Collusion Resistant Inference Control for Cadastral Databases	189
<i>Firas Al Khalil, Alban Gabillon, and Patrick Capolsini</i>	
Leveraging Ontologies upon a Holistic Privacy-Aware Access Control Model . . .	209
<i>Eugenia I. Papagiannakopoulou, Maria N. Koukovini, Georgios V. Lioudakis, Nikolaos Dellas, Joaquin Garcia-Alfaro, Dimitra I. Kaklamani, Iakovos S. Venieris, Nora Cuppens-Boulahia, and Frédéric Cuppens</i>	
Formal Modelling of Content-Based Protection and Release for Access Control in NATO Operations	227
<i>Alessandro Armando, Sander Oudkerk, Silvio Ranise, and Konrad Wrona</i>	

Cipher Attacks

Computational Soundness of Symbolic Blind Signatures under Active Attacker	247
<i>Hideki Sakurada</i>	
Improved Davies-Murphy's Attack on DES Revisited	264
<i>Yi Lu and Yvo Desmedt</i>	
Yet Another Fault-Based Leakage in Non-uniform Faulty Ciphertexts	272
<i>Yang Li, Yu-ichi Hayashi, Arisa Matsubara, Naofumi Homma, Takafumi Aoki, Kazuo Ohta, and Kazuo Sakiyama</i>	

Ad-hoc and Sensor Networks

A Hierarchical Anti-Counterfeit Mechanism: Securing the Supply Chain Using RFIDs	291
<i>Zeeshan Bilal and Keith Martin</i>	

A More Realistic Model for Verifying Route Validity in Ad-Hoc Networks	306
<i>Ali Kassem, Pascal Lafourcade, and Yassine Lakhnech</i>	

On the Security of a Privacy-Preserving Key Management Scheme for Location Based Services in VANETs.	323
<i>Bao Liu, Lei Zhang, and Josep Domingo-Ferrer</i>	

Resilience

CheR: Cheating Resilience in the Cloud via Smart Resource Allocation	339
<i>Di Pietro Roberto, Flavio Lombardi, Fabio Martinelli, and Daniele Sgandurra</i>	

Evaluation of Software-Oriented Block Ciphers on Smartphones	353
<i>Lukas Malina, Vlastimil Clupek, Zdenek Martinasek, Jan Hajny, Kimio Oguchi, and Vaclav Zeman</i>	

Don't Push It: Breaking iButton Security.	369
<i>Christian Brandt and Michael Kasper</i>	

Intrusion Detection

Discovering Flaws in IDS Through Analysis of Their Inputs	391
<i>Raphaël Jamet and Pascal Lafourcade</i>	

On the Reverse Engineering of the Citadel Botnet	408
<i>Ashkan Rahimian, Raha Ziarati, Stere Preda, and Mourad Debbabi</i>	

The Carna Botnet Through the Lens of a Network Telescope	426
<i>Erwan Le Malécot and Daisuke Inoue</i>	

Author Index	443
-------------------------------	-----

Foundations and Practice of Security

6th International Symposium, FPS 2013, La Rochelle,
France, October 21-22, 2013, Revised Selected Papers
Danger, J.-L.; Debbabi, M.; Marion, J.-Y.; Garcia-Alfaro, J.;
Zincir-Heywood, N. (Eds.)

2014, XIII, 444 p. 134 illus., Softcover

ISBN: 978-3-319-05301-1