Contents

Keynote Address

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

Security Protocols

On the Feasibility of a Censorship Resistant Decentralized Name System . . 19
  Matthias Wachs, Martin Schanzenbach, and Christian Grothoff

A General Framework for Group Authentication and Key Exchange Protocols ................................................................... 31
  Huihui Yang, Lei Jiao, and Vladimir A. Oleshchuk

Modelling Simultaneous Mutual Authentication for Authenticated Key Exchange .............................................................. 46
  Zheng Yang

Formal Methods

Model-Based Specification and Validation of Security and Dependability Patterns ............................................................... 65
  Brahim Hamid and Christian Percebois

Enforcing Information Flow by Combining Static and Dynamic Analysis . . 83
  Andrew Bedford, Josée Desharnais, Théophane G. Godonou, and Nadia Tawbi

Physical Security

Fault Injection to Reverse Engineer DES-Like Cryptosystems ............... 105
  Hélène Le Bouder, Sylvain Guilley, Bruno Robisson, and Assia Tria

Software Camouflage .......................................................................................................................... 122
  Sylvain Guilley, Damien Marion, Zakaria Najm, Youssef Souissi, and Antoine Wurcker

Investigation of Parameters Influencing the Success of Optical Fault Attacks . . 140
  Thomas Korak
Attack Classification and Assessment

ONTIDS: A Highly Flexible Context-Aware and Ontology-Based Alert Correlation Framework .................................................. 161
Alireza Sadighian, José M. Fernandez, Antoine Lemay, and Saman T. Zargar

Quantitative Evaluation of Enforcement Strategies ......................... 178
Vincenzo Ciancia, Fabio Martinelli, Matteucci Ilaria, and Charles Morisset

Access Control

Collusion Resistant Inference Control for Cadastral Databases ........... 189
Firas Al Khalil, Alban Gabillon, and Patrick Capolsini

Leveraging Ontologies upon a Holistic Privacy-Aware Access Control Model ................................................................. 209
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

Formal Modelling of Content-Based Protection and Release for Access Control in NATO Operations ................................. 227
Alessandro Armando, Sander Oudkerk, Silvio Ranise, and Konrad Wrona

Cipher Attacks

Computational Soundness of Symbolic Blind Signatures under Active Attacker ................................................................. 247
Hideki Sakurada

Improved Davies-Murphy’s Attack on DES Revisited ...................... 264
Yi Lu and Yvo Desmedt

Yet Another Fault-Based Leakage in Non-uniform Faulty Ciphertexts .... 272
Yang Li, Yu-ichi Hayashi, Arisa Matsubara, Naofumi Homma, Takafumi Aoki, Kazuo Ohta, and Kazuo Sakiyama

Ad-hoc and Sensor Networks

A Hierarchical Anti-Counterfeit Mechanism: Securing the Supply Chain Using RFIDs ............................................................. 291
Zeeshan Bilal and Keith Martin
### Contents XIII

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A More Realistic Model for Verifying Route Validity in Ad-Hoc Networks.</td>
<td>306</td>
</tr>
<tr>
<td><em>Ali Kassem, Pascal Lafourcade, and Yassine Lakhnech</em></td>
<td></td>
</tr>
<tr>
<td>On the Security of a Privacy-Preserving Key Management Scheme for Location Based Services in VANETs.</td>
<td>323</td>
</tr>
<tr>
<td><em>Bao Liu, Lei Zhang, and Josep Domingo-Ferrer</em></td>
<td></td>
</tr>
<tr>
<td><strong>Resilience</strong></td>
<td></td>
</tr>
<tr>
<td>CheR: Cheating Resilience in the Cloud via Smart Resource Allocation.</td>
<td>339</td>
</tr>
<tr>
<td><em>Di Pietro Roberto, Flavio Lombardi, Fabio Martinelli, and Daniele Sgandurra</em></td>
<td></td>
</tr>
<tr>
<td>Evaluation of Software-Oriented Block Ciphers on Smartphones.</td>
<td>353</td>
</tr>
<tr>
<td><em>Lukas Malina, Vlastimil Clupek, Zdenek Martinasek, Jan Hajny, Kimio Oguchi, and Vaclav Zeman</em></td>
<td></td>
</tr>
<tr>
<td>Don’t Push It: Breaking iButton Security.</td>
<td>369</td>
</tr>
<tr>
<td><em>Christian Brandt and Michael Kasper</em></td>
<td></td>
</tr>
<tr>
<td><strong>Intrusion Detection</strong></td>
<td></td>
</tr>
<tr>
<td>Discovering Flaws in IDS Through Analysis of Their Inputs.</td>
<td>391</td>
</tr>
<tr>
<td><em>Raphaël Jamet and Pascal Lafourcade</em></td>
<td></td>
</tr>
<tr>
<td>On the Reverse Engineering of the Citadel Botnet.</td>
<td>408</td>
</tr>
<tr>
<td><em>Ashkan Rahimian, Raha Ziarati, Stere Preda, and Mourad Debbabi</em></td>
<td></td>
</tr>
<tr>
<td>The Carna Botnet Through the Lens of a Network Telescope.</td>
<td>426</td>
</tr>
<tr>
<td><em>Erwan Le Malécot and Daisuke Inoue</em></td>
<td></td>
</tr>
<tr>
<td><strong>Author Index</strong></td>
<td>443</td>
</tr>
</tbody>
</table>
Foundations and Practice of Security
6th International Symposium, FPS 2013, La Rochelle, France, October 21–22, 2013, Revised Selected Papers
2014, XIII, 444 p. 134 illus., Softcover
ISBN: 978-3-319-05301-1