Foundations and Practice of Security

6th International Symposium, FPS 2013
La Rochelle, France, October 21–22, 2013
Revised Selected Papers
Preface

The 6th International Symposium on Foundations and Practice of Security (FPS 2013) was held at the Hotel Mercure, La Rochelle, France, during October 21–22, 2013. The symposium was organized by the Institut Mines-Télécom and sponsored by Télécom Bretagne and LabSTICC. FPS 2013 received 65 submissions, from countries all over the world. Each paper was reviewed by at least three committee members. The Program Committee selected 25 papers for presentation. The program was completed with two excellent invited talks given by Jean Goubault-Larrecq (LSV, ENS Cachan) and Bruno Crispo (DISI, University of Trento).

Many people contributed to the success of FPS 2013. First we would like to thank all the authors who submitted their research results. The selection was a challenging task and we sincerely thank all the Program Committee members, as well as the external reviewers, who volunteered to read and discuss the papers. We greatly thank the two general chairs, Frédéric Cuppens (Télécom Bretagne) and Ali A. Ghorbani (University of New Brunswick), for steering FPS 2013 and choosing the magnificent place of La Rochelle. We are also indebted to the two organizing committee chairs, Nora Cuppens-Boulahia (Télécom Bretagne) and Ghislaine Le Gall (Télécom Bretagne), for their great efforts with the symposium logistics, including the nice restaurant and the visit to La Rochelle. Finally, we also want to express our gratitude to the two publication chairs, Joaquin Garcia-Alfaro (Télécom SudParis) and Nur Zincir Heywood (Dalhousie University), and the webmaster Said Oulmakhzoune (Télécom Bretagne), for the great work they provided in programming, editing the proceedings, and managing the informations on the website.

As security becomes an essential issue in information and communication technologies, there is a growing need to develop efficient methods to analyze and design systems providing a high level of security and privacy. We hope the articles in this proceedings volume will be valuable for your professional activities in this area.

December 2013

Jean-Luc Danger
Mourad Debbabi
Jean-Yves Marion
Organization

General Chairs

Frédéric Cuppens  Telecom Bretagne, France
Ali A. Ghorbani  University of New Brunswick, Canada

Program Chairs

Jean-Luc Danger  Telecom Paristech, France
Mourad Debbabi  Concordia University, Canada
Jean-Yves Marion  Mines de Nancy, France

Organizing Chairs

Nora Cuppens-Boulahia  Telecom Bretagne, France
Ghislaine Le Gall  Telecom Bretagne, France

Publication Chairs

Joaquin Garcia-Alfaro  Telecom SudParis, France
Nur Zincir Heywood  Dalhousie University, Canada

Webmaster

Said Oulmakhzoune  Telecom Bretagne, France

Program Committee

Diala Abihaidar  Dar Al Hekma College, Saudi Arabia
Carlisle Adams  Ottawa University, Canada
Kamel Adi  Université du Québec en Outaouais, Canada
Gildas Avoine  Catholic University of Louvain, Belgium
Michel Barbeau  Carleton University, Canada
Guillaume Bonfante  Université de Lorraine, France
Jordi Castella-Roca  Rovira i Virgili University, Spain
Ana Cavalli  Telecom SudParis, France
Frédéric Cuppens  Telecom Bretagne, France
Nora Cuppens-Boulahia  
Mila Dalla Preda  
Jean-Luc Danger  
Vanessa Daza  
Mourad Debbabi  
Roberto Di Pietro  
Nicola Dragoni  
Jose M. Fernandez  
Sara Foresti  
Eric Freyssinet  
Sebastien Gambs  
Flavio D. Garcia  
Jose M. Garcia-Alfaro  
Ali Ghorbani  
Roberto Giacobazzi  
Sylvain Guilley  
Abdelwahab Hamou-Ladj  
Jordi Herrera  
Bruce Kapron  
Hyungshick Kim  
Evangelos Kranakis  
Pascal Lafourcade  
Yassine Lakhnech  
Georgios Lioudakis  
Luigi Logrippo  
Javier Lopez  
Stefan Mangard  
Jean-Yves Marion  
Joan Melia-Segui  
Ali Miri  
Guillermo Navarro-Arribas  
Jordi Nin  
Andreas Pashalidis  
Emmanuel Prouff  
Silvio Ranise  
Jean-Marc Robert  
Rei Safavi-Naini  
Kazuo Sakiyama  
Werner Schindler  
Alessandro Sorniotti  
Anna Squicciarini  
Chamseddine Talhi  
Nadia Tawbi  
Issa Traore  
Alexandre Viejo

Telecom Bretagne, France  
Verona University, Italy  
Telecom ParisTech, France  
Universitat Pompeu Fabra, Spain  
Concordia University, Canada  
Roma Tre University, Italy  
Technical University of Denmark, Denmark  
Ecole Polytechnique de Montreal, Canada  
Universitè degli Studi di Milano, Italy  
Université Paris 6, France  
Université de Rennes 1, France  
Radboud University Nijmegen, The Netherlands  
Telecom SudParis, France  
University of New Brunswick, Canada  
University of Verona, Italy  
Telecom ParisTech, France  
Concordia University, Canada  
Universitat Autonoma de Barcelona, Spain  
University of Victoria, Canada  
SungKyunKwan University, South Korea  
Carleton University, Canada  
Joseph Fourier University, France  
Joseph Fourier University, France  
National Technical University of Athens, Greece  
Université du Quebec en Outaouais, Canada  
University of Malaga, Spain  
Infineon Technologies, Germany  
Mines de Nancy, France  
Universitat Pompeu Fabra, Spain  
Ryerson University, Canada  
Autonomous University of Barcelona, Spain  
Universitat Politecnica de Catalunya, Spain  
K.U.Leuven, Belgium  
ANSSI, France  
Fondazione Bruno Kessler, Italy  
Ecole de technologie superieure, Canada  
Calgary University, Canada  
University of Electro-Communications, Japan  
Bundesamt für Sicherheit in der Informationstechnik, Germany  
IBM Research Zurich, Switzerland  
The Pennsylvania State University, USA  
ETS, Montreal, Canada  
Université Laval, Canada  
University of Victoria, Canada  
Universitat Rovira i Virgili, Spain
<table>
<thead>
<tr>
<th>Lena Wiese</th>
<th>University of Göttingen, Germany</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nicola Zannone</td>
<td>Eindhoven University of Technology, The Netherlands</td>
</tr>
<tr>
<td>Mohammad Zulkernine</td>
<td>Queen’s University, Canada</td>
</tr>
</tbody>
</table>

**Additional Reviewers**

<table>
<thead>
<tr>
<th>Alessio Di Mauro</th>
<th>Sherif Saad</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tongjie Zhang</td>
<td>Cedric Lauradoux</td>
</tr>
<tr>
<td>Mahavir Jhawar</td>
<td>Anil Kurmus</td>
</tr>
<tr>
<td>Yang Li</td>
<td>Laurent Mounier</td>
</tr>
<tr>
<td>Shivam Bhasin</td>
<td>Yosr Jarraya</td>
</tr>
<tr>
<td>Asem Kitana</td>
<td>Isabella Mastroeni</td>
</tr>
<tr>
<td>Elli Androulaki</td>
<td>Eugenia Papagiannakopoulou</td>
</tr>
<tr>
<td>Samiha Ayed</td>
<td>Samir Ouchani</td>
</tr>
<tr>
<td>Mohammad Hajiabadi</td>
<td>Maria Koukovini</td>
</tr>
<tr>
<td>Benedikt Schmidt</td>
<td>Clara Bertolissi</td>
</tr>
<tr>
<td>Liangfeng Zhang</td>
<td>Martin Gagne</td>
</tr>
<tr>
<td>Fatih Turkmen</td>
<td></td>
</tr>
</tbody>
</table>
Contents

Keynote Address

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

Security Protocols

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

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

Modelling Simultaneous Mutual Authentication for Authenticated Key Exchange
Zheng Yang 46

Formal Methods

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

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

Physical Security

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

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

Investigation of Parameters Influencing the Success of Optical Fault Attacks
Thomas Korak 140
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
<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>Ali Kassem, Pascal Lafourcade, and Yassine Lakhnech</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>Bao Liu, Lei Zhang, and Josep Domingo-Ferrer</td>
<td></td>
</tr>
<tr>
<td>Resilience</td>
<td></td>
</tr>
<tr>
<td>CheR: Cheating Resilience in the Cloud via Smart Resource Allocation</td>
<td>339</td>
</tr>
<tr>
<td>Di Pietro Roberto, Flavio Lombardi, Fabio Martinelli, and Daniele Sgandurra</td>
<td></td>
</tr>
<tr>
<td>Evaluation of Software-Oriented Block Ciphers on Smartphones</td>
<td>353</td>
</tr>
<tr>
<td>Lukas Malina, Vlastimil Clupek, Zdenek Martinasek, Jan Hajny, Kimio Oguchi, and Vaclav Zeman</td>
<td></td>
</tr>
<tr>
<td>Don’t Push It: Breaking iButton Security</td>
<td>369</td>
</tr>
<tr>
<td>Christian Brandt and Michael Kasper</td>
<td></td>
</tr>
<tr>
<td>Intrusion Detection</td>
<td></td>
</tr>
<tr>
<td>Discovering Flaws in IDS Through Analysis of Their Inputs</td>
<td>391</td>
</tr>
<tr>
<td>Raphaël Jamet and Pascal Lafourcade</td>
<td></td>
</tr>
<tr>
<td>On the Reverse Engineering of the Citadel Botnet</td>
<td>408</td>
</tr>
<tr>
<td>Ashkan Rahimian, Raha Ziarati, Stere Preda, and Mourad Debbabi</td>
<td></td>
</tr>
<tr>
<td>The Carna Botnet Through the Lens of a Network Telescope</td>
<td>426</td>
</tr>
<tr>
<td>Erwan Le Malécot and Daisuke Inoue</td>
<td></td>
</tr>
<tr>
<td>Author Index</td>
<td>443</td>
</tr>
</tbody>
</table>