

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, Lancaster, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Friedemann Mattern

*ETH Zurich, Zürich, Switzerland*

John C. Mitchell

*Stanford University, Stanford, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*TU Dortmund University, Dortmund, Germany*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbrücken, Germany*

More information about this series at <http://www.springer.com/series/7410>

Joaquin Garcia-Alfaro · Evangelos Kranakis  
Guillaume Bonfante (Eds.)

# Foundations and Practice of Security

8th International Symposium, FPS 2015  
Clermont-Ferrand, France, October 26–28, 2015  
Revised Selected Papers

*Editors*

Joaquin Garcia-Alfaro  
Télécom SudParis  
Evry  
France

Evangelos Kranakis  
School of Computer Science  
Carleton University  
Ottawa, ON  
Canada

Guillaume Bonfante  
École des Mines de Nancy  
Université de Lorraine  
Nancy Cedex  
France

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-30302-4            ISBN 978-3-319-30303-1 (eBook)  
DOI 10.1007/978-3-319-30303-1

Library of Congress Control Number: 2016932326

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing Switzerland 2016

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

This Springer imprint is published by SpringerNature  
The registered company is Springer International Publishing AG Switzerland

## Preface

This volume contains the proceedings of the 8th International Symposium on Foundations and Practice of Security, hosted by the University of Auvergne, in Clermont-Ferrand, France, during October 26–28, 2015.

The FPS Symposium was initiated in 2008, following the Canada-France Meeting on Security held at Simon Fraser University, Vancouver, during December 6–8, 2007. Since then, FPS has been held annually, alternating between Canadian and French locations, including Montréal, Grenoble, Toronto, La Rochelle, and Paris.

This year's symposium received 58 submissions, out of which 12 papers were selected as full papers and eight as short papers. All submissions went through a careful anonymous review process (three or more reviews per submission) aided by members of the Technical Program Committee and several external reviewers. The program was completed with two keynote addresses by Evangelos Kranakis (Carleton University, Ottawa, Canada) and David Pointcheval (Ecole Normale Supérieure, Paris, France).

Many people contributed to the success of FPS 2015. 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 general chair, Pascal Lafourcade (University of Auvergne), and his organizing team, for their great efforts in organizing and dealing with the logistics during the symposium. We also want to express our gratitude to the publicity chairs, Giovanni Livraga (University of Milan, Italy), Zhiqiang Lin (University of Texas at Dallas, US), and Mizuhito Ogawa (Advanced Institute of Science and Technology, Japan), for their efforts at advertising the symposium. Last but by no means least we want to thank all the sponsors for making the event possible.

We hope the articles in this proceedings volume will be valuable for your professional activities in the area.

December 2015

Joaquin Garcia-Alfaro  
Evangelos Kranakis  
Guillaume Bonfante

# Organization

## General Chair

Pascal Lafourcade

University of Auvergne, France

## Program Co-chairs

Guillaume Bonfante

Mines de Nancy, France

Joaquin Garcia-Alfaro

Télécom SudParis, France

Evangelos Kranakis

Carleton University, Canada

## Publicity Co-chairs

Giovanni Livraga

University of Milan, Italy

Zhiqiang Lin

University of Texas at Dallas, USA

Mizuhito Ogawa

Advanced Institute of Science and Technology, Japan

## Program Committee

Samiha Ayed

Télécom Bretagne, France

Michel Barbeau

Carleton University, Canada

Jordi Castella-Roca

Rovira i Virgili University, Spain

Frédéric Cuppens

Télécom Bretagne, France

Nora Cuppens-Boulahia

Télécom Bretagne, France

Mila Dalla Preda

University of Bologna, Italy

Mourad Debbabi

University of Concordia, Canada

Nicola Dragoni

Technical University of Denmark, Denmark

Josep Domingo-Ferrer

Universitat Rovira i Virgili, Spain

Jean-Luc Danger

Telecom ParisTech, France

Sara Foresti

University of Milan, Italy

Marc Frappier

University of Sherbrooke, Canada

Martin Gagne

Wheaton College, USA

Sebastien Gamsb

Université de Rennes, France

Flavio D. Garcia

University of Birmingham, UK

Diala Haidar

Dar Al Hekma College, Saudi Arabia

Jordi Herrera-Joancomarti

Autonomous University of Barcelona, Spain

Bruce Kapron

University of Victoria, Canada

Hyounghick Kim

Sungkyunkwan University, South Korea

Giovanni Livraga

University of Milan, Italy

Luigi Logrippo

Université du Quebec en Outaouais, Canada

Javier Lopez

University of Malaga, Spain

Flaminia Luccio	Ca'Foscari University of Venice, Italy
Joan Melia-Segui	Universitat Oberta de Catalunya, Spain
Ali Miri	Ryerson University, Canada
Guillermo Navarro-Arribas	Autonomous University of Barcelona, Spain
Jordi Nin	Universitat Politècnica de Catalunya, Spain
Melek Önen	Eurecom, France
Andreas Pashalidis	K.U. Leuven, Belgium
Thomas Peters	Ecole Normale Supérieure, France
Marie-Laure Potet	Ensimag, France
Silvio Ranise	FBK, Security and Trust Unit, Italy
Claudio Soriente	ETH Zurich, Switzerland
Chamseddine Talhi	ETS Montréal, Canada
Nadia Tawbi	Université Laval, Canada
Emmanuel Thomé	Inria Lorraine, France
Alexandre Viejo	Rovira i Virgili University, Spain
Lena Wiese	Göttingen University, Germany
Nicola Zannone	Eindhoven University of Technology, The Netherlands
Nur Zincir Heywood	Dalhousie University, Canada
Mohammad Zulkernine	Queen's University, Canada

### **Additional Reviewers**

Saed Alrabaee	Djedjiga Mouheb
Carles Anglès-Tafalla	David Nuñez
Khodakhast Bibak	David Oswald
Olivier Blazy	Cristina Pérez-Solà
Amine Boukhtouta	Marta Pujol
Marie-Angela Cornélie	Jordi Ribes-González
Vicenç Creus-García	Ruben Rios
Guenaëlle de Julis	Jean-Claude Royer
Joeri de Ruiter	Julián Salas
Mohammad Hajiabadi	Saeed Shafieian
Shahreaz Iqbal	Stefan Thaler
Amrit Kumar	Sam L. Thomas
Bo Mi	Tim Waage

### **Steering Committee**

Frédéric Cuppens	Télécom Bretagne, France
Nora Cuppens-Boulahia	Télécom Bretagne, France
Mourad Debbabi	University of Concordia, Canada
Joaquín García-Alfaro	Télécom SudParis, France
Evangelos Kranakis	Carleton University, Canada
Pascal Lafourcade	University of Auvergne, France

Jean-Yves Marion

Ali Miri

Rei Safavi-Naini

Nadia Tawbi

Lorraine University, France

Ryerson University, Canada

Calgary University, Canada

Université Laval, Canada



# Contents

## Keynote Talks

- Optimization Problems in Infrastructure Security . . . . . 3  
*Evangelos Kranakis and Danny Krizanc*
- Secure Distributed Computation on Private Inputs . . . . . 14  
*Geoffroy Couteau, Thomas Peters, and David Pointcheval*

## RFID, Sensors and Secure Computation

- Survey of Distance Bounding Protocols and Threats . . . . . 29  
*Agnès Brelurut, David Gerault, and Pascal Lafourcade*
- Inferring Touch from Motion in Real World Data . . . . . 50  
*Pascal Bissig, Philipp Brandes, Jonas Passerini, and Roger Wattenhofer*
- Point-Counting Method for Embarrassingly Parallel Evaluation in Secure Computation. . . . . 66  
*Toomas Krips and Jan Willemson*

## Security Policies and Biometrics

- Security Mechanisms Planning to Enforce Security Policies . . . . . 85  
*Anis Bkakria, Frédéric Cuppens, Nora Cuppens-Boulahia, and David Gross-Amblard*
- Runtime Enforcement with Partial Control . . . . . 102  
*Raphaël Khoury and Sylvain Hallé*
- Privacy-Preserving Fuzzy Commitment for Biometrics via Layered Error-Correcting Codes . . . . . 117  
*Masaya Yasuda, Takeshi Shimoyama, Narishige Abe, Shigefumi Yamada, Takashi Shinzaki, and Takeshi Koshiba*

## Evaluation of Protocols and Obfuscation Security

- Performance Evaluations of Cryptographic Protocols Verification Tools Dealing with Algebraic Properties . . . . . 137  
*Pascal Lafourcade and Maxime Puy*
- AnBx: Automatic Generation and Verification of Security Protocols Implementations . . . . . 156  
*Paolo Modesti*

Evaluating Obfuscation Security: A Quantitative Approach. . . . . 174  
*Rabih Mohsen and Alexandre Miranda Pinto*

**Spam Emails, Botnets and Malware**

Fast and Effective Clustering of Spam Emails Based on Structural Similarity. . . . . 195  
*Mina Sheikhalishahi, Andrea Saracino, Mohamed Mejri, Nadia Tawbi, and Fabio Martinelli*

A Closer Look at the HTTP and P2P Based Botnets from a Detector’s Perspective. . . . . 212  
*Fariba Haddadi and A. Nur Zincir-Heywood*

Obfuscation Code Localization Based on CFG Generation of Malware . . . . . 229  
*Nguyen Minh Hai, Mizuhito Ogawa, and Quan Thanh Tho*

**Short Papers**

Runtime Monitoring of Stream Logic Formulae . . . . . 251  
*Sylvain Hallé and Raphaël Khoury*

MIME: A Formal Approach to (Android) Emulation Malware Analysis. . . . . 259  
*Fabio Bellini, Roberto Chiodi, and Isabella Mastroeni*

Information Classification Enablers . . . . . 268  
*Erik Bergström and Rose-Mharie Åhlfeldt*

Information Flow Control on a Multi-paradigm Web Application for SQL Injection Prevention. . . . . 277  
*Meriam Ben-Ghorbel-Talbi, François Lesueur, and Gaetan Perrin*

Searchable Encryption in Apache Cassandra. . . . . 286  
*Tim Waage, Ramaninder Singh Jhaggi, and Lena Wiese*

AndroSSL: A Platform to Test Android Applications Connection Security . . . 294  
*François Gagnon, Marc-Antoine Ferland, Marc-Antoine Fortier, Simon Desloges, Jonathan Ouellet, and Catherine Boileau*

Onion Routing in Deterministic Delay Tolerant Networks . . . . . 303  
*Adrian Antunez-Veas and Guillermo Navarro-Arribas*

Security Enforcement by Rewriting: An Algebraic Approach . . . . . 311  
*Guangye Sui and Mohamed Mejri*

**Author Index** . . . . . 323