

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, Zurich, 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>


Abdessamad Imine · José M. Fernandez
Jean-Yves Marion · Luigi Logrippo
Joaquin Garcia-Alfaro (Eds.)

Foundations and Practice of Security

10th International Symposium, FPS 2017
Nancy, France, October 23–25, 2017
Revised Selected Papers


Editors

Abdessamad Imine
University of Lorraine
Villers-lès-Nancy
France

José M. Fernandez 
Polytechnique de Montréal
Montreal, QC
Canada

Jean-Yves Marion
LORIA
Vandœuvre-lès-Nancy
France

Luigi Logrippo 
Université du Québec en Outaouais
Gatineau, QC
Canada

Joaquin Garcia-Alfaro 
Télécom SudParis
Evry Cedex
France

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-75649-3 ISBN 978-3-319-75650-9 (eBook)
<https://doi.org/10.1007/978-3-319-75650-9>

Library of Congress Control Number: 2018934322

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG, part of Springer Nature 2018

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. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by the registered company Springer International Publishing AG part of Springer Nature
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland



Preface

This volume contains the papers presented at the 10th International Symposium on Foundations and Practice of Security (FPS 2017), which was hosted by Lorraine Research Laboratory in Computer Science and Its Applications (LORIA), Nancy, France, during October 23–25, 2017.

FPS 2017 attracted 53 submissions. At least three reviews were made for each submitted paper. The decision on acceptance or rejection in the review process was completed after intensive discussions over a one-week period. The Program Committee accepted 17 full research papers and three short research papers for presentation. The selected papers deal with diverse research themes, ranging from classic topics, such as access control models, formal verification for secure protocols and network security to emerging issues, such as security in blockchain and encrypted databases.

The best paper award of FPS 2017 was awarded to the contribution “Defending Against Adversarial Attacks Using Statistical Hypothesis Testing” presented by Sunny Raj, Sumit Kumar Jha, Laura Pullum, and Arvind Ramanathan. The program was completed with three excellent invited talks given by Véronique Cortier (LORIA-CNRS, France), Krishna Gummadri (Max Planck Institute for Software Systems, Germany), and Florian Kerschbaum (University of Waterloo, Canada).

Many people contributed to the success of FPS 2017. 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 chairs, Luigi Logrippo (Université du Québec en Outaouais, Canada) and Jean-Yves Marion (Mines de Nancy, France), and the local organizer, Abdessamad Imine, for the great efforts to organize and perfectly manage the logistics during the symposium. Finally, we also want to express our gratitude to the publication chair, Joaquin Garcia-Alfaro (Télécom SudParis), for his work on editing the proceedings. Last but not least, thanks to all the attendees. As security becomes an essential property in the 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.

November 2017

José M. Fernandez
Abdessamad Imine
Luigi Logrippo
Jean-Yves Marion

Organization

General Chairs

Luigi Logrippo	Université du Québec en Outaouais, Canada
Jean-Yves Marion	Mines de Nancy, France

Program Co-chairs

José M. Fernandez	Polytechnique Montréal, Canada
Abdessamad Imine	Université de Lorraine, Nancy, France

Publications Chair

Joaquin Garcia-Alfaro	Télécom SudParis, France
-----------------------	--------------------------

Local Organizing Committee

Abdessamad Imine	Université de Lorraine, Nancy, France
------------------	---------------------------------------

Publicity Chairs

Pascal Lafourcade	Université d'Auvergne, France
Raphaël Khoury	Université du Québec à Chicoutimi, Canada

Program Committee

Esma Aimeur	University of Montreal, Canada
Jeremy Clark	Concordia University, Canada
Frédéric Cuppens	IMT Atlantique, France
Nora Cuppens	IMT Atlantique, France
Jean-Luc Danger	Télécom Paris-Tech, France
Mourad Debbabi	Concordia University, Canada
Josée Desharnais	Laval University, Canada
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Samuel Dubus	NOKIA Bell Labs, France
Sébastien Gambs	Université du Québec à Montréal, Canada
Joaquin Garcia-Alfaro	Telecom SudParis, France
Dieter Gollmann	Hamburg University of Technology, Germany
Sushil Jajodia	George Mason University, USA
Martin Johns	SAP Research, Germany
Bruce Kapron	University of Victoria, Canada
Nizar Kheir	THALES, France

Raphaël Khoury	Université du Québec à Chicoutimi, Canada
Hyoungshick Kim	Sungkyunkwan University, Republic of Korea
Igor Kotenko	SPIIRAS, Russia
Evangelos Kranakis	Carleton University Computer Science, Canada
Pascal Lafourcade	Université d'Auvergne, France
Luigi Logrippo	Université du Québec en Outaouais, Canada
Javier Lopez	University of Malaga, Spain
Jean-Yves Marion	Mines de Nancy, France
Fabio Martinelli	National Research Council of Italy, CNR, Italy
David Mentré	Mitsubishi Electric R&D Centre Europe, France
Paliath Narendran	University at Albany, USA
Guillermo Navarro-Arribas	Universitat Autònoma de Barcelona, Spain
Jun Pang	University of Luxembourg, Luxembourg
Marie-Laure Potet	VERIMAG, France
Silvio Ranise	FBK, Security and Trust Unit, Italy
Indrakshi Ray	Colorado State University, USA
Michaël Rusinowitch	LORIA-Inria Nancy, France
Basit Shafiq	Lahore University of Management Sciences, Pakistan
Anna Squicciarini	Pennsylvania State University, USA
Natalia Stakhanova	University of New Brunswick, Canada
Chamseddine Talhi	École de Technologie Supérieure, Canada
Nadia Tawbi	Université Laval, Canada
Rakesh Verma	University of Houston, USA
Lingyu Wang	Concordia University, Canada
Edgar Weippl	SBA Research, Austria
Lena Wiese	Georg-August Universität Göttingen, Germany
Xun Yi	RMIT University, Australia
Nur Zincir-Heywood	Dalhousie University, Canada
Mohammad Zulkernine	Queen's University, Canada

Additional Reviewers

Zumrut Akcam	University at Albany, USA
Saed Alrabae	Concordia University, Canada
Carles Anglès	Universitat Rovira i Virgili, Spain
Andrew Bedford	Université Laval, Canada
Bruhadeshwar Bezawada	Colorado State University, USA
Alexander Branitskiy	SPIIRAS, Russia
Wenyaw Chan	University of Texas Health Science Center - Houston, USA
Andrey Chechulin	SPIIRAS, Russia
Vincent Cheval	LORIA-Inria Nancy, France
Mónica Del Carmen Muñoz	Universitat Rovira i Virgili, Spain

Luis Miguel Del Vasto	Universitat Rovira i Virgili, Spain
Vasily Desnitsky	SPIIRAS, Russia
Lena Doynikova	SPIIRAS, Russia
Jannik Dreier	Université de Lorraine, Nancy, France
Arthur Dunbar	University of Houston, USA
Gerardo Fernandez	University of Malaga, Spain
Carmen Fernandez-Gago	University of Malaga, Spain
David Gérard	Université d'Auvergne, France
Sanjay Goel	University at Albany, USA
Daniel Homann	Georg-August Universität Göttingen, Germany
Amrit Kumar	National University of Singapore, Singapore
Amirreza Masoumzadeh	University at Albany, USA
Maxime Puy	VERIMAG, France
Veena Ravishankar	University at Albany, USA
Sara Ricci	Universitat Rovira i Virgili, Spain
Igor Saenko	SPIIRAS, Russia
Paria Shirani	Concordia University, Canada
Wojciech Widel	IRISA, Rennes, France

Steering Committee

Frédéric Cuppens	IMT Atlantique, France
Nora Cuppens-Bouahia	IMT Atlantique, France
Mourad Debbabi	University of Concordia, Canada
Joaquin Garcia-Alfaro	Télécom SudParis, France
Evangelos Kranakis	Carleton University, Canada
Pascal Lafourcade	Université d'Auvergne, France
Jean-Yves Marion	Mines de Nancy, France
Ali Miri	Ryerson University, Canada
Rei Safavi-Naini	Calgary University, Canada
Nadia Tawbi	Université Laval, Canada

Contents

Access Control

Attribute-Based Encryption as a Service for Access Control in Large-Scale Organizations	3
<i>Johannes Blömer, Peter Günther, Volker Krummel, and Nils Löken</i>	
Relationship-Based Access Control for Resharing in Decentralized Online Social Networks	18
<i>Richard Gay, Jinwei Hu, Heiko Mantel, and Sogol Mazaheri</i>	
Secure Protocol of ABAC Certificates Revocation and Delegation.	35
<i>Alexey Rabin and Ehud Gudes</i>	

Formal Verification

Formal Analysis of Combinations of Secure Protocols	53
<i>Elliott Blot, Jannik Dreier, and Pascal Lafourcade</i>	
Formal Analysis of the FIDO 1.x Protocol	68
<i>Olivier Pereira, Florentin Rochet, and Cyrille Wiedling</i>	
A Roadmap for High Assurance Cryptography	83
<i>Harry Halpin</i>	

Privacy

Privacy-Preserving Equality Test Towards Big Data	95
<i>Tushar Kanti Saha and Takeshi Koshiba</i>	
Multi-level Access Control, Directed Graphs and Partial Orders in Flow Control for Data Secrecy and Privacy	111
<i>Luigi Logrippo</i>	

Physical Security

Generation of Applicative Attacks Scenarios Against Industrial Systems	127
<i>Maxime Puy, Marie-Laure Potet, and Abdelaziz Khaled</i>	

HuMa: A Multi-layer Framework for Threat Analysis in a Heterogeneous Log Environment	144
<i>Julio Navarro, Véronique Legrand, Sofiane Lagraa, Jérôme François, Abdelkader Lahmadi, Giulia De Santis, Olivier Festor, Nadira Lammari, Fayçal Hamdi, Aline Deruyver, Quentin Goux, Morgan Allard, and Pierre Parrend</i>	
Monitoring of Security Properties Using BeepBeep	160
<i>Mohamed Recem Boussaha, Raphaël Khoury, and Sylvain Hallé</i>	
Network Security, Encrypted DBs and Blockchain	
More Lightweight, yet Stronger 802.15.4 Security Through an Intra-layer Optimization.	173
<i>Konrad-Felix Krentz, Christoph Meinel, and Hendrik Graupner</i>	
ObliviousDB: Practical and Efficient Searchable Encryption with Controllable Leakage	189
<i>Shujie Cui, Muhammad Rizwan Asghar, Steven D. Galbraith, and Giovanni Russello</i>	
Ethereum: State of Knowledge and Research Perspectives	206
<i>Sergei Tikhomirov</i>	
Vulnerability Analysis and Deception Systems	
Bounding the Cache-Side-Channel Leakage of Lattice-Based Signature Schemes Using Program Semantics	225
<i>Nina Bindel, Johannes Buchmann, Juliane Krämer, Heiko Mantel, Johannes Schickel, and Alexandra Weber</i>	
Extinguishing Ransomware - A Hybrid Approach to Android Ransomware Detection	242
<i>Alberto Ferrante, Mirosław Malek, Fabio Martinelli, Francesco Mercaldo, and Jelena Milosevic</i>	
Deception in Information Security: Legal Considerations in the Context of German and European Law	259
<i>Daniel Fraunholz, Christoph Lipps, Marc Zimmermann, Simon Duque Antón, Johannes Karl Martin Mueller, and Hans Dieter Schotten</i>	

Defence Against Attacks and Anonymity

<i>SATYA</i> : Defending Against Adversarial Attacks Using Statistical Hypothesis Testing	277
<i>Sunny Raj, Laura Pullum, Arvind Ramanathan, and Sumit Kumar Jha</i>	
Attack Graph-Based Countermeasure Selection Using a Stateful Return on Investment Metric.	293
<i>Gustavo Gonzalez-Granadillo, Elena Doynikova, Igor Kotenko, and Joaquin Garcia-Alfaro</i>	
Weighted Factors for Evaluating Anonymity.	303
<i>Khalid Shahbar and A. Nur Zincir-Heywood</i>	
Author Index	319