

## Founding Editors

Gerhard Goos

*Karlsruhe Institute of Technology, Karlsruhe, Germany*

Juris Hartmanis

*Cornell University, Ithaca, NY, USA*

## Editorial Board Members

Elisa Bertino

*Purdue University, West Lafayette, IN, USA*

Wen Gao

*Peking University, Beijing, China*

Bernhard Steffen 

*TU Dortmund University, Dortmund, Germany*

Gerhard Woeginger 

*RWTH Aachen, Aachen, Germany*

Moti Yung

*Columbia University, New York, NY, USA*

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

Abdelmalek Benzekri · Michel Barbeau ·  
Guang Gong · Romain Laborde ·  
Joaquin Garcia-Alfaro (Eds.)


# Foundations and Practice of Security


12th International Symposium, FPS 2019  
Toulouse, France, November 5–7, 2019  
Revised Selected Papers

### *Editors*

Abdelmalek Benzekri  
Université Paul Sabatier (CNRS IRIT)  
Toulouse, France

Guang Gong  
University of Waterloo  
Waterloo, ON, Canada

Joaquin Garcia-Alfaro   
Telecom SudParis, IMT  
Palaiseau, France

Michel Barbeau   
Carleton University  
Ottawa, ON, Canada

Romain Laborde  
Université Paul Sabatier (CNRS IRIT)  
Toulouse, France

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-45370-1              ISBN 978-3-030-45371-8 (eBook)  
<https://doi.org/10.1007/978-3-030-45371-8>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2020

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, expressed 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.

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

# Preface

This volume contains the papers presented at the 12th International Symposium on Foundations and Practice of Security (FPS 2019), which was held at Crowne Plaza, Toulouse, France, during November 5–7, 2019. The symposium received 50 submissions from countries all over the world. At least two reviews were made for each paper. The Program Committee selected 19 full papers and 9 short papers that cover diverse security research themes including attack prevention, trustworthiness, access control models, cryptography, or blockchain. A strong focus was on artificial intelligence and machine learning approaches with three sessions dedicated to this topic. The Best Paper Award of FPS 2019 was granted to the contribution “PAC: Privacy-preserving Arrhythmia Classification with Neural Networks” presented by Mohamad Mansouri, Beyza Bozdemir, Melek Önen, and Orhan Ermis.

Three excellent invited talks completed the program. Sokratis Katsikas from University of Science and Technology (Norway) and Open University of Cyprus (Cyprus) presented the challenges of securing Industrial Internet of Things, David W. Chadwick from University of Kent (UK) explained the evolution of Identity Management, and Soumaya Cherkaoui from Université de Sherbrooke (Canada) highlighted the challenges and opportunities related to securing 5G Internet of Vehicles. Finally, we introduced this year a new session dedicated to collaborative projects. Adrien Bécue from Airbus Defense and Space presented CyberFactory#1 and Abdelmalek Benzekri from Université Paul Sabatier (France) outlined Cybersec4Europe.

We would like to thank all the authors who submitted their research results allowing for such a great program. 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 Local Organizing Committee: Marie-Angele Albouy, Abdelmalek Benzekri, François Barrère, Romain Laborde, Benoit Morgan, Florence Sedes, A. Samer Wazan, and Wafa Abdelghani; and the publications and publicity chair, Joaquin Garcia-Alfaro. We would also like to express our gratitude to all the attendees. Last, but by no means least, we want to thank all the sponsors for making the event possible.

To conclude, we would like to dedicate this FPS 2019 edition to François Barrère who left us much too young. François demonstrated during his career not only sound and thorough scientific qualities, but above all, he developed incomparable human qualities. May he rest in peace.

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

December 2019

Abdelmalek Benzekri  
Michel Barbeau  
Guang Gong  
Romain Laborde

# Organization

## General Chairs

|                     |  |
|---------------------|--|
| Abdelmalek Benzekri | Université Paul Sabatier, IRIT, France |
| Michel Barbeau      | Carleton University, Canada            |

## Program Committee Chairs

|                |  |
|----------------|--|
| Guang Gong     | University of Waterloo, Canada         |
| Romain Laborde | Université Paul Sabatier, IRIT, France |

## Publications Chair

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

## Local Organizing Committee

|                     |  |
|---------------------|--|
| Wafa Abdelghani     | Université Paul Sabatier, IRIT, France |
| Marie-Angele Albouy | Université Paul Sabatier, IRIT, France |
| Abdelmalek Benzekri | Université Paul Sabatier, IRIT, France |
| François Barrère    | Université Paul Sabatier, IRIT, France |
| Romain Laborde      | Université Paul Sabatier, IRIT, France |
| Benoit Morgan       | INPT, ENSEEEIHT, IRIT, France          |
| Florence Sedes      | Université Paul Sabatier, IRIT, France |
| Ahmad Samer Wazan   | Université Paul Sabatier, IRIT, France |

## Program Committee

|                       |   |
|-----------------------|---|
| Diala Abi Haidar      | Dar Al-Hekma University, Saudi Arabia     |
| Kamel Adi             | University of Quebec in Outaouais, Canada |
| Esma Aïmeur           | Université de Montréal, Canada            |
| Michel Barbeau        | Carleton University, Canada               |
| Mostafa Belkasmi      | Mohammed V University in Rabat, Morocco   |
| Abdelmalek Benzekri   | Université Paul Sabatier, France          |
| Guillaume Bonfante    | Université de Lorraine, LORIA, France     |
| Driss Bouzidi         | Mohammed V University in Rabat, Morocco   |
| Jordi Castellà-Roca   | Universitat Rovira i Virgili, Spain       |
| Ana Cavalli           | Télécom SudParis, France                  |
| Frédéric Cuppens      | IMT Atlantique, France                    |
| Nora Cuppens-Boulahia | IMT Atlantique, France                    |
| Mila Dalla Preda      | University of Verona, Italy               |
| Jean-Luc Danger       | Télécom Paris, France                     |

|                           |   |
|---------------------------|---|
| Vanesa Daza               | Universitat Pompeu Fabra, Spain                     |
| Mourad Debbabi            | Concordia University, Canada                        |
| Roberto Di Pietro         | Hamad Bin Khalifa University, Qatar                 |
| Josep Domingo-Ferrer      | Universitat Rovira i Virgili, Spain                 |
| Nicola Dragoni            | Technical University of Denmark, Denmark            |
| Eric Freyssinet           | LORIA, France                                       |
| Sebastien Gambs           | Université du Québec à Montréal, Canada             |
| Joaquin Garcia-Alfaro     | Télécom SudParis, France                            |
| Guang Gong                | University of Waterloo, Canada                      |
| Abdelwahab Hamou-Lhadj    | Concordia University, Canada                        |
| Jordi Herrera-Joancomarti | Universitat Autònoma de Barcelona, Spain            |
| Bruce Kapron              | University of Victoria, Canada                      |
| Raphaël Khoury            | Université du Québec à Chicoutimi, Canada           |
| Hyoungshick Kim           | Sungkyunkwan University, South Korea                |
| Evangelos Kranakis        | Carleton University, Canada                         |
| Igor Kotenko              | SPIIRAS, Russia                                     |
| Romain Laborde            | Université Paul Sabatier, France                    |
| Pascal Lafourcade         | Université Clermont Auvergne, France                |
| Luigi Logrippo            | University of Quebec in Outaouais, Canada           |
| Suryadipita Majumdar      | University at Albany, USA                           |
| Jean-Yves Marion          | Université de Lorraine, LORIA, France               |
| Ali Miri                  | Ryerson University, Canada                          |
| Benoit Morgan             | INP Toulouse, France                                |
| Paliath Narendran         | University at Albany, USA                           |
| Guillermo Navarro-Arribas | Autonomous University of Barcelona, Spain           |
| Jun Pang                  | University of Luxembourg, Luxembourg                |
| Milan Petkovic            | Philips Research, The Netherlands                   |
| Marie-Laure Potet         | Université Grenoble Alpes, VERIMAG, France          |
| Silvio Ranise             | Fondazione Bruno Kessler, Italy                     |
| Indrakshi Ray             | Colorado State University, USA                      |
| Jean-Marc Robert          | École de technologie supérieure, Canada             |
| Michaël Rusinowitch       | LORIA, Inria Nancy, France                          |
| Reyhaneh Safavi-Naini     | University of Calgary, Canada                       |
| Kazuo Sakiyama            | The University of Electro-Communications, Japan     |
| Paria Shirani             | Concordia University, Canada                        |
| Chamseddine Talhi         | École de Technologie Supérieure, Canada             |
| Nadia Tawbi               | Université Laval, Canada                            |
| Alexandre Viejo           | Universitat Rovira i Virgili, Spain                 |
| Edgar Weippl              | SBA Research, Austria                               |
| Nicola Zannone            | Eindhoven University of Technology, The Netherlands |
| Nur Zincir-Heywood        | Dalhousie University, Canada                        |

## **Additional Reviewers**

Kevin Atighehchi  
Olivier Blazy  
Salimeh Dashti  
Michele De Donno  
Alberto Giaretta  
Yoshikazu Hanatani  
Yota Katsikouli

Vinh Hoa La  
Marius Lombard-Platet  
Wissam Mallouli  
Cristina Onete  
Bagus Santoso  
Mariana Segovia  
Eunil Seo

## **Steering Committee**

Frédéric Cuppens  
Nora Cuppens-Boulahia  
Mourad Debbabi  
Joaquin Garcia-Alfaro  
Evangelos Kranakis  
Pascal Lafourcade  
Jean-Yves Marion  
Ali Miri  
Rei Safavi-Naini  
Nadia Tawbi

IMT Atlantique, France  
IMT Atlantique, France  
University of Concordia, Canada  
Télécom SudParis, France  
Carleton University, Canada  
Université d'Auvergne, France  
Mines de Nancy, France  
Ryerson University, Canada  
Calgary University, Canada  
Université Laval, Canada



# Contents

## Machine Learning Approaches

|  |    |
|--|----|
| PAC: Privacy-Preserving Arrhythmia Classification with Neural Networks . . .               | 3  |
| <i>Mohamad Mansouri, Beyza Bozdemir, Melek Önen, and Orhan Ermis</i>                       |    |
| Ransomware Network Traffic Analysis for Pre-encryption Alert . . . . .                     | 20 |
| <i>Routa Moussaileb, Nora Cuppens, Jean-Louis Lanet, and Hélène Le Bouder</i>              |    |
| Using Machine Learning to Detect Anomalies in Embedded Networks in Heavy Vehicles. . . . . | 39 |
| <i>Hossein Shirazi, Indrakshi Ray, and Charles Anderson</i>                                |    |
| Selection and Performance Analysis of CICIDS2017 Features Importance . . .                 | 56 |
| <i>Bruno Reis, Eva Maia, and Isabel Praça</i>  |    |
| Semantic Representation Based on Deep Learning for Spam Detection . . . .                  | 72 |
| <i>Nadjate Saidani, Kamel Adi, and Mohand Said Allili</i>                                  |    |
| Interpreting Machine Learning Malware Detectors Which Leverage N-gram Analysis. . . . .    | 82 |
| <i>William Briguglio and Sherif Saad</i>   |    |
| Labelled Network Capture Generation for Anomaly Detection . . . . .                        | 98 |
| <i>Maël Nogues, David Brosset, Hanan Hindy, Xavier Bellekens, and Yvon Kermarrec</i>       |    |

## Attack Prevention and Trustworthiness

|   |     |
|---|-----|
| Lempel-Ziv Compression with Randomized Input-Output for Anti-compression Side-Channel Attacks Under HTTPS/TLS . . . . .                     | 117 |
| <i>Meng Yang and Guang Gong</i>   |     |
| Secure Logging with Security Against Adaptive Crash Attack . . . . .  | 137 |
| <i>Sepideh Avizheh, Reihaneh Safavi-Naini, and Shuai Li</i>   |     |
| Enroll, and Authentication Will Follow: eID-Based Enrollment for a Customized, Secure, and Frictionless Authentication Experience . . . . . | 156 |
| <i>Silvio Ranise, Giada Sciarretta, and Alessandro Tomasi</i>   |     |
| TATIS: Trustworthy APIs for Threat Intelligence Sharing with UMA and CP-ABE . . . . .   | 172 |
| <i>Davy Preuveneers and Wouter Joosen</i>   |     |

|  |     |
|--|-----|
| Protecting Android Apps from Repackaging Using Native Code . . . . . | 189 |
| <i>Simon Tanner, Ilian Vogels, and Roger Wattenhofer</i>             |     |

### Access Control Models and Cryptography

|   |     |
|---|-----|
| Command Dependencies in Heuristic Safety Analysis of Access<br>Control Models. . . . .                              | 207 |
| <i>Peter Amthor and Martin Rabe</i>   |     |
| On Attribute Retrieval in ABAC. . . . .   | 225 |
| <i>Charles Morisset, Sowmya Ravidas, and Nicola Zannone</i>   |     |
| Incorporating Off-Line Attribute Delegation into Hierarchical Group<br>and Attribute-Based Access Control . . . . . | 242 |
| <i>Daniel Servos and Michael Bauer</i>  |     |
| U-EPS: An Ultra-small and Efficient Post-quantum Signature Scheme. . . . .  | 261 |
| <i>Guang Gong, Morgan He, Raghvendra Rohit, and Yunjie Yi</i>   |     |
| An Efficient Identification Scheme Based on Rank Metric . . . . .   | 273 |
| <i>Edoukou Berenger Ayebie, Hafsa Assidi, and El Mamoun Soudi</i>   |     |
| Security Analysis of Auctionity: A Blockchain Based E-Auction. . . . .  | 290 |
| <i>Pascal Lafourcade, Mike Nopere, J  r  my Picot, Daniela Pizzuti,<br/>and Etienne Roud  ix</i>                    |     |
| Dynamic Searchable Encryption with Access Control . . . . .   | 308 |
| <i>Johannes Bl  mer and Nils L  ken</i>   |     |

### Short Papers

|  |     |
|--|-----|
| Get-your-ID: Decentralized Proof of Identity . . . . .                           | 327 |
| <i>Pascal Lafourcade and Marius Lombard-Platet</i>                               |     |
| Towards Secure TMIS Protocols. . . . .   | 337 |
| <i>David Gerault and Pascal Lafourcade</i>                                       |     |
| Detecting Ransomware in Encrypted Web Traffic . . . . .                          | 345 |
| <i>Jaimin Modi, Issa Traore, Asem Ghaleb, Karim Ganame,<br/>and Sherif Ahmed</i> |     |
| Digital Forensics in Vessel Transportation Systems . . . . .                     | 354 |
| <i>Alessandro Cantelli-Forti and Michele Colajanni</i>                           |     |
| A Privacy Protection Layer for Wearable Devices . . . . .                        | 363 |
| <i>Muhammad Mohzary, Srikanth Tadisetty, and Kambiz Ghazinour</i>                |     |

|  |            |
|--|------------|
| Validating the DFA Attack Resistance of AES (Short Paper) . . . . .  | 371        |
| <i>Hakuei Sugimoto, Ryota Hatano, Natsu Shoji, and Kazuo Sakiyama</i>  |            |
| A Rejection-Based Approach for Detecting SQL Injection Vulnerabilities<br>in Web Applications . . . . .          | 379        |
| <i>Lalia Saoudi, Kamel Adi, and Younes Boudraa</i>   |            |
| Lightweight IoT Mutual Authentication Scheme Based on Transient<br>Identities and Transactions History . . . . . | 387        |
| <i>Mohammed Alshahrani, Issa Traore, and Sherif Saad</i>   |            |
| Towards Privacy-Aware Smart Surveillance . . . . .   | 398        |
| <i>Emil Shirima and Kambiz Ghazinour</i>   |            |
| <b>Author Index . . . . .</b>  | <b>407</b> |