



**HAL**  
open science

# Information Security Theory and Practice

Maryline Laurent, Thanassis Giannetsos

► **To cite this version:**

Maryline Laurent, Thanassis Giannetsos. Information Security Theory and Practice. Springer, LNCS-12024, pp.(X-253), 2020, Lecture Notes in Computer Science, 978-3-030-41701-7. 10.1007/978-3-030-41702-4 . hal-03173895

**HAL Id: hal-03173895**

**<https://inria.hal.science/hal-03173895v1>**

Submitted on 18 Mar 2021

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

## 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>

Maryline Laurent · Thanassis Giannetsos (Eds.)

# Information Security Theory and Practice

13th IFIP WG 11.2 International Conference, WISTP 2019  
Paris, France, December 11–12, 2019  
Proceedings

*Editors*

Maryline Laurent   
Telecom SudParis  
Evry, France

Thanassis Giannetsos   
Technical University of Denmark  
Lyngby, Denmark

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-41701-7              ISBN 978-3-030-41702-4 (eBook)  
<https://doi.org/10.1007/978-3-030-41702-4>

LNCS Sublibrary: SL4 – Security and Cryptology

© IFIP International Federation for Information Processing 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

It was our great pleasure to organize the 13th International Conference on Information Security Theory and Practice (WISTP 2019), held December 2019 at Conservatoire National des Arts et Métiers (CNAM) in Paris, France. This year marked the 13th edition of the conference, and we were thrilled to continue fostering collaboration among researchers and practitioners to discuss the various facets of cyber- and information-security. WISTP covers a wide range of topics on theoretical and practical aspects of security and privacy, as well as experimental studies of fielded systems, and thus benefits the cyber-security community by encouraging the emergence of novel research avenues of the aforementioned areas. The conference considered all complex facets and double-edged sword aspects of the cyber-security ecosystem, in particular, how new security algorithms and technologies can impact the security posture of existing and future ICT systems.

The WISTP 2019 call for papers attracted submissions from 24 countries, from a wide variety of academic and corporate institutions. In total, we received 42 valid submissions, of which 12 papers were selected as full papers and 2 were accepted as short papers after a double-blind review by our Program Committee comprised of 44 members, leading to a full acceptance rate of 28.5% and an overall acceptance rate of 33.3%. These papers cover a wide range of topics on the pressing challenges of security and privacy, including authentication, software security, threats and attacks, post-quantum cryptography, security analysis and proofs, and combining theoretical expertise and practical experiments that rely on emerging technologies (like Blockchain) with direct application of and impact on emerging domains of Internet of Things.

Two papers received extra praise: “Fault Injection Characterization on modern CPUs - From the ISA to the Micro-Architecture” by Thomas Troughkine, Guillaume Bouffard, and Jessy Clediere received the Best Student Paper Award; and “Threat Analysis of Poisoning Attack against Ethereum Blockchain” by Teppei Sato, Mitsuyoshi Imamura, and Kazumasa Omote received the Best Paper Award.

The program also included two invited talks by David Naccache (ENS, France) on “How to Compartment Secrets - Trust Everybody, but Cut the Cards -” and Pascal Paillier (CryptoExperts, France) on “Homomorphic encryption for deep learning: a revolution in the making.”

Putting together WISTP 2019 was a team effort. We first thank all the authors for the quality of their submissions. We are grateful to the Program Committee who worked very hard in reviewing papers and providing valuable feedback to authors. In addition, we would like to thank the General Chairs, Wojciech Mazurczyk from Warsaw University of Technology (WUT), Poland, and Samia Bouzefrane from Conservatoire National des Arts et Métiers (CNAM), France, for their valuable support and help with the planning and organization of the conference, as well as the Steering Committee, especially Damien Sauveron from the University of Limoges, France, for their

continuous efforts in making the event evolve throughout the years. Finally, special thanks to the Local Organizing Committee, Yulliwas Ameer (CNAM, France), Abou-Bakr Djaker (University of Oran, Algeria), Xiaotian Fu (CNAM, France), Thiziri Saad (CNAM, France), and Mamoudou Sangaré (CNAM, France) for hosting the conference in a beautiful and historical location.

We also want to thank the IDfix project, whose support helped to keep registration fees as low as possible and for providing great prizes to the best paper awards winners, as well as the IFIP WG 11.2: Pervasive Systems Security for their continued confidence in the organization of the WISTP editions.

January 2020

Maryline Laurent  
Thanassis Giannetsos

# Organization

## Program Committee Chairs

Maryline Laurent	Télécom SudParis, France
Thanassis Giannetsos	Danmarks Tekniske Universitet, Denmark

## Steering Committee

Angelos Bilas	University of Crete, Greece
Olivier Blazy	University of Limoges, France
Konstantinos Markantonakis	Royal Holloway University of London, UK
Joachim Posegga	University of Passau, Germany
Jean-Jacques Quisquater	Catholic University of Louvain, Belgium
Damien Sauveron	University of Limoges, France
Chan Yeob Yeun	Khalifa University, UAE

## Program Committee

Raja Naeem Akram	Royal Holloway University of London, UK
Claudio Ardagna	University of Milan, Italy
Kadri Benamar	University of Tlemcen, Algeria
Olivier Blazy	University of Limoges, France
Samia Bouzeffrane	Conservatoire National des Arts et Métiers, France
Xavier Bultel	University of Auvergne, France
Serge Chaumette	University of Bordeaux, France
Liqun Chen	University of Surrey, UK
Céline Chevalier	University of Pantheon-Assas Paris II, France
Emmanuel Conchon	University of Limoges, France
Mauro Conti	University of Padua, Italy
Gabriele Costa	IMT Lucca, Italy
Tassos Dimitriou	Computer Technology Institute, Greece
Ruggero Donida Labati	University of Milan, Italy
Sara Foresti	University of Milan, Italy
Thanassis Giannetsos	Danmarks Tekniske Universitet, Denmark
Johann Groszschaedl	University of Luxembourg, Luxembourg
Yong Guan	Iowa State University, USA
Nesrine Kaaniche	The University of Sheffield, UK
Süleyman Karda	Batman University, Turkey
Mehmet Sabir Kiraz	De Montfort University, UK
Ioannis Krontiris	Huawei Technologies, Germany
Andrea Lanzi	University of Milan, Italy
Albert Levi	Sabancı University, Turkey



Olivier Levillain	Télécom SudParis, France
Javier Lopez	NICS Lab, Spain
Sjouke Mauw	University of Luxembourg, Luxembourg
Keith Mayes	Royal Holloway University of London, UK
Alessio Merlo	University of Genoa, Italy
Antonios Michalas	Tampere University of Technology, Finland
Jiaxin Pan	Norwegian University of Science and Technology, Norway
Joachim Posegga	University of Passau, Germany
Kouichi Sakurai	Kyushu University, Japan
Pierangela Samarati	University of Milan, Italy
Siraj A. Shaikh	Coventry University, UK
Dave Singelee	Catholic University of Louvain, Belgium
Denis Trcek	University of Ljubljana, Slovenia
Umut Uludag	TUBITAK-BILGEM-UEKAE, Turkey
Paulo Verissimo	University of Luxembourg, Luxembourg
Anjia Yang	Jinan University, China
Stefano Zanero	Politecnico di Milano, Italy
Gongxuan Zhang	Nanjing University of Science and Technology, China

## Additional Reviewers

Angèle Bossuat	Eleonora Losiouk
Stefano Ceconello	Shahid Mahmood
Luca Demetrio	Ameer Mohammed
Atif Hussain	Paolo Montesel
Elif Bilge Kavun	Enrico Russo
Rhys Kirk	Korbinian Spielvogel
Felix Klement	Federico Turrin
Huimin Lao	Andrea Valenza
Yuxian Li	Axin Wu
Stefano Longari	Yuriy Zacchia Lun

## Sponsor



# Contents

## Invited Paper

- How to Compartment Secrets: Trust Everybody, but Cut the Cards . . . . . 3  
*Gaëlle Candèl, Rémi Géraud-Stewart, and David Naccache*

## Authentication

- A Lattice-Based Enhanced Privacy ID . . . . . 15  
*Nada EL Kassem, Luís Fiolhais, Paulo Martins, Liqun Chen, and Leonel Sousa*
- A Generic View on the Unified Zero-Knowledge Protocol and Its Applications. . . . . 32  
*Diana Maimuț and George Teșeleanu*

## Cryptography

- Verifiable and Private Oblivious Polynomial Evaluation. . . . . 49  
*Hardik Gajera, Matthieu Giraud, David Gérardt, Manik Lal Das, and Pascal Lafourcade*
- Monomial Evaluation of Polynomial Functions Protected by Threshold Implementations: With an Illustration on AES . . . . . 66  
*Simon Landry, Yanis Linge, and Emmanuel Prouff*
- Strong Designated Verifier Signature Based on the Rank Metric . . . . . 85  
*Hafsa Assidi and El Mamoun Souidi*
- A Lightweight Implementation of NTRU Prime for the Post-quantum Internet of Things . . . . . 103  
*Hao Cheng, Daniel Dinu, Johann Großschädl, Peter B. Rønne, and Peter Y. A. Ryan*

## Threats

- Fault Injection Characterization on Modern CPUs: From the ISA to the Micro-Architecture . . . . . 123  
*Thomas Troughkine, Guillaume Bouffard, and Jessy Clédière*
- Threat Analysis of Poisoning Attack Against Ethereum Blockchain. . . . . 139  
*Tepei Sato, Mitsuyoshi Imamura, and Kazumasa Omote*

**A Template-Based Method for the Generation of Attack Trees . . . . . 155**  
*Jeremy Bryans, Lin Shen Liew, Hoang Nga Nguyen,  
Giedre Sabaliauskaite, Siraj Shaikh, and Fengjun Zhou*

**Cybersecurity**

**Analysis of QUIC Session Establishment and Its Implementations. . . . . 169**  
*Eva Gagliardi and Olivier Levillain*

**CompactFlow: A Hybrid Binary Format for Network Flow Data. . . . . 185**  
*Michal Piskozub, Riccardo Spolaor, and Ivan Martinovic*

**SSI-AWARE: Self-sovereign Identity Authenticated Backup  
with Auditing by Remote Entities . . . . . 202**  
*Philipp Jakubeit, Albert Dercksen, and Andreas Peter*

**Internet of Things**

**Automated Security Analysis of IoT Software Updates . . . . . 223**  
*Nicolas Dejon, Davide Caputo, Luca Verderame, Alessandro Armando,  
and Alessio Merlo*

**Towards a Context-Aware Security and Privacy as a Service  
in the Internet of Things . . . . . 240**  
*Tidiane Sylla, Mohamed Aymen Chalouf, Francine Krief,  
and Karim Samaké*

**Author Index . . . . . 253**