

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board Members

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, Chennai, 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


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

Olivier Blazy · Chan Yeob Yeun (Eds.)

Information Security Theory and Practice

12th IFIP WG 11.2 International Conference, WISTP 2018
Brussels, Belgium, December 10–11, 2018
Revised Selected Papers

Editors

Olivier Blazy 
Université de Limoges
Limoges, France

Chan Yeob Yeun 
Khalifa University
Abu Dhabi, United Arab Emirates

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-20073-2 ISBN 978-3-030-20074-9 (eBook)
<https://doi.org/10.1007/978-3-030-20074-9>

LNCS Sublibrary: SL4 – Security and Cryptology

© IFIP International Federation for Information Processing 2019

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

The 12th WISTP International Conference on Information Security Theory and Practice attracted research contributions covering theoretical and practical aspects of security and privacy. Technical concepts from machine learning to real-world security, provide a global vision of current cybersecurity concerns.

This volume contains the papers presented at WISTP 2018 held during December 10–11 in Brussels.

There were 45 submissions. Each submission was reviewed on average by 3.1 Program Committee members. The reviewing was double-blind, with the identities of the authors not revealed to the reviewers of the papers and the identities of the reviewers not revealed to the authors, with some papers leading to intense discussions. The committee decided to accept 11 papers, yielding a 24% selection rate, together with two additional short papers. The program also included three invited talks by Amandine Jambert, Emil C. Lupu, and Damien Vergnaud.

Two papers received extra praised: “First Deep Learning Application in Security and Privacy – Theory and Practice: A Position Paper,” received the best Student Paper Award, and “Efficient Information Theoretic Multi-Party Computation from Oblivious Linear Evaluation.”

We would like to thank the General chairs (Jean-Michel Dricot, Olivier Markowitch, Yves Roggeman from ULB, Belgium) and the local organizers (Gaurav Sharma, Rajeev Anand Sahu, Dimitrios Sisiaridis, Suman Bala, Tania Ellinidou from ULB, Belgium).

We thank all the authors and participants who contributed to make this event a great success, the Technical Program Committee members and additional reviewers who worked on the program, and the volunteers who handled aspects of the organization behind the scenes. We greatly appreciate the input from members of the WISTP Steering Committee, whose help and advice was invaluable, and the support of IFIP WG 11.2: Pervasive Systems Security.

And we also want to thank our various sponsors (Centre for Cyber Security, Belgium; Fédération, Wallonie-Bruxelles, Belgium; IDfix), whose support helped to keep the registration costs as low as possible and at the same time allowed us to provide best paper awards and social activities to increase the networking opportunities. We also look forward to working together again in future WISTP events.

December 2018

Olivier Blazy
Chan Yeob Yeun

Organization

Program Committee

Mohamed Ahmed	SICS, Swedish ICT, Sweden
Raja Naeem Akram	ISG-Smart Card Centre, Royal Holloway, University of London, UK
Claudio Ardagna	Università degli Studi di Milano, Italy
Selcuk Baktir	Bahcesehir University, Turkey
Olivier Blazy	Université de Limoges, France
Samia Bouzefrane	CEDRIC Lab Conservatoire National des Arts et Métiers, France
Xavier Bultel	Université d'Auvergne, France
Céline Chevalier	ENS, France
Emmanuel Conchon	XLIM, France
Mauro Conti	University of Padua, Italy
José María De Fuentes	Universidad Carlos III de Madrid, Spain
Ruggero Donida Labati	Università degli Studi di Milano, Italy
Sara Foresti	Università degli Studi di Milano, Italy
Johann Groszschaedl	University of Luxembourg, Luxembourg
Yong Guan	Iowa State University, USA
Brahim Hamid	IRIT, University of Toulouse, France
Ben Hermann	Paderborn University, Germany
Julio Hernandez	University of Kent, UK
Sushil Jajodia	George Mason University, USA
Amandine Jambert	CNIL, France
Saqib A. Kakvi	Paderborn University, Germany
Süleyman Kardaş	Batman University, Turkey
Mehmet Sabir Kiraz	De Montfort University, UK
Ioannis Krontiris	Huawei Technologies, Germany
Andrea Lanzi	Università degli studi di Milano, Italy
Albert Levi	Sabanci University, Turkey
Olivier Levillain	French National and Information Security Agency, France
Javier Lopez	UMA, Spain
David M'Raihi	Pure Storage, USA
Vashek Matyas	Masaryk University, Czech Republic
Sjouke Mauw	University of Luxembourg, Luxembourg
Keith Mayes	ISG-Smart Card Centre, Royal Holloway, University of London, UK
Nele Mentens	Katholieke Universiteit Leuven, Belgium
Alessio Merlo	University of Genoa, Italy
Vladimir Oleshchuk	University of Agder, Norway

Jiaxin Pan	HGI, Ruhr University Bochum, Germany
Duong-Hieu Phan	University of Limoges, France
Joachim Posegga	University of Passau, Germany
Carla Ràfols	Universitat Pompeu Fabra, Spain
Kouichi Sakurai	Kyushu University, Japan
Pierangela Samarati	Università degli Studi di Milano, Italy
Siraj A. Shaikh	Coventry University, UK
Dave Singelee	Katholieke Universiteit Leuven, Belgium
Denis Treck	University of Ljubljana, Slovenia
Umut Uludag	TUBITAK-BILGEM-UEKAE, Turkey
Anjia Yang	Jinan University, China
Stefano Zanero	Politecnico di Milano, Italy

Steering Committee

Angelos Bilas	FORTH-ICS and University of Crete, Greece
Ernesto Damiani	Università degli Studi di Milano, Italy
Gerhard Hancke	City University of Hong Kong, Hong Kong, SAR China
Konstantinos Markantonakis	ISG-SCC, Royal Holloway University of London, UK
Joachim Posegga	Institute of IT-Security and Security Law at the University of Passau, Germany
Jean-Jacques Quisquater	ICTEAM, Catholic University of Louvain, Belgium
Damien Sauveron	XLIM, University of Limoges, France

Additional Reviewers

Anada, Hiroaki	Longari, Stefano	Ramírez-Cruz, Yuniór
Belgacem, Boutheyna	Marin, Eduard	Sauveron, Damien
Biondo, Andrea	Naccache, David	Sun, Bo
David, Michael	Nguyen, Hoang Nga	Tomlinson, Andrew
Gangwal, Ankit	Pogliani, Marcello	Trujillo, Rolando
Hary, Estelle	Polino, Mario	Xie, Fei
Kaliyar, Pallavi	Pöhls, Henrich C.	Xiong, Kaiya

Sponsors



CENTRE FOR
CYBER SECURITY
BELGIUM



FÉDÉRATION
WALLONIE-BRUXELLES

Contents

Invited Papers

Blockchain and the GDPR: A Data Protection Authority Point of View	3
<i>Amandine Jambert</i>	
Secure Outsourcing in Discrete-Logarithm-Based and Pairing-Based Cryptography (Invited Talk)	7
<i>Damien Vergnaud</i>	

Real World

Bringing Kleptography to Real-World TLS	15
<i>Adam Janovsky, Jan Krhovjak, and Vashek Matyas</i>	
Generic Architecture for Lightweight Block Ciphers: A First Step Towards Agile Implementation of Multiple Ciphers	28
<i>Etienne Tehrani, Jean-Luc Danger, and Tarik Graba</i>	
Generating a Real-Time Constraint Engine for Network Protocols	44
<i>Mohamed Sami Rakha, Fahim T. Imam, and Thomas R. Dean</i>	

Cryptography

On the Non-repudiation of Isogeny Based Signature Scheme	63
<i>Sookyung Eom, Hyang-Sook Lee, and Seongan Lim</i>	
Efficient Information Theoretic Multi-party Computation from Oblivious Linear Evaluation	78
<i>Louis Cianiullo and Hossein Ghodosi</i>	
Linear Depth Integer-Wise Homomorphic Division	91
<i>Hiroki Okada, Carlos Cid, Seira Hidano, and Shinsaku Kiyomoto</i>	

Artificial Learning

Prediction-Based Intrusion Detection System for In-Vehicle Networks Using Supervised Learning and Outlier-Detection	109
<i>Khaled Karray, Jean-Luc Danger, Sylvain Guilley, and Moulay Abdelaziz Elaabid</i>	

Deep Learning Application in Security and Privacy – Theory and Practice:
A Position Paper. 129
Julia A. Meister, Raja Naeem Akram, and Konstantinos Markantonakis

Cybersecurity

Cybersecurity Behaviour: A Conceptual Taxonomy. 147
Thulani Mashiane and Elmarie Kritzinger

Remote Credential Management with Mutual Attestation for Trusted
Execution Environments 157
*Carlton Shepherd, Raja Naeem Akram,
and Konstantinos Markantonakis*

Detection of Bitcoin-Based Botnets Using a One-Class Classifier 174
*Bruno Bogaz Zarpelão, Rodrigo Sanches Miani,
and Muttukrishnan Rajarajan*

Internet of Things

A Family of Lightweight Twisted Edwards Curves for the Internet
of Things 193
Sankalp Ghatpande, Johann Großschädl, and Zhe Liu

A Generic Lightweight and Scalable Access Control Framework
for IoT Gateways 207
Juan D. Parra Rodriguez

Author Index 223