Lecture Notes in Computer Science **10543**

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

Pooya Farshim · Emil Simion (Eds.)

Innovative Security Solutions for Information Technology and Communications

10th International Conference, SecITC 2017
Bucharest, Romania, June 8–9, 2017
Revised Selected Papers

Springer

Editors
Pooya Farshim
École Normale Supérieure
Paris
France

Emil Simion
Polytechnic University of Bucharest
Bucharest
Romania

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-69283-8 ISBN 978-3-319-69284-5 (eBook)
https://doi.org/10.1007/978-3-319-69284-5

Library of Congress Control Number: 2017956772

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

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

Preface

This volume contains the papers presented at SecITC 2017, the 10th International Conference on Security for Information Technology and Communications (www.secitc.eu), held during June 8–9, 2017, in Bucharest. There were 22 submissions and each submitted paper was reviewed by at least three Program Committee members. The committee decided to accept seven papers (one paper was withdrawn by the authors, after the conference, from the LNCS volume) as well as a further seven invited speakers. For ten years SecITC has been bringing together computer security researchers, cryptographers, industry representatives, and graduate students. The conference focuses on research on any aspect of security and cryptography. The papers present advances in the theory, design, implementation, analysis, verification, or evaluation of secure systems and algorithms. One of SecITC's primary goals is to bring together researchers belonging to different communities and provide a forum that facilitates the informal exchanges necessary for the emergence of new scientific collaborations. We would like to acknowledge the work of the Program Committee, whose great efforts provided a proper framework for the selection of the papers. The conference was organized by Advanced Technologies Institute, Bucharest University of Economic Studies and Military Technical Academy.

July 2017

Pooya Farshim
Emil Simion

Foreword

It is a priviledge for me to write the foreword to the proceedings to this 10th anniversary of the conference. Indeed, SECITC 2017 is the 10th edition of the International Conference on Information Technology and Communication Security held in Bucharest, Romania every year.

Throughout the years, SECITC has become a truely competitive publication venus with an acceptance rate of 1/3, an Program Committee of 50 experts from 20 countries and a long series of distinguished invited speakers. Since three years the conference proceedings are published in Springer's Lecture Notes in Computer Science, and articles published in SECITC are indexed in most science databases.

The conference is unique in that it serves as an exchange forum between confirmed researchers and students entering the field as well as industry players.

I would like to particularly thank the PC chairs Pooya Farshim and Emil Simion for an outstanding paper selection process conducted electronically. In response to the call for papers the Program Committee got 22 submissions of which seven were chosen. To those the PC added seven invited keynote lectures by Sylvain Guilley, Konstantinos Markantonakis, Claudio Orlandy, Peter Ryan, Ferucio-Laurentiu Tiplea, Damien Vergnaud, and myself.

I also warmly thank the conference's Organization Committee and Technical Support Team Mihai Doinea, Cristian Ciurea, Luciana Morogan, Andrei-George Oprina, Marius Popa, Mihai Pura, Mihai Togan, and Marian Haiducu for their precious contribution to the success of the event and for their dedication to the community.

I am certain that in the coming years SECITC will continue to grow and expand into a major cryptography and information security venue making Bucharest a traditional summertime scientific meeting habit to the IT security research community.

August 2017 David Naccache

Organization

Program Committee

Elena Andreeva	COSIC, KU Leuven, Belgium
Ludovic Apvrille	Telecom ParisTech, France
Gildas Avoine	INSA Rennes, France; UCL, Belgium
Manuel Barbosa	HASLab - INESC TEC and FCUP
Ion Bica	Military Technical Academy, Romania
Catalin Boja	Bucharest Academy of Economic Studies, Romania
Sanjit Chatterjee	Indian Institute of Science, India
Liqun Chen	University of Surrey, UK
Christophe Clavier	Université de Limoges, France
Paolo D'Arco	University of Salerno, Italy
Joan Daemen	STMicroelectronics and Radboud University in Nijmegen, The Netherlands
Roberto De Prisco	University of Salerno, Italy
Eric Diehl	Sony Pictures, USA
Itai Dinur	Ben-Gurion University, Israel
Stefan Dziembowski	University of Warsaw, Poland
Pooya Farshim	ENS, France
Bao Feng	Huawei, China
Eric Freyssinet	LORIA, France
Nicolas Gama	University of Versailles, France
Helena Handschuh	COSIC, KU Leuven, Belgium
Shoichi Hirose	University of Fukui, Japan
Xinyi Huang	Fujian Normal University, China
Miroslaw Kutylowski	Wroclaw University of Technology, Poland
Jean-Louis Lanet	Inria-RBA, France
Giovanni Livraga	Università degli Studi di Milano, Italy
Konstantinos Markantonakis	ISG-Smart Card Centre, Founded by Vodafone, G&D and the Information Security Group of Royal Holloway, University of London, UK
Florian Mendel	TU Graz, Austria
Bart Mennink	Digital Security Group, Radboud University, Nijmegen, The Netherlands
Kazuhiko Minematsu	NEC Corporation, Japan
David Naccache	ENS, France
Rene Peralta	NIST, USA
Bart Preneel	KU Leuven COSIC and iMinds, Belgium
Reza Reyhanitabar	NEC Laboratories Europe, Germany
P.Y.A. Ryan	University of Luxembourg, Luxembourg

Damien Sauveron	XLIM, UMR University of Limoges/CNRS 7252, France
Emil Simion	University Politehnica of Bucharest, Romania
Agusti Solanas	Smart Health Research Group, Rovira i Virgili University, Spain
Rainer Steinwandt	Florida Atlantic University, USA
Willy Susilo	University of Wollongong, Australia
Ferucio Laurentiu Tiplea	Alexandru Ioan Cuza University of Iasi, Romania
Mihai Togan	Military Technical Academy, Romania
Cristian Toma	Bucharest Academy of Economic Studies, Romania
Denis Trcek	University of Ljubljana, Slovenia
Michael Tunstall	Cryptography Research, USA
Victor Valeriu	Military Technical Academy, Romania
Serge Vaudenay	EPFL, Switzerland
Ingrid Verbauwhede	ESAT - COSIC, Belgium
Guilin Wang	Huawei International Pte. Ltd., China
Qianhong Wu	Beihang University, China
Lei Zhang	East China Normal University, China

Additional Reviewers

Balasch, Josep
Balli, Fatih
Bogos, Sonia
Chen, Siyuan
Li, Jiangtao
Li, Letitia
Li, Yanan
Lugou, Florian
Maimut, Diana
Slowik, Marcin
Unterluggauer, Thomas
Werner, Mario
Wszola, Marta
Zhang, Wentao

Contents

Faster Zero-Knowledge Protocols and Applications (Invited Talk Abstract) 1
Claudio Orlandi

Stochastic Side-Channel Leakage Analysis *via* Orthonormal Decomposition . . . 12
Sylvain Guilley, Annelie Heuser, Tang Ming, and Olivier Rioul

Key-Policy Attribute-Based Encryption from Bilinear Maps 28
Ferucio Laurenţiu Ţiplea, Constantin Cătălin Drăgan, and Anca-Maria Nica

Security of Pseudo-Random Number Generators with Input (Invited Talk) 43
Damien Vergnaud

Securing the Foundations of Democracy 52
Peter Y.A. Ryan

Exploring Naccache-Stern Knapsack Encryption 67
Éric Brier, Rémi Géraud, and David Naccache

Proximity Assurances Based on Natural and Artificial Ambient Environments 83
Iakovos Gurulian, Konstantinos Markantonakis, Carlton Shepherd, Eibe Frank, and Raja Naeem Akram

Challenges of Federating National Data Access Infrastructures 104
Margus Freudenthal and Jan Willemson

Strongly Deniable Identification Schemes Immune to Prover's and Verifier's Ephemeral Leakage 115
Łukasz Krzywiecki and Marcin Słowik

Evolution of the McEliece Public Key Encryption Scheme 129
Dominic Bucerzan, Vlad Dragoi, and Hervé Talé Kalachi

New Algorithm for Modeling S-box in MILP Based Differential and Division Trail Search 150
Yu Sasaki and Yosuke Todo

Secretly Embedding Trapdoors into Contract Signing Protocols 166
Diana Maimuţ and George Teşeleanu

On a Key Exchange Protocol 187
Mugurel Barcau, Vicenţiu Paşol, Cezar Pleşca, and Mihai Togan

Author Index 201