Lecture Notes in Computer Science 12596

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

Diana Maimut · Andrei-George Oprina ·
Damien Sauveron (Eds.)

Innovative Security Solutions for Information Technology and Communications

13th International Conference, SecITC 2020
Bucharest, Romania, November 19–20, 2020
Revised Selected Papers

Springer

Editors
Diana Maimut
Advanced Technologies Institute
Bucharest, Romania

Damien Sauveron
Faculté des Sciences et Techniques
University of Limoges
Limoges, France

Andrei-George Oprina
Advanced Technologies Institute
Bucharest, Romania

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-69254-4 ISBN 978-3-030-69255-1 (eBook)
https://doi.org/10.1007/978-3-030-69255-1

LNCS Sublibrary: SL4 – Security and Cryptology

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 during the 13th International Conference on Information Technology and Communications Security (SECITC 2020) held on November 19–20, 2020 online via ZOOM.

There were 41 submissions. Each submission was reviewed by at least 2, and on average 3 program committee members. The committee decided to accept 17 papers. The program also included 3 invited talks.

The SECITC conference started 13 years ago, when, in a small room at the Bucharest University of Economic Studies, was held the first edition of the event. At that time, the auditorium held approximately 15 students and professors.

Since then, the conference has grown significantly: the quality of the TPC and of the submitted papers has been improved from year to year, and, of course, we had valuable keynote speakers. Our conference is now indexed in several databases and probably a notable thing to mention is that SECITC is listed within the IACR cryptologic events calendar. Also, Springer agreed to publish the post proceedings (since 2015). The conference covers topics from cryptographic algorithms to digital forensics and cyber security and if this conference were to be initiated today, probably a better name for it would be "CyberSecurity Conference", but for now SECITC is already a brand and is not yet the time for rebranding.

The conference was organized by the master programs for information security within the Military Technical Academy and the Bucharest University of Economic Studies, as well as the Institute for Advanced Technologies (two of this year's co-chairs are representatives of the Institute). At the same time, partners of the conference included the master program Coding Theory and Information Storage within the Faculty of Applied Sciences, Politehnica University of Bucharest and the Center for Research and Training in Innovative Techniques of Applied Mathematics in Engineering from the same university.

A special word of gratitude to the invited keynote speakers, Constantin Catalin Dragan, Rémi Géraud-Stewart and Gerhard Hancke, who have certainly improved the quality of our conference SECITC 2020.

Last but not least, we would like to thank all the TPC members for reviewing the papers, the organizers and the technical committee for their efforts, and the sponsors for their support.

November 2020

Diana Maimut
Andrei-George Oprina
Damien Sauveron

Organization

Program Committee

Raja Naeem Akram	ISG Smart Card and IoT Security Centre, Royal Holloway, University of London, UK
Ludovic Apvrille	Télécom Paris, France
Claudio Ardagna	Università degli Studi di Milano - Dipartimento di Informatica, Italy
Lasse Berntzen	University of South-Eastern Norway, Norway
Ion Bica	Military Technical Academy, Romania
Catalin Boja	Bucharest University of Economic Studies, Romania
Guillaume Bouffard	National Cybersecurity Agency of France (ANSSI), France
Samia Bouzefrane	CEDRIC Lab, Conservatoire National des Arts et Métiers, France
Paolo D'Arco	University of Salerno, Italy
Roberto De Prisco	Dip. Informatica ed Appl., Università di Salerno, Italy
Eric Diehl	Sony Pictures Entertainment, USA
Pooya Farshim	University of York, France
Dieter Gollmann	Hamburg University of Technology, Germany
Johann Groszschaedl	University of Luxembourg, Luxembourg
Rémi Géraud-Stewart	École normale supérieure, France
Gerhard Hancke	City University of Hong Kong, China
Julio Hernandez Castro	University of Kent, UK
Shoichi Hirose	University of Fukui, Japan
Nesrine Kaaniche	The University of Sheffield, UK
Mehmet Sabir Kiraz	De Montfort University, UK
Chhagan Lal	University of Padova, Norway
Jean-François Lalande	CentraleSupélec, France
Maryline Laurent	Institut Mines-Télécom, France
Giovanni Livraga	University of Milan, Italy
Diana Maimut	Advanced Technologies Institute, École normale supérieure, University of Bucharest, Bucharest, Romania
Sjouke Mauw	University of Luxembourg, Luxembourg
Kazuhiko Minematsu	NEC Corporation, Japan
Stig Mjølsnes	Norwegian University of Science and Technology, Norway
David Naccache	ENS, France
Vincent Nicomette	University of Toulouse, France
Svetla Nikova	KU Leuven, Dept. ESAT/COSIC and iMinds, Belgium

Ruxandra F. Olimid	Norwegian University of Science and Technology and University of Bucharest, Norway
Victor Valeriu Patriciu	Military Technical Academy, Romania
Cezar Pleşca	Military Technical Academy, Romania
Andrei-George Oprina	Advanced Technologies Institute, Bucharest, Romania
Marius Popa	Bucharest University of Economic Studies, Faculty of Cybernetics, Statistics and Economic Informatics, Romania
Joachim Posegga	Univ. of Passau, Germany
Reza Reyhanitabar	TE Connectivity Germany GmbH, Germany
Peter Rønne	SnT, University of Luxembourg, Luxembourg
Damien Sauveron	University of Limoges, Limoges, France
Emil Simion	University Politehnica of Bucharest, Romania
Daniel Smith-Tone	NIST, USA
Agusti Solanas	Rovira i Virgili University, Spain
Riccardo Spolaor	University of Oxford, UK
Pantelimon Stanica	Naval Postgraduate School, USA
Rainer Steinwandt	Florida Atlantic University, USA
Ferucio Laurentiu Tiplea	Alexandru Ioan Cuza University, Romania
Mihai Togan	Military Technical Academy, Romania
Cristian Toma	Bucharest University of Economic Studies, Romania
Denis Trček	University of Ljubljana, Slovenia
Valérie Viet Triem Tong	CentraleSupélec, France
Qianhong Wu	Beihang University, China
Sule Yildirim-Yayilgan	Norwegian University of Science and Technology, Norway
Alin Zamfiroiu	Bucharest University of Economic Studies, Romania
Stefano Zanero	Politecnico di Milano, Italy
Lei Zhang	East China Normal University, China

Additional Reviewers

Atashpendar, Arash
Berro, Sahar
Claudepierre, Ludovic
Deo, Amit
Dhooghe, Siemen
Diehl, Eric
Fang, Qihao
Han, Shangbin
Hristea, Cristian
Klement, Felix
Madhusudan, Akash
Mohammadi, Farnaz
Nugier, Cyrius
Panait, Andreea-Elena
Perez Kempner, Octavio
Sedaghat, Mahdi
Shen, Kunyu
Soroush, Najmeh
Tronel, Frédéric
van Wier, Jeroen
Velciu, Alexandru
Zhong, Liangyu

Contents

Elementary Attestation of Cryptographically Useful Composite Moduli 1
Rémi Géraud-Stewart and David Naccache

Off-the-Shelf Security Testing Platform for Contactless Systems 13
Yuanzhen Liu, Gerhard Petrus Hancke, and Umair Mujtaba Qureshi

A New Generalisation of the Goldwasser-Micali Cryptosystem Based on the Gap 2^k-Residuosity Assumption 24
Diana Maimuţ and George Teşeleanu

New Insights on Differential and Linear Bounds Using Mixed Integer Linear Programming 41
Anubhab Baksi

Secure Card-Based Cryptographic Protocols Using Private Operations Against Malicious Players 55
Yoshifumi Manabe and Hibiki Ono

Decentralized Multi-authority Anonymous Credential System with Bundled Languages on Identifiers 71
Hiroaki Anada

A Scalable Simulation of the BB84 Protocol Involving Eavesdropping 91
Mihai-Zicu Mina and Emil Simion

Approach to Cryptography from Differential Geometry with Example 110
Tetsuya Nagano and Hiroaki Anada

On Using zk-SNARKs and zk-STARKs in Blockchain-Based Identity Management. 130
Andreea-Elena Panait and Ruxandra F. Olimid

Manager Asks: Which Vulnerability Must be Eliminated First?. 146
David Pecl, Yehor Safonov, Zdenek Martinasek, Matej Kacic, Lubomir Almer, and Lukas Malina

An IND-CCA2 Attack Against the 1st- and 2nd-Round Versions of NTS-KEM 165
Tung Chou

Behaviour-Based Biometrics for Continuous User Authentication to Industrial Collaborative Robots 185
Shurook S. Almohamade, John A. Clark, and James Law

Secure Speaker Recognition System Using Homomorphic Encryption 198
Mihai-Cristian Chindriş, Mihai Togan, and Ştefan-Ciprian Arseni

Reliable RFID Offline Privacy 212
Cristian Hristea

Virtualization and Automation for Cybersecurity Training and Experimentation 227
Ion Bica, Roxana Larisa Unc, and Ştefan Ţurcanu

Long-Term Secure Deniable Group Key Establishment 242
Kashi Neupane

Card-Based Covert Lottery 257
Yuto Shinoda, Daiki Miyahara, Kazumasa Shinagawa, Takaaki Mizuki, and Hideaki Sone

Hardware-Accelerated Cryptography for Software-Defined Networks with P4 271
Lukas Malina, David Smekal, Sara Ricci, Jan Hajny, Peter Cíbik, and Jakub Hrabovsky

Security Analysis Using Subjective Attack Trees. 288
Nasser Al-Hadhrami, Matthew Collinson, and Nir Oren

Author Index 303