

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

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, 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

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

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

Ion Bica · Reza Reyhanitabar (Eds.)

Innovative Security Solutions for Information Technology and Communications

9th International Conference, SECITC 2016
Bucharest, Romania, June 9–10, 2016
Revised Selected Papers

Editors

Ion Bica
Military Technical Academy
Bucharest
Romania

Reza Reyhanitabar
NEC Laboratories Europe
Heidelberg
Germany

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-319-47237-9

ISBN 978-3-319-47238-6 (eBook)

DOI 10.1007/978-3-319-47238-6

Library of Congress Control Number: 2016953301

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 2016

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, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

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 2016: The 9th International Conference on Security for Information Technology and Communications (www.secitc.eu), held during June 9–10, 2016, in Bucharest.

SECITC 2016 received 35 submissions from 14 different countries. Each submission was reviewed by at least three Program Committee members. Moreover, 13 external reviewers gave comments on their areas of expertise. The committee decided to accept 16 papers, and the program also featured four invited talks.

For nine 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 the conference'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.

Many people contributed to the success of SECITC 2016. First, we would like to thank the authors for submitting their work to SECITC 2016. We deeply thank the Program Committee members as well as the external reviewers for their volunteer work of reading and discussing the submissions. We would like to thank our distinguished invited speakers for accepting our invitation and for their papers. We thank the Organizing Committee and Technical Support Team for their dedication in organizing and running the conference. We would like to thank the members of the SECITC International Advisory Board. Finally, we would like to express our thanks to Springer for continuing to support the SECITC conference.

The conference was organized by the Military Technical Academy, Bucharest University of Economic Studies and Advanced Technologies Institute, Romania.

August 2016

Ion Bica
Reza Reyhanitabar

Organization

Program Committee

Elena Andreeva	KU Leuven, Belgium
Ludovic Apvrille	Telecom ParisTech, France
Gildas Avoine	INSA Rennes, France
Ion Bica (Chair)	Military Technical Academy, Romania
Catalin Boja	Bucharest University of Economic Studies, Romania
Christophe Clavier	Université de Limoges, France
Paolo D'Arco	University of Salerno, Italy
Roberto De Prisco	University of Salerno, Italy
Eric Freyssinet	Ministry of Interior/Cyberthreats Delegation, France
Helena Handschuh	Rambus – Cryptography Research, USA
Shoichi Hirose	University of Fukui, Japan
Xinyi Huang	Fujian Normal University, China
Mirosław Kutylowski	Wrocław University of Technology, Poland
Bart Mennink	KU Leuven, Belgium
Kazuhiko Minematsu	NEC Corporation, Japan
Yi Mu	University of Wollongong, Australia
David Naccache	Ecole Normale Supérieure, France
Udaya Parampalli	The University of Melbourne, Australia
Victor Patriciu	Military Technical Academy, Romania
Josef Pieprzyk	Queensland University of Technology, Australia
Reza Reyhanitabar (Chair)	NEC Laboratories Europe, Germany
Pierangela Samarati	Università degli Studi di Milano, Italy
Damien Sauveron	University of Limoges, France
Emil Simion	Advanced Technologies Institute and University Politehnica of Bucharest, Romania
Agusti Solanas	Smart Health Research Group, Rovira i Virgili University, Spain
Rainer Steinwandt	Florida Atlantic University, USA
Cristian Toma	Bucharest University of Economic Studies, Romania
Denis Trcek	University of Ljubljana, Slovenia
Michael Tunstall	Rambus – Cryptography Research, USA
Qianhong Wu	Beihang University, China
Kan Yasuda	NTT Corporation, Japan
Lei Zhang	East China Normal University, China

Additional Reviewers

Batista, Edgar
Best, Scott
Blazy, Olivier
Casino, Fran
Catuogno, Luigi

De Mulder, Elke
Hamburg, Mike
Li, Jiangtao
Lugou, Florian
Marson, Mark

Wu, Xin-Wen
Zhang, Yuexin
Zheng, James

Contents

Invited Talks

Circular Security Reconsidered	3
<i>F. Betül Durak and Serge Vaudenay</i>	
Visual Cryptography: Models, Issues, Applications and New Directions. . . .	20
<i>Paolo D'Arco and Roberto De Prisco</i>	
Paper Tigers: An Endless Fight.	40
<i>Mozhdeh Farhadi and Jean-Louis Lanet</i>	
Security of Identity-Based Encryption Schemes from Quadratic Residues. . . .	63
<i>Ferucio Laurențiu Țiplea, Sorin Iftene, George Teșleanu, and Anca-Maria Nica</i>	

Cryptographic Algorithms and Protocols

Long-Term Secure One-Round Group Key Establishment from Multilinear Mappings.	81
<i>Kashi Neupane</i>	
RSA Weak Public Keys Available on the Internet.	92
<i>Mihai Barbulescu, Adrian Stratulat, Vlad Traista-Popescu, and Emil Simion</i>	
A Tweak for a PRF Mode of a Compression Function and Its Applications . . .	103
<i>Shoichi Hirose and Atsushi Yabumoto</i>	
May-Ozerov Algorithm for Nearest-Neighbor Problem over \mathbb{F}_q and Its Application to Information Set Decoding.	115
<i>Shoichi Hirose</i>	
A Cryptographic Approach for Implementing Semantic Web's Trust Layer. . . .	127
<i>Bogdan Iancu and Cristian Sandu</i>	
Schnorr-Like Identification Scheme Resistant to Malicious Subliminal Setting of Ephemeral Secret	137
<i>Łukasz Krzywiecki</i>	
Homomorphic Encryption Based on Group Algebras and Goldwasser-Micali Scheme.	149
<i>Cezar Pleșca, Mihai Togan, and Cristian Lupașcu</i>	

Increasing the Robustness of the Montgomery <i>kP</i> -Algorithm Against SCA by Modifying Its Initialization	167
<i>Estuardo Alpirez Bock, Zoya Dyka, and Peter Langendoerfer</i>	
Security Technologies for ITC	
When Pythons Bite	181
<i>Alecsandru Pătraşcu and Ştefan Popa</i>	
Secure Virtual Machine for Real Time Forensic Tools on Commodity Workstations	193
<i>Dan Luţaş, Adrian Coleşa, Sándor Lukács, and Andrei Luţaş</i>	
Pushing the Optimization Limits of Ring Oscillator-Based True Random Number Generators.	209
<i>Andrei Marghescu and Paul Svasta</i>	
TOR - Didactic Pluggable Transport	225
<i>Ioana-Cristina Panait, Cristian Pop, Alexandru Sirbu, Adelina Vidovici, and Emil Simion</i>	
Preparation of SCA Attacks: Successfully Decapsulating BGA Packages	240
<i>Christian Wittke, Zoya Dyka, Oliver Skibitzki, and Peter Langendoerfer</i>	
Comparative Analysis of Security Operations Centre Architectures; Proposals and Architectural Considerations for Frameworks and Operating Models	248
<i>Sabina Georgiana Radu</i>	
Secure Transaction Authentication Protocol	261
<i>Pardis Pourghomi, Muhammad Qasim Saeed, and Pierre E. Abi-Char</i>	
Proposed Scheme for Data Confidentiality and Access Control in Cloud Computing	274
<i>Ana-Maria Ghimeş and Victor Valeriu Patriciu</i>	
Author Index	287