

*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, 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>

Jean-Louis Lanet · Cristian Toma (Eds.)

# Innovative Security Solutions for Information Technology and Communications

11th International Conference, SecITC 2018  
Bucharest, Romania, November 8–9, 2018  
Revised Selected Papers

*Editors*

Jean-Louis Lanet   
Inria-RBA  
Rennes, France

Cristian Toma   
Bucharest University of Economic Studies  
Bucharest, Romania

ISSN 0302-9743 ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-12941-5 ISBN 978-3-030-12942-2 (eBook)  
<https://doi.org/10.1007/978-3-030-12942-2>

Library of Congress Control Number: 2019930852

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 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, express 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

# Foreword

It is a privilege for me to write the foreword to the proceedings of this 11th anniversary of the conference. Indeed, SecITC 2018 was the 11th edition of the International Conference on Information Technology and Communication Security, which is held in Bucharest, Romania, every year. Throughout the years, SecITC has become a truly competitive publication venue with an acceptance rate between 33 and 50%, with a Program Committee of 50 experts from 20 countries, and with a long series of distinguished invited speakers. Starting four years ago, the conference proceedings are published in Springer's *Lecture Notes in Computer Science* series, and articles published in SecITC are indexed in most science databases.

The conference is unique in that it serves as an exchange forum between established researchers and students entering the field as well as industry players. I would like to particularly thank the Program Committee (PC) chairs, Jean-Louis Lanet and Cristian Toma, for an outstanding paper selection process conducted electronically. In response to the call for papers, the PC received 70 submissions of which 35 were chosen. To those the PC added seven invited keynote lectures by Paolo D'Arco, Jean-François Lalande and myself, and Denis Jean-Michel Baheux.

I also warmly thank the conference's Organizing Committee and Technical Support Team—Catalin Boja, Mihai Doinea, Cristian Ciurea, Bogdan Iancu, Diana Maimut, Luciana Morogan, Andrei-George Oprina, Marius Popa, Mihai Pura, Mihai Togan, George Teseleanu, 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 scientific meeting for the IT security research community.

December 2018

David Naccache

# Preface

This volume contains the papers presented at SecITC 2018, the 11th International Conference on Security for Information Technology and Communications ([www.secitc.eu](http://www.secitc.eu)), held during November 8–9, 2018, in Bucharest. There were 70 submissions (three withdrawn by the authors) and each submitted paper was reviewed by at least two, and on average 2.7, Program Committee members. The committee decided to accept 35 papers and also three invited papers from the keynote talks. For 11 years, SecITC has been bringing together cybersecurity researchers, cryptographers, industry representatives, and graduate students. The conference focuses on research of any aspect of cyber security and cryptography. The papers present advances in the theory, design, implementation, analysis, verification, or evaluation of secure systems and algorithms.

The conference topics comprise all aspects of information security, including but not limited to the following areas: access control; cryptography, biometrics, and watermarking; application security; attacks and defenses; blockchain security and security aspects of alternative currencies; censorship and censorship-resistance; cloud and Web security; distributed systems security; embedded systems security; digital forensics; hardware security; information flow analysis; Internet of Things (IoT) security; intrusion detection and prevention system; language-based security; machine learning (artificial intelligence) used in security; malware and ransomware; mobile security; network security; new exploits; policy enforcements; privacy and anonymity; protocol security; reverse-engineering and code obfuscation; security architectures; side channel attacks; surveillance and anti-surveillance; system security; trust management.

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 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 the Bucharest University of Economic Studies, the Military Technical Academy, and the Advanced Technologies Institute.

December 2018

Jean-Louis Lanet  
Cristian Toma

# Organization

## Program Committee

Elena Andreeva	Katholieke Universiteit Leuven, Belgium
Ludovic Apvrille	Telecom ParisTech, France
Lasse Berntzen	Buskerud and Vestfold University College, Norway
Ion Bica	Military Technical Academy, Romania
Catalin Boja	Bucharest Academy of Economic Studies, Romania
Guillaume Bouffard	ANSSI, France
Xiaofeng Chen	Xidian University, China
Cristian Ciurea	Academy 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 Diehl	Sony Pictures, USA
Mihai Doinea	Bucharest University of Economic Studies, Romania
Eric Freyssinet	LORIA, France
Helena Handschuh	Rambus, USA
Shoichi Hirose	University of Fukui, Japan
Xinyi Huang	Fujian Normal University, China
Mirosław Kutylowski	Wrocław University of Technology, Poland
Jean-Louis Lanet	Inria-RBA, France
Giovanni Livraga	University of Milan, Italy
Florian Mendel	TU Graz, Austria
Kazuhiko Minematsu	NEC Corporation, Japan
David Naccache	ENS, France
Vincent Nicomette	LAAS/CNRS, France
Calinel Pasteanu	Oracle, Germany
Victor Patriciu	Military Technical Academy, Romania
Cezar Plesca	Military Technical Academy, Romania
Marius Popa	Bucharest University of Economic Studies, Romania
Reza Reyhanitabar	Katholieke Universiteit Leuven, Belgium
P. Y. A. Ryan	University of Luxembourg, Luxembourg
Emil Simion	University Politehnica of Bucharest, Romania
Agusti Solanas	Rovira i Virgili University, Spain
Rainer Steinwandt	Florida Atlantic University, USA
Ferucio Laurentiu Tiplea	Alexandru Ioan Cuza University of Iasi, Romania
Mihai Togan	Military Technical Academy, Romania
Cristian Toma	Bucharest University of Economic Studies, Romania
Tiberiu Vasilache	University Politehnica of Bucharest, Romania
Valérie Viet Triem Tong	CentraleSupélec, France

Guilin Wang	Huawei International Pte Ltd., Singapore
Qianhong Wu	Beihang University, China
Sule Yildirim-Yayilgan	Norwegian University of Science and Technology, Norway
Alin Zamfiroiu	Bucharest University of Economic Studies, Romania
Lei Zhang	East China Normal University, China

## **Additional Reviewers**

Batista, Edgar	Reynaud, Léo
Casino, Fran	Roenne, Peter
Catuogno, Luigi	Rozic, Vladimir
Genc, Ziya A.	Symeonidis, Iraklis
Kang, Burong	Teseleanu, George
Lin, Chao	Trouchkine, Thomas
Ma, Xu	Velciu, Alexandru
Maimut, Diana	Visoiu, Adrian
Meng, Xinyu	Wang, Jian
Moussaileb, Routa	Zhang, Xiaoyu
Pasteanu, Calinel	Zhao, Hong
Pura, Mihai Lica	Zurini, Madalina



# Contents

Ultralightweight Cryptography: Some Thoughts on Ten Years of Efforts . . . .	1
<i>Paolo D'Arco</i>	
Android Malware Analysis: From Technical Difficulties to Scientific Challenges . . . . .	17
<i>Jean-François Lalande</i>	
Post-quantum Cryptography and a (Qu)Bit More. . . . .	22
<i>Diana Maimuț and Emil Simion</i>	
Normalization of Java Source Codes . . . . .	29
<i>Léopold Ouairy, Hélène Le-Bouder, and Jean-Louis Lanet</i>	
HiddenApp - Securing Linux Applications Using ARM TrustZone . . . . .	41
<i>Veronica Velciu, Florin Stancu, and Mihai Chiroiu</i>	
Security Knowledge Management in Open Source Software Communities . . .	53
<i>Shao-Fang Wen, Mazaher Kianpour, and Basel Katt</i>	
Formal Security Analysis of Cloud-Connected Industrial Control Systems . . .	71
<i>Tomas Kulik, Peter W. V. Tran-Jørgensen, and Jalil Boudjadar</i>	
A Hybrid Searchable Encryption Scheme for Cloud Computing . . . . .	85
<i>Stefania Loredana Nita and Marius Iulian Mihailescu</i>	
Securing Cloud Storage by Transparent Biometric Cryptography. . . . .	97
<i>Leith Abed, Nathan Clarke, Bogdan Ghita, and Abdulrahman Alruban</i>	
Examining the Use of Neural Networks for Intrusion Detection in Controller Area Networks. . . . .	109
<i>Camil Jichici, Bogdan Groza, and Pal-Stefan Murvay</i>	
An Evaluation of OCR Systems Against Adversarial Machine Learning. . . .	126
<i>Dan Sporici, Mihai Chiroiu, and Dan Ciocîrlan</i>	
Intrusion Detection and Classification with Autoencoded Deep Neural Network . . . . .	142
<i>Shahadate Rezvy, Miltos Petridis, Aboubaker Lasebae, and Tahmina Zebin</i>	
Detecting Malicious Windows Commands Using Natural Language Processing Techniques. . . . .	157
<i>Muhammd Mudassar Yamin and Basel Katt</i>	

Evolutionary Computation Algorithms for Detecting Known and Unknown Attacks . . . . .	170
<i>Hasanen Alyasiri, John A. Clark, and Daniel Kudenko</i>	
Assuring Privacy in Surfing the Internet. . . . .	185
<i>Stefan Bodoarca and Mihai-Lica Pura</i>	
Roaming Interface Signaling Security for LTE Networks . . . . .	204
<i>Isha Singh, Silke Holtmanns, and Raimo Kantola</i>	
Limited Proxying for Content Filtering Based on X.509 Proxy Certificate Profile . . . . .	218
<i>Islam Faisal and Sherif El-Kassas</i>	
Anomaly-Based Network Intrusion Detection Using Wavelets and Adversarial Autoencoders. . . . .	234
<i>Samir Puuska, Tero Kokkonen, Janne Alatalo, and Eppu Heilimo</i>	
Analysis and Evaluation of Dynamic Feature-Based Malware Detection Methods . . . . .	247
<i>Arzu Gorgulu Kakisim, Mert Nar, Necmettin Carkaci, and Ibrahim Sogukpinar</i>	
Trends in Design of Ransomware Viruses . . . . .	259
<i>Vlad Constantin Craciun, Andrei Mogage, and Emil Simion</i>	
Efficient Implementation of the SHA-512 Hash Function for 8-Bit AVR Microcontrollers . . . . .	273
<i>Hao Cheng, Daniel Dinu, and Johann Großschädl</i>	
Secure IoT Supply Chain Management Solution Using Blockchain and Smart Contracts Technology. . . . .	288
<i>Cristian Toma, Bogdan Talpiga, Catalin Boja, Marius Popa, Bogdan Iancu, and Madalina Zurini</i>	
ADvoCATE: A Consent Management Platform for Personal Data Processing in the IoT Using Blockchain Technology . . . . .	300
<i>Konstantinos Rantos, George Drosatos, Konstantinos Demertzis, Christos Ilioudis, Alexandros Papanikolaou, and Antonios Kritsas</i>	
Development of the Unified Security Requirements of PUFs During the Standardization Process . . . . .	314
<i>Nicolas Bruneau, Jean-Luc Danger, Adrien Facon, Sylvain Guilley, Soshi Hamaguchi, Yohei Hori, Yousung Kang, and Alexander Schaub</i>	
A PUF-Based Destructive Private Mutual Authentication RFID Protocol . . . .	331
<i>Cristian Hristea and Ferucio Laurențiu Țiplea</i>	

Weakened Random Oracle Models with Target Prefix . . . . .	344
<i>Masayuki Tezuka, Yusuke Yoshida, and Keisuke Tanaka</i>	
An Improved Algorithm for Iterative Matrix-Vector Multiplications over Finite Fields . . . . .	358
<i>Ceyda Mangır, Murat Cenk, and Murat Manguoğlu</i>	
On the Security of Jhanwar-Barua Identity-Based Encryption Scheme . . . . .	368
<i>Adrian G. Schipor</i>	
Vulnerabilities of the McEliece Variants Based on Polar Codes . . . . .	376
<i>Vlad Drăgoi, Valeriu Beiu, and Dominic Bucerzan</i>	
Binary Data Analysis for Source Code Leakage Assessment. . . . .	391
<i>Adrien Facon, Sylvain Guilley, Matthieu Lec'hvien, Damien Marion, and Thomas Perianin</i>	
Zero in and TimeFuzz: Detection and Mitigation of Cache Side-Channel Attacks . . . . .	410
<i>ZiHao Wang, ShuangHe Peng, XinYue Guo, and WenBin Jiang</i>	
A Comparison of the Homomorphic Encryption Libraries HELib, SEAL and FV-NFLib. . . . .	425
<i>Carlos Aguilar Melchor, Marc-Olivier Kilijian, Cédric Lefebvre, and Thomas Ricosset</i>	
A New DNA-Combining Chaos Scheme for Fast and Secure Image Encryption . . . . .	443
<i>Augustin Ousmanou Ahgue, Jean De Dieu Nkapkop, Joseph Yves Effa, Samuel Franz, Raul Malutan, and Monica Borda</i>	
Implementing Searchable Encryption Schemes over Multilinear Maps . . . . .	458
<i>Victor-Mihai Talif</i>	
A Unified Security Perspective on Legally Fair Contract Signing Protocols . . . . .	477
<i>Diana Maimuț and George Teșeleanu</i>	
Relating Different Polynomial-LWE Problems . . . . .	492
<i>Madalina Bolboceanu</i>	
Monoidal Encryption over $(\mathbb{F}_2, \cdot)$ . . . . .	504
<i>Mugurel Barcau, Vicențiu Pașol, and Cezar Pleșca</i>	
Geometric Pairwise Key-Sharing Scheme. . . . .	518
<i>Koki Nishigami and Keiichi Iwamura</i>	
<b>Author Index</b> . . . . .	529