

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>

Phong Q. Nguyen · Jianying Zhou (Eds.)

Information Security

20th International Conference, ISC 2017

Ho Chi Minh City, Vietnam, November 22–24, 2017

Proceedings

Editors
Phong Q. Nguyen
Inria
Paris
France

Jianying Zhou
Singapore University of Technology and
Design
Singapore
Singapore

and

Inria
Tokyo
Japan

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-69658-4 ISBN 978-3-319-69659-1 (eBook)
<https://doi.org/10.1007/978-3-319-69659-1>

Library of Congress Control Number: 2017956937

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 2017

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.

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 ISC 2017: the 20th Information Security Conference held during November 22–24, 2017, in Ho Chi Minh City, Vietnam.

The Information Security Conference is an annual international conference covering research in theory and applications of information security. ISC aims to attract high-quality papers in all technical aspects of information security. ISC 2017 was hosted by the Vietnamese German University (VGU).

There were 97 submissions to ISC 2017. Each submission was reviewed by three Program Committee members on average, and the reviewing process was double-blind. After careful reviews and intensive discussions, 25 papers were selected for presentation at the conference. In addition to the contributed talks, there were two invited talks given by Thai Duong (Google, USA) and Adi Shamir (Weizmann Institute, Israel), whom we heartily thank for accepting our invitation despite a very busy schedule. Adi Shamir talked about “Towards Quantitative Analysis of Cyber Security”, and Thai Duong talked about “Security at Scale: Shipping Secure Software at Google.”

We would like to thank the Program Committee members and the external reviewers for all the hard work they put in evaluating the papers. We thank Easy Chair for providing a good platform on paper submission and review. We also thank Springer for supporting the conference and publishing the conference proceedings in the LNCS series. We are very grateful to all the people whose work ensured a smooth organization process: the ISC Steering Committee, and Masahiro Mambo in particular, for their advice; the local organizing team led by General Chairs Martin Kappes and Dinh-Thuc Nguyen, and Local Chairs Thuc-Vien Ha and Van-Song Pham. Last but not least, our thanks go to all the authors who submitted papers and all the attendees.

September 2017

Phong Q. Nguyen
Jianying Zhou

ISC 2017

20th International Conference on Information Security Ho Chi Minh City, Vietnam November 22–24, 2017

Program Chairs

Phong Q. Nguyen Inria, France and CNRS/JFLI/University of Tokyo, Japan
Jianying Zhou Singapore University of Technology and Design,
Singapore

General Chairs

Martin Kappes Vietnamese German University, Vietnam
and Frankfurt am Main University, Germany
Dinh-Thuc Nguyen University of Science, VNU-HCM, Vietnam

Steering Committee

Ed Dawson Queensland University of Technology, Australia
Javier Lopez University of Malaga, Spain
Masahiro Mambo Kanazawa University, Japan
Dinh-Thuc Nguyen University of Science, VNU-HCM, Vietnam
Eiji Okamoto University of Tsukuba, Japan
Susanne Wetzel Stevens Institute of Technology, USA
Rui Zhang University of Delaware, USA
Yuliang Zheng University of Alabama at Birmingham, USA

Program Committee

Shweta Agrawal Indian Institute of Technology Madras, India
Gail-Joon Ahn Arizona State University, USA
Yoshinori Aono National Institute of Information and Communications
Technology, Japan
Jean-Philippe Aumasson Kudelski Security, Switzerland
Gildas Avoine INSA Rennes, France
Sherman S.M. Chow Chinese University of Hong Kong, SAR China
Carlos Cid Royal Holloway, University of London, UK
Yuval Elovici Ben-Gurion University, Israel
Debin Gao Singapore Management University, Singapore
Juan A. Garay Texas A&M University, USA
Stefanos Gritzalis University of the Aegean, Greece

Tibor Jager	Paderborn University, Germany
Sokratis Katsikas	Norwegian University of Science and Technology, Norway
Stefan Katzenbeisser	TU Darmstadt, Germany
Noboru Kunihiro	University of Tokyo, Japan
Qi Li	Tsinghua University, China
Zhiqiang Lin	University of Texas at Dallas, USA
Javier Lopez	University of Malaga, Spain
Mark Manulis	University of Surrey, UK
Weizhi Meng	Technical University of Denmark, Denmark
Chris Mitchell	Royal Holloway, University of London, UK
David Naccache	Ecole Normale Supérieure, France
Khoa Nguyen	Nanyang Technological University, Singapore
Martín Ochoa	Singapore University of Technology and Design, Singapore
Tatsuaki Okamoto	NTT, Japan
Yanbin Pan	Chinese Academy of Sciences, China
Duong-Hieu Phan	University of Limoges, France
Indrakshi Ray	Colorado State University, USA
Matt Robshaw	Impinj, USA
Pierangela Samarati	Università degli Studi di Milano, Italy
Gang Tan	Penn State University, USA
Lei Wang	Shanghai Jiao Tong University, China

Local Organizing Chairs

Thuc-Vien Ha	Vietnamese German University, Vietnam
Van-Song Pham	Vietnamese German University, Vietnam

Local Organizing Committee

Quoc-Binh Nguyen	Vietnamese German University, Vietnam
Thanh-Duy Nguyen	Vietnamese German University, Vietnam
Quoc-Hung Nguyen	Vietnamese German University, Vietnam
Thuy-Trang Nguyen	Vietnamese German University, Vietnam
Hai-Dinh Pham	Vietnamese German University, Vietnam
Thuan-Anh Tran	Vietnamese German University, Vietnam
Thu-Huong Tran	Vietnamese German University, Vietnam
Hong-Ngoc Tran	Vietnamese German University, Vietnam

Additional Reviewers

Albrecht, Martin	Janson, Christian	Rizomiliotis, Panagiotis
Alcaraz, Cristina	Jin, Xin	Rothstein, Eric
Alderman, James	Kakvi, Saqib A.	Scotti, Fabio
Anagnostopoulos, Marios	Kalloniatis, Christos	Shiehian, Sina
Bai, Shi	Karande, Vishal	Striecks, Christoph
Bauman, Erick	Katsumata, Shuichi	Su, Chunhua
Belyaev, Kirill	Kolokotronis, Nicholas	Sun, Bing
Bezawada, Bruhadeshwar	Konstantinou, Elisavet	Tai, Raymond K.H.
Bhattacharjee, Sanjay	Kundu, Ashish	Tan,
Bi, Jingguo	Kurek, Rafael	Benjamin Hong Meng
Bost, Raphael	Lacovazzi, Alfonso	Tang, Bo
Bourse, Florian	Lai, Russell W.F.	Tardif, Florent
Brotzman-Smith, Robert	Le Trieu, Phong	Toffalini, Flavio
Castellanos, John Henry	Lee, Hyung Tae	Trinh, Viet Cuong
Chakraborty, Suvradip	Li, Baiyu	V., Santhoshini
Chandra, Swarup	Li, Jianwei	Wang, Huibo
Chang, Jinyong	Li, Qinyi	Wang, Jiafan
Chen, Zhigang	Liu, Shen	Wang, Xiuhua
Chotard, Jeremy	Ma, Jack P.K.	Wang, Yuntao
Chuahry, Mujeeb	Maitra, Monosij	Wong, Harry W.H.
Datta, Pratish	Mukherjee, Subhojeet	Wudel, Wojciech
Davidson, Alex	Niehues, David	Xagawa, Keita
Du, Minxin	Nieto, Ana	Xu, Yanhong
Fernandez, Carmen	Nuñez, David	Zeng, Dongrui
Gellert, Kai	Papamartzivanos,	Zhang, Juanyang
Gong, Junqing	Dimitrios	Zhang, Kai
Gougeon, Thomas	Patsakis, Constantinos	Zhang, Tao
Guarnizo, Juan David	Pelosi, Gerardo	Zhao, Qingchuan
Haefner, Kyle	Quinonez Tirado, Raul	Zhao, Yongjun
Harilal, Athul	Ramanna, Somindu C.	Zuo, Chaoshun
Hou, Xiaolu	Rios, Ruben	

Contents

Symmetric Cryptography

Rate-One AE with Security Under RUP	3
<i>Shoichi Hirose, Yu Sasaki, and Kan Yasuda</i>	
An Improved SAT-Based Guess-and-Determine Attack on the Alternating Step Generator	21
<i>Oleg Zaikin and Stepan Kochemazov</i>	
Efficient Masking of ARX-Based Block Ciphers Using Carry-Save Addition on Boolean Shares	39
<i>Daniel Dinu, Johann Großschädl, and Yann Le Corre</i>	
Improved Automatic Search Tool for Related-Key Differential Characteristics on Byte-Oriented Block Ciphers	58
<i>Li Lin, Wenling Wu, and Yafei Zheng</i>	

Post-quantum Cryptography

Choosing Parameters for the Subfield Lattice Attack Against Overstretched NTRU	79
<i>Dung Hoang Duong, Masaya Yasuda, and Tsuyoshi Takagi</i>	
Zero-Knowledge Password Policy Check from Lattices	92
<i>Khoa Nguyen, Benjamin Hong Meng Tan, and Huaxiong Wang</i>	
Generic Forward-Secure Key Agreement Without Signatures	114
<i>Cyprien de Saint Guilhem, Nigel P. Smart, and Bogdan Warinschi</i>	

Public-Key Cryptography

A Constant-Size Signature Scheme with Tighter Reduction from CDH Assumption	137
<i>Kaisei Kajita, Kazuto Ogawa, and Eiichiro Fujisaki</i>	
Homomorphic-Policy Attribute-Based Key Encapsulation Mechanisms	155
<i>Jérémy Chotard, Duong Hieu Phan, and David Pointcheval</i>	
Watermarking Public-Key Cryptographic Functionalities and Implementations	173
<i>Foteini Baldimtsi, Aggelos Kiayias, and Katerina Samari</i>	

Authentication

Contactless Access Control Based on Distance Bounding 195
Handan Kilinç and Serge Vaudenay

Improving Gait Cryptosystem Security Using Gray Code Quantization
and Linear Discriminant Analysis 214
Lam Tran, Thang Hoang, Thuc Nguyen, and Deokjai Choi

Attacks

Low-Level Attacks in Bitcoin Wallets 233
Andriana Gkaniatsou, Myrto Arapinis, and Aggelos Kiayias

Improving Password Guessing Using Byte Pair Encoding 254
*Xingxing Wang, Dakui Wang, Xiaojun Chen, Rui Xu, Jinqiao Shi,
and Li Guo*

How to Make Information-Flow Analysis Based Defense Ineffective:
An ART Behavior-Mask Attack 269
Xueyi Yang, Limin Liu, Lingchen Zhang, Weiyu Jiang, and Shiran Pan

Privacy

Harvesting Smartphone Privacy Through Enhanced Juice Filming
Charging Attacks 291
Weizhi Meng, Fei Fei, Wenjuan Li, and Man Ho Au

A Differentially Private Encryption Scheme 309
*Carlo Brunetta, Christos Dimitrakakis, Bei Liang,
and Aikaterini Mitrokotsa*

Mobile Security

Droid Mood Swing (DMS): Automatic Security Modes Based on Contexts . . . 329
Md Shahrear Iqbal and Mohammad Zulkernine

T-MAC: Protecting Mandatory Access Control System Integrity from
Malicious Execution Environment on ARM-Based Mobile Devices 348
Diming Zhang, Liangqiang Chen, Fei Xue, Hao Wu, and Hao Huang

Enforcing ACL Access Control on Android Platform. 366
*Xiaohai Cai, Xiaozhuo Gu, Yuewu Wang, Quan Zhou,
and Zhenhuan Cao*

Software Security

Nightingale: Translating Embedded VM Code in x86 Binary Executables . . . 387
Xie Haijiang, Zhang Yuanyuan, Li Juanru, and Gu Dawu

Run-Time Verification for Observational Determinism Using Dynamic
 Program Slicing 405
Mohammad Ghorbani and Mehran S. Fallah

Automated Analysis of Accountability 417
Alessandro Bruni, Rosario Giustolisi, and Carsten Schuermann

Network and System Security

Visualization of Intrusion Detection Alarms Collected
 from Multiple Networks. 437
Boyeon Song, Sang-Soo Choi, Jangwon Choi, and Jungsuk Song

Curtain: Keep Your Hosts Away from USB Attacks 455
Jianming Fu, Jianwei Huang, and Lanxin Zhang

Author Index 473