Lecture Notes in Computer Science 10892

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

Bart Preneel · Frederik Vercauteren (Eds.)

Applied Cryptography and Network Security

16th International Conference, ACNS 2018
Leuven, Belgium, July 2–4, 2018
Proceedings

Springer

Editors

Bart Preneel
imec-COSIC
KU Leuven
Heverlee
Belgium

Frederik Vercauteren
imec-COSIC
KU Leuven
Heverlee
Belgium

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-93386-3 ISBN 978-3-319-93387-0 (eBook)
https://doi.org/10.1007/978-3-319-93387-0

Library of Congress Control Number: 2018944429

LNCS Sublibrary: SL4 – Security and Cryptology

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 the registered company Springer International Publishing AG
part of Springer Nature
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

ACNS 2018, the 16th International Conference on Applied Cryptography and Network Security, was held during July 2–4, 2018, at KU Leuven, Belgium. The local organization was in the capable hands of the COSIC team at KU Leuven and we are deeply indebted to them for their support and smooth collaboration.

We received 173 paper submissions, out of which 36 were accepted, resulting in an acceptance rate of 20%. These proceedings contain revised versions of all the papers. The invited keynotes were delivered by Gilles Barthe, who spoke on formal verification of side-channel resistance and Haya Shulman who shared with the audience her perspective on RPKI's Deployment and Security of BGP.

The Program Committee consisted of 52 members with diverse backgrounds and broad research interests. The review process was double-blind. Each paper received at least three reviews; for submissions by Program Committee members, this was increased to five. During the discussion phase, additional reviews were solicited when necessary. An intensive discussion was held to clarify issues and to converge toward decisions. The selection of the program was challenging; in the end some high-quality papers had to be rejected owing to lack of space. The committee decided to give the Best Student Paper Award to the paper "Non-interactive zaps of knowledge" by Georg Fuchsbauer and Michele Orrù.

We would like to sincerely thank the authors of all submissions for contributing high-quality submissions and giving us the opportunity to compile a strong and diverse program. We know that the Program Committee's decisions can be very disappointing, especially rejections of good papers that did not find a slot in the sparse number of accepted papers.

Special thanks go to the Program Committee members; we value their hard work and dedication to write careful and detailed reviews and to engage in interesting discussions. A few Program Committee members, whom we asked to serve as shepherds, spent additional time in order to help the authors improve their works. More than 160 external reviewers contributed to the review process; we would like to thank them for their efforts.

Finally, we thank everyone else — speakers and session chairs — for their contribution to the program of ACNS 2018. We would also like to thank the sponsors for their generous support.

We hope that the papers in this volume prove valuable for your research and professional activities and that ACNS will continue to play its unique role in bringing together researchers and practitioners in the area of cryptography and network security.

April 2018

Bart Preneel
Frederik Vercauteren

ACNS 2018

Applied Cryptography and Network Security 2018

KU Leuven, Belgium
July 2–4, 2018

General Chair

Bart Preneel	KU Leuven, Belgium

Program Chairs

Bart Preneel	KU Leuven, Belgium
Frederik Vercauteren	KU Leuven, Belgium

Program Committee

Michel Abdalla	ENS and CNRS, France
Masayuki Abe	NTT, Japan
Elli Androulaki	IBM Research, Switzerland
Alex Biryukov	University of Luxembourg, Luxembourg
Marina Blanton	University at Buffalo, The State University of New York, USA
Jan Camenisch	IBM Research, Switzerland
Liqun Chen	University of Surrey, UK
Chen-Mou Cheng	National Taiwan University, Taiwan
Naccache David	ENS, France
Dieter Gollmann	Hamburg University of Technology, Germany
Peter Gutmann	University of Auckland, New Zealand
Shai Halevi	IBM Research, USA
Goichiro Hanaoka	AIST, Japan
Amir Herzberg	University of Connecticut, USA
Tibor Jager	Paderborn University, Germany
Marc Joye	NXP Semiconductors, USA
Aniket Kate	Purdue University, USA
Stefan Katzenbeisser	TU Darmstadt, Germany
Florian Kerschbaum	University of Waterloo, Canada
Aggelos Kiayias	University of Edinburgh, UK
Kwangjo Kim	KAIST, Korea
Kaoru Kurosawa	Ibaraki University, Japan
Ralf Kusters	University of Stuttgart, Germany

Xuejia Lai	Shanghai Jiaotong University, China
Benoit Libert	CNRS and ENS de Lyon, France
Dongdai Lin	SKLOIS, Chinese Academy of Sciences, China
Michael Locasto	SRI International, USA
Javier Lopez	University of Malaga, Spain
Mark Manulis	University of Surrey, UK
Atefeh Mashatan	Ryerson University, Canada
Bart Mennink	Radboud University, The Netherlands
Atsuko Miyaji	JAIST, Japan
Refik Molva	Eurecom, France
Michael Naehrig	Microsoft Research, USA
Miyako Ohkubo	NICT, Japan
Panos Papadimitratos	KTH Royal Institute of Technology, Sweden
Thomas Peyrin	Nanyang Technological University, Singapore
Josef Pieprzyk	QUT, Australia
Benny Pinkas	Bar-Ilan University, Israel
Bart Preneel	KU Leuven, Belgium
Christian Rechberger	TU Graz, Austria
Matt Robshaw	Impinj, USA
Ahmad Sadeghi	TU Darmstadt, Germany
Yu Sasaki	NTT Secure Platform Laboratories, Japan
Willy Susilo	University of Wollongong, Australia
Mehdi Tibouchi	NTT Secure Platform Laboratories, Japan
Damien Vergnaud	ENS, France
Ivan Visconti	University of Salerno, Italy
Frederik Vercauteren	KU Leuven, Belgium
Avishai Wool	Tel Aviv University, Israel
Moti Yung	Colombia University, USA
Jianying Zhou	Singapore University of Technology and Design, Singapore

Additional Reviewers

Aydin Abadi
Mai Ben Adar-Bessos
Megha Agrawal
Hyeongcheol Ahn
Muhamad Erza Aminanto
Hassan Asghar
Nuttapong Attrapadung
Joonsang Baek
Anubhab Baksi
Josep Balasch
Harry Barlett
Pascal Bemmann
Fabrice Benhamouda
Cecilia Boschini
Florian Bourse
Ferdinand Brasser
Niklas Büscher
Seyit Camtepe
Luigi Catuogno
Avik Chakraborti
Jagmohan Chauhan
Hao Chen
Jiageng Chen
Rongmao Chen
Yu Chen
Céline Chevalier
Rakyong Choi
Tung Chou
Sherman S. M. Chow
Peter Chvojka
Michele Ciampi
Craig Costello
Angelo De Caro

Yi Deng
David Derler
Christoph Dobraunig
Manu Drijvers
Li Duan
Maria Eichlseder
Kaoutar Elkhiyaoui
Keita Emura
Oguzhan Ersoy
Thomas Espitau
Gerardo Fenandez
Carmen Fernandez
Daniel Fett
Dario Fiore
Steven Galbraith
Adria Gascon
Romain Gay
Kai Gellert
Junqing Gong
Zheng Gong
Alonso Gonzalez
Lorenzo Grassi
Clémentine Gritti
Jian Guo
Jinguang Han
Yoshikazu Hanatani
Lin Hou
Guifang Huang
Jialin Huang
Ilia Iliashenko
Vincenzo Iovino
Ai Ishida
Dirmanto Jap
Saqib Kakvi
Daniel Kales
Jean-Gabriel Kammerer
Julien Keuffer
Jongkil Kim
Markulf Kohlweiss
Florian Kohnhäuser
Takeshi Koshiba
Hugo Krawczyk
Po-Chun Kuo
Rafael Kurek
Jianchang Lai
Qiqi Lai
Ben Lapid
Jeeun Lee
Qi Li
Christopher Liebchen
Tingting Lin
Helger Lipmaa
Patrick Longa
Xiapu Luo
Yiyuan Luo
Xuecheng Ma
Takahiro Matsuda
Matthew McKague
Siang Meng Sim Meng
Weizhi Meng
Markus Miettinen
Takaaki Mizuki
Kirill Morozov
Fabrice Mouhartem
Johannes Mueller
Zakaria Najm
Toru Nakanishi
Surya Nepal
Khoa Nguyen
David Niehues
Ana Nieto
Ariel Nof
David Nuñez
Kazuma Ohara
Shinya Okumura
Kazumasa Omote
Melek Önen
Leo Perrin
Thomas Peters
Le Trieu Phong
Tran Viet Xuan Phuong
Thomas Pöppelmann
Jeyavijayan Rajendran
Sebastian Ramacher
Somindu Ramanna
Daniel Rausch
Joost Renes
Sietse Ringers
Ruben Rios
Rodrigo Roman
Yusuke Sakai
Katerina Samari
John Schanck
Guido Schmitz
Jacob Schuldt
Hwajeong Seo
Mike Simon
Luisa Siniscalchi
Chunhua Su
Koutarou Suzuki
Akira Takahashi
Katsuyuki Takashima
Harry Chandra Tanuwidjaja
Tadanori Teruya
Yosuke Todo
Junichi Tomida
Patrick Towa
Yiannis Tselekounis
Ida Tucker
Aleksei Udovenko
Cédric Van Rompay
Dimitrios Vasilopoulos
Vesselin Velichkov
Nikita Veshchikov
Haoyang Wang
Qingju Wang
Yohei Watanabe
Keita Xagawa
Weijia Xue
Shota Yamada
Takashi Yamakawa
Hailun Yan
Guomin Yang
Kazuki Yoneyama
Hirotaka Yoshida
Hongbo Yu
Zheng Yuan
Thomas Zacharias
Rina Zeitoun
Bingsheng Zhang
Lei Zhang
Tao Zhang
Vincent Zucca

Contents

Cryptographic Protocols

Side Channel Attacks and Tamper Resistance

Digital Signatures

Privacy Preserving Computation

Multi-party Computation

Symmetric Key Primitives

Symmetric Key Cryptanalysis

Public Key Encryption

Authentication and Biometrics

Cloud and Peer-to-Peer Security