Lecture Notes in Computer Science 11060

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

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

Liqun Chen · Mark Manulis
Steve Schneider (Eds.)

Information Security

21st International Conference, ISC 2018
Guildford, UK, September 9–12, 2018
Proceedings

Springer

Editors
Liqun Chen
University of Surrey
Guildford
UK

Steve Schneider
University of Surrey
Guildford
UK

Mark Manulis
University of Surrey
Guildford
UK

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-99135-1 ISBN 978-3-319-99136-8 (eBook)
https://doi.org/10.1007/978-3-319-99136-8

Library of Congress Control Number: 2018950931

LNCS Sublibrary: SL4 – Security and Cryptology

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The 21st Information Security Conference, ISC 2018, took place September 9–12, 2018, in Guildford, UK, and was organized by the Surrey Centre for Cyber Security (SCCS) at the University of Surrey.

ISC is an annual conference focusing on original research in cyber security, applied cryptography, and privacy. Both academic research with high relevance to real-world problems and developments in industrial and technical frontiers fall within the scope of the conference.

ISC 2018 received 59 submissions, which were reviewed by the Program Committee. Each of the 46 Program Committee members was assigned an average of four submissions for review. Each paper was assigned to at least three reviewers. The Program Committee was helped by the reports and opinions of 54 external reviewers. The submission process was not anonymous and author names were visible to all reviewers. The review process was organized and managed through EasyChair. The reviewers were asked to declare any conflicts of interest for all submissions in the beginning of the process. The selection process was competitive and after highly interactive discussions and a careful deliberation, 26 papers were selected by the Program Committee for presentation at the conference.

The invited talks at ISC 2018 were given by Jan Camenisch from IBM Research Zurich and Aggelos Kiayias from the University of Edinburgh. Invited speakers were offered the opportunity to publish an invited paper in the conference proceedings. The prize for the Best Paper was awarded to Masahito Ishizaka and Kanta Matsuura for their paper "Strongly Unforgeable Signature Resilient to Polynomially Hard-to-Invert Leakage Under Standard Assumptions."

ISC 2018 was organized by Liqun Chen and Mark Manulis, who served as program chairs, selected the Program Committee, and led their efforts in selecting papers that you will find in this volume, and by Steve Schneider, who served as general chair and was helped in local organization by Ioana Boureanu and Kaitai Liang. ISC 2018 received generous sponsorship from Springer.

The ISC 2018 chairs would like to thank everyone who contributed to the success of the conference. We are grateful to the Program Committee and external reviewers for their commitment, hard work and enthusiasm, to ensure that each paper received a thorough and fair review. Last but not least, we wish to thank all conference participants for making ISC 2018 an enjoyable experience.

September 2018

Liqun Chen
Mark Manulis
Steve Schneider

Organization

Program Committee

Jean-Philippe Aumasson	Kudelski Security, Switzerland
Paulo Barreto	University of Washington, USA
Marina Blanton	University at Buffalo, USA
Ioana Boureanu	University of Surrey, UK
Colin Boyd	Norwegian University of Science and Technology, Norway
Liqun Chen	University of Surrey, UK
Sherman S. M. Chow	The Chinese University of Hong Kong, SAR China
Mauro Conti	University of Padua, Italy
James H. Davenport	University of Bath, UK
Lucas Davi	University of Duisburg-Essen, Germany
Alexandra Dmitrienko	University of Würzburg, Germany
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
François Dupressoir	University of Surrey, UK
Thomas Espitau	Sorbonne Université, UPMC LiP6, France
Nils Fleischhacker	Johns Hopkins University/Carnegie Mellon University, USA
Danilo Gligoroski	Norwegian University of Science and Technology, Norway
Tibor Jager	Paderborn University, Germany
Stefan Katzenbeisser	TU Darmstadt, Germany
Franziskus Kiefer	Mozilla, Germany
Xuejia Lai	Shanghai Jiao Tong University, China
Shujun Li	University of Kent, UK
Joseph Liu	Monash University, Australia
Javier Lopez	University of Malaga, Spain
Masahiro Mambo	Kanazawa University, Japan
Mark Manulis	University of Surrey, UK
Catherine Meadows	US Naval Research Laboratory, USA
Florian Mendel	Infineon Technologies, Germany
Chris Mitchell	Royal Holloway, University of London, UK
Atsuko Miyaji	Japan Advanced Institute of Science and Technology, Japan
Maire O'Neill	Queen's University Belfast, UK
Yanbin Pan	AMSS, China
Andreas Peter	University of Twente, The Netherlands
Duong Hieu Phan	Limoges University, France

Bertram Poettering	Royal Holloway, University of London, UK
Jeyavijayan Rajendran	University of Texas at Dallas, USA
Mark Ryan	University of Birmingham, UK
Peter Y. A. Ryan	University of Luxembourg, Luxembourg
Peter Scholl	Aarhus University, Denmark
Joerg Schwenk	Ruhr University Bochum, Germany
Luisa Siniscalchi	University of Salerno, Italy
Willy Susilo	University of Wollongong, Australia
Melanie Volkamer	Karlsruhe Institute of Technology, Germany
Ding Wang	Peking University, China
Lei Wang	Shanghai Jiao Tong University, China
Qian Wang	Wuhan University, China
Jianying Zhou	Singapore University of Technology and Design, Singapore

Additional Reviewers

Anglès-Tafalla, Carles
Bamiloshin, Michael
Bemmann, Pascal
Bernieri, Giuseppe
Cazorla, Lorena
Chen, Rongmao
Chow, Yang-Wai
Chvojka, Peter
Ciampi, Michele
Ding, Ning
Felsch, Dennis
Fernandez, Carmen
Fu, Ximing
Gao, Fei
Hagen, Christoph
Hupperich, Thomas
Kakvi, Saqib A.
Kulyk, Oksana
Lauer, Sebastian
Li, Juanru
Losiouk, Eleonora
Luo, Yiyuan
Nguyen, Khoa
Ning, Jianting
Omote, Kazumasa
Reinheimer, Benjamin Maximmilian
Ribes-González, Jordi
Rodler, Michael
Rubio, Juan E.
Shojafar, Mohammad
Silva, Javier
Spreitzer, Raphael
Surminski, Sebastian
Takano, Yuuki
Yan, Hailun
Zhao, Yongjun
Zhong, Jingli
Zollinger, Marie-Laure

Contents

Data Privacy and Anonymization

Outsourcing and Assisted Computing

Advanced Encryption

Privacy-Preserving Applications

Advanced Signatures

Network Security