

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

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

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

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

© Springer Nature Switzerland AG 2018

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

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

Contents

Invited Paper

Relaxed Lattice-Based Signatures with Short Zero-Knowledge Proofs	3
<i>Cecilia Boschini, Jan Camenisch, and Gregory Neven</i>	

Software Security

Secure Code Execution: A Generic PUF-Driven System Architecture	25
<i>Stephan Kleber, Florian Unterstein, Matthias Hiller, Frank Slomka, Matthias Matousek, Frank Kargl, and Christoph Bösch</i>	
<i>Lumus</i> : Dynamically Uncovering Evasive Android Applications	47
<i>Vitor Afonso, Anatoli Kalysch, Tilo Müller, Daniela Oliveira, André Grégio, and Paulo Lício de Geus</i>	
ICUFuzzer: Fuzzing ICU Library for Exploitable Bugs in Multiple Software	67
<i>Kun Yang, Yuan Deng, Chao Zhang, Jianwei Zhuge, and Haixin Duan</i>	
How Safe Is Safety Number? A User Study on SIGNAL’s Fingerprint and Safety Number Methods for Public Key Verification	85
<i>Kemal Bicakci, Enes Altuncu, Muhammet Sakir Sahkulubey, Hakan Ezgi Kiziloz, and Yusuf Uzunay</i>	

Symmetric Ciphers and Cryptanalysis

Speeding up MILP Aided Differential Characteristic Search with Matsui’s Strategy	101
<i>Yingjie Zhang, Siwei Sun, Jiahao Cai, and Lei Hu</i>	
Automatic Search for Related-Key Differential Trails in SIMON-like Block Ciphers Based on MILP.	116
<i>Xuzi Wang, Baofeng Wu, Lin Hou, and Dongdai Lin</i>	
Linear Cryptanalysis of Reduced-Round Speck with a Heuristic Approach: Automatic Search for Linear Trails	132
<i>Daniël Bodden</i>	
Conditional Cube Searching and Applications on Trivium-Variant Ciphers. . .	151
<i>Xiaojuan Zhang, Meicheng Liu, and Dongdai Lin</i>	

Data Privacy and Anonymization

Practical Attacks on Relational Databases Protected via Searchable Encryption	171
<i>Mohamed Ahmed Abdelraheem, Tobias Andersson, Christian Gehrman, and Cornelius Glackin</i>	
A Simple Algorithm for Estimating Distribution Parameters from n -Dimensional Randomized Binary Responses	192
<i>Staal A. Vinterbo</i>	

Outsourcing and Assisted Computing

Enforcing Access Controls for the Cryptographic Cloud Service Invocation Based on Virtual Machine Introspection.	213
<i>Fangjie Jiang, Quanwei Cai, Le Guan, and Jingqiang Lin</i>	
Multi-authority Fast Data Cloud-Outsourcing for Mobile Devices	231
<i>Yanting Zhang, Jianwei Liu, Zongyang Zhang, and Yang Hu</i>	
Hide the Modulus: A Secure Non-Interactive Fully Verifiable Delegation Scheme for Modular Exponentiations via CRT	250
<i>Osmanbey Uzunkol, Jothi Rangasamy, and Lakshmi Kuppusamy</i>	
Offline Assisted Group Key Exchange.	268
<i>Colin Boyd, Gareth T. Davies, Kristian Gjøsteen, and Yao Jiang</i>	

Advanced Encryption

Function-Dependent Commitments for Verifiable Multi-party Computation	289
<i>Lucas Schabhüser, Denis Butin, Denise Demirel, and Johannes Buchmann</i>	
On Constructing Pairing-Free Identity-Based Encryptions.	308
<i>Xin Wang, Bei Liang, Shimin Li, and Rui Xue</i>	
Multi-key Homomorphic Proxy Re-Encryption	328
<i>Satoshi Yasuda, Yoshihiro Koseki, Ryo Hiromasa, and Yutaka Kawai</i>	
Verifiable Decryption for Fully Homomorphic Encryption	347
<i>Fucai Luo and Kunpeng Wang</i>	

Privacy-Preserving Applications

Platform-Independent Secure Blockchain-Based Voting System	369
<i>Bin Yu, Joseph K. Liu, Amin Sakzad, Surya Nepal, Ron Steinfeld, Paul Rimba, and Man Ho Au</i>	
Privacy in Crowdsourcing: A Systematic Review	387
<i>Abdulwhab Alkharashi and Karen Renaud</i>	

Advanced Signatures

Anonymous yet Traceable Strong Designated Verifier Signature	403
<i>Veronika Kuchta, Rajeev Anand Sahu, Vishal Saraswat, Gaurav Sharma, Neetu Sharma, and Olivier Markowitch</i>	
Strongly Unforgeable Signature Resilient to Polynomially Hard-to-Invert Leakage Under Standard Assumptions	422
<i>Masahito Ishizaka and Kanta Matsuura</i>	
A Revocable Group Signature Scheme with Scalability from Simple Assumptions and Its Implementation	442
<i>Keita Emura and Takuya Hayashi</i>	

Network Security

Fast Flux Service Network Detection via Data Mining on Passive DNS Traffic	463
<i>Pierangelo Lombardo, Salvatore Saeli, Federica Bisio, Davide Bernardi, and Danilo Massa</i>	
Beyond Cookie Monster Amnesia: Real World Persistent Online Tracking. . .	481
<i>Nasser Mohammed Al-Fannah, Wanpeng Li, and Chris J. Mitchell</i>	
Cyber-Risks in the Industrial Internet of Things (IIoT): Towards a Method for Continuous Assessment	502
<i>Carolina Adaros Boye, Paul Kearney, and Mark Josephs</i>	
Author Index	521