

*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>

Lidong Chen · David McGrew  
Chris Mitchell (Eds.)

# Security Standardisation Research

Third International Conference, SSR 2016  
Gaithersburg, MD, USA, December 5–6, 2016  
Proceedings

*Editors*

Lidong Chen  
Computer Security Division  
NIST  
Gaithersburg, MD  
USA

Chris Mitchell  
University of London  
Egham  
UK

David McGrew  
Cisco Systems Inc.  
San Jose  
USA

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-49099-1              ISBN 978-3-319-49100-4 (eBook)  
DOI 10.1007/978-3-319-49100-4

Library of Congress Control Number: 2016955996

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 2016

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.

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

The Third International Conference on Research in Security Standardization was held at the National Institute for Standards and Technology (NIST), in Gaithersburg, MD, USA, during December 5–6, 2016. This event was the third in what is now an established series of conferences focusing on the theory, technology, and applications of security standards.

SSR 2016 built on the successful SSR 2014 and SSR 2015 conferences, held near London, UK, in December 2014 and in Tokyo, Japan, during December 2015. The proceedings of the 2014 and 2015 conferences were published in volumes 8893 and 9497 of the *Lecture Notes in Computer Science*.

The conference program consisted of two invited talks, 12 contributed papers, and a panel session. We would like to express our special thanks to the distinguished keynote speakers, John Kelsey (NIST, USA) and William Whyte (Security Innovation, USA), who gave very enjoyable and enlightening talks. Special thanks are also due to Salvatore Francomacaro (NIST, USA) who organized the panel session on “Can Security Standards Be Ahead of the Game?,” and to the panel members, who included: Liqun Chen, Eric Hibbard, Russ Housley, and David McGrew.

Out of 18 submissions with authors from nine countries, 12 papers were selected, presented at the conference, and included in these proceedings. The accepted papers cover a range of topics in the field of security standardization research, including hash-based signatures, algorithm agility, secure protocols, access control, secure APIs, payment security, and key distribution.

The success of this event depended critically on the help and hard work of many people, whose help we gratefully acknowledge. First, we heartily thank the Program Committee and the additional reviewers, listed on the following pages, for their careful and thorough reviews. Each paper was reviewed by at least three people, and on average by almost four. A significant time was spent discussing the papers. Thanks must also go to an (anonymous) hard-working shepherd for guidance and helpful advice on improving one of the papers. We also thank the general chair for her excellent organization of the conference, as well as Sara Kerman from NIST for her expert and dedicated assistance in ensuring the success of the conference.

We must also sincerely thank the authors of all submitted papers. We further thank all the authors of papers in this volume for revising their papers in accordance with the various referee suggestions and for returning the source files in good time. The revised versions were not checked by the Program Committee, and so authors bear final responsibility for their contents.

Thanks are due to the staff at Springer for their help with producing the proceedings. We must further thank the developers and maintainers of the EasyChair software, which greatly helped simplify the submission and review processes, as well as the production of these proceedings.

# Organization

## Security Standardization Research 2016

NIST, Gaithersburg, MD, USA

December 5–6, 2016

### General Chair

Lidong Chen                      NIST, USA

### Program Chairs

David McGrew                      Cisco, USA

Chris Mitchell                      Royal Holloway, University of London, UK

### Steering Committee

Liquan Chen                      Hewlett-Packard Labs, UK

Shin'ichiro Matsuo                      MagicCube Inc., USA

Chris Mitchell                      Royal Holloway, University of London, UK

Bart Preneel                      Katholieke Universiteit Leuven, Belgium

Sihan Qing                      Peking University, China

### Program Committee

Colin Boyd                      NTNU, Norway

Nancy Cam-Winget                      Cisco Systems, USA

Liquan Chen                      Hewlett Packard Labs, UK

Takeshi Chikazawa                      IPA, Japan

Cas Cremers                      University of Oxford, UK

Riaal Domingues                      DDSI ISD, South Africa

Scott Fluhrer                      Cisco Systems, USA

Aline Gouget                      Gemalto, France

Feng Hao                      Newcastle University, UK

Jens Hermans                      KU Leuven - ESAT/COSIC and iMinds, Belgium

Deukjo Hong                      Chonbuk National University, Republic of Korea

Dirk Kuhlmann                      HP Enterprise Labs, UK

Xuejia Lai                      Shanghai Jiaotong University, China

Pil Joong Lee                      Postech, Republic of Korea

Peter Lipp                      Graz University of Technology, Austria

Joseph Liu                      Monash University, Australia

Javier Lopez                      University of Malaga, Spain

Shin'ichiro Matsuo                      MagicCube Inc., USA

Catherine Meadows	NRL, USA
Jinghua Min	China Electronic Cyberspace Great Wall Co., Ltd., China
Atsuko Miyaji	School of Information Science, Japan Advanced Institute of Science and Technology, Japan
Valtteri Niemi	University of Turku, Finland
Pascal Paillier	CryptoExperts, France
Kenneth Paterson	Royal Holloway, University of London, UK
Sihan Qing	School of Software and Microelectronics, Peking University, China
Kai Rannenberg	Goethe University Frankfurt, Germany
Matt Robshaw	Impinj, USA
Christoph Ruland	University of Siegen, Germany
Mark Ryan	University of Birmingham, UK
Kazue Sako	NEC, Japan
Ben Smyth	Huawei, France
Jacques Traore	Orange Labs, France
Claire Vishik	Intel Corporation, UK
Debby Wallner	National Security Agency, USA
Michael Ward	MasterCard, UK
Yanjiang Yang	Huawei Singapore Research Center, Singapore
Jiaying Zhou	Institute for Infocomm Research, Singapore

## **Additional Reviewers**

Eom, Sungwook	Schmitz, Christopher
Lee, Eunsung	Szepieniec, Alan
Long, Yu	Tesfay, Welderufael
Mori, Kengo	Tran, Thao
Omote, Kazumasa	

# Contents

Analyzing and Fixing the QACCE Security of QUIC . . . . .	1
<i>Hideki Sakurada, Kazuki Yoneyama, Yoshikazu Hanatani, and Maki Yoshida</i>	
Cross-Tool Semantics for Protocol Security Goals. . . . .	32
<i>Joshua D. Guttman, John D. Ramsdell, and Paul D. Rowe</i>	
Cryptanalysis of GlobalPlatform Secure Channel Protocols. . . . .	62
<i>Mohamed Sabt and Jacques Traoré</i>	
NFC Payment Spy: A Privacy Attack on Contactless Payments . . . . .	92
<i>Maryam Mehrnezhad, Mohammed Aamir Ali, Feng Hao, and Aad van Moorsel</i>	
Security Analysis of the W3C Web Cryptography API . . . . .	112
<i>Kelsey Cairns, Harry Halpin, and Graham Steel</i>	
Algorithm Agility – Discussion on TPM 2.0 ECC Functionalities . . . . .	141
<i>Liqun Chen and Rainer Urian</i>	
Reactive and Proactive Standardisation of TLS . . . . .	160
<i>Kenneth G. Paterson and Thyla van der Merwe</i>	
Extending the UML Standards to Model Tree-Structured Data and Their Access Control Requirements. . . . .	187
<i>Alberto De la Rosa Algarin and Steven A. Demurjian</i>	
Attribute-Based Access Control Architectures with the eIDAS Protocols . . . .	205
<i>Frank Morgner, Paul Bastian, and Marc Fischlin</i>	
Secure Multicast Group Management and Key Distribution in IEEE 802.21. . . . .	227
<i>Yoshikazu Hanatani, Naoki Ogura, Yoshihiro Ohba, Lidong Chen, and Subir Das</i>	
State Management for Hash-Based Signatures. . . . .	244
<i>David McGrew, Panos Kampanakis, Scott Fluhrer, Stefan-Lukas Gazdag, Denis Butin, and Johannes Buchmann</i>	
Analysis of a Proposed Hash-Based Signature Standard . . . . .	261
<i>Jonathan Katz</i>	
<b>Author Index</b> . . . . .	275