# Lecture Notes in Computer Science 10074

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

Springer

*Editors*

Lidong Chen
Computer Security Division
NIST
Gaithersburg, MD
USA

David McGrew
Cisco Systems Inc.
San Jose
USA

Chris Mitchell
University of London
Egham
UK

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

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.

December 2016

David McGrew
Chris Mitchell

# 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

| | |
|---|---|
| Liqun 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 |
| Liqun 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 |
| Jianying Zhou | Institute for Infocomm Research, Singapore |

## Additional Reviewers

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

# Contents