

*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, Zürich, 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>

Liqun Chen · Shin'ichiro Matsuo (Eds.)

# Security Standardisation Research

Second International Conference, SSR 2015  
Tokyo, Japan, December 15–16, 2015  
Proceedings

*Editors*

Liquan Chen  
Hewlett Packard Laboratories  
Bristol  
UK

Shin'ichiro Matsuo  
NICT  
Tokyo  
Japan

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-27151-4              ISBN 978-3-319-27152-1 (eBook)  
DOI 10.1007/978-3-319-27152-1

Library of Congress Control Number: 2015955372

LNCS Sublibrary: SL4 – Security and Cryptology

Springer Cham Heidelberg New York Dordrecht London  
© Springer International Publishing Switzerland 2015

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

Springer International Publishing AG Switzerland is part of Springer Science+Business Media  
([www.springer.com](http://www.springer.com))

# Preface

The Second International Conference on Research in Security Standardisation was hosted by the Internet Initiative of Japan, in Tokyo, Japan, during December 15–16, 2015. This event was the second in what is planned to become a series of conferences focusing on the theory, technology, and applications of security standards.

SSR 2015 built on the successful SSR 2014 conference, held at Royal Holloway, University of London, UK, in December 2014. The proceedings of SSR 2014, containing 14 papers, were published in volume 8893 of the *Lecture Notes in Computer Science*.

The conference program consisted of two invited talks, 13 contributed papers, and a panel session. We would like to express our special thanks to the distinguished keynote speakers, Kenny Paterson and Pindar Wong, who gave very enlightening talks. Special thanks are due also to the panel organizer, Randall Easter, and the panel members.

Out of 18 submissions from 10 countries, 13 papers were selected, presented at the conference, and are included in these proceedings. The accepted papers cover a range of topics in the field of security standardisation research, including Bitcoin and payment, protocol and API, analysis of cryptographic algorithms, privacy, and trust and formal analysis.

The success of this event depended critically on the 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 most by four. A significant amount of time was spent discussing the papers. Thanks must also go to the hard-working shepherds for their guidance and helpful advice on improving a number of papers. We also thank the general co-chairs for their excellent organization of the conference.

We sincerely thank the authors of all submitted papers. We further thank the authors of accepted papers for revising papers according to the various reviewer suggestions and for returning the source files in good time. The revised versions were not checked by the Program Committee, and thus 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 process.

December 2015

Liqun Chen  
Shin'ichiro Matsuo



|                    |   |
|--------------------|---|
| Chris Mitchell     | Royal Holloway, University of London, UK  |
| Atsuko Miyaji      | School of Information Science, Japan Advanced Institute<br>of Science and Technology, Japan |
| Kenny Paterson     | Royal Holloway, University of London, UK  |
| Angelika Plate     | HelpAG, UAE   |
| Kai Rannenberg     | Goethe University Frankfurt, Germany  |
| Christoph Ruland   | University of Siegen, Germany   |
| Mark Ryan          | University of Birmingham, UK  |
| Gautham Sekar      | The Indian Statistical Institute, India   |
| Ben Smyth          | Huawei, France  |
| Jacques Traore     | Orange Labs, France   |
| Vijay Varadharajan | Macquarie University, Australia   |
| Claire Vishik      | Intel Corporation, UK   |
| Debby Wallner      | National Security Agency, USA   |
| Michael Ward       | MasterCard, UK  |
| Yanjiang Yang      | Institute for Infocomm Research, Singapore  |

## **Additional Reviewers**

|                   |                   |
|-------------------|-------------------|
| Batten, Ian       | Mancini, Loretta  |
| Chen, Jiageng     | Moody, Dustin     |
| Costello, Craig   | Omote, Kazumasa   |
| Franklin, Joshua  | Pape, Sebastian   |
| Hegen, Marvin     | Schantin, Andreas |
| Kim, Geonwoo      | Shin, Jinsuh      |
| Künnemann, Robert | Slamanig, Daniel  |
| Lee, Jinwoo       |                   |

# Contents

## Bitcoin and Payment

- Authenticated Key Exchange over Bitcoin . . . . . 3  
*Patrick McCorry, Siamak F. Shahandashti, Dylan Clarke,  
and Feng Hao*
- Tap-Tap and Pay (TTP): Preventing the Mafia Attack in NFC Payment. . . . . 21  
*Maryam Mehrnezhad, Feng Hao, and Siamak F. Shahandashti*

## Protocol and API

- Robust Authenticated Key Exchange Using Passwords and Identity-Based Signatures . . . . . 43  
*Jung Yeon Hwang, Seung-Hyun Kim, Daeseon Choi, Seung-Hun Jin,  
and Boyeon Song*
- Non-repudiation Services for the MMS Protocol of IEC 61850. . . . . 70  
*Karl Christoph Ruland and Jochen Sassmannshausen*
- Analysis of the PKCS#11 API Using the Maude-NPA Tool. . . . . 86  
*Antonio González-Burgueño, Sonia Santiago, Santiago Escobar,  
Catherine Meadows, and José Meseguer*

## Analysis on Cryptographic Algorithm

- How to Manipulate Curve Standards: A White Paper for the Black Hat <http://bada55.cr.yp.to> . . . . . 109  
*Daniel J. Bernstein, Tung Chou, Chitchanok Chuengsatiansup,  
Andreas Hülsing, Eran Lambooj, Tanja Lange, Ruben Niederhagen,  
and Christine van Vredendaal*
- Security of the SM2 Signature Scheme Against Generalized Key Substitution Attacks. . . . . 140  
*Zhenfeng Zhang, Kang Yang, Jiang Zhang, and Cheng Chen*
- Side Channel Cryptanalysis of Streebog. . . . . 154  
*Gautham Sekar*

## Privacy

- Improving Air Interface User Privacy in Mobile Telephony . . . . . 165  
*Mohammed Shafiul Alam Khan and Chris J. Mitchell*



Generating Unlinkable IPv6 Addresses . . . . . 185  
*Mwawi Nyirenda Kayuni, Mohammed Shafiul Alam Khan, Wanpeng Li,  
Chris J. Mitchell, and Po-Wah Yau*

**Trust and Formal Analysis**

A Practical Trust Framework: Assurance Levels Repackaged Through  
Analysis of Business Scenarios and Related Risks. . . . . 203  
*Masatoshi Hokino, Yuri Fujiki, Sakura Onda, Takeaki Kaneko,  
Natsuhiko Sakimura, and Hiroyuki Sato*

First Results of a Formal Analysis of the Network Time Security  
Specification. . . . . 218  
*Kristof Teichel, Dieter Sibold, and Stefan Milius*

Formal Support for Standardizing Protocols with State. . . . . 246  
*Joshua D. Guttman, Moses D. Liskov, John D. Ramsdell,  
and Paul D. Rowe*

**Author Index** . . . . . 267