Lecture Notes in Computer Science 9497

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

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

Springer

Editors
Liqun 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

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media (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 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

Security Standardisation Research 2015

Tokyo, Japan
December 15–16, 2015

General Chairs

Yuji Suga	Internet Initiative Japan, Japan
Hajime Watanabe	National Institute of Advanced Industrial Science and Technology, Japan

Program Chairs

Liqun Chen	Hewlett-Packard Laboratories, UK
Shin'ichiro Matsuo	NICT, Japan

Steering Committee

Liqun Chen	Hewlett-Packard Laboratories, UK
Shin'ichiro Matsuo	NICT, Japan
Chris Mitchell	Royal Holloway, University of London, UK
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Sihan Qing	Peking University, China

Program Committee

David Chadwick	University of Kent, UK
Lily Chen	NIST, USA
Liqun Chen	Hewlett-Packard Laboratories, UK
Takeshi Chikazawa	IPA, Japan
Cas Cremers	University of Oxford, UK
Andreas Fuchsberger	Microsoft, Germany
Phillip H. Griffin	Griffin Information Security Consulting, USA
Feng Hao	Newcastle University, UK
Jens Hermans	KU Leuven - ESAT/COSIC and iMinds, Belgium
Dirk Kuhlmann	HP, UK
Eva Kuiper	Hewlett-Packard, Canada
Pil Joong Lee	Postech, Republic of Korea
Peter Lipp	IT-Security, Austria
Joseph Liu	Monash University, Australia
Javier Lopez	University of Malaga, Spain
Shin'Ichiro Matsuo	NICT, Japan
Catherine Meadows	NRL, USA
Jinghua Min	China Electronic Cyberspace Great Wall Co., Ltd., China

Contents