Lecture Notes in Computer Science 8893

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

Liqun Chen Chris Mitchell (Eds.)

Security Standardisation Research

First International Conference, SSR 2014
London, UK, December 16-17, 2014
Proceedings

Springer

Volume Editors

Liqun Chen
HP Labs
Bristol, UK
E-mail: liqun.chen@hp.com

Chris Mitchell
University of London
Information Security Group
Egham, UK
E-mail: me@chrismitchell.net

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-319-14053-7 e-ISBN 978-3-319-14054-4
DOI 10.1007/978-3-319-14054-4
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014956396

LNCS Sublibrary: SL 4 – Security and Cryptology

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The First International Conference on Research in Security Standardisation was held at Royal Holloway, University of London, UK during December 16–17, 2014. This event was the first in what is planned to become a series of conferences focusing on the theory, technology, and applications of security standards.

The conference program consisted of two invited talks, 14 contributed papers, and a panel session. We would like to express our special thanks to the distinguished keynote speakers, Charles Brookson (Zeata Security, UK) and Marijke De Soete (Security4Biz, Oostkamp, Belgium), who gave very enlightening talks. Special thanks are due also to the panel organizer, Joshua D. Guttman (MITRE Corporation), and the panel members, who included Karthikeyan Bhargavan (INRIA), Cas Cremers (University of Oxford), and Kenneth Paterson (Royal Holloway, University of London).

Out of 22 submissions from 12 countries, 14 papers were selected, presented at the conference, and included in the proceedings. The accepted papers cover a range of topics in the field of security standardisation research, including cryptographic evaluation, standards development, analysis with formal methods, potential future areas of standardisation, and improving existing standards.

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 Programme Committee and the external 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. Significant 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 must also sincerely thank the authors of all submitted papers. We further thank the authors of accepted papers for revising papers according to the various referee suggestions and for returning the source files in good time. The revised versions were not checked by the Programme 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 process.

December 2014

Liqun Chen
Chris Mitchell

Security Standardisation Research 2014

Royal Holloway, University of London, UK
December 16–17, 2014

General Chair

Chris Mitchell	Royal Holloway, University of London, UK

Programme Chair

Liqun Chen	Hewlett-Packard Laboratories, UK

Programme Committee

Ian Bryant	Trustworthy Software Initiative, UK
David W. Chadwick	University of Kent, UK
Takeshi Chikazawa	Information-technology Promotion Agency, Japan
Lizzie Coles-Kemp	Royal Holloway, University of London, UK
Cas Cremers	University of Oxford, UK
Riaal Domingues	South Africa
Andreas Fuchsberger	Microsoft
Aline Gouget	Gemalto, France
Phillip H. Griffin	Griffin Information Security, USA
Bridget Kenyon	University College London, UK
Eva Kuiper	Hewlett-Packard, Canada
Xuejia Lai	Shanghai Jiaotong University, China
Pil Joong Lee	Postech, Republic of Korea
Jiangtao Li	Facebook, USA
Peter Lipp	Graz University of Technology, Austria
Joseph Liu	Institute for Infocomm Research, Singapore
Javier Lopez	University of Malaga, Spain
Andrew Martin	University of Oxford, UK
Shin'ichiro Matsuo	National Institute of Information and Communications Technology, Japan
Jinghua Min	China Electronic Cyberspace Great Wall Corporation, China
Atsuko Miyaji	Japan Advanced Institute of Science and Technology, Japan

Kenji Naemura	Institute of Information Security, Japan
Valtteri Niemi	University of Turku, Finland
Kenny Paterson	Royal Holloway, University of London, UK
Angelika Plate	help AG, UAE
Bart Preneel	KU Leuven and iMinds, Belgium
Sihan Qing	Peking University, China
Kai Rannenberg	Goethe University Frankfurt, Germany
Phillip Rogaway	UC Davis, USA
Christoph Ruland	University of Siegen, Germany
Kazue Sako	NEC, Japan
Dieter Sommer	IBM Zurich Research Laboratory, Switzerland
Jacques Traore	Orange Labs, France
Thyla Van Der Merwe	Royal Holloway, University of London, UK
Vijay Varadharajan	Macquarie University, Australia
Claire Vishik	Intel Corporation, UK
Debby Wallner	USA
Michael Ward	MasterCard, UK
Yanjiang Yang	Institute for Infocomm Research, Singapore
Jianying Zhou	Institute for Infocomm Research, Singapore

External Reviewers

Futa, Yuichi	Mori, Kengo
Ji, Qingguang	Shin, Jinsuh
Kim, Geonwoo	Su, Chunhua
Lee, Eunsung	Tabatabaei, Amir
Luo, Rui	Teranishi, Isamu

Table of Contents

Cryptographic Evaluation

Standards Development

Analysis with Formal Methods

Potential Future Areas of Standardisation

Improving Existing Standards