

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, 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, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, 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, Saarbruecken, Germany

Liqun Chen Chris Mitchell (Eds.)

Security Standardisation Research

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

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

© Springer International Publishing Switzerland 2014

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. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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 Easy-Chair software, which greatly helped simplify the submission and review process.

December 2014

Liqun Chen
Chris Mitchell

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

Unpicking PLAID: A Cryptographic Analysis of an ISO-Standards-Track Authentication Protocol	1
<i>Jean Paul Degabriele, Victoria Fehr, Marc Fischlin, Tommaso Gagliardoni, Felix Günther, Giorgia Azzurra Marson, Arno Mittelbach, and Kenneth G. Paterson</i>	
The SPEKE Protocol Revisited	26
<i>Feng Hao and Siamak F. Shahandashti</i>	
Analyzing Proposals for Improving Authentication on the TLS/SSL-Protected Web	39
<i>Christopher W. Brown and Michael Jenkins</i>	

Standards Development

Standardization Transparency: An Out of Body Experience	57
<i>Phillip H. Griffin</i>	
Size-Efficient Digital Signatures with Appendix by Truncating Unnecessarily Long Hashcode	69
<i>Jinwoo Lee and Pil Joong Lee</i>	
Blinded Diffie-Hellman: Preventing Eavesdroppers from Tracking Payments	79
<i>Duncan Garrett and Michael Ward</i>	

Analysis with Formal Methods

Security Goals and Evolving Standards	93
<i>Joshua D. Guttman, Moses D. Liskov, and Paul D. Rowe</i>	
Analysis of the IBM CCA Security API Protocols in Maude-NPA	111
<i>Antonio González-Burqueño, Sonia Santiago, Santiago Escobar, Catherine Meadows, and José Meseguer</i>	
Robustness Modelling and Verification of a Mix Net Protocol	131
<i>Efstathios Stathakidis, Steve Schneider, and James Heather</i>	

Potential Future Areas of Standardisation

Stego Quality Enhancement by Message Size Reduction and Fibonacci
Bit-Plane Mapping 151
Alan A. Abdulla, Harin Sellahewa, and Sabah A. Jassim

Secure Modular Password Authentication for the Web Using Channel
Bindings 167
Mark Manulis, Douglas Stebila, and Nick Denham

A Modular Framework for Multi-Factor Authentication and Key
Exchange 190
Nils Fleischhacker, Mark Manulis, and Amir Azodi

Improving Existing Standards

Improving the ISO/IEC 11770 Standard for Key Management
Techniques 215
Cas Cremers and Marko Horvat

Computationally Analyzing the ISO 9798–2.4 Authentication
Protocol 236
Britta Hale and Colin Boyd

Author Index 257