Ron Steinfeld Philip Hawkes (Eds.)

Information Security and Privacy

15th Australasian Conference, ACISP 2010
Sydney, Australia, July 5-7, 2010
Proceedings

Springer

Volume Editors

Ron Steinfeld
Macquarie University, Department of Computing
North Ryde, NSW 2109, Australia
E-mail: rons@science.mq.edu.au

Philip Hawkes
Qualcomm Incorporated
Suite 301, Level 3, 77 King Street, Sydney, NSW 2000, Australia
E-mail: phawkes@qualcomm.com

Library of Congress Control Number: 2010929205

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2, J.1, G.2.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-14080-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-14080-8 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

The annual Australasian Conference on Information Security and Privacy is the premier Australian academic conference in its field, showcasing research from around the globe on a range of topics. ACISP 2010 was held during July 5-7, 2010, at Macquarie University in Sydney, Australia.

There were 97 paper submissions for the conference. These submission were reviewed by the Program Committee and a number of other individuals, whose names can be found overleaf. The Program Committee then selected 24 papers for presentation at the conference. These papers are contained in these proceedings.

In addition to the peer-reviewed papers, two invited speakers presented talks at the conference: Craig Gentry (IBM, USA); and Stephan Overbeek (Shearwater Solutions, Australia). We would like to express our gratitude to Craig and Stephan for contributing their knowledge and insight, and thus expanding the horizons of the conference delegates.

We would like to thank the authors of all of submission for offering their research for publication in ACISP 2010. We extend our sincere thanks to the Program Committee and other reviewers for the high-quality reviews and in-depth discussion. The Program Committee made use of the iChair electronic submission and reviewing software written by Thomas Baignères and Matthieu Finiasz at EPFL, LASEC. We would like to express our thanks to Springer for continuing to support the ACISP conference and for help in the conference proceedings production. We also thank the Organizing Committee, led by the ACISP 2010 General Chair Josef Pieprzyk, for their contribution to the conference.

Finally, we would like to thank our sponsors, iRobot, and our hosts, Qualcomm Inc. and the Centre for Advanced Computing - Algorithms and Cryptography (ACAC) at Macquarie University.

July 2010

Ron Steinfeld
Philip Hawkes

Organization

General Chair

Josef Pieprzyk	Macquarie University, Australia

Program Co-chairs

Ron Steinfeld	Macquarie University, Australia
Philip Hawkes	Qualcomm Incorporated, Australia

Program Committee

Michel Abdalla	École Normale Supérieure, France
Masayuki Abe	NTT, Japan
Magnus Almgren	Chalmers University of Technology, Sweden
Joonsang Baek	Institute for Infocomm Research, Singapore
Feng Bao	Institute for Infocomm Research, Singapore
Lynn Batten	Deakin University, Australia
Alex Biryukov	University of Luxembourg, Luxembourg
Colin Boyd	Queensland University of Technology, Australia
Joo Yeon Cho	Nokia A/S, Denmark
Carlos Cid	Royal Holloway, University of London, UK
Andrew Clark	Queensland University of Technology, Australia
Nicolas Courtois	University College London, UK
Yvo Desmedt	University College London, UK and RCIS, AIST, Japan
Christophe Doche	Macquarie University, Australia
Ulrich Flegel	SAP Research, Germany
Steven Galbraith	University of Auckland, New Zealand
Juan Gonzalez Nieto	Queensland University of Technology, Australia
Maria Isabel Gonzalez Vasco	Universidad Rey Juan Carlos, Spain
Peter Gutmann	University of Auckland, New Zealand
Svein Knapskog	Norwegian University of Science and Technology, Norway
Xuejia Lai	Shanghai Jiao Tong University, China
Mark Manulis	TU Darmstadt, Germany
Keith Martin	Royal Holloway, University of London, UK
Mitsuru Matsui	Mitsubishi Electric, Japan
Krystian Matuiesewicz	Technical University of Denmark, Denmark
Chris Mitchell	Royal Holloway, University of London, UK
Atsuko Miyaji	JAIST, Japan

Yi Mu	University of Wollongong, Australia
C. Pandu Rangan	IIT, Madras, India
Vincent Rijmen	KU Leuven, Belgium and TU Graz, Austria
Rei Safavi Naini	University of Calgary, Canada
Palash Sarkar	Indian Statistical Institute, India
Berry Schoenmakers	TU Eindhoven, The Netherlands
Jennifer Seberry	University of Wollongong, Australia
Damien Stehlé	CNRS, France and University of Sydney, Australia and Macquarie University, Australia
Willy Susilo	University of Wollongong, Australia
Serge Vaudenay	EPFL, Switzerland
Damien Vergnaud	École Normale Supérieure, France
Huaxiong Wang	Nanyang Technological University, Singapore and Macquarie University, Australia
Duncan Wong	City University of Hong Kong, Hong Kong
Kan Yasuda	NTT, Japan
Yuliang Zheng	University of North Carolina at Charlotte, USA

External Reviewers

Hadi Ahmadi	Jialin Huang	Kaisa Nyberg
Man Ho Au	Qiong Huang	Tomas Olovsson
Gleb Beliakov	Ralf Hund	Kazumasa Omote
Simon R. Blackburn	Shaoquan Jiang	Khaled Ouafi
Thomas Bläsing	Charanjit Jutla	Vijayakrishnan Pasupathinathan
Jens-Matthias Bohli	Dmitry Khovratovich	Serdar Pehlivanoglu
Ignacio Cascudo	Andreas Larsson	Henning Rogge
Rafik Chaabouni	Pho Le	Markus Rueckert
Xiaofeng Chen	Gregor Leander	Minoru Saeki
Zhengjie Cheng	Benoit Libert	Yu Sasaki
Cline Chevalier	Tingting Lin	Takashi Satoh
Sebastiaan de Hoogh	Joseph K. Liu	Jacob Schuldt
Georg Fuchsbauer	Shengli Liu	Sharmila Deva Selvi
Jun Furukawa	Yi Lu	Pouyan Sepehrdad
Martin Gagne	Yiyuan Luo	Siamak F. Shahandashti
Choudary Gorantla	Takahiro Matsuda	Masaaki Shirase
Vipul Goyal	Florian Mendel	Magnus Själander
Jian Guo	Ivan Morel	Benjamin Smith
Fuchun Guo	Sumio Morioka	Boyeon Song
Hua Guo	Sean Murphy	Suriadi Suriadi
Gerhard Hancke	Jorge Nakahara Jr	Daisuke Suzuki
Javier Herranz	Kris Narayan	Christophe Tartary
Fumitaka Hoshino	Andrew Novocin	Alan Tickle
Xinyi Huang	Attrapadung Nuttapong	

Ashraful Tuhin
Oriol Farrs Ventura
Jorge Luis Villar
Ulrich Vollmer
Christian Wachsmann
Yan Wang
Guilin Wang
Peishun Wang
Benne de Weger
Puwen Wei
Ralf-Philipp Weinmann
Andrew White
Wei Wu
Yongdong Wu
Guomin Yang
Po-Wah Yau
Tsz Hon Yuen
Huafei Zhu

Table of Contents

Symmetric Key Encryption

Hash Functions

Public Key Cryptography

Protocols

Network Security