Lecture Notes in Computer Science 2384
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Tokyo

Lynn Batten Jennifer Seberry (Eds.)

Information Security and Privacy

7th Australasian Conference, ACISP 2002
Melbourne, Australia, July 3-5, 2002
Proceedings

Springer

Volume Editors

Lynn Batten
Deakin University, Rusden Campus
Burwood Road, Melbourne, Victoria, Australia
E-mail: lmbatten@deakin.edu.au

Jennifer Seberry
University of Wollongong, Department of Computer Science
Northfields Avenue, Wollongong, NSW, Australia
E-mail: jennifer.seberry@uow.edu.au

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information security and privacy : 7th Australasian conference ; proceedings / ACISP 2002, Melbourne, Australia, July 3 - 5, 2002. Lynn Batten ; Jennifer Seberry (ed.). - Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2384)
ISBN 3-540-43861-0

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2, E.4, F.2.1, K.4.1

ISSN 0302-9743
ISBN 3-540-43861-0 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Typesetting: Camera-ready by author, data conversion by PTP Berlin, Stefan Sossna e. K.
Printed on acid-free paper SPIN 10870504 06/3142 5 4 3 2 1 0

Preface

The Seventh Australasian Conference in Information Security and Privacy (ACISP) was held in Melbourne, 3–5 July, 2002. The conference was sponsored by Deakin University and iCORE, Alberta, Canada and the *Australian Computer Society*.

The aims of the *annual* ACISP conferences have been to bring together people working in different areas of computer, communication, and information security from universities, industry, and government institutions. The conferences give the participants the opportunity to discuss the latest developments in the rapidly growing area of information security and privacy.

The reviewing process took six weeks and we heartily thank all the members of the program committee and the external referees for the many hours of valuable time given to the conference.

The program committee accepted 36 papers from the 94 submitted. From those papers accepted 10 papers were from Australia, 5 each from Korea and USA, 4 each from Singapore and Germany, 2 from Japan, and 1 each from The Netherlands, UK, Spain, Bulgaria, and India. The authors of every paper, whether accepted or not, made a valued contribution to the conference.

In addition to the contributed papers, we were delighted to have presentations from the Victorian Privacy Commissioner, Paul Chadwick, and eminent researchers Professor Hugh Williams, Calgary, Canada, Professor Bimal Roy, ISI, Kolkota, India (whose invited talk was formally referred and accepted by the program committee), and Dr Hank Wolfe from Otago, New Zealand.

In addition we would like to thank Beom Sik Song, Willy Susilo, and especially Ken Finlayson for the vast work they put into getting this volume together in the time available.

July 2002

Lynn Batten
Jennifer Seberry

ACISP 2002

July 3-5, 2002, Melbourne, Australia

General Chair

Lynn Batten, Deakin University, Australia

Program Co-chairs

Lynn Batten, Deakin University, Australia
Jennifer Seberry, University of Wollongong, Australia

Program Committee

Colin Boyd	Queensland University of Technology, Australia
Mike Burmester	Florida State University, USA
Ed Dawson	Queensland University of Technology, Australia
Cunsheng Ding	University of Science & Technology, Hong Kong
Paul England	Microsoft, USA
Dieter Gollman	Microsoft, United Kingdom
Thomas Hardjono	VeriSign, USA
Kathy Horadam	RMIT, Australia
Kwangjo Kim	ICU, South Korea
Lars Knudsen	Technical University of Denmark, Denmark
Keith Martin	Royal Holloway, United Kingdom
Atsuko Miyaji	JAIST, Japan
Sangjae Moon	Kyungpook National University, South Korea
Yi Mu	Macquarie University, Australia
Eiji Okamoto	Toho University, Japan
Josef Pieprzyk	Macquarie University, Australia
Greg Rose	QUALCOMM, Australia
Rei Safavi-Naini	University of Wollongong, Australia
Qing Sihan	Academy of Science, China
John Snare	Adacel, Australia
Vijay Varadharajan	Macquarie University, Australia
Hugh Williams	University of Calgary, Canada
Yuliang Zheng	University of North Carolina, USA

External reviewers

Joonsang Baek, Monash University, Australia
Asha Baliga, RMIT University, Australia
Niklas Borselius, Royal Holloway, United Kingdom
Serdar Boztas, RMIT University, Australia
Laurence Bull, Monash University, Australia
Bernard Colbert, Telstra Research Laboratories, Australia
Robert Coulter, Deakin University, Australia
Ken Finlayson, Wollongong University, Australia
Goichiro Hanaoka, University of Tokyo, Japan
Marie Henderson, RMIT University, Australia
Matt Henricksen, QUT, Australia
Yvonne Hithchenson, QUT, Australia
Hartono Kurino, Wollongong University, Australia
Hiroaki Kikuchi, Japan
Jun Kogre, Fujitsu, Japan
Tanja Lange, Ruhr University, Germany
Bill Millan, QUT, Australia
Kenji Ohkuma, Toshiba, Japan
Marcus Peinado, Microsoft, USA
Ian Piper, Wollongong University, Australia
Chengxi Qu, University of New England, Australia
Matt Robshaw, Royal Holloway, United Kingdom
Nickolas Sheppard, Wollongong University, Australia
Igor Shparlinski, Macquarie University, Australia
Leonie Simpson, QUT, Australia
Masakazu Soshi, JAIST, Japan
Ron Steinfeld, Monash University, Australia
Karolyn Sprinks, Wollongong University, Australia
Willy Susilo, Wollongong University, Australia
Mitsuru Tada, Chiba University, Japan
Kapali Viswanthan, QUT, Australia
Yejing Wang, Wollongong University, Australia
Huaxiong Wang, Macquarie University, Australia
Tianbing Xia, Wollongong University, Australia
Masato Yamamichi, Japan
Jin Yuan, Hong Kong University of Science and Technology
Fangguo Zhang, ICU, Korea
Xianmo Zhang, Macquarie University, Australia

Table of Contents

Key Handling

Trust and Secret Sharing

Fast Computation

Cryptanalysis I

Elliptic Curves

AES

Security Management

Authentication

Invited Talk

Oblivious Transfer

Cryptanalysis II

Dealing with Adversaries