Lecture Notes in Computer Science 2119
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

Vijay Varadharajan   Yi Mu (Eds.)

Information Security and Privacy

6th Australasian Conference, ACISP 2001
Sydney, Australia, July 11-13, 2001
Proceedings

Springer

Volume Editors

Vijay Varadharajan
Yi Mu
Macquarie University, Department of Computing
North Ryde, NSW 2109, Australia
E-mail: {vijay,ymu}@ics.mq.edu.au

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information security and privacy : 6th Australasian conference ; proceedings / ACISP 2001, Sydney, Australia, July 11 - 13, 2001. Vijay Varadharajan ; Yi Mu (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2001
(Lecture notes in computer science ; Vol. 2119)
ISBN 3-540-42300-1

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 3-540-42300-1 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 Boller Mediendesign
Printed on acid-free paper SPIN: 10839883 06/3142 5 4 3 2 1 0

Preface

ACISP 2001, the Sixth Australasian Conference on Information Security and Privacy, was held in Sydney, Australia. The conference was sponsored by Information and Networked System Security Research (INSSR), Macquarie University, the Australian Computer Society, and the University of Western Sydney. I am grateful to all these organizations for their support of the conference.

The aim of this conference was to draw together researchers, designers, and users of information security systems and technologies. The conference program addressed a range of aspects from system and network security to secure Internet applications to cryptography and cryptanalysis. This year the program committee invited two international keynote speakers Dr. Yacov Yacobi from Microsoft Research (USA) and Dr. Clifford Neumann from the University of Southern California (USA). Dr. Yacobi's talk addressed the issues of trust, privacy, and anti-piracy in electronic commerce. Dr. Neumann's address was concerned with authorization policy issues and their enforcement in applications.

The conference received 91 papers from America, Asia, Australia, and Europe. The program committee accepted 38 papers and these were presented in some 9 sessions covering system security, network security, trust and access control, Authentication, cryptography, cryptanalysis, Digital Signatures, Elliptic Curve Based Techniques, and Secret Sharing and Threshold Schemes. This year the accepted papers came from a range of countries, including 7 from Australia, 8 from Korea, 7 from Japan, 3 from UK, 3 from Germany, 3 from USA, 2 from Singapore, 2 from Canada and 1 from Belgium, Estonia, and Taiwan.

Organizing a conference such as this one is a time-consuming task and I would like to thank all the people who worked hard to make this conference a success. In particular, I would like to thank Program Co-chair Yi Mu for his tireless work and the members of the program committee for putting together an excellent program, and all the session chairs and speakers for their time and effort. Special thanks to Yi Mu, Laura Olsen, Rajan Shankaran, and Michael Hitchens for their help with local organization details. Finally, I would like to thank all the authors who submitted papers and all the participants of ACISP 2001. I hope that the professional contacts made at this conference, the presentations, and the proceedings have offered you insights and ideas that you can apply to your own efforts in security and privacy.

July 2001 Vijay Varadharajan

AUSTRALASIAN CONFERENCE ON INFORMATION SECURITY AND PRIVACY ACISP 2001

Sponsored by
Macquarie University
Australian Computer Society

General Chair:

Vijay Varadharajan	*Macquarie University, Australia*

Program Chairs:

Vijay Varadharajan	*Macquarie University, Australia*
Yi Mu	*Macquarie University, Australia*

Program Committee:

Ross Anderson	*Cambridge University, UK*
Colin Boyd	*Queensland University of Technology, Australia*
Ed Dawson	*Queensland University of Technology, Australia*
Yvo Desmedt	*Florida State University, USA*
Paul England	*Microsoft*
Yair Frankel	*Columbia University, USA*
Ajoy Ghosh	*UNISYS, Australia*
Dieter Gollman	*Microsoft*
John Gordon	*ConceptLabs, UK*
Kwangjo Kim	*ICU, Korea*
Chuchang Liu	*DSTO, Australia*
Masahiro Mambo	*Tohoku University, Japan*
Wenbo Mao	*Hewlett-Packard Lab., UK*
Chris Mitchell	*London University, UK*
Eiji Okamoto	*University of Wisconsin, USA*
Joe Pato	*Hewlett-Packard Lab., USA*
Josef Pieprzyk	*Macquarie University, Australia*
Bart Preneel	*Katholieke University, Belgium*
Steve Roberts	*Witham Pty Ltd, Australia*
Qing Sihan	*Academy of Science, China*
Rei Safavi-Naini	*University of Wollongong, Australia*
Jennifer Seberry	*University of Wollongong, Australia*
Yuliang Zheng	*Monash University, Australia*

Table of Contents