Lecture Notes in Computer Science 1270
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Vijay Varadharajan
Josef Pieprzyk Yi Mu (Eds.)

Information Security and Privacy

Second Australasian Conference, ACISP'97
Sydney, NSW, Australia, July 7-9, 1997
Proceedings

Springer

Volume Editors

Vijay Varadharajan
Yi Mu
University of Western Sydney, Nepean, Department of Computing
Second Avenue, Kingswood, NSW 2747, Australia
E-mail: (vijay/yimu)@st.nepean.uws.edu.au

Josef Pieprzyk
University of Wollongong, Department of Computer Science
Northfields Avenue, Wollongong, NSW 2522, Australia
E-mail: josef@osiris.cs.uow.edu.au

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information security and privacy : second Australasian conference ; proceedings / ACISP '97, Sydney, NSW, Australia, July 7 - 9, 1997. Vijay Varadharajan ... (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1997
(Lecture notes in computer science ; Vol. 1270)
ISBN 3-540-63232-8

CR Subject Classification (1991): E.3, K.6.5, D.4.6, C.2, E.4,F.2.1-2, K.4.1

ISSN 0302-9743
ISBN 3-540-63232-8 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10548864 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

PREFACE

ACISP'97, the Second Australasian Conference on Information Security and Privacy, was held in Sydney, Australia. The conference was sponsored by Distributed System and Network Security Research, University of Western Sydney, Nepean, the Australian Computer Society (NSW), and the Distributed Systems Technology Centre, Queensland. The conference was organized in co-operation with the International Association of Cryptologic Research (IACR) and the Institute of Electrical and Electronic Engineers (NSW). I am grateful to all these organizations for their support of the conference.

The aim of this conference was to draw together researchers, designers, implementators, and users of information security systems and technologies. The conference program addresssed a range of aspects from security theory and modelling to system designs and implementations to user-oriented management and applications. This year the program committee invited a distinguished academic, Professor Fred Piper from London University, UK, as the keynote speaker of the conference. Professor Piper's talk questioned the role and the need for trusted third parties in the area of secure electronic commerce. On the second day, Kenneth Mendelson, Corporate Counsel of Trusted Information Systems, USA, was invited to speak on recent developments in US cryptographic policy. Following this presentation, the conference hosted a related panel session on cryptographic policy guidelines with international members Scott Charney (USA), Stephanie Perrin (Canada), Steve Orlowski, Norman Reaburn (Australia), Nigel Hickson (UK) and Philippe Dejean (France). The speaker at the conference dinner was Michael Lappen, Managing Director, Wang Australia, who addressed security issues and the emerging new technologies.

The program committee accepted 29 papers and these were presented in nine sessions covering security models and access control, network security, secure hardware and implementation issues, cryptographic functions and ciphers, authentication codes and secret sharing schemes, cryptanalysis, key escrow, security protocols and key management, and secure applications. This year the accepted papers came from a range of countries, including 13 from Australia, 5 from Japan, 2 each from the USA, UK, and Germany, the rest from Norway, Singapore, Belgium, China, and Poland.

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 the members of the program committee for putting together an excellent program, and all the session chairs, speakers, and panelists for their time and effort. Special thanks to Irene Ee and Yi Mu for their tireless work in organizing and helping with many local details. Finally, I would like to thank all the authors who submitted papers and all the participants of ACISP'97. 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.

May 1997 Vijay Varadharajan

AUSTRALASIAN CONFERENCE ON INFORMATION SECURITY AND PRIVACY ACISP'97

Sponsored by
Distributed System & Network Security Research Unit, UWSN
Australian Computer Society (NSW)
Distributed Systems Technology Centre (DSTC), Australia

In cooperation with
International Association for Cryptologic Research (IACR)
Institute of Electrical & Electronics Engineers (IEEE, NSW)

General Chair:

Vijay Varadharajan	*University of Western Sydney*

Program Chairs:

Josef Pieprzyk	*University of Wollongong*
Vijay Varadharajan	*University of Western Sydney*

Programme Committee:

Yun Bai	*University of Western Sydney*
Colin Boyd	*Queensland University of Technology*
William Caelli	*Queensland University of Technology*
Robert Davids	*Westpac Banking Corporation, Australia*
Ed Dawson	*Queensland University of Technology*
Nick Demytko	*Telstra, Australia*
Yong Fei Han	*National University of Singapore*
Thomas Hardjono	*University of Western Sydney*
Michael Hitchens	*Sydney University*
Chiang Lim	*Australian Standards Institute*
Wenbo Mao	*Hewlett-Packard Lab., UK*
Yi Mu	*University of Western Sydney*
Yuko Muraya	*Hiroshima City University*
Luke O'Connor	*IBM, Zurich, Switzerland*
John Rogers	*Department of Defence, Australia*
Rei Safavi-Naini	*University of Wollongong*
Jim Schindler	*Hewlett-Packard Lab., USA*
Jennifer Seberry	*University of Wollongong*
Yuliang Zheng	*Monash University*

* Conference Satchels donated by Westpac Banking Cooperation, Australia

CONTENTS

Keynote Lecture:

1. Security Models And Access Control

2. Network Security

3. Secure Hardware And Implementation Issues

4. Cryptographic Functions And Ciphers

5. Authentication Codes And Secret Sharing Schemes

6. Cryptanalysis

7. Key Escrow

8. Security Protocols And Key Management

9. Applications