

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.

**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
Yi Mu

Macquarie University, Australia
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

Yi Mu

Macquarie University, Australia

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

Qing Sihan

Academy of Science, China

Rei Safavi-Naini

University of Wollongong, Australia

Jennifer Seberry

University of Wollongong, Australia

Yuliang Zheng

Monash University, Australia

Referees:

Joonsang Baek, Yun Bai, Gareth Brisbane, Mike Burmester, Andrew Clark, Jung Hee Cheon, Hyun-Jin Choi, Stephen Crane, Mark Crosbie, Peter Duffett, Steven Galbraith, Juanma Gonzalez-Nieto, Marie Henderson, Tri V. Le, Byoungcheon Lee, Mark Looi, Greg Maitland, Marco Casassa Mont, Yuichi Nakai, Maris A Ozols, Marcus Peinado, Jakob Rehof, Jason Reid, Rajan Shankaran, Nickolas Sheppard, Leonie Simpson, Jeff Stehlin, Ron Steinfeld, Frederik Vercauteren, Kapali Viswanathan, Yejing Wang, Chuan Kun Wu, Jianxin Yan, and John Yesberg.