Preface

ACISP 2000, the Fifth Australasian Conference on Information Security and Privacy, was held in Brisbane, Australia, 10–12 July, 2000. The conference was sponsored by the Information Security Research Centre at Queensland University of Technology, the Australian Computer Society, Telstra, Boeing Australia Limited, SecureGate Limited, and RSA Security Pty Ltd. We are grateful to all these organizations for their support of the conference.

The conference brought together researchers, designers, implementors, and users of information security systems. The aim of the conference is to have a series of technical refereed and invited papers to discuss all different aspects of information security. The program committee invited seven distinguished speakers: Mike Burmester, G.R. Blakley, Bob Blakley, Brian Denehy, Roger Lyle, John Snare, and Alan Underwood. Mike Burmester from Royal Holloway College, University of London presented a paper entitled "A Survey of Key Distribution"; G.R. Blakley from Texas A&M University and Bob Blakley from the IBM Tivoli Security Business Unit presented a paper entitled "All Sail, No Anchor, I: Cryptography, Risk, and e-Commerce"; Brian Denehy from SecureGate Limited presented a paper entitled "Secure Networks or Network Security – Approaches to Both"; Roger Lyle from Standards Australia and John Snare from Telstra presented a paper entitled "Perspectives on Australia's New Information Security Management Standard"; and Alan Underwood from the Australian Computer Society presented a paper entitled "Professional Ethics in a Security and Privacy Context – The Perspective of a National Computing Society".

There were 81 technical papers submitted to the conference from an international authorship. These papers were refereed by the program committee and 37 papers were accepted for the conference. We would like to thank the authors of all papers which were submitted to the conference, both those whose work is included in these proceedings, and those whose work could not be accommodated.

The papers included in the conference came from a number of countries including 13 from Australia, six from Japan, five from the USA, four from Singapore, three from Korea, two from Greece, and one each from the UK, Germany, Norway, and Yugoslavia. These papers covered topics in network security, public key cryptography, cryptographic implementation issues, electronic commerce, key recovery, public key infrastructure, Boolean functions, intrusion detection, codes, digital signatures, secret sharing, and protocols.

The conference included a panel session entitled "Future Directions in Secure E-Commerce". This panel was chaired by William Caelli and included leaders in technology, law, and public policy related to the security issues and problems of electronic commerce.

We would like to thank all the people involved in organizing this conference. In particular we would like to thank members of the program committee for their

effort in reviewing papers and designing an excellent program. Special thanks to members of the organizing committee for their time and effort in organizing the conference, especially Ernest Foo, Gary Gaskell, Betty Hansford, Liz Lipowitz, Mark Looi, Lauren May, and Christine Orme. Finally we would like to thank all the participants at ACISP 2000.

May 2000

Ed Dawson
Andrew Clark
Colin Boyd

Australasian Conference on Information Security and Privacy ACISP 2000

Sponsored by
Information Security Research Centre, QUT, Australia
Australian Computer Society
Telstra
Boeing Australia Limited
SecureGate Limited
RSA Security Pty Ltd

General Chair

Ed Dawson	*Queensland University of Technology, Australia*

Organizing Chair

Mark Looi	*Queensland University of Technology, Australia*

Program Chairs

Colin Boyd	*Queensland University of Technology, Australia*
Ed Dawson	*Queensland University of Technology, Australia*

Program Committee

Mark Ames	*Telstra, Australia*
Bob Blakley	*Texas A&M University, USA*
Mike Burmester	*Royal Holloway College, UK*
William Caelli	*Queensland University of Technology, Australia*
Dieter Gollmann	*Microsoft Research, UK*
Yongfei Han	*SecurEworld, Singapore*
Wenbo Mao	*Hewlett-Packard Laboratories, UK*
SangJae Moon	*Kyungpook National University, Korea*
Winfried Müller	*University of Klagenfurt, Austria*
Eiji Okamoto	*University of Wisconsin, USA*
Josef Pieprzyk	*University of Wollongong, Australia*
Bart Preneel	*Catholic University Leuven, Belgium*
Steve Roberts	*Witham Pty Ltd, Australia*
John Rogers	*Department of Defence, Australia*
Greg Rose	*Qualcomm, Australia*
Rei Safavi-Naini	*University of Wollongong, Australia*

Stafford Tavares	*Queen's University, Canada*
Vijay Varadharajan	*University of Western Sydney, Australia*
Henry Wolfe	*University of Otago, New Zealand*
Yuliang Zheng	*Monash University, Australia*
Ed Zuk	*Rotek Consulting, Australia*

Referees

Mark Ames
Paul Ashley
G.R. Blakley
Colin Boyd
Mike Burmester
William Caelli
Nathan Carey
Gary Carter
Liqun Chen
Choo Chong Cher
Jong U. Choi
Andrew Clark
Ed Dawson
Ernest Foo
Gary Gaskell
Mickey Gittler
Dieter Gollmann
Juanma Gonzalez Nieto
Yongfei Han
Mark Looi
Greg Maitland
Wenbo Mao
Keith Martin
William Millan
George Mohay
Marco Casassa Mont
SangJae Moon
Yi Mu
Winfried Müller
Eiji Okamoto
Dong-Gook Park
Ji-Hwan Park
Chris Pavlovski
Josef Pieprzyk
Bart Preneel
Jason Reid
Vincent Rijmen
Steve Roberts
John Rogers
Greg Rose
Rei Safavi-Naini
Andrew Salleh
Leonie Simpson
David Soldera
Willy Susilo
Stafford Tavares
Vijay Varadharajan
Kapali Viswanathan
Huaxiong Wang
Henry Wolfe
Chuan Wu
Yuliang Zheng
Ed Zuk