Preface

This volume contains the proceedings of the 4th International Conference on Information and Communications Security (ICICS 2002). The three previous conferences were held in Beijing (ICICS 97), Sydney (ICICS 99) and Xian (ICICS 01), where we had an enthusiastic and well-attended event. ICICS 2002 is sponsored and organized by the Laboratories for Information Technology, Singapore, in co-operation with the Engineering Research Center for Information Security Technology of the Chinese Academy of Sciences and the International Communications and Information Security Association (ICISA).

During the past five years the conference has placed equal emphasis on the theoretical and practical aspects of information and communications security and has established itself as a forum at which academic and industrial people meet and discuss emerging security challenges and solutions. We hope to uphold this tradition by offering you yet another successful meeting with a rich and interesting program.

The response to the Call For Papers was overwhelming, 161 paper submissions were received. Therefore, the paper selection process was very competitive and difficult – only 41 papers were accepted and many good papers had to be rejected. The success of the conference depends on the quality of the program. We are indebted to our program committee members and the external referees for the wonderful job they did.

Before letting you enjoy the technical program, we would like to thank several individuals who skilfully and tirelessly put this conference together. First, Robert Deng would like to thank Prof. Sihan Qing for proposing to have this conference in Singapore. Next, our special thanks to the conference organizing committee, in particular Feng Bao (Local Arrangements), Jianying Zhou (Publicity and Publication), and Patricia Loh (Logistics and Registration). Without the hard work by all these folks, this conference would not have been possible.

Finally, we would like to thank the authors who submitted papers and the participants from all over the world who chose to honor us with their attendance.

September 2002

Robert Deng
Sihan Qing

ICICS 2002

Fourth International Conference
on Information and Communications Security

Singapore
December 9-12, 2002

Program Chairs

Robert Deng	Laboratories for Information Technology, Singapore
Sihan Qing	Chinese Academy of Sciences, China

Program Committee

Feng Bao	Laboratories for Information Technology, Singapore
Colin Boyd	Queensland University of Technology, Australia
Xiaotie Deng	City University of Hong Kong, Hong Kong
Dengguo Feng	Chinese Academy of Sciences, China
Li Gong	Sun Microsystems, USA
Dieter Gollmann	Microsoft Research, Cambridge, UK
Yongfei Han	Onets, China
Mohan Kankanhalli	National University of Singapore, Singapore
Kwangjo Kim	Information and Communications University, Korea
Chi-Sung Laih	National Cheng Kung University, Taiwan
Wenbo Mao	Hewlett-Packard Labs, Bristol, UK
Masahiro Mambo	Tohoku University, Japan
David Naccache	Gemplus, France
Eiji Okamoto	University of Tsukuba, Japan

Jean-Jacques Quisquater   UCL, Belgium
Mike Reiter   Carnegie Mellon University, USA
Bimal Roy   Indian Statistical Institute, India
Avi Rubin   AT&T Labs, USA
Ravi Sandhu   SingleSignOn.Net and George Mason University, USA
Shiuhpyng Shieh   National Chiao Tung University, Taiwan
Paul Syverson   Naval Research Lab, USA
Doug Tygar   University of California at Berkeley, USA
Vijay Varadharajan   Macquarie, Australia
Yumin Wang   Xidian University, China
Yiqun Lisa Yin   NTT MCL, USA
Yuliang Zheng   University of North Carolina at Charlotte, USA
Jianying Zhou   Laboratories for Information Technology, Singapore

Organizing Committee

Feng Bao   Laboratories for Information Technology, Singapore
Patricia Loh   Laboratories for Information Technology, Singapore
Jianying Zhou   Laboratories for Information Technology, Singapore