PREFACE

ICICS'99, the Second International Conference on Information and Communication Security, was held in Sydney, Australia, 9-11 November 1999. The conference was sponsored by the Distributed System and Network Security Research Unit, University of Western Sydney, Nepean, the Australian Computer Society, IEEE Computer Chapter (NSW), and Harvey World Travel. I am grateful to all these organizations for their support of the conference.

The conference brought together researchers, designers, implementors and users of information security systems and technologies. A range of aspects was addressed from security theory and modeling to system and protocol designs and implementations to applications and management. The conference consisted of a series of refereed technical papers and invited technical presentations. The program committee invited two distinguished key note speakers. The first keynote speech by Doug McGowan, a Senior Manager from Hewlett-Packard, USA, discussed cryptography in an international setting. Doug described the current status of international cryptography and explored possible future trends and new technologies. The second keynote speech was delivered by Sushil Jajodia of George Mason University, USA. Sushil's talk addressed the protection of critical information systems. He discussed issues and methods for survivability of systems under malicious attacks and proposed a fault-tolerance based approach. The conference also hosted a panel on the currently much debated topic of Internet censorship. The panel addressed the issue of censorship from various viewpoints namely legal, industrial, governmental and technical. It was chaired by Vijay Varadharajan with panel members from the Australian National Office of the Information Economy, Electronic Frontiers Association, the Australian Computer Society, and the Internet Industry Association.

There were 62 technical papers submitted to the conference from an international authorship. The program committee accepted 24 papers and these were presented in eight sessions covering cryptanalysis, language based approach to security, electronic commerce and secret sharing, digital signatures, security protocols, applications, cryptography, and complexity functions. The accepted papers came from a range of countries, including some 7 papers from Australia, 6 from Japan, 3 from the USA, 2 from Sweden, 2 from the UK, 1 from China, France, Spain, and Singapore. I would like to thank the authors of all the papers submitted to the conference, both those whose work is included in the proceedings and those whose work could not be accommodated.

I would like to thank all the people involved in organizing the conference. In particular, I would like to thank the members of the program committee for

their effort in reviewing the papers and putting together an excellent program. I would like to thank all the speakers, session chairs, and panelists for their time and effort. Special thanks to members of the organizing committee for their tireless work in organizing and helping with many local details, especially Yi Mu, Irene Ee, Rajan Shankaran, Kenny Nguyen, and Chuan Kun Wu. Finally, I would like to thank all the participants of ICICS'99. I hope that the professional contacts made at this conference, the presentations, and the proceedings have offered you additional insights and ideas that you can apply to your own efforts in information and communication security.

August 1999   Vijay Varadharajan