Preface

This volume contains the proceedings of the 8th International Information Security Conference (ISC 2005), which took place in Singapore, from 20th to 23rd September 2005. ISC 2005 brought together individuals from academia and industry involved in many research disciplines of information security to foster the exchange of ideas. During recent years this conference has tried to place special emphasis on the practical aspects of information security, and since it passed from being an international workshop to being an international conference in 2001, it has become one of the most relevant forums at which researchers meet and discuss emerging security challenges and solutions.

Advised by the ISC Steering Committee, and in order to provide students with more opportunities for publication, ISC 2005 accepted extra student papers besides the regular papers. The initiative was very well accepted by the young sector of the scientific community, and we hope that the success of this idea will remain for next ISC events. Another important factor for the success of ISC 2005 was that selected papers in the proceedings will be invited for submission to a special issue of the International Journal of Information Security. The result was an incredible response to the call for papers; we received 271 submissions, the highest since ISC events started. It goes without saying that the paper selection process was more competitive and difficult than ever before — only 33 regular papers were accepted, plus 5 student papers for a special student session.

As always, the success of an international conference does not depend on the number of submissions only, but on the quality of the program too. Therefore, we are indebted to our Program Committee members and the external reviewers for the great job they did. The proceedings contain revised versions of the accepted papers. However, revisions were not checked and the authors bear full responsibility for the content of their papers.

More people deserve thanks for their contribution to the success of the conference. We sincerely thank general chairs Robert Deng and Feng Bao for their support and encouragement. Our special thanks are due to Ying Qiu for managing the website for paper submission, review and notification. Guilin Wang did an excellent job as publicity chair. Patricia Loh was kind enough to arrange for the conference venue and took care of the administration in running the conference. Without the hard work of these colleagues and the rest of the local organizing team, this conference would not have been possible. We would also like to thank all the authors who submitted papers and the participants from all over the world who chose to honor us with their attendance.

Last but not least, we are grateful to Institute for Infocomm Research and Singapore Management University for sponsoring the conference.

July 2005

Jianying Zhou
Javier Lopez

ISC 2005

8th Information Security Conference

Singapore
September 20–23, 2005

Organized by

Institute for Infocomm Research, Singapore

Sponsored by

Institute for Infocomm Research, Singapore
and
Singapore Management University, Singapore

General Chair

Robert H. Deng ..... Singapore Management University, Singapore
Feng Bao ..... Institute for Infocomm Research, Singapore

Program Chairs

Jianying Zhou ..... Institute for Infocomm Research, Singapore
Javier Lopez ..... University of Malaga, Spain

Program Committee

Tuomas Aura ..... Microsoft Research, UK
Giampaolo Bella ..... Univ. of Catania, Italy
Joan Borrell ..... Univ. Autonoma de Barcelona, Spain
Mike Burmester ..... Florida State Univ., USA
Liqun Chen ..... HP Labs, UK
Ed Dawson ..... QUT, Australia
Xiaotie Deng ..... City Univ. of Hong Kong, China
Xuhua Ding ..... SMU, Singapore
Philippe Golle ..... PARC, USA
Dieter Gollmann ..... TU Hamburg-Harburg, Germany
Sokratis Katsikas ..... Univ. of the Aegean, Greece
Angelos D. Keromytis ..... Columbia Univ., USA
Kwangjo Kim ..... ICU, Korea
Chi-Sung Laih ..... NCKU, Taiwan
Ruby Lee ..... Princeton Univ., USA

Helger Lipmaa ..... Univ. of Tartu, Estonia
Josep Lluis Ferrer ..... Univ. Islas Baleares, Spain
Subhamoy Maitra ..... Indian Statistical Institute, India
Masahiro Mambo ..... Univ. of Tsukuba, Japan
Catherine Meadows ..... Naval Research Laboratory, USA
Chris Mitchell ..... RHUL, UK
David Naccache ..... Gemplus, France
Eiji Okamoto ..... Univ. of Tsukuba, Japan
Rolf Oppliger ..... eSECURITY Technologies, Switzerland
Susan Pancho ..... Univ. of the Philippines, Philippines
Hwee-Hwa Pang ..... I2R, Singapore
Rene Peralta ..... Yale Univ., USA
Guenther Pernul ..... Univ. of Regensburg, Germany
Adrian Perrig ..... CMU, USA
Giuseppe Persiano ..... Univ. of Salerno, Italy
Josef Pieprzyk ..... Macquarie Univ., Australia
David Pointcheval ..... ENS, France
Bart Preneel ..... K.U.Leuven, Belgium
Sihan Qing ..... CAS, China
Leonid Reyzin ..... Boston Univ., USA
Vincent Rijmen ..... Graz Univ. of Technology, Austria
Reihaneh Safavi-Naini ..... Univ. of Wollongong, Australia
Kouichi Sakurai ..... Kyushu Univ., Japan
Pierangela Samarati ..... Univ. of Milan, Italy
Shiuhpyng Shieh ..... Chiao Tung Univ., Taiwan
Paul Syverson ..... Naval Research Laboratory, USA
Vijay Varadharajan ..... Macquarie Univ., Australia
Victor K. Wei ..... Chinese Univ. of Hong Kong, China
Moti Yung ..... Columbia Univ., USA
Kan Zhang ..... Independent Consultant, USA
Yuliang Zheng ..... UNCC, USA

Publicity Chair

Guilin Wang ..... Institute for Infocomm Research, Singapore

Organizing Committee

Patricia Loh ..... Institute for Infocomm Research, Singapore
Ying Qiu ..... Institute for Infocomm Research, Singapore

External Reviewers

Michel Abdalla, Joonsang Baek, Claude Barral, Rana Barua, Colin Boyd, Julien Brouchier, Matthew Burnside, Jan Cappaert, Dario Catalano, Dibyendu Chakraborty, Xi Chen, Shirley H.C. Cheung, Benoit Chevallier-Mames, J.H. Chiu, Mathieu Ciet, Andrew Clark, Christian Collberg,

Scott Contini, Debra Cook, Gabriela Cretu, Paolo D'Arco, Tanmoy Kanti Das, Sabrina De Capitani di Vimercati, Breno de Medeiros, Bart De Win, Nenad Dedić, Dimitrios Delivasilis, Alex Dent, Wolfgang Dobmeier, Stelios Dritsas, Jiang Du, Dang Nruyen Duc, J. Dwoskin, Murat Erdem, Nelly Fazio, Pierre-Alain Fouque, Y.J. Fu, Soichi Furuya, Clemente Galdi, Jorg Gilberg, Pierre Girard, D.J. Guan, Junghoon Ha, Helena Handschuh, W.H. He, Y. Hilewitz, Jeff Horton, Ren-Junn Hwang, John Iliadis, Kenji Imamoto, Sarath Indrakanti, Dhem Jean-Francois, Jianchun Jiang, Marc Joye, Georgios Kambourakis, Shinsaku Kiyomoto, P. Kwan, Costas Lambrinoudakis, Peeter Laud, Tri Van Le, Byoungcheon Lee, Homin Lee, Dimitrios Lekkas, GaiCheng Li, Liping Li, Pengfei Li, Zhuowei Li, Vo Duc Liem, Ching Lin, Chu-Hsing Lin, Becky Liu, Michael Locasto, Ling Luo, Hengtai Ma, John Magee, Tal Malkin, John Malone-Lee, Barbara Masucci, Shin'ichiro Matsuo, Vassilios C. Moussas, Bjorn Muschall, Gregory Neven, Lan Nguyen, Antonio Nicolosi, Pascal Paillier, Subhasis Kumar Pal, Janak Parekh, Andreas Pashalidis, Kun Peng, Duong Hieu Phan, Angela Piper, Geraint Price, Torsten Priebe, YongMan Ro, Scott Russell, Palash Sarkar, Naveen Sastry, Christian Schlaeger, Nicholas Sheppard, Igor Shparlinski, Angelos Stavrou, Ron Steinfeld, Hung-Ming Sun, Liuying Tang, Ferucio Tiplea, Dongvu Tonien, Uday K. Tupakula, Yoshifumi Ueshige, Ben Vanik, Lionel Victor, Ivan Visconti, Guilin Wang, Huaxiong Wang, Ke Wang, Xinyuan Wang, Yan Wang, Z. Wang, Weiping Wen, Jan Willemson, Yanxue Xiong, Tommy Yang, Yangjiang Yang, Yiqun Lisa Yin, Quan Yuan, Stefano Zanero, Xianmo Zhang, Weliang Zhao, Qimin Zhou, Huafei Zhu