

# Preface

This volume contains the proceedings of the *6th International Conference on Information and Communications Security (ICICS 2004)*, Torremolinos (Málaga), Spain, 27–29 October 2004. The five previous conferences were held in Beijing, Sydney, Xian, Singapore and Huhehaote City, where we had an enthusiastic and well-attended event. The proceedings were released as volumes 1334, 1726, 2229, 2513 and 2836 of the LNCS series of Springer, respectively.

During these last 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, 245 paper submissions were received. Therefore, the paper selection process was very competitive and difficult – only 42 papers were accepted. The success of the conference depends on the quality of the program. Thus, we are indebted to our Program Committee members and the external referees for the great job they did. These proceedings contain revised versions of the accepted papers. Revisions were not checked and the authors bear full responsibility for the content of their papers.

Other persons deserve many thanks for their contribution to the success of the conference. Prof. José M. Troya was the Conference Chair, and Prof. Eiji Okamoto was General Co-chair. We sincerely thank both of them for their total support and encouragement, and for their contribution to all organizational issues. Our special thanks to José A. Onieva, one of the major driving forces in the organization. He did a great job in the successful promotion of the conference, management of the WebReview application and assistance in the editorial process for the accepted papers. We also thank José A. Montenegro and Isaac Agudo for their help in those tasks. Without the hard work by these colleagues and the other members of the local organization team, this conference would not have been possible.

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

October 2004

Javier López  
Sihan Qing

**ICICS 2004**  
**6th International Conference**  
**on Information and Communications Security**

Málaga, Spain  
October 27–29, 2004

*Organized by*  
Computer Science Department  
University of Málaga  
(Spain)

**Conference Chairman**

José M. Troya

University of Málaga, Spain

**Program Co-chair**

Sihan Qing

Chinese Academy of Sciences, China

**Program Co-chair, General Co-chair**

Javier López

University of Málaga, Spain

**General Co-chair**

Eiji Okamoto

University of Tsukuba, Japan

**Program Committee**

Tuomas Aura

Microsoft Research, UK

Tom Berson

Anagram Laboratories, USA

Jeremy Bryans

University of Newcastle, UK

Alex Biryukov

Katholieke Universiteit Leuven, Belgium

Colin Boyd

Queensland Univ. of Technology, Australia

Chin-Chen Chang

National Chung Cheng University, Taiwan

Joris Claessens

European Microsoft Innov. Center, Germany

George Davida

University of Wisconsin-Milwaukee, USA

Ed Dawson

Queensland Univ. of Technology, Australia

Robert Deng

Institute for Infocomm Research, Singapore

Yvo Desmedt

University College London, UK

Josep Domingo

Universitat Rovira i Virgili, Spain

Pierre-Alain Fouque

École Normale Supérieure, France

Yair Frankel

TechTegrity LLC, USA

Dieter Gollmann	TU Hamburg-Harburg, Germany
Yongfei Han	ONETS, China
Goichiro Hanaoka	University of Tokyo, Japan
Ki-Yoong Hong	Secuve, Korea
Sokratis Katsikas	University of the Aegean, Greece
Kwangjo Kim	Information and Comm. University, Korea
Chi-Sung Laih	National Cheng Kung University, Taiwan
Wenbo Mao	HP Labs. Bristol, UK
Masahiro Mambo	Tohoku University, Japan
Fabio Massacci	Università di Trento, Italy
Catherine Meadows	Naval Research Laboratory, USA
Chris Mitchell	Royal Holloway, UK
Guevara Noubir	Northeastern University, USA
Rene Peralta	Yale University, USA
Giuseppe Persiano	Università di Salerno, Italy
Josef Pieprzyk	Macquarie University, Australia
David Pointcheval	École Normale Supérieure, France
Jean-Jacques Quisquater	Université Catholique de Louvain, Belgium
Kouichi Sakurai	Kyushu University, Japan
Miguel Soriano	Universidad Politécnica de Catalunya, Spain
Routo Terada	University of Sao Paulo, Brazil
Victor K. Wei	Chinese Univ. Hong Kong, China
Vijay Varadharajan	Macquarie University, Australia
Moti Yung	Columbia University, USA
Yulian Zheng	University of North Carolina, USA
Jianying Zhou	Institute for Infocomm Research, Singapore

**External Referees**

Michel Abdalla	Ioanna Kantzavelou	Bart Preneel
Habtamu Abie	Tansel Kaya	Wei Qian
Mohammed Anish	Hyung Kim	Nataliya Rassadko
Nuttapong Attrapadung	Shinsaku Kiyomoto	Jason Reid
Mauro Barni	Tetsutaro Kobayashi	Michael Roe
Lejla Batina	Satoshi Koga	Rodrigo Roman
Giampaolo Bella	Spyros Kokolakis	Carsten Rudolph
Siddika Berna Ors	Hristo Koshutanski	Tatsiana Sabel
Enrico Blanzieri	Hartono Kurnio	Ryuichi Sakai
Andrea Boni	Kaoru Kurosawa	Taiichi Saito
An Braeken	Costas Lambrinouidakis	Francesc Sebé
Mauro Brunato	Joseph Lano	Stefaan Seys
Dario Catalano	Dimitrios Lekkas	SeongHan Shin
Christophe De Canniere	Dequan Li	Leonie Simpson
Roberto Caso	Gaicheng Li	Igor Shparlinski
Jordi Castellà	Jung-Shian Li	Ron Steinfeld
Jung-Hui Chiu	Guolong Lin	Makoto Sugita
Andrew Clark	Liping Li	Toshihiro Tabata
Yang Cui	Anna Lysyanskaya	Keisuke Takemori
Claudia Diaz	Hengtai Ma	Keisuke Tanaka
Jiang Du	Antonio Maña	Liuying Tang
Marcel Fernandez	Carlo Marchetti	Vrizlynn Thing
Ernest Foo	Gwenaëlle Martinet	Theodoros Tzouramanis
Jordi Forne	Antoni Martínez	ZhiMin Sun
Cedric Fournet	Bill Millan	Yoshifumi Ueshige
Martin Gagne	Kunihiko Miyazaki	Chao Wang
Paolo Giorgini	Anish Mohammed	Huaxiong Wang
Andy Gordon	Costas Moulinos	Shuhong Wang
Louis Granboulan	Jose A. Montenegro	Yin Wang
Fabrizio Granelli	Haris Mouratidis	Weiping Wen
Stefanos Gritzalis	Frédéric Muller	Duncan S. Wong
Joshua Goodman	Bill Munro	Hongjun Wu
Juanma Gonzalez-Nieto	Jose L. Muñoz	Mariemma Yague
Jaime Gutierrez	Anderson C.A.	Kira Yamada
DongGu Han	Nascimento	Ching-Nung Yang
Matt Henricksen	Svetla Nikova	Robbie Ye
Yvonne Hitchcock	Masayuki Numao	Nicola Zannone
Yoshiaki Hori	Koji Okada	Rui Zhang
Luigi Lo Iacono	Jose A. Onieva	Yongbin Zhou
John Iliadis	Juan J. Ortega	Xukai Zou
Kenji Imamoto	Thea Peacock	Feng Zhu
QingGuang Ji	Josep Pegueroles	Alf Zugenmaier
Jianchun Jiang	Kun Peng	