Preface

The 2003 Information Security Conference was the sixth in a series that started with the Information Security Workshop in 1997. A distinct feature of this series is the wide coverage of topics with the aim of encouraging interaction between researchers in different aspects of information security. This trend continued in the program of this year's conference.

There were 133 paper submissions to ISC 2003. From these submissions the 31 papers in these proceedings were selected by the program committee, covering a wide range of technical areas. These papers are supplemented by two invited papers; a third invited talk was presented at the conference but is not represented by a written paper.

We would like to extend our sincere thanks to all the authors that submitted papers to ISC 2003, and we hope that those whose papers were declined will be able to find an alternative forum for their work. We are also very grateful to the three eminent invited speakers at the conference: Paul van Oorschot (Carleton University, Canada), Ueli Maurer (ETH Zürich, Switzerland), and Andy Clark (Inforenz Limited, UK).

We were fortunate to have an energetic team of experts who took on the task of the program committee. Their names may be found overleaf, and we thank them warmly for their considerable efforts. This team was helped by an even larger number of individuals who reviewed papers in their particular areas of expertise. A list of these names is also provided, which we hope is complete.

We are delighted to acknowledge the generous financial sponsorship of ISC 2003 by HP Labs, Bristol and Microsoft Research, Cambridge. The British Computer Society are also thanked for their support. The excellent local organizing committee consisted of Vivienne Paulete, Michelle Davies, and Jan Ward. We would like to thank Eiji Okamoto and Javier Lopez who invited us to chair the conference and provided advice and support through all the preparations. We made use of the electronic submission and reviewing software supplied by COSIC at the Katholieke Universiteit Leuven. The software was run on the ISRC's server at QUT and perfectly maintained by Andrew Clark.

July 2003

Colin Boyd
Wenbo Mao

Information Security Conference 2003

October 1-3, 2003, Bristol, UK

General Chair and Program Co-chair

Wenbo Mao, Hewlett-Packard Laboratories, Bristol, United Kingdom

Program Co-chair

Colin Boyd, Queensland University of Technology, Australia

Program Committee

Masayuki Abe ..... NTT Laboratories, Japan
Tuomas Aura ..... Microsoft Research, UK
Feng Bao ..... Institute for Infocomm Research, Singapore
Jan Camenisch ..... IBM Research, Switzerland
Josep Domingo-Ferrer ..... Universitat Rovira i Virgili, Spain
Yair Frankel ..... TechTegrity, USA
Steven Galbraith ..... Royal Holloway, University of London, UK
Virgil Gligor ..... University of Maryland, USA
Li Gong ..... Sun Microsystems, China
Stuart Haber ..... Hewlett-Packard Laboratories, USA
Marc Joye ..... Gemplus, France
Charlie Kaufman ..... IBM, USA
Kwangjo Kim ..... Information and Communications University, Korea
Chi Sung Laih ..... Chengkung University, Taiwan
Helger Lipmaa ..... Helsinki University of Technology, Finland
Javier Lopez ..... University of Malaga, Spain
Catherine Meadows ..... Naval Research Laboratory, USA
Phong Nguyen ..... CNRS/ENS, France
Eiji Okamoto ..... University of Tsukuba, Japan
Michael Reiter ..... Carnegie-Mellon University, USA
Phillip Rogaway ..... University of California, Davis, USA
Akashi Satoh ..... IBM Research, Japan
Steve Schneider ..... Royal Holloway, University of London, UK
Nigel Smart ..... University of Bristol, UK
Paul van Oorschot ..... Carleton University, Canada
Vijay Varadharajan ..... Macquarie University, Australia
Serge Vaudenay ..... EPFL, Switzerland
Moti Yung ..... Columbia University, USA
Yuliang Zheng ..... University of North Carolina, USA

External Reviewers

Isaac Agudo
Gildas Avoine
Joonsang Baek
Endre Bangerter
Simon Blackburn
Rakesh Bobba
Alexandra Boldyreva
Emmanuel Bresson
Ahto Buldas
Mike Burmester
Benoit Chevallier-Mames
Olivier Chevassut
Jung-Hui Chiu
Andrew Clark
Christophe Clavier
Chris I. Dalton
Ed Dawson
Roberto Delicata
Neil Evans
Babak Falsafi
Cedric Fournet
Mike Freedman
Eiichiro Fujisaki
Debin Gao
Craig Gentry
Louis Granboulan
Gael Hachez
Helena Handschuh
Chris Heneghan
Florian Hess
Herbie Hopkins
Bill Horne
Himanshu Khurana
R. Koleva
Susanna Leisten
Vo Duc Liem
Yi Lu
John Malone-Lee
Antonio Maña
Keith Martin
Lauren May
James McKee
George Mohay
Jose A. Montenegro
Scott Moskowitz
Sean Murphy
Chanathip Namprempre
Gregory Neven
Philippe Oechslin
Katsuyuki Okeya
Francis Olivier
Juan J. Ortega
Dan Page
Kenny Paterson
Benny Pinkas
David Pointcheval
Jonathan Poritz
Jason Reid
Matt Robshaw
Rei Safavi-Naini
Tomas Sander
Mike Scott
Francesc Sebé
Jamshid Shokrollahi
Igor Shparlinski
Jessica Staddon
Ron Steinfeld
Koutaro Suzuki
Mike Szydlo
Gelareh Taban
Frederik Vercauteren
Mariemma Yague
Sung-Ming Yen
Alf Zugenmaier

http://www.springer.com/978-3-540-20176-2

Information Security
6th International Conference, ISC 2003, Bristol, UK, October 1-3, 2003, Proceedings
Boyd, C.; Mao, W. (Eds.)
2003, XII, 448 p., Softcover
ISBN: 978-3-540-20176-2