

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