Lecture Notes in Computer Science 2200

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Tokyo

George I. Davida Yair Frankel (Eds.)

Information Security

4th International Conference, ISC 2001
Malaga, Spain, October 1-3, 2001
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

George I. Davida
University of Wisconsin-Milwaukee, Department of EECS
Milwaukee, WI 53201, USA
E-mail: davida@cs.uwm.edu

Yair Frankel
Techtegrity, LLC
122 Harrison, Westfield NJ 07090, USA
E-mail: yfrankel@cryptographers.com

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information security : 4th international conference ; proceedings / ISC 2001, Malaga, Spain, October 1 - 3, 2001. George I. Davida ; Yair Frankel (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2001
(Lecture notes in computer science ; Vol. 2200)
ISBN 3-540-42662-0

CR Subject Classification (1998): E.3, D.4.6, K.6.5, F.2.1, C.2, J.1, C.3

ISSN 0302-9743
ISBN 3-540-42662-0 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Stefan Sossna
Printed on acid-free paper SPIN: 10840698 06/3142 5 4 3 2 1 0

Preface

The Information Security Conference 2001 brought together individuals involved in multiple disciplines of information security to foster the exchange of ideas. The conference, an outgrowth of the Information Security Workshop (ISW) series, was held in Málaga, Spain, on October 1–3, 2001. Previous workshops were ISW '97 at Ishikawa, Japan; ISW '99 at Kuala Lumpur, Malaysia; and ISW 2000 at Wollongong, Australia. The General Co-chairs, Javier López and Eiji Okamoto, oversaw the local organization, registration, and performed many other tasks.

Many individuals deserve thanks for their contribution to the success of the conference. José M. Troya was the Conference Chair. The General Co-chairs were assisted with local arrangements by Antonio Maña, Carlos Maraval, Juan J. Ortega, José M. Sierra, and Miguel Soriano.

This was the first year that the conference accepted electronic submissions. Many thanks to Dawn Gibson for assisting in developing and maintaining the electronic submission servers. The conference received 98 submissions of which 37 papers were accepted for presentation. These proceedings contain revised versions of the accepted papers. Revisions were not checked and the authors bear full responsibility for the contents of their papers.

The Program Committee consisted of Elisa Bertino, Università di Milano; G. R. Blakely, Texas A&M University; John Daugman, Cambridge University; Jorge Dávila, Polytechnic Univ. of Madrid; Giovanni DiCrescenzo, Telcordia; Josep Domingo-Ferrer, Univ. Rovira i Virgili; Dieter Gollmann, Microsoft Research; Sigrid Guergens, GMD; Hiroaki Kikuchi, Tokai University; Chi-Sung Laih, Natl. Cheng Kung Univ.; Wenbo Mao, HP Laboratories; Masahiro Mambo, Tohoku University; Catherine Meadows, NRL; Sang-Jae Moon, Kyungpook Natl. University; Yuko Murayama, Iwate Prefectural University; René Peralta, Yale University; Josef Pieprzyk, University of Wollongong; Sihan Qing, Chinese Academy of Sciences; Susie Thomson, Datacard; Routo Terada, Univ. of S. Paulo; Yiannis Tsiounis, InternetCash; Moti Yung, Certco; Yuliang Zheng, Monash University; Jianying Zhou, Oracle Corp. Members of the committee spent numerous hours in reviewing papers and providing advice. The committee was also assisted by our colleagues: Marc Alba, Clemente Galdi, Sang-Wook Kim, Yi Mu, Anna Oganian, Francesc Sebé, Rajan Shankaran, Igor Shparlinski. We apologize for any inadvertent omissions. Our thanks to the program committee and all reviewers.

We thank all the authors who submitted papers to this conference. Without their submissions this conference could not have been a success.

July 2001

George I. Davida
Yair Frankel

Information Security Conference 2001

October 1–3, 2001, Málaga, Spain

Conference Chair

José M. Troya, University of Málaga (Spain)

General Co-chairs

Javier López, University of Málaga (Spain)
Eiji Okamoto, Toho University (Japan)

Program Co-chair

George I. Davida, University of Wisconsin-Milwaukee (USA)
Yair Frankel, TechTegrity L.L.C. (USA)

Program Committee

Elisa Bertino ..... Università di Milano (Italy)
G. R. Blakely..... Texas A&M University (USA)
John Daugman ..... Cambridge University (UK)
Jorge Dávila ..... Polytechnic Univ. of Madrid (Spain)
Giovanni DiCrescenzo ..... Telcordia (USA)
Josep Domingo-Ferrer..... Univ. Rovira i Virgili (Spain)
Dieter Gollmann..... Microsoft Research (UK)
Sigrid Guergens ..... GMD (Germany)
Hiroaki Kikuchi ..... Tokai University (Japan)
Chi-Sung Laih..... Natl. Cheng Kung Univ. (Taiwan)
Wenbo Mao..... HP Laboratories (UK)
Masahiro Mambo ..... Tohoku University (Japan)
Catherine Meadows..... NRL (USA)
Sang-Jae Moon ..... Kyungpook Natl. University (Korea)
Yuko Murayama ..... Iwate Prefectural University (Japan)
Rene Peralta ..... Yale University (USA)
Josef Pieprzyk ..... University of Wollongong (Australia)
Sihan Qing ..... Chinese Academy of Sciences (China)
Susie Thomson..... Datacard (UK)
Routo Terada..... Univ. of S. Paulo (Brazil)
Yiannis Tsiounis ..... InternetCash (USA)
Moti Yung..... CertCo (USA)
Yuliang Zheng ..... Monash University (Australia)
Jianying Zhou ..... Oracle Corp. (USA)

Table of Contents

Key Distribution

Protocols

Enhancing Technologies

Privacy

Software Protection

Message Hiding I

PKI Issues and Protocols

Hardware Implementations

Cryptanalysis and Prevention

Implementations

Non-repudiation Techniques

Contracts and Auctions

Message Hiding II

Payments

Security Applications

Network and OS Security