Lecture Notes in Computer Science 1975

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

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

Josef Pieprzyk Eiji Okamoto
Jennifer Seberry (Eds.)

Information Security

Third International Workshop, ISW 2000
Wollongong, Australia, December 20-21, 2000
Proceedings

Springer

Series Editors

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

Volume Editors

Josef Pieprzyk
Jennifer Seberry
Wollongong University
School of Information Technology and Computer Science
Center for Computer Security Research
Wollongong, NSW 2522, Australia
E-mail: {josef/j.seberry}@uow.edu.au

Eiji Okamoto
Toho University, Faculty of Science
Department of Information Science
2-2-1, Miyama, Funabashi, Chiba 274-8510, Japan
E-mail: okamoto@sci.toho-u.ac.jp

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information security : third international workshop ; proceedings /
ISW 2000, Wollongong, Australia, December 20 - 21, 2000.
Josef Pieprzyk . . . (ed.)_. - Berlin ; Heidelberg ; New York ; Barcelona ;
Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2000
(Lecture notes in computer science ; Vol. 1975)
ISBN 3-540-41416-9

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

ISSN 0302-9743
ISBN 3-540-41416-9 Springer-Verlag Berlin Heidelberg New York

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

Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Stefan Sossna
Printed on acid-free paper SPIN: 10781179 06/3142 5 4 3 2 1 0

Preface

The third International Workshop on Information Security was held at the University of Wollongong, Australia. The conference was sponsored by the Centre for Computer Security Research, University of Wollongong. The main themes of the conference were the newly emerging issues of Information Security. Multimedia copyright protection and security aspects of e-commerce were two topics that clearly reflect the focus of the conference. Protection of the copyright of electronic documents seems to be driven by strong practical demand from the industry for new, efficient and secure solutions. Although e-commerce is already booming, it has not reached its full potential in terms of new, efficient and secure e-commerce protocols with added properties.

There were 63 papers submitted to the conference. The program committee accepted 23. Of those accepted, six papers were from Australia, five from Japan, two each from Spain, Germany and the USA, and one each from Finland and Sweden. Four papers were co-authored by international teams from Canada and China, Korea and Australia, Taiwan and Australia, and Belgium, France and Germany, respectively.

Final versions of the accepted papers were gathered using computing and other resources of the Institute of Mathematics, Polish Academy of Sciences, Warsaw, Poland. We are especially grateful to Jerzy Urbanowicz and Andrzej Pokrzywa for their help during preparation of the proceedings.

We would like to thank the members of the program committee who gave generously of their time to read and evaluate papers. We would also like to thank members of the organising committee. Finally we thank the authors of all the submitted papers, in particular the accepted ones, and all the participants who contributed to the success of the conference.

October 2000

Josef Pieprzyk
Eiji Okamoto
Jennifer Seberry

THIRD INFORMATION SECURITY WORKSHOP ISW2000

Sponsored by

Center for Computer Security Research
University of Wollongong, Australia

General Chair:

Jennifer Seberry — *University of Wollongong, Australia*

Program Co-chairs:

Josef Pieprzyk — *University of Wollongong, Australia*
Eiji Okamoto — *University of Wisconsin-Milwaukee, USA*

Program Committee:

George Davida — *University of Wisconsin-Milwaukee, USA*
Josep Domingo-Ferrer — *University of Rovira i Virgili, Spain*
Ed Dawson — *Queensland University of Technology, Australia*
Thomas Hardjono — *Nortel Networks, USA*
Hiroaki Kikuchi — *Tokai University, Japan*
Masahiro Mambo — *Tohoku University, Japan*
Yi Mu — *Western Sydney University, Australia*
Fabien Petitcolas — *Microsoft Research, UK*
Vijay Varadharajan — *Western Sydney University, Australia*
Yuliang Zheng — *Monash University, Australia*

Referees

Marc Alba
Jordi Castellá
Ed Dawson
Josep Domingo-Ferrer
Cédric Fournet
Dieter Gollmann
Goichiro Hanaoka
Thomas Hardjono
J. Herrera-Joancomartí
Stefan Katzenbeisser
Hiroaki Kikuchi
Helger Lipmaa
Patrick Loo
Masahiro Mambo
Kenta Matsuura
Yi Mu
Yuko SJ Murayama
Kenny Nguyen

Khanh Quoc Nguyen
Ryutarou Ohbuchi
Eiji Okamoto
Adrian Perrig
Fabien Petitcolas
Josef Pieprzyk
Michael Roe
Francesc Sebé
Mitsuru Tada
Yuji Watanabe
Bennet Yee
Yuliang Zheng

Table of Contents

Multimedia Copyright Protection

E-Commerce

Key Management

Network Security and Access Control

Cryptographic Systems