

Lecture Notes in Computer Science
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

1975

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

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH
© Springer-Verlag Berlin Heidelberg 2000
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
Eiji Okamoto

*University of Wollongong, Australia
University of Wisconsin-Milwaukee, USA*

Program Committee:

George Davida
Josep Domingo-Ferrer
Ed Dawson
Thomas Hardjono
Hiroaki Kikuchi
Masahiro Mambo
Yi Mu
Fabien Petitcolas
Vijay Varadharajan
Yuliang Zheng

*University of Wisconsin-Milwaukee, USA
University of Rovira i Virgili, Spain
Queensland University of Technology, Australia
Nortel Networks, USA
Tokai University, Japan
Tohoku University, Japan
Western Sydney University, Australia
Microsoft Research, UK
Western Sydney University, Australia
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

VIII Organization

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

A Watermarking Scheme Based on the Characteristic of Addition among DCT Coefficients <i>Minoru Kuribayashi and Hatsukazu Tanaka</i>	1
Affine Invariant Watermarks for 3D Polygonal and NURBS Based Models <i>Oliver Benedens</i>	15
A Steganographic Framework for Reference Colour Based Encoding and Cover Image Selection <i>René Rosenbaum and Heidrun Schumann</i>	30
Spatial-Domain Image Watermarking Robust against Compression, Filtering, Cropping, and Scaling <i>Francesc Sebé, Josep Domingo-Ferrer, and Jordi Herrera</i>	44
Region-Based Watermarking by Distribution Adjustment <i>Gareth Brisbane, Rei Safavi-Naini, and Philip Ogunbona</i>	54
Hiding Information in Color Images Using Small Color Palettes <i>Tapio Seppänen, Kaisu Mäkelä, and Anja Keskinarkaus</i>	69
An Approach to the Objective and Quantitative Evaluation of Tamper-Resistant Software <i>Hideaki Goto, Masahiro Mambo, Kenjiro Matsumura, and Hiroki Shizuya</i> ..	82
Characteristics of Some Binary Codes for Fingerprinting <i>Tina Lindkvist</i>	97

E-Commerce

An Anonymous Auction Protocol with a Single Non-trusted Center Using Binary Trees <i>Kazumasa Omote and Atsuko Miyaji</i>	108
Unlinkable Divisible Electronic Cash <i>Toru Nakanishi and Yuji Sugiyama</i>	121
Weighted One-Way Hash Chain and Its Applications <i>Sung-Ming Yen and Yuliang Zheng</i>	135
Linkability in Practical Electronic Cash Design <i>Greg Maitland, Jason Reid, Ernest Foo, Colin Boyd, and Ed Dawson</i>	149

Towards a Practical Secure Framework for Mobile Code Commerce
*Gaël Hachez, Laurent Den Hollander, Mehrdad Jalali,
Jean-Jacques Quisquater, and Christophe Vasserot*.....164

Key Management

Probabilistic Methods in Multicast Key Management
Ali Aydın Selçuk and Deepinder Sidhu.....179

Classification of Authentication Protocols: A Practical Approach
DongGook Park, Colin Boyd, and Ed Dawson.....194

Exploring Fair Exchange Protocols Using Specification Animation
Colin Boyd and Peter Kearney.....209

A Practical Implementation of Hierarchically Structured Key Predistribution System and Its Evaluation
Daisuke Nojiri, Goichiro Hanaoka, and Hideki Imai.....224

Network Security and Access Control

An Efficient Protocol for Certified Electronic Mail
*Josep Lluís Ferrer-Gomila, Magdalena Payeras-Capellà, and
Llorenç Huguet i Rotger*.....237

Performance Analysis of Secure Web Server Based on SSL
Xiaodong Lin, Johnny W. Wong, and Weidong Kou.....249

Sherlock: Commercial High Assurance Network Computing
*Stephen P. Morgan, Stephen W. Neal, Melissa A. Hartman, and
Matthew R. Laue*.....262

The Role of the Development Process in Operating System Security
Christian Payne.....277

Cryptographic Systems

Threshold Fail-Stop Signature Schemes Based
on Discrete Logarithm and Factorization
Rei Safavi-Naini and Willy Susilo.....292

A Signcryption Scheme Based on Integer Factorization
Ron Steinfeld and Yuliang Zheng.....308

Author Index.....**323**