Lecture Notes in Computer Science 1729
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

Masahiro Mambo Yuliang Zheng (Eds.)

Information Security

Second International Workshop, ISW'99
Kuala Lumpur, Malaysia, November 6-7, 1999
Proceedings

Springer

Series Editors

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

Volume Editors

Masahiro Mambo
Tohoku University, Education Center for Information Processing
Kawauchi Aoba Sendai, 980-8576, Japan
E-mail: mambo@ecip.tohoku.ac.jp

Yuliang Zheng
Monash University, School of Computer and Information Technology
MacMahons Road, Frankston, Melbourne, Victoria 3199, Australia
E-mail: yuliang.zheng@infotech.monash.edu.au

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information security : second international workshop ; proceedings / ISW '99, Kuala Lumpur, Malaysia, November 6 - 7, 1999. Masahiro Mambo ; Yuliang Zheng (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1999
(Lecture notes in computer science ; Vol. 1729)
ISBN 3-540-66695-8

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

ISSN 0302-9743
ISBN 3-540-66695-8 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN: 10703333 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

The 1999 International Information Security Workshop, ISW'99, was held on Monash University's Malaysia Campus, which is about 20km to the south west of downtown Kuala Lumpur, November 6-7, 1999.

ISW'99 sought a different goal from its predecessor, ISW'97, held in Ishikawa, Japan, whose proceedings were published as Volume 1396 of Springer Verlag's LNCS series. The focus of ISW'99 was on the following emerging areas of importance in information security: multimedia watermarking, electronic cash, secure software components and mobile agents, and protection of software.

The program committee received 38 full submissions from 12 countries and regions: Australia, China, France, Germany, Hong Kong, Japan, Korea, Malaysia, Singapore, Spain, Taiwan, and USA, and selected 23 of them for presentation. Among the 23 presentations, 19 were regular talks and the remaining 4 were short talks. Each submission was reviewed by at least two expert referees.

We are grateful to the members of the program committee for reviewing and selecting papers in a very short period of time. Their comments helped the authors improve the final version of their papers. Our thanks also go to Patrick McDaniel, Masaji Kawahara, and Yasuhiro Ohtaki who assisted in reviewing papers. In addition, we would like to thank all the authors, including those whose submissions were not accepted, for their contribution to the success of this workshop.

The workshop was organized with the help of local committee members, including Cheang Kok Soon, Hiew Pang Leang, Lily Leong, and Robin Pollard. We appreciate their patience and professionalism. Robin Pollard led the committee as a general co-chair. We owe the success of the workshop to him as well as general co-chair Eiji Okamoto.

November 1999

Masahiro Mambo
Yuliang Zheng

Information Security Workshop (ISW'99)

Organizing Committee

Eiji Okamoto (**Co-chair**, Univ. of Wisconsin, Milwaukee, USA)
Robin Pollard (**Co-chair**, Monash University, Malaysia)
Hiew Pang Leang (Monash University, Malaysia)
Lily Leong (Monash University, Malaysia)
Cheang Kok Soon (Monash University, Malaysia)

Program Committee

Masahiro Mambo, (**Co-chair**, Tohoku University, Japan)
Yuliang Zheng, (**Co-chair**, Monash University, Australia)
David Aucsmith (Intel, USA)
George Davida (University of Wisconsin-Milwaukee, USA)
Robert H. Deng (Kent Ridge Digital Labs, Singapore)
Steven J. Greenwald (Independent Consultant, USA)
Ryoichi Mori (Superdistribution Laboratory, Japan)
Kazuo Ohta (NTT, Japan)
Aviel Rubin (AT&T Labs - Research, USA)
Andrew Z Tirkel (Monash University, Australia)
Moti Yung (CertCo, USA)

Contents

Digital Watermarking

Protection of Software and Data

Electronic Money, Key Recovery, and Electronic Voting

Digital Signatures