

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

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 1999
Printed in Germany

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

Electronic Money

Spending Programs: A Tool for Flexible Micropayments	1
<i>Josep Domingo-Ferrer and Jordi Herrera-Joancomartí (Uni Rovira i Virgili, Spain)</i>	
Money Conservation via Atomicity in Fair Off-Line E-Cash	14
<i>Shouhuai Xu (Fudan Univ., P. R. China), Moti Yung (CertCo, USA), Gendu Zhang, and Hong Zhu (Fudan Univ., P. R. China)</i>	
Engineering an eCash System.....	32
<i>Tim Ebringer and Peter Thorne (Univ. of Melbourne, Australia)</i>	

Electronic Payment and Unlinkability

Unlinkable Electronic Coupon Protocol with Anonymity Control	37
<i>Toru Nakanishi, Nobuaki Haruna, and Yuji Sugiyama (Okayama Univ., Japan)</i>	
On the Security of the Lee-Chang Group Signature Scheme and Its Derivatives	47
<i>Marc Joye (Gemplus, France), Narn-Yih Lee (Nan-Tai Inst. of Tech., Taiwan, R.O.C.), and Tzonelih Hwang (Cheng-Kung Univ., Taiwan, R.O.C.)</i>	

Secure Software Components, Mobile Agents, and Authentication

Security Properties of Software Components	52
<i>Khaled Khan, Jun Han, and Yuliang Zheng (Monash Univ., Australia)</i>	
Methods for Protecting a Mobile Agent's Route	57
<i>Dirk Westhoff, Markus Schneider, Claus Unger, and Firoz Kaderali (Fern Uni. Hagen, Germany)</i>	
Non-interactive Cryptosystem for Entity Authentication	72
<i>Hyung-Woo Lee (Chonan Univ., Korea), Jung-Eun Kim, and Tai-Yun Kim (Korea Univ., Korea)</i>	

Network Security

Implementation of Virtual Private Networks at the Transport Layer	85
<i>Jorge Davila (Uni Politecnica de Madrid, Spain), Javier Lopez (Uni de Malaga, Spain), and Rene Peralta (Univ. of Wisconsin-Milwaukee, USA)</i>	

Performance Evaluation of Certificate Revocation Using k -Valued Hash Tree	103
<i>Hiroaki Kikuchi, Kensuke Abe, and Shohachiro Nakanishi (Tokai Univ., Japan)</i>	

Active Rebooting Method for Proactivized System: How to Enhance the Security against Latent Virus Attacks	118
<i>Yuji Watanabe and Hideki Imai (Univ. of Tokyo, Japan)</i>	

Digital Watermarking

Highly Robust Image Watermarking Using Complementary Modulations ..	136
<i>Chun-Shien Lu, Hong-Yuan Mark Liao, Shih-Kun Huang, and Chwen-Jye Sze (Academia Sinica, Taiwan, R.O.C.)</i>	

Region-Based Watermarking for Images	154
<i>Gareth Brisbane, Rei Safavi-Naini (Wollongong, Australia), and Philip Ogunbona (Motorola Australian Research Center, Australia)</i>	

Digital Watermarking Robust Against JPEG Compression	167
<i>Hye-Joo Lee, Ji-Hwan Park (PuKyong Nat'l Univ., Korea), and Yuliang Zheng (Monash Univ., Australia)</i>	

Protection of Software and Data

Fingerprints for Copyright Software Protection	178
<i>Josef Pieprzyk (Univ. of Wollongong, Australia)</i>	

A Secrecy Scheme for MPEG Video Data Using the Joint of Compression and Encryption	191
<i>Sang Uk Shin, Kyeong Seop Sim, and Kyung Hyune Rhee (PuKyong Nat'l Univ., Korea)</i>	

Electronic Money, Key Recovery, and Electronic Voting

On Anonymous Electronic Cash and Crime	202
<i>Tomas Sander and Amnon Ta-Shma (Int'l Computer Science Inst., USA)</i>	

On the Difficulty of Key Recovery Systems	207
<i>Seungjoo Kim, Insoo Lee (KISA, Korea), Masahiro Mambo (Tohoku Univ., Japan), and Sungjun Park (KISA, Korea)</i>	

An Improvement on a Practical Secret Voting Scheme	225
<i>Miyako Ohkubo, Fumiaki Miura, Masayuki Abe, Atsushi Fujioka, and Tatsuaki Okamoto (NTT Inf. Sharing Platform Lab., Japan)</i>	

Digital Signatures

Undeniable Confirmer Signature	235
<i>Khanh Nguyen, Yi Mu, and Vijay Varadharajan (Univ. of Western Sydney, Australia)</i>	
Extended Proxy Signatures for Smart Cards	247
<i>Takeshi Okamoto, Mitsuru Tada (JAIST, Japan), and Eiji Okamoto (Univ. of Wisconsin-Milwaukee, USA)</i>	
A New Digital Signature Scheme on ID-Based Key-Sharing Infrastructures	259
<i>Tsuyoshi Nishioka (Mitsubishi Electric Corp., Japan), Goichiro Hanaoka, and Hideki Imai (Univ. of Tokyo, Japan)</i>	
Cryptanalysis of Two Group Signature Schemes	271
<i>Marc Joye (Gemplus, France), Seungjoo Kim (KISA, Korea), and Narn-Yih Lee (Nan-Tai Inst. of Tech., Taiwan, R.O.C.)</i>	
Author Index	277