Lecture Notes in Computer Science 1396
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Eiji Okamoto George Davida
Masahiro Mambo (Eds.)

Information Security

First International Workshop, ISW'97
Tatsunokuchi, Ishikawa, Japan
September 17-19, 1997
Proceedings

Springer

Series Editors

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

Volume Editors

Eiji Okamoto
School of Information Science
Japan Advanced Institute of Science and Technology
1-1 Asahidai Tatsunokuchi Nomi Ishikawa, 923-1292 Japan
E-mail: okamoto@jaist.ac.jp

George Davida
Department of Electrical Engineering and Computer Science
University of Wisconsin-Milwaukee
3200 N. Cramer Street, Milwaukee, WI 53201, USA
E-mail: davida@cs.uwm.edu

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

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information security : first international workshop ; proceedings / ISW '97, Tatsunokuchi, Ishikawa, Japan, September 17 - 19, 1997. George Davida ... (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1998
(Lecture notes in computer science ; Vol. 1396)
ISBN 3-540-64382-6

CR Subject Classification (1991): E.3, G.2.1, D.4.6, K.6.5,F.2.1-2, C.2, J.1, E.4

ISSN 0302-9743
ISBN 3-540-64382-6 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10636992 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

ISW'97, the 1997 Information Security Workshop, was held at the Ishikawa High-Tech Conference Center in JAIST, Japan Advanced Institute of Science and Technology, Ishikawa, Japan, September 17-19. The workshop was sponsored by JAIST, Ministry of Education, Science, Sports and Culture, Engineering Sciences Society of IEICE (The Institute of Electronics, Information and Communication Engineers), Telecommunications Advancement Foundation, and Ishikawa Prefecture. The workshop was organized in cooperation with Tokyo Chapter of IEEE Information Theory, and Society of Information Theory and Its Applications. We are grateful to all these organizations for their support of the workshop.

One of the goals of ISW'97 was to give young researchers into the field of information security an opportunity to present papers at an international conference. For that purpose, a number of stipends were available to those unable to obtain funding to attend the workshop.

The workshop program addressed a range of topics from theory, technique, applications, and experimental work on topics relevant to information security and cryptography. The program committee invited Dr. Mihir Bellare (University of California at San Diego), Dr. Yvo Desmedt (University of Wisconsin at Milwaukee), Dr. Bart Preneel (Katholieke Universiteit Leuven, Belgium) and Dr. Yuliang Zheng (Monash University, Australia). Dr. George Robert Blakley (Texas A&M University) opened the workshop with general code theory and Dr. René Peralta (University of Wisconsin at Milwaukee) had a special talk on fast software encryption. Their talks were stimulating and informative.

The program committee accepted 25 papers from 39 submissions covering cryptanalysis, public-key cryptosystem, signature, hardware/software implementation, key management, key sharing, security management, electronic commerce and quantum cryptology. The accepted papers came from many countries: Australia, Belgium, Brazil, China, India, Korea, Singapore, Taiwan, USA, United Kingdom, and Japan. We commend the members of the program committee for this excellent program.

Organizing an international workshop is a time-consuming task. We would like to thank the steering committee members, organizing committee members, JAIST section for academic exchanges, and JAIST students in Dr. Okamoto's Laboratory for helping with many local details. We also thank all session chairs, speakers and authors who submitted papers and all participants at ISW'97.

February 1998

Eiji Okamoto
George Davida
Masahiro Mambo

Information Security Workshop (ISW'97)

Sponsored by
Japan Advanced Institute of Science and Technology
The Engineering Sciences Society of IEICE
The Ministry of Education, Science, Sports and Culture
The Telecommunications Advancement Foundation
Ishikawa Prefecture

In cooperation with
IEEE IT Society, Tokyo Chapter, and SITA

Steering Committee

Masayuki Kimura (**Co-chair**, JAIST, Japan)
Bob Blakley(**Co-chair**, Texas A&M, USA)
Masayasu Hata (Nagoya Inst. of Tech., Japan)
Hideki Imai (Univ. of Tokyo, Japan)
Yoshihiro Iwadare (Nagoya Univ., Japan)
Masao Kasahara (Kyoto Inst. of Tech., Japan)
Hatsukazu Tanaka (Kobe Univ., Japan)
Hideyoshi Tominaga (Waseda Univ., Japan)
Shigeo Tsujii (Chuo Univ., Japan)

Program Committee

George Davida (**Co-chair**, Univ. of Wisconsin, Milwaukee, USA)
Eiji Okamoto (**Co-chair**, JAIST, Japan)
Jinhui Chao (Chuo Univ., Japan)
Ivan Damgård (Århus Univ., Denmark)
Toru Fujiwara (Osaka Univ., Japan)
Akira Hayashi (Kanazawa Inst. of Tech., Japan)
Tzonelih Hwang (Cheng Kung Univ., Taiwan, R.O.C)
Toshiya Itoh (Tokyo Inst. of Tech., Japan)
Kunikatsu Kobayashi (Yamagata Univ., Japan)
Naohisa Komatsu (Waseda Univ., Japan)
Arjen Lenstra (Citibank, USA)
Tsutomu Matsumoto (Yokohama National Univ., Japan)
Shiho Moriai (TAO, Japan)
Yuko Murayama (Hiroshima City Univ., Japan)
Andrew Odlyzko (AT&T, USA)

Contents

Special Lecture

Key Management

Invited Lecture

Implementation(Hard/Soft)

Invited Lecture

Security Management

Signature/Authentication

Invited Lecture

Payment Scheme

Key Sharing