Lecture Notes in Computer Science 4867

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Sehun Kim Moti Yung
Hyung-Woo Lee (Eds.)

Information Security Applications

8th International Workshop, WISA 2007
Jeju Island, Korea, August 27-29, 2007
Revised Selected Papers

Springer

Volume Editors

Sehun Kim
KAIST, Department of Industrial Engineering
373-1, Guseong-dong, Yuseong-gu, Daejeon, 305-701, Korea
E-mail: shkim@kaist.ac.kr

Moti Yung
Google Inc.
Columbia University, Computer Science Department
RSA Laboratories
S.W.Mudd Building, New York, NY10027, USA
E-mail: moti@cs.columbia.edu

Hyung-Woo Lee
Hanshin University
School of Computer Engineering
411, Yangsan-dong, Osan, Gyunggi, 447-791, Korea
E-mail: hwlee@hs.ac.kr

Library of Congress Control Number: 2007942182

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-77534-X Springer Berlin Heidelberg New York
ISBN-13 978-3-540-77534-8 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12210664 06/3180 5 4 3 2 1 0

Preface

The 8th International Workshop on Information Security Applications (WISA 2007) was held on Jeju Island, Korea during August 27–29, 2007. The workshop was sponsored by the Korea Institute of Information Security and Cryptology (KIISC), the Electronics and Telecommunications Research Institute (ETRI) and the Ministry of Information and Communication (MIC).

WISA aims at providing a forum for professionals from academia and industry to present their work and to exchange ideas. The workshop covers all technical aspects of security applications, including cryptographic and non-cryptographic techniques.

We were very pleased and honored to serve as the Program Committee Co-chairs of WISA 2007. The Program Committee received 95 papers from 20 countries, and accepted 27 papers for the full presentation track. The papers were selected after an extensive and careful refereeing process in which each paper was reviewed by at least three members of the Program Committee.

In addition to the contributed papers, the workshop had three special talks. Moti Yung gave a tutorial talk, entitled "Somebody You Know: The Fourth Factor of Authentication." Kihong Park and Nasir Memon gave invited talks, entitled "Reactive Zero-Day Attack Protection" and "Securing Biometric Templates," respectively.

Many people deserve our gratitude for their generous contributions to the success of the workshop. We would like to thank all the people involved in the technical program and in organizing the workshop. We are very grateful to the Program Committee members and the external referees for their time and efforts in reviewing the submissions and selecting the accepted papers. We also express our special thanks to the Organizing Committee members for their hard work in organizing the workshop.

Last but not least, on behalf of all those involved in organizing the workshop, we would like to thank all the authors who submitted papers to this workshop. Without their submissions and support, WISA could not have been a success.

December 2007

Sehun Kim
Moti Yung
Hyung-Woo Lee

Organization

Advisory Committee

Man-Young Rhee	Kyung Hee University, Korea
Hideki Imai	Tokyo University, Japan
Mun Kee Choi	ETRI, Korea
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Kil-Hyun Nam	Korea National Defense University, Korea
Sang-Jae Moon	Kyungpook National University, Korea
Dong-Ho Won	Sungkyunkwan University, Korea
Pil-Joong Lee	POSTECH, Korea
Dae-Ho Kim	NSRI, Korea
Joo-Seok Song	Yonsei University, Korea

General Co-chairs

Min Surp Rhee	Dankook University, Korea
Sung-Won Sohn	ETRI, Korea

Steering Committee

Kyo-Il Chung	ETRI, Korea
TaeKyoung Kwon	Sejong University, Korea
Im-Yeong Lee	Soonchunhyang University, Korea
Dong-Il Seo	ETRI, Korea
OkYeon Yi	Kookmin University, Korea
Jae-Kwang Lee	Hannam University, Korea

Organizing Committee

Chair	Sang Choon Kim	Kangwon National University, Korea
Finance	Taenam Cho	Woosuk University, Korea
Publication	Ji-Young Lim	Korean Bible University, Korea
Publicity	Gang Shin Lee	KISA, Korea
	Heuisu Ryu	Gyeongin National University of Education, Korea
Registration	Yoonjeong Kim	Seoul Women's University, Korea
Treasurer	Jaehoon Nah	ETRI, Korea
Local Arrangements	Khi Jung Ahn	Cheju National University, Korea
	Dohoon Lee	NSRI, Korea

Program Committee

Co-chairs

Sehun Kim	KAIST, Korea
Moti Yung	Columbia University, USA
Hyung-Woo Lee	Hanshin University, Korea

Members

Gildas Avoine	MIT, CSAIL, USA
Lejla Batina	University of Leuven, Belgium
Mike Burmester	Florida State University, USA
Ki-Joon Chae	Ewha University, Korea
Myeonggil Choi	Inje University, Korea
Bruno Crispo	University of Trento, Italy
Sven Dietrich	CERT, CMU, USA
Helena Handschu	Spansion, France
Heng Swee Huay	Multimedia University, Malaysia
Maria Isabel Gonzalez Vasco	Universidad Rey Juan Carlos, Spain
Kil-Hyun Jeong	Jangan College, Korea
Gildas Avoine	MIT, CSAIL, USA
Soon-Won Jung	NITGEN, Korea
Stefan Katzenbeisser	Philips Research, Netherlands
Seungjoo Kim	Sungkyunkwan University, Korea
Seokwoo Kim	Hansei University, Korea
Brian King	Indiana University at Purdue, USA
Hong Seung Ko	Kyoto College of Graduate Studies for Informatics, Japan
Dong Hoon Lee	CIST, Korea University, Korea
Pil Joong Lee	POSTECH, Korea
Chae-Hun Lim	Sejong University, Korea
Dongdai Lin	SKLIS, Chinese Academy of Sciences, China
Mose Liskov	William and Mary College, USA
Michael Locasto	Columbia, USA
Havier Lopez	University of Malaga, Spain
Masahiro Mambo	Tsukuba, Japan
Jung Chan Na	ETRI, Korea
Shozo Naito	Kyoto College of Graduate Studies for Informatics, Japan
Yoram Ofek	University of Trento, Italy
Heekuck Oh	Hanyang University, Korea
Susan Pancho-Festin	University of the Philippines, Phillipines
In-Jae Park	Dream Security, Korea
Duong Hieu Phan,	University College London, UK
Raphael C.-W. Phan	EPFL, Switzerland
Vassilis Prevelakis	Drexel University, USA

C. Pandu Rangan	IIT Madras, India
Kyung-Hyune Rhee	Pukyong National University, Korea
Pankaj Rohatgi	IBM Resaerch, USA
Ahmad-Reza Sadeghi	Ruhr University, Bochum, Germany
Kouichi Sakurai	Kyushu University, Japan
Radu Sion	SUNY, Stony Brook, USA
Ki-Wook Sohn	NSRI, Korea
Francois-Xavier Standaert	Louvaine University, Belgium
Yannis Stamatiou	University of Ioannina, Greece
Koutarou Suzuki	NTT Labs, Japan
Huaxiong Wang	Nanyang Technological University, Singapore
Duncan Wong	City University, Hong Kong
Heung-Youl Youm	Soonchunhyang University, Korea
Rui Zhang	AIST, Japan
Jianying Zhou	Inst. for Infocomm Research, Singapore

Table of Contents

Public Key Crypto Applications

Biometrics/Information Hiding

Secure Hardware

Secure Systems

Wireless and Mobile Security

Application Security/Secure Systems

Access Control/DB Security

Smart Cards/Secure Systems

Anonymity and P2P Security