Lecture Notes in Computer Science 5379

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

Kyo-Il Chung Kiwook Sohn Moti Yung (Eds.)

Information Security Applications

9th International Workshop, WISA 2008
Jeju Island, Korea, September 23-25, 2008
Revised Selected Papers

Springer

Volume Editors

Kyo-Il Chung
Electronics and Telecommunications Research Institute (ETRI)
Information Security Research Division
161 Gajeong Dong, YuseongGu
Daejeon, 305-700, Korea
E-mail: kyoil@etri.re.kr

Kiwook Sohn
The Attached Institute of Electronics
and Telecommunications Research Institute (ETRI)
1 Yuseong-Post
Daejeon, 305-702, Korea
E-mail: kiwook@ensec.re.kr

Moti Yung
Google Inc.
Columbia University, Computer Science Department
1214 Amsterdam Avenue
New York, NY 10027, USA
E-mail: moti@cs.columbia.edu

Library of Congress Control Number: 2009920695

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 3-642-00305-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-00305-9 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12612604 06/3180 5 4 3 2 1 0

Preface

The 9th International Workshop on Information Security Applications (WISA 2008) was held in Jeju Island, Korea during September 23–25, 2008. 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 Knowledge Economy (MKE).

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 have served as the Program Committee Co-chairs of WISA 2008. The Program Committee received 161 papers from 18 countries, and accepted 24 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. Anat Zeelim-Hovav gave an invited talk, entitled "Investing in Information Security: A Coin in a Wishing Well?" Tai-Myoung Chung and Dieter Gollmann gave invited talks entitled "Today and Tomorrow of Security and Privacy" and "SOA Security: Service-Oriented Access Control," repectively.

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.

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

November 2008

Kyo-Il Chung
Kiwook Sohn
Moti Yung

Organization

Advisory Committee

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

General Co-chairs

Chaegyu Kim	ETRI, Korea
Hong-Sub Lee	KIISC, Korea

Steering Committee

Hyun-Sook Cho	ETRI, Korea
Sang-Choon Kim	Kangwon National University, Korea
Hyung-Woo Lee	Hanshin University, Korea
Jae-Kwang Lee	Hannam University, Korea
Dong-Il Seo	ETRI, Korea
OkYeon Yi	Kookmin University, Korea

Organization Committee

Chair	Jae-Cheol Ryou	Chungnam National University, Korea
Finance	Seong-Gon Choi	Chungbuk National University, Korea
	Jintae Oh	ETRI, Korea
Publication	Jaehwoon Lee	Dongguk University, Korea
Publicity	Dong Gue Park	Soonchunhyang University, Korea
	Neungsoo Park	Konkuk University, Korea
Registration	Kilsoo Chun	KISA, Korea
	Dohoon Lee	ETRI, Korea
Local Arrangements	Khi Jung Ahn	Cheju National University, Korea
	Taenam Cho	Woosuk University, Korea

Program Committee

Co-chairs	Kyo-Il Chung	ETRI, Korea
	Kiwook Sohn	ETRI, Korea
	Moti Yung	Columbia University, USA
Members	C. Pandu Rangan	IIT Madras, India
	Hyoung-Kee Choi	Sungkyunkwan University, Korea
	Hyun Cheol Chung	BCNE Global.Co., Ltd., Korea
	Debbie Cook	Columbia University, USA
	Pierre Alain Fouque	ENS, France
	JaeCheol Ha	Hoseo University, Korea
	Hoh Peter In	Korea University, Korea
	Stefan Katzenbeisser	Philips Research, The Netherlands
	Howon Kim	Pusan National University, Korea
	Hyong Shik Kim	Chungnam National University, Korea
	Hyung Jong Kim	Seoul Women University, Korea
	Seok Woo Kim	Hansei University, Korea
	Seung Joo Kim	Sungkyunkwan University, Korea
	Yongdae Kim	University of Minnesota, USA
	Brian King	Indiana University - Purdue University Indianapolis, USA
	Chiu Yuen Koo	Google Inc., USA
	Hong Seung Ko	Kyoto College of Graduate Studies for Informatics, Japan
	Jin Kwak	Soonchunhyang University, Korea
	Deok Gyu Lee	ETRI, Korea
	Dong Hoon Lee	Korea University, Korea
	Pil Joong Lee	POSTECH, Korea
	Chae-Hoon Lim	Sejong University, Korea
	Ji-Young Lim	Korean Bible University, Korea
	Dongdai Lin	SKLIS, Chinese Academy of Sciences, China
	Soohyun Oh	Hoseo University, Korea
	Dan Page	Bristol University, UK
	Susan Pancho-Festin	University of the Philippines, Philippines
	Namje Park	ETRI, Korea
	Vassilis Prevelakis	Drexel University, USA
	Kyung-Hyune Rhee	Pukyong National University, Korea
	Pankaj Rohatgi	IBM Research, USA
	Daehyun Ryu	Hansei University, Korea
	Kouichi Sakurai	Kyushu University, Japan
	Chang-ho Seo	Kongju National University, Korea
	Tsuyoshi Takagi	Future University-Hakodate, Japan
	Jeong Hyun Yi	Soongsil University, Korea
	Heung-Youl Youm	Soonchunhyang University, Korea
	Rui Zhang	AIST, Japan
	Jianying Zhou	Inst. for Infocomm Research, Singapore

Table of Contents

Smart Card and Secure Hardware(1)

Wireless and Sensor Network Security(1)

Public Key Crypto Applications

Privacy and Anonymity

N/W Security and Intrusion Detection

Application Security and Trust Management

Smart Card and Secure Hardware(2)

Wireless and Sensor Network Security(2)