Lecture Notes in Computer Science 7115

Souhwan Jung Moti Yung (Eds.)

Information Security Applications

12th International Workshop, WISA 2011
Jeju Island, Korea, August 22-24, 2011
Revised Selected Papers

Springer

Volume Editors

Souhwan Jung
Soongsil University
School of Electronic Engineering
Hyungnam Memorial Engineering Building 1105
Sangdo-Dong, Dongjak-Gu, Seoul 156-743, Korea
E-mail: souhwanj@ssu.ac.kr

Moti Yung
Google Inc. and
Columbia University, Computer Science Department
1214 Amsterdam Ave.
New York, NY 10025, USA
E-mail: moti@cs.columbia.edu

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-27889-1 e-ISBN 978-3-642-27890-7
DOI 10.1007/978-3-642-27890-7
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011944973

CR Subject Classification (1998): C.2, K.6.5, E.3, D.4.6, H.4, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The 12th international Workshop on Information Security Applications (WISA 2011) was held on Jeju Island, Korea, during August 22–24, 2011. The workshop is hosted annually by the Korea Institute of Information Security and Cryptology (KIISC), supported by the Electronics and Telecommunications Research Institute (ETRI) and the Korea Internet & Security Agency (KISA), and sponsored by the Ministry of Public Administration and Security (MoPAS) and the Korea Communications Commission (KCC).

The objective of this workshop is to cover all technical and practical aspects of security applications, representing both cryptographic and non-cryptographic works. The workshop serves as a forum for presentations of new results from the academic research community as well as from industry.

It was our great pleasure and honor to serve as the Program Committee Co-chairs of WISA 2011. The current proceedings of the workshop continue the tradition of earlier years which were also published as part of the LNCS series of Springer. The WISA 2011 Program Committee received 74 papers form 11 countries. This year the submissions were exceptionally strong, and the committee accepted 21 papers for the full-paper presentation track. All the papers were carefully evaluated through blind peer review, wherein at least three members of the Program Committee reviewed each submitted work. The numbers above indicate that the selection process was highly competitive, and, unfortunately, due to time limitation, many good papers were not accepted.

In addition to the contributed papers, the workshop had two invited talks: Kanta Matsuura and Shyhtsun Felix Wu presented distinguished special talks entitled "Passive and Active Measurements of Cybersecurity Risk Parameter" and "On Leveraging Social Informatics for Cyber Security," respectively.

Many people helped and worked hard to make WISA 2011 successful. 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 should also express our special thanks to the Organizing Committee members and the General Chair, Heungyoul Youm, for their hard work in managing the workshop.

Finally, on behalf of all those involved in organizing the workshop, we would like to thank the authors of all the submitted papers, for sending and contributing their interesting research results to the workshop, and the invited speakers. Without their submissions and support, WISA 2011 could not have been a success.

October 2011

Souhwan Jung
Moti Yung

Organization

Advisory Committee

ManYoung Rhee	Kyung Hee University, Korea
Hideki Imai	Chuo University, Japan
Bart Preneel	Katholieke University Leuven, Belgium
KilHyun Nam	Korea National Defense University, Korea
SangJae Moon	Kyungpook National University, Korea
DongHo Won	Sungkyunkwan University, Korea
SeHun Kim	KAIST, Korea
PilJoong Lee	POSTEC, Korea
DaeHo Kim	NSRI, Korea
JooSeok Song	Yonsei University, Korea
MinSub Rhee	Dankook University, Korea
HongSub Lee	Soonchunhyang University, Korea
KwanJo Kim	SKAIST, Korea

General Committee

Heung-Youl Youm	Soonchunhyang University, Korea

Steering Committee

ChangSub Park	Dankook University, Korea
KyoIl Chung	ETRI, Korea
JaeCheol Ryou	Chungnam National University, Korea
Kiwook Sohn	NSRI, Korea
KyungHyune Rhee	Pukyoung National University, Korea
JungDuk Kim	Chungang University, Korea
DaeWoo Park	Hoseo University, Korea
BeomSoo Kim	Yonsei University, Korea
SungTaek Chi	NSRI, Korea
JinHo Hahm	ETRI, Korea
HongGeun Kim	KISA, Korea

Organizing Committee

Chair

Jihong Kim	Semyung University, Korea

Members

TaeNam Cho	Woosuk University, Korea
HeuiSu Ryu	Gyeongin National University of Education, Korea
JaeMo Seung	Financial Security Agency, Korea
DaeSung Kwon	NSRI, Korea
JeongSik Park	TTA, Korea
JungTae Kim	Mokwon University, Korea
HaeSuk Kim	MOPAS, Korea
ChangKyu Kim	Dongeui University, Korea
JongSoo Jang	ETRI, Korea
SukLae Lee	KISA, Korea
DongGook Park	Sunchon National University, Korea
Seok Lae Lee	KISA, Korea

Program Committee

Co-chairs

Souhwan Jung	Soongsil University, Korea
Moti Yung	Columbia University and Google Inc., USA

Members

Gail-Joon Ahn	Arizona State University, USA
Joonsang Baek	Institute for Infocomm Research, Singapore
Rodrigo Roman Castro	University of Malaga, Spain
Kefei Chen	Shanghai Jiaotong University, China
Yongwha Chung	Korea University, Korea
Debbie Cook	Telcordia Technologies Inc., USA
Ed Dawson	University of Technology, Australia
Jun Furukawa	NEC, Japan
David Galindo	University of Luxembourg, Luxembourg
Dieter Gollmann	TU Hamburg, Germany
JaeCheol Ha	Hoseo University, Korea
Seokhie Hong	CIST, Korea
Jiankun Hu	RMIT, Australia
Seung Wook Jung	KISA, Korea
Namhi Kang	Duksung Women's University, Korea
Hiroaki Kikuchi	Tokai University, Japan
Dong Kyue Kim	Hanyang University, Korea
Howon Kim	Pusan National University, Korea
Kwangjo Kim	KAIST, Korea
Seungjoo Kim	CIST, Korea University, Korea
Brian King	Indiana University, Purdue University, Indianapolis, USA
Seungjoo Kim	CIST, Korea University, Korea

Brian King	Indiana University, Purdue University, Indianapolis, USA
Hong Seung Ko	The Kyoto College of Graduate Studies for Informatics, Japan
Helmut Kurth	ATSEC, Germany
Jin Kwak	Soonchunhyang University, Korea
Taekyoung Kwon	Sejong University, Korea
Mun-Kyu Lee	Inha University, Korea
PilJoong Lee	POSTECH, Korea
Yingjiu Li	Singapore Management University, Singapore
Dongdai Lin	Chinese Academy of Sciences, China
Peng Liu	Pennsylvania State University, USA
Atsuko Miyaji	JAIST, Japan
Yutaka Miyake	KDDI R&D Laboratories, Saitama, Japan
Kirill Morozov	Kyushu University, Japan
Rolf Oppliger	eSECURITY Technologies, Switzerland
Sung Bum Pan	Chosun University, Korea
Dusko Pavlovic	Royal Holloway, UK and University of Twente, The Netherlands
Vassilis Prevelakis	AEGIS Research, Greece
C. Pandu Rangan	IIT, Madras, India
Jae-cheol Ryou	Chungnam University, Korea
Kouichi Sakurai	Kyushu University, Fukuoka, Japan
Nitesh Saxena	Polytechnic Institute of New York University, USA
Chang-Ho Seo	Kongju National University, Korea
Sang-Uk Shin	Pukyong National University, Korea
Kiwook Sohn	NSRI, Korea
Tsuyoshi Takagi	Kyushu University, Japan
Tzong-Chen Wu	National Taiwan University, Taiwan
Chung-Huang Yang	National Kaohsiung Normal University, Taiwan
Yanjiang Yang	Institute for Infocomm Research, Singapore
Jeong Hyun Yi	Soongsil University, Korea
Okyeon Yi	Kookmin University, Korea
Rui Zhang	CAS, China
Zutao Zhu	Google Inc., USA

Table of Contents