Lecture Notes in Computer Science 7690

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

Dong Hoon Lee Moti Yung (Eds.)

Information Security Applications

13th International Workshop, WISA 2012
Jeju Island, Korea, August 16-18, 2012
Revised Selected Papers

Springer

Volume Editors

Dong Hoon Lee
Korea University, Center for Information Security Technologies
Anam-dong 5(o)-ga, Seoul 136-713, Korea
E-mail: donghlee@korea.ac.kr

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

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-35415-1 e-ISBN 978-3-642-35416-8
DOI 10.1007/978-3-642-35416-8
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012953045

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

WISA 2012, the 13th International Workshop on Information Security Applications, was held during August 16–18 in the Ocean Suites Jeju Hotel, Jeju Island, Republic of Korea. The conference was hosted by the Korea Institute of Information Security and Cryptology (KIISC) and sponsored by the Ministry of Public Administration and Security (MoPAS). It was also co-sponsored by the National Security Research Institute (NSRI), the Korea Internet Security Agency (KISA), and the Electronics and Telecommunications Research Institute (ETRI).

We received 100 valid submissions from 16 countries, of which 26 were accepted for full-paper track and 14 for short abstract track. These proceedings contain the revised versions of 26 full papers and 8 short papers. Every paper received at least three independent reviews, and papers with Program Committee (PC) contributions got five or more. To fill a final odd ten slots, partitioning the DI papers into topical categories helped.

For the Best Paper Award, the PC selected "N-Victims: An Approach to Determine N-Victims for APT Investigations" by Shun-Te Liu, Yi-Ming Chen, and Hui-ching Huang, "AIGG Threshold-Based HTTP GET Flooding Attack Detection" by Yang-seo Choi, Ik-Kyun Kim, Jin-Tae Oh, and Jong-Soo Jang and "Three Phase Dynamic Current Mode Logic: A More Secure DyCML to Achieve a More Balanced Power Consumption" by Hyunmin Kim, Vladimir Rozic, and Ingrid Verbauwhede. There were two invited talks, Suraj C. Kothari delivered "Preventing Catastrophe from Sophisticated Software Sabotage" on August 16 and Gil-young Song spoke on "Social Media Mining Technology and Applications" on August 17.

We would like to thank the authors of all submissions regardless of whether their papers were accepted or not. Their work made this conference possible. We are extremely grateful to the PC members for their enormous investment of time and effort in the difficult and delicate process of review and selection. We would like to thank Jin Kwak, who was the Organizing Chair in charge of the local organization and finances. Special thanks go to Shai Halevi for providing and setting up the splendid review software. We are most grateful to Hwaseong Lee, who provided support for the entire WISA 2012 process. We are also grateful to Souhwan Jung, the WISA 2011 Program Chair, for his timely information and replies to the host of questions we posed during the process.

August 2012

Dong Hoon Lee
Moti Yung

Organization

General Chair

Chang-Seop Park	Dankook University, Korea

Advisory Committee

Bongsik Ko	FSA, Korea
Hyunsook Cho	ETRI, Korea
Kiwook Sohn	NSRI, Korea
Sungtaek Chi	NSRI, Korea
Youjae Won	KISA, Korea

Steering Committee

Bart Preneel	Katholieke University Leuven, Belgium
Dong Ho Won	Sungkyunkwan University, Korea
Dae Ho Kim	Joongbu University, Korea
Heung-YoulYoum	Soonchunhyang University, Korea
Hideki Imai	Chuo University, Japan
Hong Sub Lee	Konkuk University, Korea
Joo Seok Song	Yonsei University, Korea
Kil Hyun Nam	Korea National Defense University, Korea
Kwan Jo Kim	KAIST, Korea
Man Young Rhee	Kyung Hee University, Korea
Min Sub Rhee	Dankook University, Korea
Pil Joong Lee	POSTEC, Korea
Sang Jae Moon	Kyungpook National University, Korea
Se Hun Kim	KAIST, Korea

Program Committee

Co-chairs

Dong Hoon Lee	Korea University, Korea
Moti Yung	Columbia University, USA

Committee Members

Gail-Joon Ahn	Arizona State University, USA
Frederik Armknecht	University of Mannheim, Germany
Kefei Chen	Shanghai Jiaotang University, China
Ed Dawson	Queensland University of Technology, Australia
Rafael Dowsley	University of California at San Diego, USA
Pierre-Alain Fouque	Ecole normale superieure, France

Shaojing Fu	National University of Defense Technology, China
David Galindo	University of Luxembourg, Luxembourg
Pierrick Gaudry	University of Lorraine, France
Dieter Gollmann	Hamburg University of Technology, Germany
JaeCheol Ha	Hoseo University Korea
Swee-Huay Heng	Multimedia University, Malaysia
Jiankun Hu	University of New South Wales, Australia
Hiroaki Kikuchi	Tokai University, Japan
Taekyoung Kwon	Sejong University, Korea
Mun-Kyu Lee	Inha University, Korea
Benoit Libert	Universite catholique de Louvain, Belgium
Dongdai Lin	Chinese Academy of Sciences, China
Atsuko Miyaji	JAIST, Japan
Yutaka Miyake	KDDI R&D Laboratories, Japan
Tae (Tom) Oh	Rochester Institute of Technology, USA
Rolf Oppliger	eSECURITY Technologies, Switzerland
Carles Padro	Nanyang Technological University, Singapore
Dan Page	University of Bristol, UK
Susan Pancho-Festin	University of the Philippines, Philippines
C. Pandu Rangan	IIT, India
Christian Rechberger	DTU, Denmark
Kouichi Sakurai	Kyushu University, Japan
Nitesh Saxena	University of Alabama at Birmingham, USA
Willy Susilo	University of Wollongong, Australia
Tzong-Chen Wu	National Taiwan University of Science and Technology, Taiwan
Wenling Wu	Chinese Academy of Sciences, China
Yongjin Yeom	NSRI, Korea
Jeong Hyun Yi	Soongsil University, Korea
Kazuki Yoneyama	NTT, Japan
Dae Hyun Yum	POSTECH, Korea
Rui Zhang	Chinese Academy of Sciences, China

Organizing Committee

Chair

Jin Kwak	Soonchunhyang University, Korea

Committee Members

Hyo Beom Ahn	Kongju National University, Korea
Im-Yeong Lee	Soonchunhyang University, Korea
Jungtaek Seo	NSRI, Korea
KijungAhn	Jeju National University, Korea
Kyungho Lee	Korea University, Korea
Namje Park	Jeju National University, Korea
Soomi Lee	FSA, Korea

Table of Contents

Symmetric Cipher

Secure Hardware/Public Key Crypto Application

Cryptographic Protocols/ Digital Forensics

Network Security

Trust Management/Database Security