Lecture Notes in Computer Science 4298

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

Jae-Kwang Lee Okyeon Yi Moti Yung (Eds.)

Information Security Applications

7th International Workshop, WISA 2006
Jeju Island, Korea, August 28-30, 2006
Revised Selected Papers

Springer

Volume Editors

Jae-Kwang Lee
Hannam University, School of Computer Engineering
133 Ojeong Dong, Daedeuk Gu, Daejeon, 306-791, Korea
E-mail: jklee@netwk.hannam.ac.kr

Okyeon Yi
Kookmin University, Department of Mathematics
861-1 Jeongneung-Dong, Songbuk-Gu, Seoul, 136-702, Korea
E-mail: oyyi@kookmin.ac.kr

Moti Yung
Columbia University, RSA Laboratories and Computer Science Department
Room 464, S.W. Mudd Building, New York, NY 10027, USA
E-mail: moti@cs.columbia.edu

Library of Congress Control Number: 2007922329

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 3-540-71092-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-71092-9 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12025299 06/3142 5 4 3 2 1 0

Preface

The 7th International Workshop on Information Security Applications (WISA 2006) was held on Jeju Island, Korea during August 28-30, 2006. 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 2006. The Program Committee received 146 papers from 11 countries, and accepted 31 papers for the full presentation track and 18 papers for a short 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 "Phishing and Authentication in Banks." Sushil Jajodia and Seong G. Kong gave invited talks in the full presentation track, entitled "Topological Analysis of Network Attack Vulnerability" and "Imaging Beyond the Visible Spectrum for Personal Identification and Threat Detection," 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 2006

Jae-Kwang Lee
Okyeon Yi
Moti Yung

Organization

Advisory Committee

Man-Young Rhee	Kyung Hee University, Korea
Hideki Imai	Tokyo University, Japan
Chu-Hwan Yim	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
Sehun Kim	KAIST, Korea
Pil-Joong Lee	POSTECH, Korea
Dae-Ho Kim	NSRI, Korea

General Co-chairs

Sung-Won Sohn	ETRI, Korea
Joo-Seok Song	Yonsei University, Korea

Steering Committee

Heung-Youl Youm	Soonchunhyang University, Korea
Suk-Woo Kim	Hansei University, Korea
Ki-Joon Chae	Ewha University, Korea
Chae-Hun Lim	Sejong University, Korea
Kyo-Il Chung	ETRI, Korea
TaeKyoung Kwon	Sejong University, Korea
Im-Yeong Lee	Soonchunhyang University, Korea

Organizing Committee

Chair:	Dong-Il Seo	ETRI, Korea
Finance:	Hyung-Woo Lee	Hanshin University, Korea
Publication:	Ji-Young Lim	Korean Bible University, Korea
Publicity:	Yoo-Jae Won	KISA, Korea
	Sang-Choon Kim	Kangwon National University, Korea
Registration:	Heuisu Ryu	Gyeongin National University of Education, Korea
Treasurer:	Do-Won Hong	ETRI, Korea
Local Arrangements:	Ki-Wook Sohn	NSRI, Korea
	Khi Jung Ahn	Cheju National University, Korea

Program Committee

Co-chairs :	Jae-Kwang Lee	Hannam University, Korea
	Moti Yung	Columbia University, USA
	Okyeon Yi	Kookmin University, Korea
Members :	Choong Seon Hong	KyungHee University, Korea
	Jae-Cheol Ryou	Chungnam University, Korea
	Dong Hoon Lee	CIST, Korea University, Korea
	Seungjoo Kim	Sungkyunkwan University, Korea
	Taekyoung Kwon	Sejong University, Korea
	Joongchan Na	ETRI, Korea
	Janghee You	ETRI, Korea
	Jung-Cheol Ahn	NSRI, Korea
	Myungsoo Rhee	KT, Korea
	Youngtae Cha	Secui.com, Korea
	Heesun Yang	KOMSCO, Korea
	Gildas Avoine	MIT, CSAIL, USA
	Sven Dietrich	CERT, CMU, USA
	Marc Joye	Gemplus, France
	Jaeyeon Jung	MIT, CSAIL
	Stefan Katzenbeisser	Philips Research, The Netherlands
	Brian King	Indiana University Purdue University, USA
	Dongdai Lin	SKLIS, Chinese Academy of Sciences, China
	Helger Lipmaa	University of Tartu, Estonia
	Havier Lopez	University of Malaga, Spain
	Lan Nguyen	CSIRO ICT Centre, Canbarra, Australia
	Yoram Ofek	University of Trento, Italy
	Susan Pancho-Festin	University of the Philippines, Phillipines
	C.Pandu Rangan	IIT Madras, India
	Duong Hieu Phan	University College London, UK
	Raphael C.-W. Phan	Swinburne University of Tech., Malaysia
	Vassilis Prevelakis	Drexel University, USA
	Pankaj Rohatgi	IBM Resaerch, USA
	Ahmad-Reza Sadeghi	Ruhr University, Bochum, Germany
	Kouichi Sakurai	Kyushu University, Japan
	Stuart Schechter	MIT, Lincoln Lab, USA
	Tom Shrimpton	Portland State University, USA
	Radu Sion, SUNY	Stony Brook, USA
	Stamatiou Iwannis	CTI, Greece
	Koutarou Suzuki	NTT Labs, Japan

Huaxiong Wang	Macquarie University, Australia
Duncan Wong	City University, Hong Kong
Rui Zhang	AIST, Japan
Jianying Zhou	Inst. for Infocomm Research, Singapore
Shozo Naito	Kyoto College of Graduate Studies for Informatics, Japan
Ko, Hong Seung	Kyoto College of Graduate Studies for Informatics, Japan

Table of Contents

Public Key Crypto Applications/Virus Protection

Controllable Ring Signatures 1
Wei Gao, Guilin Wang, Xueli Wang, and Dongqing Xie

Efficient User Authentication and Key Agreement in Wireless Sensor Networks 15
Wen-Shenq Juang

Identity-Based Key Issuing Without Secure Channel in a Broad Area .. 30
Saeran Kwon and Sang-Ho Lee

PolyI-D: Polymorphic Worm Detection Based on Instruction Distribution 45
Ki Hun Lee, Yuna Kim, Sung Je Hong, and Jong Kim

Cyber Indication/Intrusion Detection

SAID: A Self-Adaptive Intrusion Detection System in Wireless Sensor Networks 60
Jianqing Ma, Shiyong Zhang, Yiping Zhong, and Xiaowen Tong

SQL Injection Attack Detection: Profiling of Web Application Parameter Using the Sequence Pairwise Alignment 74
Jae-Chul Park and Bong-Nam Noh

sIDMG: Small-Size Intrusion Detection Model Generation of Complimenting Decision Tree Classification Algorithm 83
Seung-Hyun Paek, Yoon-Keun Oh, and Do-Hoon Lee

Biometrics/Security Trust Management

Privacy-Enhancing Fingerprint Authentication Using Cancelable Templates with Passwords 100
Daesung Moon, Sungju Lee, Seunghwan Jung, Yongwha Chung, Okyeon Yi, Namil Lee, and Kiyoung Moon

Impact of Embedding Scenarios on the Smart Card-Based Fingerprint Verification 110
Byungkwan Park, Daesung Moon, Yongwha Chung, and Jin-Won Park

Quality Assurance for Evidence Collection in Network Forensics 121
Bo-Chao Cheng and Huan Chen

Secure Software/Systems

Visualization of Permission Checks in Java Using Static Analysis 133
Yoonkyung Kim and Byeong-Mo Chang

Deployment of Virtual Machines in Lock-Keeper 147
Feng Cheng and Christoph Meinel

Smart Cards/Secure Hardware

Investigations of Power Analysis Attacks and Countermeasures for ARIA 160
HyungSo Yoo, Christoph Herbst, Stefan Mangard, Elisabeth Oswald, and SangJae Moon

Efficient Implementation of Pseudorandom Functions for Electronic Seal Protection Protocols 173
Mun-Kyu Lee, Jung Ki Min, Seok Hun Kang, Sang-Hwa Chung, Howon Kim, and Dong Kyue Kim

A Novel Key Agreement Scheme in a Multiple Server Environment 187
Chin-Chen Chang and Chia-Chi Wu

Mobile Security

Cost-Effective IDS Operating Scheme in MANETs 198
Youngok Jeong, Younggoo Han, Hyunwoo Kim, Woochul Shim, Jaehong Kim, and Sehun Kim

Authenticated Fast Handover Scheme in the Hierarchical Mobile IPv6 .. 211
Hyun-Sun Kang and Chang-Seop Park

A Method and Its Usability for User Authentication by Utilizing a Matrix Code Reader on Mobile Phones 225
Michiru Tanaka and Yoshimi Teshigawara

DRM/Information Hiding/Ubiquitous Computing Security/P2P Security

Distributed Management of OMA DRM Domains 237
Harikrishna Vasanta, Reihaneh Safavi-Naini, Nicholas Paul Sheppard, and Jan Martin Surminen

New Traceability Codes Against a Generalized Collusion Attack for Digital Fingerprinting 252
Hideki Yagi, Toshiyasu Matsushima, and Shigeichi Hirasawa

A Key Management Based on Multiple Regression in Hierarchical Sensor Network 267
Mihui Kim, Inshil Doh, and Kijoon Chae

Random Visitor: A Defense Against Identity Attacks in P2P Overlay Networks 282
Jabeom Gu, Jaehoon Nah, Cheoljoo Chae, Jaekwang Lee, and Jongsoo Jang

Privacy/Anonymity

Privacy Protection in PKIs: A Separation-of-Authority Approach 297
Taekyoung Kwon, Jung Hee Cheon, Yongdae Kim, and Jae-Il Lee

Three-Party Password Authenticated Key Agreement Resistant to Server Compromise 312
Taekyoung Kwon and Dong Hoon Lee

Privacy-Enhanced Content Distribution and Charging Scheme Using Group Signature 324
Takayuki Tobita, Hironori Yamamoto, Hiroshi Doi, and Keigo Majima

Secret Handshake with Multiple Groups 339
Naoyuki Yamashita and Keisuke Tanaka

Internet and Wireless Security

Pre-authentication for Fast Handoff in Wireless Mesh Networks with Mobile APs 349
Chanil Park, Junbeom Hur, Chanoe Kim, Young-joo Shin, and Hyunsoo Yoon

EAP Using the Split Password-Based Authenticated Key Agreement ... 364
Jongho Ryu

How Many Malicious Scanners Are in the Internet? 381
Hiroaki Kikuchi and Masato Terada

E-Passport: The Global Traceability Or How to Feel Like a UPS Package 391
Dario Carluccio, Kerstin Lemke-Rust, Christof Paar, and Ahmad-Reza Sadeghi

Author Index 405