Lecture Notes in Computer Science 3325

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

Editorial Board

David Hutchison
Lancaster University, UK

Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler
University of Surrey, Guildford, UK

Jon M. Kleinberg
Cornell University, Ithaca, NY, USA

Friedemann Mattern
ETH Zurich, Switzerland

John C. Mitchell
Stanford University, CA, USA

Moni Naor
Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz
University of Bern, Switzerland

C. Pandu Rangan
Indian Institute of Technology, Madras, India

Bernhard Steffen
University of Dortmund, Germany

Madhu Sudan
Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos
New York University, NY, USA

Doug Tygar
University of California, Berkeley, CA, USA

Moshe Y. Vardi
Rice University, Houston, TX, USA

Gerhard Weikum
Max-Planck Institute of Computer Science, Saarbruecken, Germany

Chae Hoon Lim Moti Yung (Eds.)

Information Security Applications

5th International Workshop, WISA 2004
Jeju Island, Korea, August 23-25, 2004
Revised Selected Papers

Springer

Volume Editors

Chae Hoon Lim
Sejong University
Department of Internet Engineering
98 Gunja-Dong, Kwangjin-Gu, Seoul, 143-747, Korea
E-mail: chlim@sejong.ac.kr

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

Library of Congress Control Number: 2005920313

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

ISSN 0302-9743
ISBN 3-540-24015-2 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springeronline.com

© Springer-Verlag Berlin Heidelberg 2005
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 11352440 06/3142 5 4 3 2 1 0

Preface

The 5th International Workshop on Information Security Applications (WISA 2004) was held in Jeju Island, Korea during August 23-25, 2004. 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).

The aim of the workshop is to serve as a forum for new conceptual and experimental research results in the area of information security applications from the academic community as well as from the industry. The workshop program covers a wide range of security aspects including cryptography, cryptanalysis, network/system security and implementation aspects.

The program committee received 169 papers from 22 countries, and accepted 37 papers for a full presentation track and 30 papers for a short presentation track. Each paper was carefully evaluated through peer-review by at least three members of the program committee. This volume contains revised versions of 36 papers accepted and presented in the full presentation track. Short papers were only published in the WISA 2004 pre-proceedings as preliminary versions and are allowed to be published elsewhere as extended versions.

In addition to the contributed papers, Professors Gene Tsudik and Ross Anderson gave invited talks, entitled *Security in Outsourced Databases* and *What does 'Security' mean for Ubiquitous Applications?*, respectively.

Many people have helped and worked hard to make WISA 2004 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 also express our special thanks to the organizing committee members for making the workshop possible. Finally, we would like to thank all the authors of the submitted papers and the invited speakers for enabling an interesting workshop program.

December 2004

Chae Hoon Lim
Moti Yung

Organization

Advisory Committee

Man Young Rhee	Seoul National Univ., Korea
Hideki Imai	Tokyo Univ., Japan
Chu-Hwan Yim	ETRI, Korea
Bart Preneel	Katholieke Universiteit Leuven, Belgium

General Co-Chairs

Pil Joong Lee	POSTECH/KT, Korea
Sung Won Sohn	ETRI, Korea

Steering Committee

Kil-Hyun Nam	Korea National Defense Univ., Korea
Sang Jae Moon	Kyungpook National Univ., Korea
Dong Ho Won	Sungkyunkwan Univ., Korea
Sehun Kim	KAIST, Korea

Organization Committee

Chair:	Kyo Il Chung	ETRI, Korea
Finance:	Im Yeong Lee	SoonChunHyang Univ., Korea
Publication:	Ji Young Lim	Korean Bible Univ., Korea
Publicity:	Hyung Woo Lee	Hansin Univ., Korea Registration
	Jae Cheol Ha	Korea Nazarene Univ., Korea
Treasurer:	Hyungon Kim	ETRI, Korea
	Sang Choon Kim	Samchok National Univ., Korea
Local Arrangement:	Jae Kwang Lee	Hannam Univ., Korea
	Khi Jung Ahn	Cheju National Univ., Korea

Program Commitee

Co-Chairs:	Chae Hoon Lim	Sejong Univ., Korea
	Moti Yung	Columbia Univ., USA
Members:	Giuseppe Ateniese	Johns Hopkins Univ., USA
	Tuomas Aura	Microsoft Research, UK
	Feng Bao	Institute for Infocomm Research, Singapore
	Colin Boyd	QUT, Australia
	Dario Catalano	ENS, France
	Kijoon Chae	Ewha Womans Univ., Korea
	Gene Itkis	Boston Univ., USA
	Jong Soo Jang	ETRI, Korea
	Yonghee Jeon	Catholic Univ. of Daegu, Korea
	Jonathan Katz	Univ. of Maryland, USA
	Angelos Keromytis	Columbia Univ., USA
	Seungjoo Kim	Sungkyunkwan Univ., Korea
	Yongdae Kim	Univ. of Minnesota at Twin Cities, USA
	Klaus Kursawe	KU Keuven, Belgium
	Taekyoung Kwon	Sejong Univ., Korea
	Chi Sung Laih	National Cheng Kung Univ., Taiwan
	Kwok-Yan Lam	Tsinghua Univ., China
	Chae Ho Lim	Securitymap, Korea
	Kanta Matsuura	Tokyo Univ., Japan
	Refik Molva	Institut Eurecom, France
	Pascal Paillier	Gemplus, France
	Josef Pieprzyk	Macquarie Univ., Australia
	Zulfikar Ramzan	Docomo Labs, USA
	Pankaj Rohatgi	IBM Research, USA
	Bimal Roy	Indian Statistical Institute, India
	Jaechul Ryu	Chungnam National Univ., Korea
	Kouichi Sakurai	Kyushu Univ., Japan
	Diana Smetters	Palo Alto Research Center, USA
	Bulent Yener	Rensselaer Polytechnic Institute, USA
	Okyeon Yi	Kookmin Univ., Korea
	Heungyoul Youm	SoonChunHyang Univ., Korea
	Avishai Wool	Tel-Aviv Univ., Israel
	S.Felix Wu	UC Davis, USA

Table of Contents

Network/Computer Security

Impacts of Security Protocols on Real-Time Multimedia Communications 1
Kihun Hong, Souhwan Jung, Luigi Lo Iacono, and Christoph Ruland

An Improvement on Privacy and Authentication in GSM 14
Young Jae Choi and Soon Ja Kim

Encrypted Watermarks and Linux Laptop Security 27
Markku-Juhani O. Saarinen

Inconsistency Detection of Authorization Policies in Distributed Component Environment 39
Chang-Joo Moon and Hoh Peter In

Public Key Schemes I

Custodian-Hiding Verifiable Encryption 51
Joseph K. Liu, Victor K. Wei, and Duncan S. Wong

Proving Key Usage 65
Malek Bechlaghem and Vincent Rijmen

Public Key Encryption with Conjunctive Field Keyword Search 73
Dong Jin Park, Kihyun Kim, and Pil Joong Lee

Intrusion Detection I

A Probabilistic Method for Detecting Anomalous Program Behavior 87
Kohei Tatara, Toshihiro Tabata, and Kouichi Sakurai

Service Discrimination and Audit File Reduction for Effective Intrusion Detection 99
Fernando Godínez, Dieter Hutter, and Raúl Monroy

IDS False Alarm Filtering Using KNN Classifier 114
Kwok Ho Law and Lam For Kwok

Watermarking/Anti-spamming

Content-Based Synchronization Using the Local Invariant Feature for Robust Watermarking 122
Hae-Yeoun Lee, Jong-Tae Kim, Heung-Kyu Lee, and Young-Ho Suh

Some Fitting of Naive Bayesian Spam Filtering for Japanese Environment 135
Manabu Iwanaga, Toshihiro Tabata, and Kouichi Sakurai

Public Key Schemes II

Efficient Authenticated Key Agreement Protocol for Dynamic Groups 144
Kui Ren, Hyunrok Lee, Kwangjo Kim, and Taewhan Yoo

A Ring Signature Scheme Using Bilinear Pairings 160
Jing Xu, Zhenfeng Zhang, and Dengguo Feng

Verifiable Pairing and Its Applications 170
Sherman S.M. Chow

Intrusion Detection II

Improving the Performance of Signature-Based Network Intrusion Detection Sensors by Multi-threading 188
Bart Haagdorens, Tim Vermeiren, and Marnix Goossens

An Effective Placement of Detection Systems for Distributed Attack Detection in Large Scale Networks 204
Seok Bong Jeong, Young Woo Choi, and Sehun Kim

Application of Content Computing in Honeyfarm 211
Yi-Yuan Huang, Kwok-Yan Lam, Siu-Leung Chung, Chi-Hung Chi, and Jia-Guang Sun

Digital Rights Management

License Protection with a Tamper-Resistant Token 223
Cheun Ngen Chong, Bin Ren, Jeroen Doumen, Sandro Etalle, Pieter H. Hartel, and Ricardo Corin

An Adaptive Approach to Hardware Alteration for Digital Rights Management 238
Yinyan Yu and Zhi Tang

Dynamic Fingerprinting over Broadcast Using Revocation Scheme 251
Mira Kim, Kazukuni Kobara, and Hideki Imai

Practical Pay-TV Scheme Using Traitor Tracing Scheme for Multiple Channels 264
Chong Hee Kim, Yong Ho Hwang, and Pil Joong Lee

e-Commerce Security

Vulnerability of a Mobile Payment System Proposed at WISA 2002 278
Sang Cheol Hwang, Dong Hoon Lee, Daewan Han, and Jae-Cheol Ryou

Fair Offline Payment Using Verifiable Encryption 286
Sangjin Kim and Heekuck Oh

A Limited-Use Key Generation Scheme for Internet Transactions......... 302
Supakorn Kungpisdan, Phu Dung Le, and Bala Srinivasan

Efficient Implementation

Efficient Representation and Software Implementation
of Resilient Maiorana-McFarland S-boxes 317
Kishan Chand Gupta and Palash Sarkar

Signed Digit Representation with NAF and Balanced Ternary Form
and Efficient Exponentiation in $GF(q^n)$
Using a Gaussian Normal Basis of Type II 332
Soonhak Kwon

Novel Efficient Implementations of Hyperelliptic Curve Cryptosystems
Using Degenerate Divisors 345
*Masanobu Katagi, Izuru Kitamura, Toru Akishita,
and Tsuyoshi Takagi*

Hyperelliptic Curve Coprocessors on a FPGA 360
*HoWon Kim, Thomas Wollinger, YongJe Choi, KyoIl Chung,
and Christof Paar*

Anonymous Communication

Key-Exchange Protocol Using Pre-agreed Session-ID 375
Kenji Imamoto and Kouichi Sakurai

A New ***k***-Anonymous Message Transmission Protocol.................. 388
Gang Yao and Dengguo Feng

Onions Based on Universal Re-encryption –
Anonymous Communication Immune Against Repetitive Attack 400
Marcin Gomułkiewicz, Marek Klonowski, and Mirosław Kutyłowski

Side-Channel Attacks

Side Channel Cryptanalysis on SEED 411
*HyungSo Yoo, ChangKyun Kim, JaeCheol Ha, SangJae Moon,
and IlHwan Park*

Secure and Efficient AES Software Implementation for Smart Cards 425
Elena Trichina and Lesya Korkishko

Practical Template Attacks 440
Christian Rechberger and Elisabeth Oswald

Evaluation and Improvement of the Tempest Fonts 457
Hidema Tanaka, Osamu Takizawa, and Akihiro Yamamura

Author Index 471