

Lecture Notes in Computer Science

2908

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer

Berlin

Heidelberg

New York

Hong Kong

London

Milan

Paris

Tokyo

Kijoon Chae Moti Yung (Eds.)

Information Security Applications

4th International Workshop, WISA 2003
Jeju Island, Korea, August 25-27, 2003
Revised Papers



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Kijoon Chae
Ewha Womans University, Department of Computer Science and Engineering
11-1, Daehyun-Dong, Seodaemun-Gu, Seoul 120-750, Korea
E-mail: kjchae@ewha.ac.kr

Moti Yung
Columbia University, Department of Computer Science
New York, NY 10027-7003, USA
E-mail: moti@cs.columbia.edu

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographic data is available in the Internet at <<http://dnb.ddb.de>>.

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 3-540-20827-5 Springer-Verlag 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-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag is a part of Springer Science+Business Media
springeronline.com

© Springer-Verlag Berlin Heidelberg 2004
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 10981382 06/3142 5 4 3 2 1 0

Preface

The 4th Workshop on Information Security Applications (WISA 2003) was sponsored by the following Korean organizations and government bodies: 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 workshop was held in Jeju Island, Korea during August 25–27, 2003. This international workshop provided ample technical sessions covering a large spectrum of information security applications. Subjects covered included network/mobile security, electronic commerce security, digital rights management, intrusion detection, secure systems and applications, biometrics and human interfaces, public key cryptography, and applied cryptography.

The program committee received 200 papers from 23 countries (representing most geographic areas where security and applied cryptography research is conducted throughout the world). Each submitted paper was peer-reviewed by three program committee members. This year, we had two tracks: long and short presentation tracks. We selected 36 papers for the long presentation track and 34 papers for the short presentation tracks. This volume contains revised versions of papers accepted for the long presentation track. We would like to note that getting accepted to both tracks was an achievement to be proud of, given the competitive nature of WISA this year. Papers in the short presentation track were only published in the WISA preproceedings as preliminary notes; extended versions of these notes may be published by future conferences or workshops.

Many people worked very hard to produce a successful WISA 2003 workshop and its technical program. We are grateful to the organizing committee, the steering committee and the workshop general chairs for their support. We thank Springer-Verlag editors for their careful scrutiny and guidance in preparing the workshop proceedings. We are extremely thankful to the program committee members for spending their time on and devoting their efforts to reviewing the submitted papers and selecting the technical program. We also acknowledge the help of the external reviewers: Ahto Buldas and Markku-Juhani Saarinen. We note that the program committee had members from numerous areas of research relevant to the workshop's subject and from many geographic areas, a fact that assured the breadth and the international nature of WISA. Finally, we would like to express our sincere thanks to all the authors of all the submitted papers, without whom this workshop would not have been possible.

October 2003

Kijoon Chae
Moti Yung

Organization

Advisory Committee

Man Young Rhee, Seoul National Univ., Korea
Hideki Imai, Tokyo Univ., Japan
Bart Preneel, Katholieke Universiteit Leuven, Belgium
Thomas A. Berson, Anagram Laboratories, USA
Gil Rok Oh, ETRI, Korea

General Co-chairs

Sehun Kim, KAIST, Korea
Chee Hang Park, 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
Hyun Sook Cho, ETRI, Korea
Sung Won Sohn, ETRI, Korea

Organization Committee Chair

Jae Kwang Lee, Hannam Univ., Korea

Organization Committee

Finance	Kyo Il Chung, ETRI, Korea Hong Geun Kim, Korea Information Security Agency, Korea
Publication	Gwangsoo Rhee, Sookmyung Women's Univ., Korea Ji Young Lim, Korean Bible Univ., Korea
Publicity	Hyung Woo Lee, Hanshin Univ., Korea Dong Chun Lee, Howon Univ., Korea
Registration	Jae Cheol Ha, Korea Nazarene Univ., Korea
Treasurer	Jae Hoon Nah, ETRI, Korea
Local Arrangements	Byoung Joon Min, Incheon Univ., Korea Wang-Cheol Song, Cheju National Univ., Korea

Program Co-chairs

Kijoon Chae, Ewha Womans Univ., Korea
Moti Yung, Columbia Univ., USA

Program Committee

William Arbaugh, Univ. of Maryland, USA
Feng Bao, Institute for Infocomm Research, Singapore
Chin-Chen Chang, National Chungcheng Univ., Taiwan
Jean Sebastien Coron, Gemplus, France
Ed Dawson, QUT, Australia
Carl Ellison, Intel, USA
Marc Fischlin, Fraunhofer Gesellschaft SIT, Germany
Pierre-Alain Fouque, DCSSI, France
James Hughes, StorageTek, USA
Jong Soo Jang, ETRI, Korea
Aggelos Kiayias, Univ. of Connecticut, USA
Kwangjo Kim, ICU, Korea
Seungjoo Kim, KISA, Korea
Yongdae Kim, Univ. of Minnesota, USA
Kazukuni Kobara, Tokyo Univ., Japan
Pil Joong Lee, POSTECH, Korea
Dongdai Lin, SKLOIS, China
Helger Lipmaa, Helsinki Univ. of Technology, Finland
Fabian Monrose, Johns Hopkins Univ., USA
Shiho Moriai, Sony Computer Entertainment, Japan
Giuseppe Persiano, Univ. of Salerno, Italy
Bart Preneel, Katholieke Universiteit Leuven, Belgium
Pankaj Rohatgi, IBM, USA
Jae-Cheol Ryou, Chungnam National Univ., Korea
Kouichi Sakurai, Kyushu Univ., Japan
Tomas Sander, HP, USA
Serge Vaudenay, Federal Institute of Technology, Switzerland
Sung-Ming Yen, National Central Univ., Taiwan
Okyeon Yi, Kookmin Univ., Korea

Table of Contents

Network Security

Model Checking of Security Protocols with Pre-configuration	1
<i>Kyoil Kim, Jacob A. Abraham, Jayanta Bhadra</i>	
Remote Access VPN with Port Protection Function by Mobile Codes	16
<i>Yoshiaki Shiraishi, Youji Fukuta, Masakatu Morii</i>	
A Role of DEVS Simulation for Information Assurance	27
<i>Sung-Do Chi, Jong Sou Park, Jang-Se Lee</i>	

Mobile Security

Enhancing Grid Security Infrastructure to Support Mobile Computing Nodes	42
<i>Kwok-Yan Lam, Xi-Bin Zhao, Siu-Leung Chung, Ming Gu, Jia-Guang Sun</i>	
Reliable Cascaded Delegation Scheme for Mobile Agent Environments ...	55
<i>Hyun-suk Lee, Hyeog Man Kwon, Young Ik Eom</i>	
Practical Solution for Location Privacy in Mobile IPv6	69
<i>SuGil Choi, Kwangjo Kim, ByeongGon Kim</i>	

Intrusion Detection

CTAR: Classification Based on Temporal Class-Association Rules for Intrusion Detection	84
<i>Jin Suk Kim, Hohn Gyu Lee, Sungbo Seo, Keun Ho Ryu</i>	
Viterbi Algorithm for Intrusion Type Identification in Anomaly Detection System	97
<i>Ja-Min Koo, Sung-Bae Cho</i>	
Towards a Global Security Architecture for Intrusion Detection and Reaction Management	111
<i>Renaud Bidou, Julien Bourgeois, Francois Spies</i>	

Internet Security

Intrusion-Tolerant System Design for Web Server Survivability	124
<i>Dae-Sik Choi, Eul Gyu Im, Cheol-Won Lee</i>	

PANA/IKEv2: An Internet Authentication Protocol for Heterogeneous Access	135
<i>Paulo S. Pagliusi, Chris J. Mitchell</i>	

An Automatic Security Evaluation System for IPv6 Network	150
<i>Jaehoon Nah, Hyeokchan Kwon, Sungwon Sohn, Chechang Park, Chimoon Han</i>	

Secure Software, Hardware, and Systems I

A Location Privacy Protection Mechanism for Smart Space	162
<i>Yeongsub Cho, Sangrae Cho, Daeseon Choi, Seunghun Jin, Kyoil Chung, Chechang Park</i>	

Secure System Architecture Based on Dynamic Resource Reallocation ...	174
<i>Byoung Joon Min, Sung Ki Kim, Joong Sup Choi</i>	

Fair Exchange with Guardian Angels	188
<i>Gildas Avoine, Serge Vaudenay</i>	

Secure Software, Hardware, and Systems II

Sign-Based Differential Power Analysis	203
<i>Roman Novak</i>	

Asymmetric Watermarking Scheme Using Permutation Braids	217
<i>Geun-Sil Song, Mi-Ae Kim, Won-Hyung Lee</i>	

Low-Power Design of a Functional Unit for Arithmetic in Finite Fields $GF(p)$ and $GF(2^m)$	227
<i>Johann Großschädl, Guy-Armand Kamendje</i>	

E-commerce Security

Efficient Implementation of Relative Bid Privacy in Sealed-Bid Auction	244
<i>Kun Peng, Colin Boyd, Ed Dawson, Kapalee Viswanathan</i>	

Multi-dimensional Hash Chain for Sealed-Bid Auction	257
<i>Navapot Prakobpol, Yongyuth Permpoontanalarp</i>	

An Improved Forward Integrity Protocol for Mobile Agents	272
<i>Ming Yao, Ernest Foo, Kun Peng, Ed Dawson</i>	

Digital Rights Management

Taming “Trusted Platforms” by Operating System Design	286
<i>Ahmad-Reza Sadeghi, Christian Stübke</i>	

A Software Fingerprinting Scheme for Java Using Classfiles Obfuscation	303
<i>Kazuhide Fukushima, Kouichi Sakurai</i>	

Reducing Storage at Receivers in SD and LSD Broadcast Encryption Schemes	317
<i>Tomoyuki Asano</i>	

Biometrics and Human Interfaces I

3D Face Recognition under Pose Varying Environments	333
<i>Hwanjong Song, Ukil Yang, Kwanghoon Sohn</i>	

An Empirical Study of Multi-mode Biometric Systems Using Face and Fingerprint	348
<i>H. Kang, Y. Han, H. Kim, W. Choi, Y. Chung</i>	

Fingerprint-Based Authentication for USB Token Systems	355
<i>Daesung Moon, Youn Hee Gil, Dosung Ahn, Sung Bum Pan, Yongwha Chung, Chee Hang Park</i>	

Biometrics and Human Interfaces II

Iris Recognition System Using Wavelet Packet and Support Vector Machines	365
<i>Byungjun Son, Gyundo Kee, Yungcheol Byun, Yillbyung Lee</i>	

Biometrics Identification and Verification Using Projection-Based Face Recognition System	380
<i>Hyeonjoon Moon, Jaihie Kim</i>	

Visualization of Dynamic Characteristics in Two-Dimensional Time Series Patterns: An Application to Online Signature Verification	395
<i>Suyoung Chi, Jaeyeon Lee, Jung Soh, Dohyung Kim, Weongeun Oh, Changhun Kim</i>	

Public Key Cryptography / Key Management

E-MHT. An Efficient Protocol for Certificate Status Checking	410
<i>Jose L. Muñoz, Jordi Forné, Oscar Esparza, Miguel Soriano</i>	

A Comment on Group Independent Threshold Sharing	425
<i>Brian King</i>	

Automation-Considered Logic of Authentication and Key Distribution ...	442
<i>Taekyoung Kwon, Seongan Lim</i>	

Applied Cryptography

The MESH Block Ciphers 458
Jorge Nakahara Jr, Vincent Rijmen, Bart Preneel, Joos Vandewalle

Fast Scalar Multiplication Method Using Change-of-Basis Matrix
to Prevent Power Analysis Attacks on Koblitz Curves 474
Dong Jin Park, Sang Gyoo Sim, Pil Joong Lee

Constructing and Cryptanalysis of a 16×16 Binary Matrix
as a Diffusion Layer 489
Bon Wook Koo, Hwan Seok Jang, Jung Hwan Song

Author Index 505