

Tai-hoon Kim Hojjat Adeli
Rosslin John Robles Maricel Balitanas (Eds.)

Information Security and Assurance

International Conference, ISA 2011
Brno, Czech Republic, August 15-17, 2011
Proceedings

Volume Editors

Tai-hoon Kim

Hannam University, 133 Ojeong-dong, Daeduk-gu, Daejeon 306-791, Korea

E-mail: taihoonn@hannam.ac.kr

Hojjat Adeli

The Ohio State University

470 Hitchcock Hall, 2070 Neil Avenue, Columbus, OH 43210-1275, USA

E-mail: adeli.1@osu.edu

Rosslin John Robles

Hannam University, 133 Ojeong-dong, Daeduk-gu, Daejeon 306-791, Korea

E-mail: rosslin1@sersc.org

Maricel Balitanas

Hannam University, 133 Ojeong-dong, Daeduk-gu, Daejeon, Korea

E-mail: maricel@sersc.org

ISSN 1865-0929

ISBN 978-3-642-23140-7

DOI 10.1007/978-3-642-23141-4

Springer Heidelberg Dordrecht London New York

e-ISSN 1865-0937

e-ISBN 978-3-642-23141-4

Library of Congress Control Number: 2011933824

CR Subject Classification (1998): C.2, D.4.6, K.6.5

© Springer-Verlag Berlin Heidelberg 2011

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

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)

Foreword

Information security and assurance is an area that has attracted many academic and industry professionals in research and development. The goal of the ISA conference is to bring together researchers from academia and industry as well as practitioners to share ideas, problems and solutions relating to the multifaceted aspects of information security and assurance.

We would like to express our gratitude to all of the authors of submitted papers and to all attendees for their contributions and participation. We believe in the need to continue this undertaking in the future.

We acknowledge the great effort of all the Chairs and the members of the Advisory Boards and Program Committees of the above-listed event. Special thanks go to SERSC (Science & Engineering Research Support soCiety) for supporting this conference.

We are grateful in particular to the speakers who kindly accepted our invitation and, in this way, helped to meet the objectives of the conference.

July 2011

Chairs of ISA 2011

Preface

We would like to welcome you to the proceedings of the 2011 International Conference on Information Security and Assurance (ISA 2011), which was held during August 15–17, 2011, at Brno University, Czech Republic.

ISA 2011 focused on various aspects of advances in information security and assurance with computational sciences, mathematics and information technology. It provided a chance for academic and industry professionals to discuss recent progress in the related areas. We expect that the conference and its publications will be a trigger for further related research and technology improvements in this important subject. We would like to acknowledge the great effort of all the Chairs and members of the Program Committee.

We would like to thank all of the authors of submitted papers and all the attendees for their contributions and participation.

Once more, we would like to thank all the organizations and individuals who supported this event as a whole and, in particular, helped in the success of ISA 2011.

June 2011

Tai-hoon Kim
Hojjat Adeli
Rosslin John Robles
Maricel Balitanas

Organization

Honorary Chair

Hojjat Adeli The Ohio State University, USA

General Co-chairs

Martin Drahanšký Brno University, Czech Republic
Wael Adi Technische Universität Braunschweig, Germany

Program Co-chairs

Tai-hoon Kim Hannam University, Korea
Yang Xiao The University of Alabama, USA
Filip Orság Brno University, Czech Republic

Workshop Co-chairs

Muhammad Khurram Khan King Saud University, Saudi Arabia
Byeong-joo Park Hannam University, Korea

International Advisory Board

Haeng-kon Kim Catholic University of Daegu, Korea
Kouich Sakurai Kyushu University, Japan
Justin Zhan CMU, USA
Hai Jin Huazhong University of Science and Technology, China
Edwin Sha University of Texas at Dallas, USA
Dominik Slezak Infobright, Poland and Canada

Publicity Co-chairs

Debnath Bhattacharyya SERSC, India
Ching-Hsien Hsu Chung Hua University, Taiwan
Duncan S. Wong City University of Hong Kong, Hong Kong
Deepak Laxmi Narasimha University of Malaya, Malaysia
Prabhat K. Mahanti University of New Brunswick, Canada

Publication Chair

Maricel O. Balitanas Hannam University, Korea

Program Committee

Abdelwahab Hamou-Lhadj
Ahmet Koltuksuz
Albert Levi
Andreas Jacobsson
Bonnetoi Pierre-Francois
Chantana Chantrapornchai
Chun-Ying Huang
Daniel Port
Debasis Giri
Dharma P. Agrawal
Dvorák Radim
Eduardo Fernandez
Fanguo Zhang
Filip Orsag
Hájek Josef
Han-Chieh Chao
Hejtmánková (Lodrová) Dana
Hiroaki Kikuchi
Hironori Washizaki
Hongji Yang
Hyun Sung Kim
J.H. Abawajy
Jan deMeer
Jari Veijalainen
Javier Garcia-Villalba
Jeng-Shyang Pan
Jonathan Lee
Josef Bigun
Kenichi Takahashi
Mario Freire

Martin Drahansky
Marvan Aleš
Mráček Štěpán
N. Jaisankar
Novotný Tomáš
Paolo D'Arco
Paolo Falcarin
Petr Hanacek
Pierre-François Bonnetoi
Qi Shi
Reinhard Schwarz
Rodrigo Mello
Rolf Oppliger
Rui Zhang
S.K. Barai
Serge Chaumette
Slobodan Petrovic
Stan Kurkovsky
Stefanos Gritzalis
Swee-Huay Heng
Tony Shan
Vána Jan
Victor Winter
Wei Yan
Yannis Stamatiou
YeongDeok Kim
Yi Mu
Yong Man Ro
Yoshiaki Hori

Table of Contents

Information Security Awareness Campaign: An Alternate Approach	1
<i>Bilal Khan, Khaled S. Alghathbar, and Muhammad Khurram Khan</i>	
Equivalent Key Recovery Attack on H^2 -MAC Instantiated with MD5 . . .	11
<i>Wei Wang</i>	
Recent Progress in Code-Based Cryptography	21
<i>Pierre-Louis Cayrel, Sidi Mohamed El Yousfi Alaoui, Gerhard Hoffmann, Mohammed Meziani, and Robert Niebuhr</i>	
GPU Implementation of the Keccak Hash Function Family	33
<i>Pierre-Louis Cayrel, Gerhard Hoffmann, and Michael Schneider</i>	
A Comparative Study of a New Associative Classification Approach for Mining Rare and Frequent Classification Rules	43
<i>Ines Bouzouita, Michel Liquiere, Samir Elloumi, and Ali Jaoua</i>	
Secret Key Awareness Security Public Key Encryption Scheme	53
<i>Guoyan Zhang and Qiuliang Xu</i>	
Using SAT Solving to Improve Differential Fault Analysis of Trivium . . .	62
<i>Mohamed Saied Emam Mohamed, Stanislav Bulygin, and Johannes Buchmann</i>	
Design of a Retargetable Decompiler for a Static Platform-Independent Malware Analysis	72
<i>Lukáš Ďurфина, Jakub Křoustek, Petr Zemek, Dušan Kolář, Tomáš Hruška, Karel Masařík, and Alexander Meduna</i>	
The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review	87
<i>Soltan Alharbi, Jens Weber-Jahnke, and Issa Traore</i>	
Multistep Attack Detection and Alert Correlation in Intrusion Detection Systems	101
<i>Fabio Manganiello, Mirco Marchetti, and Michele Colajanni</i>	
2SC: An Efficient Code-Based Stream Cipher	111
<i>Mohammed Meziani, Pierre-Louis Cayrel, and Sidi Mohamed El Yousfi Alaoui</i>	
Towards Algebraic Cryptanalysis of HFE Challenge 2	123
<i>Mohamed Saied Emam Mohamed, Jintai Ding, and Johannes Buchmann</i>	

S-FSB: An Improved Variant of the FSB Hash Family	132
<i>Mohammed Meziani, Özgür Dagdelen, Pierre-Louis Cayrel, and Sidi Mohamed El Yousfi Alaoui</i>	
Improved Identity-Based Identification and Signature Schemes Using Quasi-Dyadic Goppa Codes	146
<i>Sidi Mohamed El Yousfi Alaoui, Pierre-Louis Cayrel, and Meziani Mohammed</i>	
A Deterministic Factorization and Primality Testing Algorithm for Integers of the Form $Z \text{ Mod } 6 = -1$	156
<i>Noureddien Abdelrhman Noureddien, Mahmud Awadelkariem, and DeiaEldien M. Ahmed</i>	
Non-interactive Deniable Authentication Protocol Using Generalized ECDSA Signature Scheme	166
<i>Jayaprakash Kar</i>	
Lower Bounds for Interpolating Polynomials for Square Roots of the Elliptic Curve Discrete Logarithm	177
<i>Gerasimos C. Meletiou, Yannis C. Stamatiou, and Apostolos Tsiakalos</i>	
Towards Next Generation System Architecture for Emergency Services	188
<i>Jari Veijalainen and Veikko Hara</i>	
Securing Communication between SCADA Master Station and Mobile Remote Components	203
<i>Roslin John Robles and Gil-Cheol Park</i>	
Retrofit to CAIN of IP-Based Supervisory Control and Data Acquisition System	211
<i>Maricel O. Balitanas, Seung-Hwan Jeon, and Tai-hoon Kim</i>	
Application Program Interface as Back-Up Data Source for SCADA Systems	219
<i>Roslin John Robles and Tai-hoon Kim</i>	
Retracted Chapter: Supervisory Control and Data Acquisition System CAIN Issues	227
<i>Maricel O. Balitanas and Tai-hoon Kim</i>	
RFID Implementation and Security Issues	236
<i>Young B. Choi, Tae Hwan Oh, and Rajath Chouta</i>	
Vehicle Tracking Based on Kalman Filter in Tunnel	250
<i>Gyuyeong Kim, Hyuntae Kim, Jangsik Park, and Yunsik Yu</i>	

The Contents Based Music Retrieval Method Using Audio Feature Analysis against Polyphonic Music	257
<i>Chai-Jong Song, Seok-Pil Lee, and Hochong Park</i>	
A Noise Robust Echo Canceller with Post-processing Using Linear Predictor and Wiener Filter	264
<i>Hyuntae Kim, Daehyun Ryu, and Jangsik Park</i>	
Implementation Fire Detection Algorithm Using Fixed Point Digital Signal Processor	275
<i>Jangsik Park, Hyuntae Kim, and Yunsik Yu</i>	
An Efficient Private Registry Management System Using DHT Based on FIPA Agent Platform	282
<i>Seung-Hyun Lee, Kyung-Soo Jang, Kee-Hyun Choi, Choon-Sung Nam, and Dong-Ryeol Shin</i>	
A Study for Method of Construct Encryption Scheme for Supporting Range Query Based on Bucket ID Transformation about Sensor Applications	292
<i>You-Jin Song, Jae-Sang Cha, and Jang-Mook Kang</i>	
Improvement of Message Processing Method for SOA Based Digital Set-Top Box System	306
<i>Ji-Yeon Hwang, Seung-Jung Shin, and Dae-Hyun Ryu</i>	
A Data Management Method to Secure Data in Cloud Computing Environment	313
<i>You-Jin Song, Jae-Sang Cha, Jang-Mook Kang, and Wan-Sik Kim</i>	
VLSI Architecture of Adaptive Viterbi Decoder for Wireless Communication	318
<i>Dongjae Song, Soongyu Kwon, Chun-Guan Kim, and Jong Tae Kim</i>	
A Study for Security Scheme and the Right to Be Forgotten Based on Social Network Service for Smart-Phone Environment	326
<i>Jang-Mook Kang, You-Jin Song, Jae-Sang Cha, and Seon-Hee Lee</i>	
Development of Integrated Adapter Based on Multi-sensor Networks for Tracking and Surveillance	333
<i>Jun-Pil Boo and Do-Hyeun Kim</i>	
High Speed and Low-Complexity Mode Decision for Advanced Video Coding	339
<i>Byoungman An, Youngseop Kim, and Oh-Jin Kwon</i>	
Robust Congestion Control Design for Input Time Delayed AQM System	349
<i>Ji Hoon Yang, Seung Jung Shin, Dong Kyun Lim, and Jeong Jin Kang</i>	

An Intelligent Clustering Method for Highly Similar Digital Photos Using Pyramid Matching with Human Perceptual 25 Color Histogram	359
<i>Dong-Sung Ryu, Kwanghwi Kim, and Hwan-Gue Cho</i>	
Requirements Analysis and Critical Requirement Derivation Method Using Macrostruktur	367
<i>Yong-Kyun Cho and Young-Bum Park</i>	
A Scheme for Role-Based 3D CCTV Using CS-RBAC (Context-Sensitivity Role-Based Access Control)	378
<i>Jang-Mook Kang, Jae-Sang Cha, You-Jin Song, Goo-Man Park, Eun-Young Ko, Myong-chul Shin, Jeong-Jin Kang, and You-Sik Hong</i>	
Vessel Tracking Using Adaboost Algorithm and AIS Information	384
<i>Jangsik Park, Hyuntae Kim, Gyuyeong Kim, and Yunsik Yu</i>	
Relative Self-localization Base on Fish-Eye Lenses and SIFT Algorithm for Indoor Mobile Robot	389
<i>Xing Xiong and Byung-Jae Choi</i>	
User-Oriented Pseudo Biometric Image Based One-Time Password Mechanism on Smart Phone	395
<i>Wonjun Jang, Sikwan Cho, and Hyung-Woo Lee</i>	
Erratum	
Supervisory Control and Data Acquisition System CAIN Issues	E1
<i>Maricel O. Balitanas and Tai-hoon Kim</i>	
Author Index	405