Communications in Computer and Information Science 200
Information Security and Assurance

International Conference, ISA 2011
Brno, Czech Republic, August 15-17, 2011
Proceedings
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 Drahanský
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 Koltuksz
Albert Levi
Andreas Jacobsson
Bonnefoi Pierre-Francois
Chantana Chantrapornchai
Chun-Ying Huang
Daniel Port
Debasis Giri
Dharma P. Agrawal
Dvorák Radim
Eduardo Fernandez
Fangguo 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
Mrácek Štepán
N. Jaisankar
Novotný Tomáš
Paolo D’Arco
Paolo Falcarin
Petr Hanacek
Pierre-François Bonnefoi
Qi Shi
Reinhard Schwarz
Rodrigo Mello
Rolf Oppliger
Ruí 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  
_Bilal Khan, Khaled S. Alghathbar, and Muhammad Khurram Khan_  
1

Equivalent Key Recovery Attack on $H^2$-MAC Instantiated with MD5  
_Wei Wang_  
11

Recent Progress in Code-Based Cryptography  
_Pierre-Louis Cayrel, Sidi Mohamed El Yousfi Alaoui, Gerhard Hoffmann, Mohammed Meziani, and Robert Niebuhr_  
21

GPU Implementation of the Keccak Hash Function Family  
_Pierre-Louis Cayrel, Gerhard Hoffmann, and Michael Schneider_  
33

A Comparative Study of a New Associative Classification Approach for Mining Rare and Frequent Classification Rules  
_Ines Bouzouita, Michel Liquiere, Samir Elloumi, and Ali Jaoua_  
43

Secret Key Awareness Security Public Key Encryption Scheme  
_Guoyan Zhang and Qiuliang Xu_  
53

Using SAT Solving to Improve Differential Fault Analysis of Trivium  
_Mohamed Saied Emam Mohamed, Stanislav Bulygin, and Johannes Buchmann_  
62

Design of a Retargetable Decompiler for a Static Platform-Independent Malware Analysis  
_Lukáš Řurfína, Jakub Křouštěk, Petr Zemek, Dušan Kolář, Tomáš Hruška, Karel Masařík, and Alexander Meduna_  
72

The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review  
_Soltan Alharbi, Jens Weber-Jahnke, and Issa Traore_  
87

Multistep Attack Detection and Alert Correlation in Intrusion Detection Systems  
_Fabio Manganiello, Mirco Marchetti, and Michele Colajanni_  
101

2SC: An Efficient Code-Based Stream Cipher  
_Mohammed Meziani, Pierre-Louis Cayrel, and Sidi Mohamed El Yousfi Alaoui_  
111

Towards Algebraic Cryptanalysis of HFE Challenge 2  
_Mohamed Saied Emam Mohamed, Jintai Ding, and Johannes Buchmann_  
123
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>S-FSB: An Improved Variant of the FSB Hash Family</td>
<td>132</td>
</tr>
<tr>
<td>Mohammed Meziani, Özgür Dagdelen, Pierre-Louis Cayrel, and Sidi Mohamed El Yousfi Alaoui</td>
<td></td>
</tr>
<tr>
<td>Improved Identity-Based Identification and Signature Schemes Using Quasi-Dyadic Goppa Codes</td>
<td>146</td>
</tr>
<tr>
<td>Sidi Mohamed El Yousfi Alaoui, Pierre-Louis Cayrel, and Meziani Mohammed</td>
<td></td>
</tr>
<tr>
<td>A Deterministic Factorization and Primality Testing Algorithm for Integers of the Form ( Z \mod 6 = -1 )</td>
<td>156</td>
</tr>
<tr>
<td>Noureldien Abdelrhman Noureldien, Mahmoud Awadelkariem, and DeiaEldien M. Ahmed</td>
<td></td>
</tr>
<tr>
<td>Non-interactive Deniable Authentication Protocol Using Generalized ECDSA Signature Scheme</td>
<td>166</td>
</tr>
<tr>
<td>Jayaprakash Kar</td>
<td></td>
</tr>
<tr>
<td>Lower Bounds for Interpolating Polynomials for Square Roots of the Elliptic Curve Discrete Logarithm</td>
<td>177</td>
</tr>
<tr>
<td>Gerasimos C. Meletiou, Yannis C. Stamatiou, and Apostolos Tsiakalos</td>
<td></td>
</tr>
<tr>
<td>Towards Next Generation System Architecture for Emergency Services</td>
<td>188</td>
</tr>
<tr>
<td>Jari Veijalainen and Veikko Hara</td>
<td></td>
</tr>
<tr>
<td>Securing Communication between SCADA Master Station and Mobile Remote Components</td>
<td>203</td>
</tr>
<tr>
<td>Rosslin John Robles and Gil-Cheol Park</td>
<td></td>
</tr>
<tr>
<td>Retrofit to CAIN of IP-Based Supervisory Control and Data Acquisition System</td>
<td>211</td>
</tr>
<tr>
<td>Maricel O. Balitanas, Seung-Hwan Jeon, and Tai-hoon Kim</td>
<td></td>
</tr>
<tr>
<td>Application Program Interface as Back-Up Data Source for SCADA Systems</td>
<td>219</td>
</tr>
<tr>
<td>Rosslin John Robles and Tai-hoon Kim</td>
<td></td>
</tr>
<tr>
<td>Retracted Chapter: Supervisory Control and Data Acquisition System CAIN Issues</td>
<td>227</td>
</tr>
<tr>
<td>Maricel O. Balitanas and Tai-hoon Kim</td>
<td></td>
</tr>
<tr>
<td>RFID Implementation and Security Issues</td>
<td>236</td>
</tr>
<tr>
<td>Young B. Choi, Tae Hwan Oh, and Rajath Chouta</td>
<td></td>
</tr>
<tr>
<td>Vehicle Tracking Based on Kalman Filter in Tunnel</td>
<td>250</td>
</tr>
<tr>
<td>Gyuyeong Kim, Hyuntae Kim, Jangsik Park, and Yunsik Yu</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>The Contents Based Music Retrieval Method Using Audio Feature Analysis against Polyphonic Music</td>
<td>257</td>
</tr>
<tr>
<td><em>Chai-Jong Song, Seok-Pil Lee, and Hochong Park</em></td>
<td></td>
</tr>
<tr>
<td>A Noise Robust Echo Canceller with Post-processing Using Linear Predictor and Wiener Filter</td>
<td>264</td>
</tr>
<tr>
<td><em>Hyuntae Kim, Daehyun Ryu, and Jangsik Park</em></td>
<td></td>
</tr>
<tr>
<td>Implementation Fire Detection Algorithm Using Fixed Point Digital Signal Processor</td>
<td>275</td>
</tr>
<tr>
<td><em>Jangsik Park, Hyuntae Kim, and Yunsik Yu</em></td>
<td></td>
</tr>
<tr>
<td>An Efficient Private Registry Management System Using DHT Based on FIPA Agent Platform</td>
<td>282</td>
</tr>
<tr>
<td><em>Seung-Hyun Lee, Kyung-Soo Jang, Kee-Hyun Choi, Choon-Sung Nam, and Dong-Ryeol Shin</em></td>
<td></td>
</tr>
<tr>
<td>A Study for Method of Construct Encryption Scheme for Supporting Range Query Based on Bucket ID Transformation about Sensor Applications</td>
<td>292</td>
</tr>
<tr>
<td><em>You-Jin Song, Jae-Sang Cha, and Jang-Mook Kang</em></td>
<td></td>
</tr>
<tr>
<td>Improvement of Message Processing Method for SOA Based Digital Set-Top Box System</td>
<td>306</td>
</tr>
<tr>
<td><em>Ji-Yeon Hwang, Seung-Jung Shin, and Dae-Hyun Ryu</em></td>
<td></td>
</tr>
<tr>
<td>A Data Management Method to Secure Data in Cloud Computing Environment</td>
<td>313</td>
</tr>
<tr>
<td><em>You-Jin Song, Jae-Sang Cha, Jang-Mook Kang, and Wan-Sik Kim</em></td>
<td></td>
</tr>
<tr>
<td>VLSI Architecture of Adaptive Viterbi Decoder for Wireless Communication</td>
<td>318</td>
</tr>
<tr>
<td><em>Dongjae Song, Soongyu Kwon, Chun-Guan Kim, and Jong Tae Kim</em></td>
<td></td>
</tr>
<tr>
<td>A Study for Security Scheme and the Right to Be Forgotten Based on Social Network Service for Smart-Phone Environment</td>
<td>326</td>
</tr>
<tr>
<td><em>Jang-Mook Kang, You-Jin Song, Jae-Sang Cha, and Seon-Hee Lee</em></td>
<td></td>
</tr>
<tr>
<td>Development of Integrated Adapter Based on Multi-sensor Networks for Tracking and Surveillance</td>
<td>333</td>
</tr>
<tr>
<td><em>Jun-Pil Boo and Do-Hyeon Kim</em></td>
<td></td>
</tr>
<tr>
<td>High Speed and Low-Complexity Mode Decision for Advanced Video Coding</td>
<td>339</td>
</tr>
<tr>
<td><em>Byoungman An, Youngseop Kim, and Oh-In Kwon</em></td>
<td></td>
</tr>
<tr>
<td>Robust Congestion Control Design for Input Time Delayed AQM System</td>
<td>349</td>
</tr>
<tr>
<td><em>Ji Hoon Yang, Seung Jung Shin, Dong Kyun Lim, and Jeong Jin Kang</em></td>
<td></td>
</tr>
</tbody>
</table>
An Intelligent Clustering Method for Highly Similar Digital Photos Using Pyramid Matching with Human Perceptual Color Histogram ...................................................... 359
   Dong-Sung Ryu, Kwanghwi Kim, and Hwan-Gue Cho

Requirements Analysis and Critical Requirement Derivation Method Using Macrostruktur ............................................. 367
   Yong-Kyun Cho and Young-Bum Park

A Scheme for Role-Based 3D CCTV Using CS-RBAC (Context-Sensitivity Role-Based Access Control) ..................... 378
   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

Vessel Tracking Using Adaboost Algorithm and AIS Information ...... 384
   Jangsik Park, Hyuntae Kim, Gyuyeong Kim, and Yunsik Yu

Relative Self-localization Base on Fish-Eye Lenses and SIFT Algorithm for Indoor Mobile Robot ........................................ 389
   Xing Xiong and Byung-Jae Choi

User-Oriented Pseudo Biometric Image Based One-Time Password Mechanism on Smart Phone ................................. 395
   Wonjun Jang, Sikwan Cho, and Hyung-Woo Lee

Erratum

Supervisory Control and Data Acquisition System CAIN Issues ......... E1
   Maricel O. Balitanas and Tai-hoon Kim

Author Index .................................................. 405