

*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*

Alfred Kobsa

*University of California, Irvine, CA, 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

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max-Planck Institute of Computer Science, Saarbruecken, Germany*

Jong Hyuk Park Hsiao-Hwa Chen  
Mohammed Atiquzzaman Changhoon Lee  
Tai-hoon Kim Sang-Soo Yeo (Eds.)

# Advances in Information Security and Assurance

Third International Conference and Workshops, ISA 2009  
Seoul, Korea, June 25-27, 2009  
Proceedings

Volume Editors

Jong Hyuk Park

Kyungnam University, Department of Computer Science and Engineering

Masan, Kyungnam, Korea

E-mail: parkjonghyuk1@hotmail.com

Hsiao-Hwa Chen

National Sun Yat-Sen University, Institute of Communications Engineering

Kaohsiung City, Taiwan

E-mail: hshwchen@ieee.org

Mohammed Atiquzzaman

University of Oklahoma, School of Computer Science

Norman, OK, USA

E-mail: atiq@ou.edu

Changhoon Lee

Hanshin University, School of Computer Engineering

Osan, Kyeong-Gi, Korea

E-mail: cryptography1@gmail.com

Tai-hoon Kim

Hannam University, School of Multimedia, Daejeon, Korea

E-mail: taihoonn@empal.com

Sang-Soo Yeo

Mokwon University, Division of Computer Engineering, Daejeon, Korea

E-mail: ssyeo@msn.com

Library of Congress Control Number: Applied for

CR Subject Classification (1998): C.2, D.4.6, K.6.5, H.2.7, K.4.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743

ISBN-10 3-642-02616-8 Springer Berlin Heidelberg New York

ISBN-13 978-3-642-02616-4 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.com

© Springer-Verlag Berlin Heidelberg 2009

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper SPIN: 12702749 06/3180 5 4 3 2 1 0

## Preface

Welcome to the Third International Conference on Information Security and Assurance (ISA 2009). ISA 2009 was the most comprehensive conference focused on the various aspects of advances in information security and assurance. The concept of security and assurance is emerging rapidly as an exciting new paradigm to provide reliable and safe life services. Our conference provides a chance for academic and industry professionals to discuss recent progress in the area of communication and networking including modeling, simulation and novel applications associated with the utilization and acceptance of computing devices and systems. ISA 2009 was a successor of the First International Workshop on Information Assurance in Networks (IAN 2007, Jeju-island, Korea, December, 2007), and the Second International Conference on Information Security and Assurance (ISA 2008, Busan, Korea, April 2008). The goal of this 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 technology.

ISA 2009 contained research papers submitted by researchers from all over the world. In order to guarantee high-quality proceedings, we put extensive effort into reviewing the papers. All submissions were peer reviewed by at least three Program Committee members as well as external reviewers. As the quality of the submissions was quite high, it was extremely difficult to select the papers for oral presentation and publication in the proceedings of the conference. After extensive discussion and review, we finally decided to accept a total of 41 full papers for publication in LNCS volume 5576 from 137 submitted papers. We believe that the chosen papers and topics provide novel ideas on future research activities.

It would have been impossible to organize our program without the help of many enthusiastic individuals. We owe special thanks to Sajid Hussain and Alan Chin-Chen Chang for serving as Workshop Co-chairs. We also thank all the members of the Program Committee (PC) who reviewed all of the papers submitted to the conference and provided their feedback to the authors. We appreciate the help of Hangbae Chang, Soo Kyun Kim, and Deok Gyu Lee for serving as the Local Chairs of the conference. They coordinated the use of the conference facilities and set up the registration website. And we would like to take this opportunity to thank all the authors and participants for their contributions to the conference.

Finally, we acknowledge the work of Doo-soon Park as Honorary Chair and the members of our International Advisory Board who have provided long-term guidance for the conference.

Jong Hyuk Park  
Hsiao-Hwa Chen  
M. Atiquzzaman  
Changhoon Lee  
Justin Zhan  
Guilin Wang  
Sang-Soo Yeo

# Organization

## Organizing Committee

Honorary Chair	Doo-soon Park (SoonChunHyang University, Korea)
General Chairs	Jong Hyuk Park (Kyungnam University, Korea) Hsiao-Hwa Chen (National Sun Yat-Sen University, Taiwan) M. Atiquzzaman (University of Oklahoma, USA)
International Advisory Board	Peng Ning (North Carolina State University, USA) Tai-hoon Kim (Hannam University, Korea) Kyo Il Chung (ETRI, Korea) Laurence T. Yang (St. Francis Xavier University, Canada) Stefanos Gritzalis (University of the Aegean, Greece) Alan Chin-Chen Chang (National Chung Cheng University, Taiwan) Sung-Eon Cho (Sunchon National University, Korea) Wai Chi Fang (National Chiao Tung University, Taiwan) Tughrul Arslan (University of Edinburgh, UK) Javier Lopez (University of Malaga, Spain) Hamid R. Arabnia (The University of Georgia, USA) Dominik Slezak (Infobright Inc., Canada)
Program Chairs	Justin Zhan (CMU, USA) Changhoon Lee (Hanshin University, Korea) Guilin Wang (University of Birmingham, UK)
Publication Chair	Sang-Soo Yeo (Mokwon University, Korea)

## Program Committee

Alessandro Piva	Dharma P. Agrawal	Guojun Wang
Binod Vaidya	Dieter Gollmann	Hee-Jung Lee
Bo Zhu	Dorothy Denning	Ioannis G. Askoxylakis
Boniface Hicks	Duncan S. Wong	Isaac Agudo
Byoungcheon Lee	Edward Jung	Jaechul Sung
Chin-Chen Chang	Francesca Saglietti	Jan deMeer
Chunming Rong	Gail-Joon Ahn	Jeng-Shyang Pan
Claudio Ardagna	George Ghinea	Jianying Zhou
Dawu Gu	Golden G. Richard III	Jie Li

VIII Organization

Jongsung Kim	Nancy Mead	Stephen Wolthusen
Julio Cesar Hernandez-Castro	Ning Zhang	Steven M. Furnell
Jung-Taek Seo	Pierre Dusart	Swee Keow Goo
Kevin Butler	Pierre-François Bonnefoi	Theodore Tryfonas
Konstantinos Markantonakis	Raphael Phan	Tieyan Li
Kouichi Sakurai	Rui Xue	Vrizlynn L.L. Thing
Kui Ren	Sara Foresti	Wade Trappe
Lei Hu	Seokhie Hong	Wei Yan
Liwen He	Serge Chaumette	Will Enck
Martin Loeb	Shambhu Upadhyaya	Willy Susilo
Michael Tunstall	Shuhong Wang	Xuhua Ding
Michael W. Sobolewski	Soonseok Kim	Yafei Yang
Min-Shiang Hwang	Sos Agaian	Yan Wang
	Stephen R. Tate	Yi Mu

## **Welcome Message from the MoWiN 2009 Organizers**

We are happy to welcome you to the proceedings of the First International workshop on Mobile and Wireless Networks (MoWiN 2009). The symposium was held in conjunction with the Third International Conference on Information Security and Assurance ISA 2009), Seoul, South Korea, June 25–27, 2009. This workshop is intended to cover contributions on both the design and analysis of mobile, wireless, ad-hoc, and sensor networks. The goal of this workshop is to bring together researchers and practitioners from academia and industry to focus on advanced wireless and mobile computing concepts and to establish new collaborations in these areas. It is clear that the mobile and wireless networks technology has attracted increasing enthusiastic researchers from diverse backgrounds, including computer sciences, computer engineering, communication engineering and others.

We received 44 submissions overall, out of which 17 were accepted to be presented in the workshop. The submissions came from all over the world which reflects the value of the workshop as an international event. We were also pleased to see the broad range of subjects addressed by the submissions which covered the workshop interests.

We sincerely hope MoWiN 2009 will be the first in a series of many such technical meetings and we hope the community is involved in organizing future MoWiN events. The AIRCC and Program Committee members and the referees deserve praise for providing timely and valuable reviews, and producing the excellent final program. We wish to thank the MoWiN 2009 Chairs, Co-chairs, for coordinating and organizing the review process. We would also like to thank the Workshop Chairs of ISA 2009 and the Organizing Committee for support given to MoWiN 2009.

We believe this workshop complements perfectly the topic focus of ISA 2009 and provides additional breadth and depth to the main conference.

Jacques Demerjian  
Balasubramanian K  
Natarajan Meghanathan  
Rajendra Akerkar  
Sri Ramaswamy



## **Welcome Message from the NASSUE-2009 Organizers**

We would like to welcome you to the proceedings of the 2009 International Workshop on Network Assurance and Security Services in Ubiquitous Environments (NASSUE-2009) held in conjunction with the Third International Conference on Information Security and Assurance (ISA 2009) in Seoul, Republic of Korea.

NASSUE-2009 focused on network assurance and security (NAS) measures, which has become an important research issue in ubiquitous environments. A large number of good papers were submitted to NASSUE-2009. All the submitted papers underwent a rigorous review process by the Technical Program Committee (TPC) members and some external reviewers. Only 17 high-quality papers were accepted for presentation and publication in the conference proceedings.

We would like to sincerely thank all the people who contributed directly or indirectly to making NASSUE-2009 a grand success. We would like to express our appreciation to all TPC members and IAB members for the valuable time and their professional support of this workshop. Finally, we would like to show our gratitude to all the authors for choosing NASSUE-2009 as a forum to discuss their research contributions.

Binod Vaidya  
James B.D. Joshi  
Joel Rodrigues

# NASSUE-2009 Organization

## Organizing Committee

Steering Chair	Jong Hyuk Park (Kyungnam University, Korea)
Workshop Program Chairs	Binod Vaidya (Gwangju Institute of Science and Technology, Korea) James B.D. Joshi (University of Pittsburgh, USA) Joel Rodrigues (Instituto de Telecomunicações/University of Beira Interior, Portugal)
International Advisory Board	Dimitrios Makrakis (University of Ottawa, Canada) Elisa Bertino (Purdue University, USA) Pascal Lorenz (University of Haute Alsace, France) Yoshito Tobe (Tokyo Denki University, Japan)

## Program Committee

Abdelhamid Mellouk	Jiankun Hu	Niwat
António Nogueira	Joel Rodrigues	Thepvilojapanong
Bai Xiaoying	Jorge Sá Silva	Pascal Lorenz
Binod Vaidya	Jouni Ikonen	Paulo Salvador
Bo Zhu	K. P. Chow	Pavel Gladyshev
ByungRae Cha	Katsikas Sokratis	Seungjoo Kim
Chae Hoon Lim	Khaled Salah	Shiguo Lian
Eul Gyu Im	Mário Lemos Proença	Surya Nepal
Farid Farahmand	Junior	Tapio Frantti
Gail-Joon Ahn	Masato Terada	Willy Susilo
Hiroshi Yoshiura	Min-Shiang Hwang	Yafei Yang
James B.D. Joshi	Ning Zhang	Yoshihiro Kawahara

## **Message from the IAWSN 2009 Workshop Chairs**

It is our great pleasure to welcome you to the proceedings of the First International Workshop on Information Assurance in Wireless Sensor Networks (IAWSN 2009), which was held in conjunction with the Third International Conference on Information Security and Assurance (ISA 2009) Seoul, Korea.

This workshop is intended to establish definitive areas of learning and development for further venturing into WSN security research areas. The recent widespread desire for connectivity has led to exponential advances in wireless communication. The ongoing IT revolution has changed the way we conduct our daily activities, business and communication. It is vital that network researchers and practitioners keep up with evolving technologies and infrastructure. Wireless sensor networks and their associated applications form a major part of this communication evolution. Advanced fundamental research in this domain puts security and assurance as the first priority.

We imposed a very tight submission deadline, giving less than 8 weeks for the authors to prepare and submit the papers. We received 16 submissions overall, out of which 8 were accepted to be presented in the workshop. The quality of the submissions is excellent and reflects the broad range of subjects covered by the workshop.

It is a challenge to organize such an international workshop under a tight timeframe. Many people contributed their time and effort to the success of IAWSN 2009. The Program Committee members deserve all the praise for providing timely and valuable reviews. Finally, we would like to express our sincere appreciation to all those who contributed to the success of this workshop. We hope you enjoy the workshop proceedings.

Firdous Kausar  
Farag Azzedin  
Ayesha Naureen

## **Welcome Message from the WNGS/CGMS 2009 Organizers**

It is a great pleasure to welcome you to the proceedings of the WNGS/CGM 2009 workshop, which was held in conjunction with the Third International Conference on Information Security and Assurance (ISA 2009), at Korea University, Seoul, Korea.

The workshops cover topics on computer graphics, multimedia and security and next-generation security systems. All submitted papers underwent a rigorous review process by the Technical Program Committee members and external reviewers. WNGS/CGM received 30 papers from 8 countries, and accepted 9 papers for the presentation track.

WNGS/CGM 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 would like to thank everyone who directly or indirectly contributed to the success of these workshops. In particular, we would like to thank Soo Kyun Kim and Deok Gyu Lee for coordinating WNGS 2009 and the TPC members for extending their professional support to the workshop. Last but not least, we would like to thank all authors of WNGS/CGM for supporting the workshop by choosing it as a forum for reporting their quality research results.

Deok Gyu Lee  
Sankar Kumar Pal  
Soo Kyun Kim  
Yan Zhang

# WNGS/CGMS 2009 Organization

## WNGS Organizing Committee

### International Advisory Committee

Kyo-II Chung (ETRI, Korea)  
Im Yeong Lee (Soonchunhyang University, Korea)  
Heekuck Oh (Hanyang University, Korea)  
Chang Seop Park (Dankook University, Korea)

### Workshop Chair

Deok Gyu Lee (ETRI, Korea)

## WNGS Program Committee

Daniel Page	Heang Suk Oh	Seoung Hyeon Lee
Debra Lee Cook	Jean-Henry Morin	Tsuyoshi Takagi
Dimitrios Katsaros	Jin Kwak	Hong Seung Ko
Do-Woo Kim	Jong Wook Han	Dongdai Lin
Gianluca Moro	Sajid Hussain	Susan Pancho-Festin

## CGMS Organizing Committee

### Workshop Chairs

Sankar Kumar Pal (Indian Statistical Institute, India)  
Soo Kyun Kim (PaiChai University, Korea)  
Yan Zhang (Simula Research Laboratory, Norway)

### International Advisory Committee

Tai-hoon Kim (Hannam University, Korea)  
Jong Hyuk Park (Kyungnam University, Korea)  
Jianhua Ma (Hosei University, Japan)  
Edwin H-M. Sha (University of Texas at Dallas, USA)

## CGMS Program Committee

Fanguo Zhang	Paolo Remagnino	Karl Leung
Rui Zhang	Joonsang Baek	Hongji Yang
Francesco Masulli	Ryszard Tadeusiewicz	Paolo D'Arco
Kenneth Lam	Swee-Huay Heng	Salah Bourenane
Pablo de Heras	Yong Man Ro	Mark Manulis
Hyun-Sung Kim	Jin Kwak	Roman Neruda
MalRey Lee	Raphael C.-W. Phan	Jacques Blanc-Talon
Fabrice Mériaudeau	Mirosław Swiercz	Gérard Medioni
	Białystok	

Stefan Katzenbeisser

Abdelwahab

Hamou-Lhadj

Seenith Siva

Mototaka Suzuki

Jocelyn Chanussot

Mei-Ling Shyu

Christine

Fernandez-Maloigne

Junzhong Gu

Chi Sung Laih

Young Ik Eom

Hironori Washizaki

Shu-Ching Chen

Atsuko Miyaji

Hiroaki Kikuchi

Min Hong

Sun-Jeong

Shin Jin

Nikos Komodakis

Lejla Batina

Dieter Gollmann

Andrzej Dzielinski

Dimitris Iakovidis

Kouichi Sakurai

Yi Mu

## **Welcome Message from the SHCI 2009 Organizers**

Welcome to the Proceedings of SHCI 2009.

The fields of human-computer interaction (HCI) and ubiquitous computing (UC) focus on efforts to overcome obstacles between humans and computers. HCI is a discipline that studies the interaction between people and computers. Context-aware (CA) and ambient intelligence (Aml) are central issues in HCI, which consider the user context when creating user interfaces in ubiquitous environments. For this purpose, many technologies are involved including terminal technology, system technology, network technology, platform technology, application technology, artificial intelligence etc. However, users may get wrong results when there are many attackers present during the communication, and therefore security technology is needed for effective and reliable communication in HCI. This workshop allowed researchers in the field of security technology and HCI to present novel ideas, problems and solutions.

Dr. Ko

# SHCI 2009 Organization

## Organizing Committee

Organizers	Carlos Ramos (Institute of Engineering-Polytechnic of Porto (ISEP/IPP))
	Hoon Ko (Institute of Engineering-Polytechnic of Porto (ISEP/IPP))
	Goreti Marreiros (Institute of Engineering-Polytechnic of Porto (ISEP/IPP))
	Ning Chen (Institute of Engineering-Polytechnic of Porto (ISEP/IPP))
	Hussein Khodr (Institute of Engineering-Polytechnic of Porto (ISEP/IPP))

## Program Committee

An Chen  
António Costa  
Carlos Ramos  
Haesuck Oh  
Goreti Marreiros  
Giyong Kim  
Hoon Ko  
Hussein Khodr  
Joao Jose Pinto Ferreira  
JongMyoung Choi  
Jongjin Jung  
KyungSang Sung  
Ning Chen  
Yeonsuk Chang  
Yongtae Shin



# Table of Contents

## Cryptographic Algorithms

Update on SEED: SEED-192/256 . . . . .	1
<i>Kitae Jeong, Joongeun Choi, Yuseop Lee, Changhoon Lee, Jaechul Sung, Haeryong Park, and Yeonjung Kang</i>	

A New Double-Block-Length Hash Function Using Feistel Structure . . . .	11
<i>Jesang Lee, Seokhie Hong, Jaechul Sung, and Haeryong Park</i>	

## Authentication and Identity Management

The Dark Side of Timed Opacity . . . . .	21
<i>Franck Cassez</i>	

Certificateless Signature Scheme without Random Oracles . . . . .	31
<i>Yumin Yuan, Da Li, Liwen Tian, and Haishan Zhu</i>	

## Authorization and Access Control

Fine-Grain Access Control Using Shibboleth for the Storage Resource Broker . . . . .	41
<i>Vineela Muppavarapu and Soon M. Chung</i>	

Grouping Provenance Information to Improve Efficiency of Access Control . . . . .	51
<i>Amril Syalim, Yoshiaki Hori, and Kouichi Sakurai</i>	

Tagging the Turtle: Local Attestation for Kiosk Computing . . . . .	60
<i>Ronald Toegl</i>	

Selective Regression Test for Access Control System Employing RBAC . . . . .	70
<i>Chao Huang, Jianling Sun, Xinyu Wang, and Yuanjie Si</i>	

Formal Verification for Access Control in Web Information Sharing System . . . . .	80
<i>Akihiro Sakai, Yoshiaki Hori, and Kouichi Sakurai</i>	

## Biometrics and Computer Forensics

Adaptive Iris Segmentation . . . . .	90
<i>Rahib Abiyev and Kemal Kilic</i>	

Recognizing Partially Occluded Faces from a Single Exemplar Image Per Person .....	100
<i>Hamidreza Rashidy Kanan and M. Shahram Moin</i>	

Methodology and Tools of IS Audit and Computer Forensics – The Common Denominator .....	110
<i>Magdalena Szeżyńska, Ewa Huebner, Derek Bem, and Chun Ruan</i>	

## Cryptographic Protocols

What about Vulnerability to a Fault Attack of the Miller’s Algorithm During an Identity Based Protocol? .....	122
<i>Nadia El Mrabet</i>	

A New Strongly Secure Authenticated Key Exchange Protocol .....	135
<i>Qingfeng Cheng, Chuangui Ma, and Xuexian Hu</i>	

Improved Implementations of Cryptosystems Based on Tate Pairing ....	145
<i>Chang-An Zhao, Dongqing Xie, Fangguo Zhang, Chong-Zhi Gao, and Jingwei Zhang</i>	

Efficient Secure Multiparty Computation Protocol in Asynchronous Network .....	152
<i>Zheng Huang, Weidong Qiu, Qiang Li, and Kefei Chen</i>	

## Data Integrity and Privacy

Clustering-Based Frequency $l$ -Diversity Anonymization .....	159
<i>Mohammad-Reza Zare-Mirakabad, Aman Jantan, and Stéphane Bressan</i>	

Protect Disk Integrity: Solid Security, Fine Performance and Fast Recovery .....	169
<i>Fangyong Hou, Nong Xiao, Yuhua Tang, Hongjun He, and Fang Liu</i>	

A Kademlia-Based Node Lookup System for Anonymization Networks .....	179
<i>Benedikt Westermann, Andriy Panchenko, and Lexi Pimenidis</i>	

## Key Management and Recovery

A Computationally-Efficient Construction for the Matrix-Based Key Distribution in Sensor Network .....	190
<i>Abdelaziz Mohaisen, Nam-Su Jho, and Dowon Hong</i>	

Key-Insulated Encryption Based Key Pre-distribution Scheme for WSN .....	200
<i>Weidong Qiu, Yaowei Zhou, Bo Zhu, Yanfei Zheng, Mi Wen, and Zheng Gong</i>	

## Mobile and RFID Network Security

Securing Mobile Phone Calls with Identity-Based Cryptography .....	210
<i>Matthew Smith, Christian Schridde, Björn Agel, and Bernd Freisleben</i>	
On the Security Properties and Attacks against Mobile Agent Graph Head Sealing (MAGHS) .....	223
<i>Abid Khan, Qasim Arshad, Xiamu Niu, Zhang Yong, and Muhammad Waqas Anwar</i>	

## Firewall, IDS, Anti-virus, and Other Security Products

A New Approach to Malware Detection .....	229
<i>Hongying Tang, Bo Zhu, and Kui Ren</i>	
ATTENTION: ATTackEr Traceback Using MAC Layer AbNormality DetectTION .....	239
<i>Yongjin Kim</i>	
A Deployment Value Model for Intrusion Detection Sensors .....	250
<i>Siraj A. Shaikh, Howard Chivers, Philip Nobles, John A. Clark, and Hao Chen</i>	

## Internet and Web Services Security

Security Evaluation of an Intrusion Tolerant Web Service Architecture Using Stochastic Activity Networks .....	260
<i>Zahra Aghajani and Mohammad Abdollahi Azgomi</i>	
Counteracting Phishing Page Polymorphism: An Image Layout Analysis Approach .....	270
<i>Ieng-Fat Lam, Wei-Cheng Xiao, Szu-Chi Wang, and Kuan-Ta Chen</i>	

## Cyber-attack and Cyber-terrorism

Signaling-Oriented DoS Attacks in UMTS Networks .....	280
<i>Georgios Kambourakis, Constantinos Kolias, Stefanos Gritzalis, and Jong Hyuk-Park</i>	

Detecting DDoS Attacks Using Dispersible Traffic Matrix and Weighted Moving Average . . . . .	290
<i>Tae Hwan Kim, Dong Seong Kim, Sang Min Lee, and Jong Sou Park</i>	
Attack Patterns Discovery by Frequent Episodes Mining from Honeypot Systems . . . . .	301
<i>Ming-Yang Su, Kai-Chi Chang, and Chun-Yuen Lin</i>	
<b>Other Security Research</b>	
Efficient and Automatic Instrumentation for Packed Binaries . . . . .	307
<i>Yanjun Wu, Tzi-cker Chiueh, and Chen Zhao</i>	
Secure Cover Selection Steganography . . . . .	317
<i>Hedieh Sajedi and Mansour Jamzad</i>	
Side-Channel Leakage in Masked Circuits Caused by Higher-Order Circuit Effects . . . . .	327
<i>Zhimin Chen, Syed Haider, and Patrick Schaumont</i>	
Performance Analysis of Digital Secure Voice Transmission over HF Radio Channel . . . . .	337
<i>Kihong Kim and Jinkeun Hong</i>	
Energy Analysis of Multimedia Video Streaming on Mobile Devices . . . .	347
<i>Chu-Hsing Lin, Jung-Chun Liu, Mao-Hua Cheng, Tsung-Che Yang, and Mei-Chun Chou</i>	
Combating Index Poisoning in P2P File Sharing . . . . .	358
<i>Lingli Deng, Yeping He, and Ziyao Xu</i>	
A Cryptanalytic View of the NSA's Skipjack Block Cipher Design . . . . .	368
<i>Jongsung Kim and Raphael C.-W. Phan</i>	
MinuCode: A Fixed-Value Representation of Fingerprint Minutiae for Biometric Cryptosystem . . . . .	382
<i>Jinyang Shi and Kwok-Yan Lam</i>	
Self-initialized Distributed Certificate Authority for Mobile Ad Hoc Network . . . . .	392
<i>Meng Ge and Kwok-Yan Lam</i>	
Design and Delivery of Undergraduate IT Security Management Course . . . . .	402
<i>Jemal H. Abawajy</i>	

## MoWiN 2009

Secure Multi-party Computation Using Virtual Parties for Computation on Encrypted Data . . . . .	412
<i>Rohit Pathak and Satyadhar Joshi</i>	
Using a Link Metric to Improve Communication Mechanisms and Real-Time Properties in an Adaptive Middleware for Heterogeneous Sensor Networks . . . . .	422
<i>Edison Pignaton de Freitas, Tales Heimfarth, Marco Aurélio Wehrmeister, Flávio Rech Wagner, Armando Morado Ferreira, Carlos Eduardo Pereira, and Tony Larsson</i>	
Performance Evaluation of DSR in Multi-services Ad Hoc Networks . . . .	432
<i>Ronald Beaubrun and Badji Molo</i>	
Implementation and Evaluation of WiMedia MAC LSI . . . . .	438
<i>Kazuyuki Sakoda, Yuichi Morioka, Chihiro Fujita, Erica Tanimoto, Kenzoh Nishikawa, and Mitsuhiro Suzuki</i>	
A Reliable and Efficient Pedal Back Data Disseminating Scheme for Ad-Hoc WSNs . . . . .	450
<i>Nomica Imran and A.I. Khan</i>	
Improved Location Acquisition Algorithms for the Location-Based Alert Service . . . . .	461
<i>So-Young Kang, Jin-Woo Song, Kwang-Jo Lee, Ju-Hee Lee, Ji-Hoon Kim, and Sung-Bong Yang</i>	
An Enhanced Trust Center Based Authentication in ZigBee Networks . . . . .	471
<i>Kyunghwa Lee, Joohyun Lee, Bongduk Zhang, Jaeho Kim, and Yongtae Shin</i>	
Sensor Disposition Problem in Wireless Ad-Hoc Sensor Networks . . . . .	485
<i>Takahide Yanaka, Toshihiko Sasama, and Hiroshi Masuyama</i>	
Performance Evaluation of Cost Effective Routing for Packet Transmissions in Mobile Ad Hoc Networks . . . . .	494
<i>Kentaro Kishida, Toshihiko Sasama, and Hiroshi Masuyama</i>	
Energy Lesser Broadcasting Algorithms Using Adjustable Transmission Ranges in Mobile Ad Hoc Networks . . . . .	502
<i>Toshihiko Sasama, Yasuhiro Abe, and Hiroshi Masuyama</i>	
A Multi-Path Routing Supported Scheduling Algorithm for Multi-Channel Single-Transceiver Wireless Mesh Networks . . . . .	512
<i>Chen Mei-Jhen and Yu Gwo-Jong</i>	

Predictive Scheme for Location Service in Mobile Ad-Hoc Networks . . . . 522  
*Ebtisam Amar, Selma Boumerdassi, and Éric Renault*

An Efficient Hybrid Routing Approach for Hybrid Wireless Mesh  
 Networks . . . . . 532  
*Anh-Ngoc Le, Dong-Won Kum, and You-Ze Cho*

Relationship between Motivation and Satisfaction of Online Computer  
 Games: Evidence from Adolescent Players Using Wireless Service in  
 Taiwan . . . . . 543  
*Lily Shui-Lien Chen, Michael Chih-Hung Wang, and Yung-Hsin Lee*

DISHES: A Distributed Shell System for Ubiquitous Computing . . . . . 553  
*Chih-Chung Lai and Ren-Song Ko*

Error Control Scheme of Hybrid ARQ Based on Majority Voting Bit  
 by Bit . . . . . 563  
*Hsin-Kun Lai, Chia-Chin Ma, and Erl-Huei Lu*

Secure Error-Correction Network Coding in a Randomized Setting . . . . . 570  
*Yejun Zhou, Hui Li, and Jianfeng Ma*

Bayesian Approach Based Comment Spam Defending Tool . . . . . 578  
*Beatrice Cynthia Dhinakaran, Dhinakaran Nagamalai, and  
 Jae-Kwang Lee*

**NASSUE 2009**

An Improved Secure Identity-Based On-Line/Off-Line Signature  
 Scheme . . . . . 588  
*Jianhong Zhang, Yixian Yang, Xinxin Niu, Shengnan Gao,  
 Hua Chen, and Qin Geng*

Honeybee-Based Model to Detect Intrusion . . . . . 598  
*Ghassan Ahmed Ali, Aman Jantan, and Abdulghani Ali*

A Data Mining Framework for Building Intrusion Detection Models  
 Based on IPv6 . . . . . 608  
*Zenghui Liu and Yingxu Lai*

FPGA Implementation of Elliptic Curve Point Multiplication over  
 $GF(2^{191})$  . . . . . 619  
*Sameh m. Shohdy, Ashraf b. El-sisi, and Nabil Ismail*

A Forward-Secrecy WTLS Handshake Protocol Based on XTR . . . . . 635  
*Bin Li*

Application of 2D Barcode in Hardcopy Document Verification  
 System . . . . . 644  
*Mazleena Salleh and Teoh Chin Yew*

Protecting Global SOA from DoS and Other Security Threats . . . . .	652
<i>Deven Shah, Ashish Mangal, Mayank Agarwal, Mahendra Mehra, Tushar Dave, and Dhiren Patel</i>	

CRYPTEX Model for E-Commercial Contract of Software Source Code Using Secrete Sharing Scheme . . . . .	662
<i>ByungRae Cha and YoungIl Kim</i>	

HOTP-Based User Authentication Scheme in Home Networks . . . . .	672
<i>Binod Vaidya, Jong Hyuk Park, and Joel J.P.C. Rodrigues</i>	

## **IAWSN 2009**

A Comparative Analysis of HC-128 and Rabbit Encryption Schemes for Pervasive Computing in WSN Environment . . . . .	682
<i>Firdous Kausar and Ayesha Naureen</i>	

A Comparative Analysis of PKC and Semi-PKC Based Key Management Schemes for Hierarchical Sensor Networks . . . . .	692
<i>Ayesha Naureen, Attiya Akram, Rabia Riaz, Ki-Hyung Kim, and H. Farooq Ahmed</i>	

A Mathematical Approach towards Trust Based Security in Pervasive Computing Environment . . . . .	702
<i>Naima Iltaf, Mukhtar Hussain, and Farrukh Kamran</i>	

A Secure Group Rekeying Scheme with Compromised Node Revocation in Wireless Sensor Networks . . . . .	712
<i>Asma Khalid and Mukhtar Hussain</i>	

Fault Tolerant Secure Routing in Cluster Based Mobile Sensor Networks . . . . .	722
<i>Usama Ahmed, Muhammad Arif Wahla, and Firdous Kausar</i>	

Hardware-Based Random Number Generation in Wireless Sensor Networks(WSNs) . . . . .	732
<i>Rabia Latif and Mukhtar Hussain</i>	

Authenticated Encryption in WSN Using eSTREAM Ciphers . . . . .	741
<i>Shakil Ahmad, Arif Wahla, and Firdous Kausar</i>	

## **WNGS 2009 and CGMS 2009**

Aggregate and Verifiably Encrypted Signatures from Multilinear Maps without Random Oracles . . . . .	750
<i>Markus Rückert and Dominique Schröder</i>	

Device Authentication/Authorization Protocol for Home Network in Next Generation Security .....	760
<i>Jong Sik Moon, Deok Gyu Lee, and Im-Yeong Lee</i>	
A Study on Feasibility and Establishment of a Security Grade Certification Scheme for the New IT Services .....	769
<i>Hangbae Chang, Jonggu Kang, and Hyukjun Kwon</i>	
Domain Specific Intended Use Evaluation Method: Intrusion Detection Specific Intended Use Evaluation Method .....	778
<i>Albert Park</i>	
A Study of International Trend Analysis on Web Service Vulnerabilities in OWASP and WASC .....	788
<i>Soonseok Kim, Haeyoung Han, Donghwi Shin, Inkyung Jeun, and HyunCheol Jeong</i>	
Cryptanalysis of Secure Key Exchange Protocol between STB and Smart Card in IPTV Broadcasting .....	797
<i>Song-Hee Lee, Nam-Sup Park, Soo-Kyun Kim, and Jin-Young Choi</i>	
Free-Form Deformation Axis Aligned Bounding Box .....	804
<i>Sunhwa Jung, Min Hong, and Min-Hyung Choi</i>	
<b>SHCI-ISA 2009</b>	
A Study on Mosaic Based CCTV System Using Localization .....	814
<i>Jong-Min Kim and Myung-A Kang</i>	
Selecting the Wireless Communication Methods for Establishing Ubiquitous City-Gas Facilities in Korea .....	823
<i>Jeong Seok Oh, Jang Sik Park, and Jeong Rock Kwon</i>	
Safety High Accuracy Context-Aware Matrix (CAM) Making Based on X.509 Proxy Certificate .....	829
<i>Hoon Ko, Ning Chen, Goreti Marreiros, and Carlos Ramos</i>	
<b>Author Index</b> .....	839