Lecture Notes in Computer Science 5576

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

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

Springer

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

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

Jongsung Kim
Julio Cesar Hernandez-Castro
Jung-Taek Seo
Kevin Butler
Konstantinos Markantonakis
Kouichi Sakurai
Kui Ren
Lei Hu
Liwen He
Martin Loeb
Michael Tunstall
Michael W. Sobolewski
Min-Shiang Hwang
Nancy Mead
Ning Zhang
Pierre Dusart
Pierre-François Bonnefoi
Raphael Phan
Rui Xue
Sara Foresti
Seokhie Hong
Serge Chaumette
Shambhu Upadhyaya
Shuhong Wang
Soonseok Kim
Sos Agaian
Stephen R. Tate
Stephen Wolthusen
Steven M. Furnell
Swee Keow Goo
Theodore Tryfonas
Tieyan Li
Vrizlynn L.L. Thing
Wade Trappe
Wei Yan
Will Enck
Willy Susilo
Xuhua Ding
Yafei Yang
Yan Wang
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 divers 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
Srini 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
António Nogueira
Bai Xiaoying
Binod Vaidya
Bo Zhu
ByungRae Cha
Chae Hoon Lim
Eul Gyu Im
Farid Farahmand
Gail-Joon Ahn
Hiroshi Yoshiura
James B.D. Joshi
Jiankun Hu
Joel Rodrigues
Jorge Sá Silva
Jouni Ikonen
K. P. Chow
Katsikas Sokratis
Khaled Salah
Mário Lemos Proença Junior
Masato Terada
Min-Shiang Hwang
Ning Zhang
Niwat Thepvilojapanong
Pascal Lorenz
Paulo Salvador
Pavel Gladyshev
Seungjoo Kim
Shiguo Lian
Surya Nepal
Tapio Frantti
Willy Susilo
Yafei Yang
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-Il 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

Fangguo Zhang	Paolo Remagnino	Karl Leung
Rui Zhang	Joonsang Baek	Hongji Yang
Francesco Masulli	Ryszard Tadeusiewicz	Paolo D'Arco
Kenneth Lam	Swee-Huay Heng	Salah Bourennane
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	Miroslaw Swiercz Bialystok	Gérard Medioni

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 (AmI) 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
Giyoung 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

Authentication and Identity Management

Authorization and Access Control

Biometrics and Computer Forensics

Cryptographic Protocols

Data Integrity and Privacy

Key Management and Recovery

Mobile and RFID Network Security

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

Internet and Web Services Security

Cyber-attack and Cyber-terrorism

Other Security Research

MoWiN 2009

NASSUE 2009

IAWSN 2009

WNGS 2009 and CGMS 2009

SHCI-ISA 2009