

**Editors:**

**Michael N. Katehakis, Rutgers Business School, New Jersey, USA**

**Antonio Zamora, Universidad de Alicante, Spain**

**Rafael Alvarez, Universidad de Alicante, Spain**



# **ADVANCED TOPICS in INFORMATION SECURITY and PRIVACY**

**Published by WSEAS Press**  
[www.wseas.org](http://www.wseas.org)

**PROCEEDINGS OF the 6th WSEAS International  
Conference on INFORMATION SECURITY and PRIVACY (ISP '07)**



**Electrical and Computer Engineering Series**  
**A Series of Reference Books and Textbooks**

**Puerto De La Cruz, Tenerife, Canary Islands, Spain,  
December 14-16, 2007**

**ISBN: 978-960-6766-23-7**

**ISSN: 1790-5117**



# **ADVANCED TOPICS in INFORMATION SECURITY and PRIVACY**

**Proceedings of the  
6th WSEAS International Conference on  
INFORMATION SECURITY and PRIVACY  
(ISP '07)**

**Puerto De La Cruz, Tenerife, Canary Islands, Spain, December  
14-16, 2007**

# **ADVANCED TOPICS in INFORMATION SECURITY and PRIVACY**

## **Proceedings of the 6th WSEAS International Conference on INFORMATION SECURITY and PRIVACY (ISP '07)**

### **Electrical and Computer Engineering Series A Series of Reference Books and Textbooks**

Published by WSEAS Press  
[www.wseas.org](http://www.wseas.org)

**Copyright © 2007, by WSEAS Press**

All the copyright of the present book belongs to the World Scientific and Engineering Academy and Society Press. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the Editor of World Scientific and Engineering Academy and Society Press.

All papers of the present volume were peer reviewed by two independent reviewers. Acceptance was granted when both reviewers' recommendations were positive.  
See also: <http://www.worldses.org/review/index.html>

ISSN: 1790-5117  
ISBN: 978-960-6766-23-7



World Scientific and Engineering Academy and Society

**Editors:**

Michael N. Katehakis, Rutgers Business School, New Jersey, USA

Antonio Zamora, Universidad de Alicante, Spain

Rafael Alvarez, Universidad de Alicante, Spain

**Scientific Committee:**

Asad A. Abidi, USA	Bruce H. Krogh, USA
Andreas Antoniou, USA	David D. Yao, USA
Antonio Cantoni, Australia	Donald Towsley, USA
George Szentirmai, USA	Eduardo D. Sontag, USA
Michael Peter Kennedy, Ireland	Edward J. Davison, Canada
Henk Nijmeijer, The Netherlands	G. George Yin, USA
Paresh C. Sen, Canada	Giorgio Picci, Italy
Michel Gevers, Belgium	Graham C. Goodwin, Australia
James S. Thorp, USA	Han-Fu Chen, China
Armen H. Zemanian, USA	Harold J. Kushner, USA
Guanrong Chen, Hong Kong	Hidenori Kimura, Japan
Edgar Sánchez-Sinencio, USA	Ian Postlethwaite, UK
Yannis P. Tsividis, USA	Ian R. Petersen, Australia
A. J. van der Schaft, The Netherlands	Jan C. Willems, Netherlands
István Nagy, Hungary	Jim S. Freudenberg, USA
Wasfy B. Mikhael, USA	Karl Johan Astrom, Sweden
M. N. S. Swamy, Canada	Lennart Ljung, Sweden
Abbas El Gamal, USA	M. Vidyasagar, India
Franco Maloberti, Italy	Mark W. Spong, USA
Alan N. Willson Jr., USA	Matthew R. James, Australia
Yoji Kajitani, Japan	Munther A. Dahleh, USA
Mohammed Ismail, USA	P .R. Kumar, USA
Kemin Zhou, USA	Peter E. Caines, Canada
Ruey-Wen Liu, USA	Pramod P. Khargonekar, USA
Nabil H. Farhat, USA	Richard T. Middleton, Australia
John I. Sewell, UK	Roberto Tempo, Italy
Chung-Yu Wu, Taiwan	Roger W. Brockett, USA
Jerry M. Mendel, USA	Shankar Sastry, USA
James B. Kuo, Taiwan	Steven I. Marcus, USA
Magdy A. Bayoumi, USA	T. E. Duncan, USA
Bertram E. Shi, Hong Kong	Tamer Basar, USA
Irwin W. Sandberg, USA	W. M. Wonham, Canada
M. Omair Ahmad, Canada	Weibo Gong, USA
N. K. Bose, USA	Xi-Ren Cao, Hong Kong
Alfred Fettweis, Germany	Yu-Chi Ho, United Kingdom
Brockway McMillan, USA	Noor Raihan Ab hamid, MALAYSIA
H. J. Orchard, USA	Siti Soraya Abdul Rahman, MALAYSIA
Jacob Katzenelson, Israel	Joerg Abendroth, GERMANY
Vincent Poor, USA	Sattar J Aboud, JORDAN
Abraham Kandel, USA	Cherif adnen, TUNISIA
Bor-Sen Chen, China	Tiron Tudor Adriana, ROMANIA
C. S. George Lee, USA	Ryoji Akimoto, JAPAN
Hamid R. Berenji, USA	Mohamed Ali, LIBYA
Jim C. Bezdek, USA	Rafael Alvarez, SPAIN
Kevin M. Passino, USA	Paolo Amato, ITALY
Lawrence O. Hall, USA	Yasar Amin, PAKISTAN
Ronald R. Yager, USA	Tan Fong Ang, MALAYSIA
Witold Pedrycz, Canada	Noor Habibah Arshad, MALAYSIA
Agoryaswami J. Paulraj, USA	Dursun Aydin, TURKEY
Ahmed H. Tewfik, USA	Michael Bank, ISRAEL
Alan V. Oppenheim, USA	Robert Andrei Buchmann, ROMANIA
Alfonso Farina, Italy	Jacques Calmet, GERMANY
Alfred O. Hero, USA	Eduardo Casilari, SPAIN
Ali H. Sayed, USA	Maiga Chang, TAIWAN

Anders Lindquist, Sweden	Huay Chang, TAIWAN
Arthur B. Baggeroer, USA	Kausik Chatterjee, UNITED STATES
Arye Nehorai, USA	Ming-puu Chen, TAIWAN
Benjamin Friedlander, USA	Zhigang Chen, CHINA
Bernard C. Levy, USA	Nian-Shing Chen, TAIWAN
Bhaskar D. Rao, USA	Rong-Chang Chen, TAIWAN
Boualem Boashash, Australia	Hong-Ren Chen, TAIWAN
Bruce A. Francis, Canada	ChingWen Chen, TAIWAN
C. Richard Johnson, USA	Zhongdi Chen, CHINA
C. Sidney Burrus, USA	Franco Chiaraluze, ITALY
Charles M. Rader, USA	Suphamit Chittayasothorn, THAILAND
Desmond P. Taylor, New Zealand	Shihchieh Chou, TAIWAN
Donald L. Duttweiler, USA	Lucian-Ionel Cioca, ROMANIA
Donald W. Tufts, USA	Joan-Josep Climent, SPAIN
Douglas L. Jones, USA	Krzysztof Cyran, POLAND
Earl E. Swartzlander, USA	Miguel Diaz, SPAIN
Ed F. Deprettere, Netherlands	Juli?n Dorado, SPAIN
Edward A. Lee, USA	Hiroshi Dozono, JAPAN
Ehud Weinstein, Israel	Dan-Maniu Duse, ROMANIA
Eli Brookner, USA	Neamat El Gayar, EGYPT
Ezio Biglieri, Italy	Cheng-Kiang Farn, TAIWAN
Faye Boudreaux-Bartels, USA	Kre?imir Fertalj, CROATIA (HRVATSKA)
Georgios B. Giannakis, USA	Kun Gao, CHINA
Gonzalo R. Arce, USA	Angel Garcia-Beltran, SPAIN
H. Vincent Poor, USA	Julio Garrido Campos, SPAIN
Hagit Messer, Israel	Morgavi Giovanna, ITALY
Harold S. Stone, USA	Daphne Halkias, GREECE
Harry L. Van Trees, USA	Sungwan Han, KOREA
Henrique S. Malvar, USA	Nicholas Harkiolakis, GREECE
Hsueh-Ming Hang, ROC	Athanasios Hatzigaidas, GREECE
Jaakko Astola, Finland	Koichi Higuchi, JAPAN
James R. Zeidler, USA	Jaroslav Hlava, CZECH REPUBLIC
Jan P. Allebach, USA	Kun-Lin Hsieh, TAIWAN
Jitendra K. Tugnait, USA	Chin-pao Hung, TAIWAN
John M. Cioffi, USA	Mousa Hussein, UNITED ARAB EMIRATES
John R. Treichler, USA	Bozidar Jakovic, CROATIA (HRVATSKA)
John V. McCanny, United Kingdom	Tomaz Javornik, SLOVENIA
Joos Vandewalle, Belgium	Devinder Kaur, UNITED STATES
Jose C. Principe, USA	Derk Jan Kiewiet, "NETHERLANDS
Jose M. F. Moura, USA	Il-hwan Kim, KOREA
K. J. Ray Liu, USA	Chom Kimpan, THAILAND
Kaushik Roy, USA	George Kliros, GREECE
Kenneth Rose, USA	Hana Kopackova, CZECH REPUBLIC
Keshab K. Parhi, USA	Niksa Kovac, CROATIA (HRVATSKA)
Kon Max Wong, Canada	Jiri Krupka, CZECH REPUBLIC
Kung Yao, USA	Cheng-chien Kuo, TAIWAN
Martin Vetterli, USA	Eungyong Lee, KOREA
Mati Wax, USA	Jeong Ho Lee, KOREA
Meir Feder, Israel	Lily Li, AUSTRALIA
Michael C. Wicks, USA	Xinben Li, CHINA
Michael D. Zoltowski, USA	Qian Li, CHINA
Michael T. Orchard, USA	Chunping Li, CHINA
Michael Unser, Switzerland	Lina-Maria Stanca, ROMANIA
Miguel Angel Lagunas, Spain	Shieh-Shing Lin, TAIWAN
Moeness G. Amin, USA	Virginia Little, UNITED STATES
Mohamed Najim, France	Shi-Jer Lou, TAIWAN
Neil J. Bershad, USA	Martin Macko, CZECH REPUBLIC
P. P. Vaidyanathan, USA	Supawee Makdee, THAILAND
Patrick Dewilde, Netherlands	Charalampos Manifavas, GREECE
Peter Willett, USA	Niculescu Marius-Cristian, ROMANIA

Petre Stoica, Sweden	Enrique Merida-Casermeiro, SPAIN
Phillip A. Regalia, France	Hiroyuki Mitsuhashi, JAPAN
Pierre Duhamel, France	Djouadi Mohand Saed, ALGERIA
Pierre Moulin, USA	Mihael Mohorcic, SLOVENIA
Pramod K. Varshney, USA	Gholam Ali Montazer, IRAN
Rabab Kreidieh Ward, Canada	Bernard Moulin, CANADA
Robert M. Gray, USA	Nabil Moussa, BAHRAIN
Rolf Unbehauen, Germany	Mihaela Muntean, ROMANIA
Ronald W. Schafer, USA	Seung Na, KOREA
Rui J. P. Figueiredo, USA	Kuo Nai-Wen, TAIWAN
Russell M. Mersereau, USA	Nobuo Nakajima, JAPAN
Shun-Ichi Amari, Japan	Elias Nassar, LEBANON
Simon Haykin, Canada	Victor-Emil Neagoe, ROMANIA
Soo-Chang Pei, China	Roman Neruda, CZECH REPUBLIC
Soura Dasgupta, USA	Michiko Oba, JAPAN
Stefan L. Hahn, Poland	Kyu-Cheol Oh, KOREA
Steven Kay, USA	Tiejun Pan, CHINA
Takao Hinamoto, Japan	ang-Sung Park, KOREA
Takashi Matsumoto, Japan	Anca Petrisor, ROMANIA
Tapio Saramaki, Finland	Mircea Popa, ROMANIA
Tariq S. Durrani, U.K.	Marius Constantin Popescu, ROMANIA
Thomas F. Quatieri, USA	Domenico Porto, ITALY
Thomas L. Marzetta, USA	Wichian Premchaiswadi, THAILAND
Thomas S. Huang, USA	Khalid Qaraq, UNITED STATES
Thomas W. Parks, USA	Elias Rachid, LEBANON
Uri Shaked, Israel	Mindaugas Rybokas, LITHUANIA
V. John Mathews, USA	Jean Saade, LEBANON
Vladimir Cuperman, USA	Kassem Saleh, UNITED ARAB EMIRATES
William A. Pearlman, USA	Rocio Sanchez, SPAIN
Wolfgang Fichtner, Switzerland	Eugenio Santos, SPAIN
Wu-Sheng Lu, Canada	Hyun Soon Shin, KOREA
Yaakov Bar-Salom, USA	G. Silahatoglu, TURKEY
Yingbo Hua, USA	Seppo Sirkemaa, FINLAND
Yong Ching Lim, Singapore	Igor Skrjanc, SLOVENIA
Zhi Ding, USA	Andre Slabbert, SOUTH AFRICA
A. A. Goldenberg, Canada	Pamela Solvie, UNITED STATES
Aggelos K. Katsaggelos, USA	Moon Ting Su, MALAYSIA
Angel Rodriguez-Vasquez, Spain	Anna Trifonova, ITALY
Erol Gelenbe, USA	Chieh-yuan Tsai, TAIWAN
F. L. Lewis, USA	Vasilis Tsoukalas, GREECE
Harry Wechsler, USA	Anghel Vasile, ROMANIA
Howard C. Card, Canada	Roman Vitenberg, ISRAEL
Leon O. Chua, USA	Yi-Shun Wang, TAIWAN
Marco Gori, Italy	Chi-jui Wu, TAIWAN
Narasimhan Sundararajan, Singapore	Jianbo Xu, CHINA
Sankar K. Pal, India	Pelin Yildiz, TURKEY
Tamas Roska, USA	Mustapha C.E. Yagoub, CANADA
A. Stephen Morse, USA	Xiaoyan Yang, CHINA
Alberto Isidori, USA	Xiaobo Yang, UNITED KINGDOM
Ali Saberi, USA	Aimin Yang, CHINA
Andrew R. Teel, USA	Shoujian Yu, CHINA
Antonio Vicino, Italy	Pao-Ta Yu, TAIWAN
Anuradha M. Annaswamy, USA	Liangbin Zhang, CHINA
Benjamin Melamed, USA	Janis Zuters, LATVIA

## Preface

The book you are currently holding contains the proceedings of the 6th WSEAS International Conference on INFORMATION SECURITY and PRIVACY (ISP '07) which was held in Puerto De La Cruz, Tenerife, Canary Islands, Spain, December 14-16, 2007

The ISP started in 2002 in Rio De Janeiro, Brazil. In 2003, the conference was organized in New York, USA, while in 2004 we moved it to Rio De Janeiro, Brazil again. In 2005, it was held also in Puerto De La Cruz, Tenerife and in 2006 in Venice (Italy). The ISP is the internationally recognized forum for the dissemination of the latest advances on Information Security, Privacy, Cryptography, Cryptology etc as well as their impact and their interaction with other areas of Computer Science and Engineering. The various WSEAS conferences on information security and privacy have been successfully held each year since 2002 and has produced several volumes of Proceedings while the best papers and the invited papers after extension and after peer review from 4 international referees, are published in WSEAS Journals covered by all the major scientific indices. The ISP'07 aims to disseminate the latest research and applications in the afore mentioned fields. The friendliness and openness of the WSEAS conferences, adds to their ability to grow by constantly attracting young researchers. The meetings have always had a special appeal to young researchers and are characterized by a friendly atmosphere in which delegates at different stages of their careers can talk to each other. Scientists within the areas of Information Technologies will benefit from attending the meeting. As a conclusion, the conference offers to the engineers and scientists a unique forum for establishing new collaborations within present or upcoming research projects, exchanging useful ideas, presenting recent research results, participating in discussions and establishing new academic collaborations, linking university with the industry.

We would like to address to each of you a warm invitation for the AIKED, SEPADS, ISPR and EHAC 2008 international conferences that will be held inside the University of Cambridge where our "father" Prof. **Lotfi A. Zadeh** will be for 4th time Plenary Speaker in a WSEAS Congress presenting the Plenary Lecture: "*Toward Human-Level Machine Intelligence*". Details:  
<http://www.wseas.org/conferences/2008/cambridge/aiked/Plenary1.htm>

We would like to thank all members of the organizing laboratories for their contribution to the organization of the conference.

The contents of this Book are also published in the CD-ROM Proceedings of the Conference. Both will be sent to the WSEAS collaborating indices after the conference: [www.worldses.org/indexes](http://www.worldses.org/indexes).

In addition, papers of this book are permanently available to all the scientific community via the WSEAS E-Library.

Expanded and enhanced versions of papers published in these conference proceedings are also going to be considered for possible publication in one of the WSEAS journals that participate in the major International Scientific Indices (Elsevier, Scopus, EI, Compendex, INSPEC, CSA .... see: [www.worldses.org/indexes](http://www.worldses.org/indexes) ) these papers must be of high-quality (break-through work) and a new round of a very strict review will

follow. (No additional fee will be required for the publication of the extended version in a journal).

We cordially thank all the people of WSEAS for their efforts to maintain the high scientific level of conferences, proceedings and journals.

The Editors



**Proceedings of the 6th WSEAS International Conference on  
INFORMATION SECURITY and PRIVACY  
(ISP '07)**

**TABLE OF CONTENTS**

<b>Improving Unconditional Oblivious Transfer from Noisy Channels</b> <i>Minh-Dung Dang</i>	1
<b>The Applications of Ameso Optimization in Supply Chains</b> <i>M. N. Katehakis, Wen Chen</i>	10
<b>Supply Chain for a High Stakes Testing Agency</b> <i>Ronald Armstrong, Dmitry Belov, Mabel Kung</i>	16
<b>Quickest Path Distances on Context-Free Labeled Graphs</b> <i>Phillip G. Bradford</i>	22
<b>An Information-Theoretic Security Analysis of Quantum String Sealing</b> <i>Masaki Nakanishi, Seiichiro Tani, Shigeru Yamashita</i>	30
<b>A New Public Key Cryptosystem based on Matrices</b> <i>Rafael Alvarez, Francisco-Miguel Martinez, Jose-Francisco Vicent, Antonio Zamora</i>	36
<b>Generating Pseudo-Random Sequences from Cellular Automata and Bent Functions</b> <i>Francisco J. Garcia, Veronica Requena, Virtudes Tomas</i>	40
<b>A Characterization of Bent Functions on <math>n + 1</math> Variables</b> <i>Joan-Josep Climent, Francisco J. Garcia, Veronica Requena</i>	44
<b>Construction of a Convolutional Code based Symmetric Cryptosystem</b> <i>Joan-Josep Climent, Francisco Ferrandez, Virtudes Tomas</i>	48
<b>Distributed Information Systems and Data Security Problem</b> <i>Agnieszka Dardzinska-Glebocka</i>	52
<b>Posterior Distributions for Rare Events in Multivariate Categorical Data</b> <i>Douglas H. Jones</i>	58
<b>Truststrings in Mobile Wireless Network Settings</b> <i>Dagmara Spiewak, Volker Fusenig, Thomas Engel</i>	63
<b>A Survey on IDS Alerts Processing Techniques</b> <i>Safaa O. Al-Mamory, Hong Li Zhang</i>	69
<b>Study on Information Security Strategy for Ubiquitous Society</b> <i>Eungyong Lee, Lim Hee Jun, Min Kounng Sik</i>	79
<b>Home Area Network: A Security Perspective</b> <i>Hira Sathu, Ranjana Shukla</i>	85
<b>A Quantum Secure Direct Communication Protocol for Sending a Quantum State and its Security Analysis</b> <i>Yumiko Murakami, Masaki Nakanishi, Shigeru Yamashita, Yasuhiko Nakashima, Manabu Hagiwara</i>	91
<b>Fast Pseudorandom Generator based on Packed Matrices</b> <i>Jose-Vicente Aguirre, Rafael Alvarez, Leandro Tortosa, Antonio Zamora</i>	98

<b>Depth-in-Defense Approach against DDoS</b> <i>Rabia Sirhindi, Asma Basharat, Ahmad Raza Cheema</i>	102
<b>A Novel Solution for IP Spoofing Attacks</b> <i>Asma Basharat, Rabia Sirhindi, Ahmad Raza Cheema, Imtiaz Khokhar</i>	107
<b>Towards a Corporate IT Risk Management Model</b> <i>Mario Spremic, Matija Popovic</i>	111
<b>Methods of Privacy Protection Certification Systems</b> <i>Ki-Ho Lee, Tae-Hee Cho, Kyu-Cheol Oh, Dae-Yong Byun, Sang-Soo Jang</i>	117
<b>Nested Encryption Library for automated IPsec-based Anonymous Circuits Establishment</b> <i>Herve Aiache, Matteo Lauriano, Corinne Sieux, Cedric Tavernier</i>	123
<b>Privacy from an Individuals' Point of View in German Speaking Countries: Assessments and Empirical Results</b> <i>Ulrike Hugl, Harald Valkanover</i>	130
<b>IP Trace Back Techniques to Ferret out Denial of Service Attack Source</b> <i>Adnan Aijaz, Syed Raza Mohsin, Mofassir-Ul-Haque</i>	135
<b>Multi-Purpose Code Generation Using Fingerprint Images</b> <i>H. A. Ali, B. M. Ne'ma</i>	141
<b>A Static or Dynamic Reconfiguration Method of Security Functions for Mobile Devices by Using the Security Profiles</b> <i>Wonjoo Park, Dongho Kang, Kiyoung Kim</i>	146
<b>Study on Spam Endurance Index in On-Line Environment</b> <i>Kiyeon Baek, Youngha Yang, Jinho Yoo</i>	151
<b>The Design of SSO Service Architecture for Mashup Service in Web Portals</b> <i>SoHee Park, JeongNyeo Kim</i>	155
<b>Implementation of a Cryptographic Co-Processor</b> <i>A. P. Kakarountas, H. Michail</i>	160
<b>CESNET Intrusion Detection System</b> <i>Pavel Vachek</i>	166
<b>Image Contrast Enhancement and Quantitative Measuring of Information Flow</b> <i>Zhengmao Ye, Habib Mohamadian, Su-Seng Pang, Sitharama Iyengar</i>	172
<b>A New and Comprehensive Taxonomy of DDoS Attacks and Defense Mechanism</b> <i>Abbass Asosheh, Naghmeh Ramezani</i>	178

## Authors Index

Aguirre, J. V.	98	Iyengar, S.	172	Park, W.	146
Aiache, H.	123	Jang, S. S.	117	Popovic, M.	111
Aijaz, A.	135	Jones, D. H.	58	Ramezani, N.	178
Ali, H. A.	141	Jun, L. H.	79	Requena, V.	40 44
Al-Mamory, S. O.	69	Kakarountas, A. P.	160	Sathu, H.	85
Alvarez, R.	36 98	Kang, D.	146	Shukla, R.	85
Armstrong, R.	16	Katehakis, M. N.	10	Sieux, C.	123
Asosheh, A.	178	Khokhar, I.	107	Sik, M. K.	79
Baek, K.	151	Kim, J. N.	155	Sirhindi, R.	102 107
Basharat, A.	102 107	Kim, K.	146	Spiewak, D.	63
Belov, D.	16	Kung, M.	16	Spremic, M.	111
Bradford, P. G.	22	Lauriano, M.	123	Tani, S.	30
Byun, D. Y.	117	Lee, E.	79	Tavernier, C.	123
Cheema, A. R.	102 107	Lee, K. H.	117	Tomas, V.	40 48
Chen, W.	10	Martinez, F. M.	36	Tortosa, L.	98
Cho, T. H.	117	Michail, H.	160	Ul-Haque, M.	135
Climent, J. J.	44 48	Mohamadian, H.	172	Vachek, P.	166
Dang, M. D.	1	Mohsin, S. R.	135	Valkanover, H.	130
Dardzinska-Glebocka, A.	52	Murakami, Y.	91	Vicent, J. F.	36
Engel, T.	63	Nakanishi, M.	30 91	Yamashita, S.	30 91
Ferrandez, F.	48	Nakashima, Y.	91	Yang, Y.	151
Fusenig, V.	63	Ne'ma, B. M.	141	Ye, Z.	172
Garcia, F. J.	40 44	Oh, K. C.	117	Yoo, J.	151
Hagiwara, M.	91	Pang, S. S.	172	Zamora, A.	36 98
Hugl, U.	130	Park, S.	155	Zhang, H. L.	69