



ARES 2008 - International Conference on Availability, Reliability and Security  
The Dependability Conference

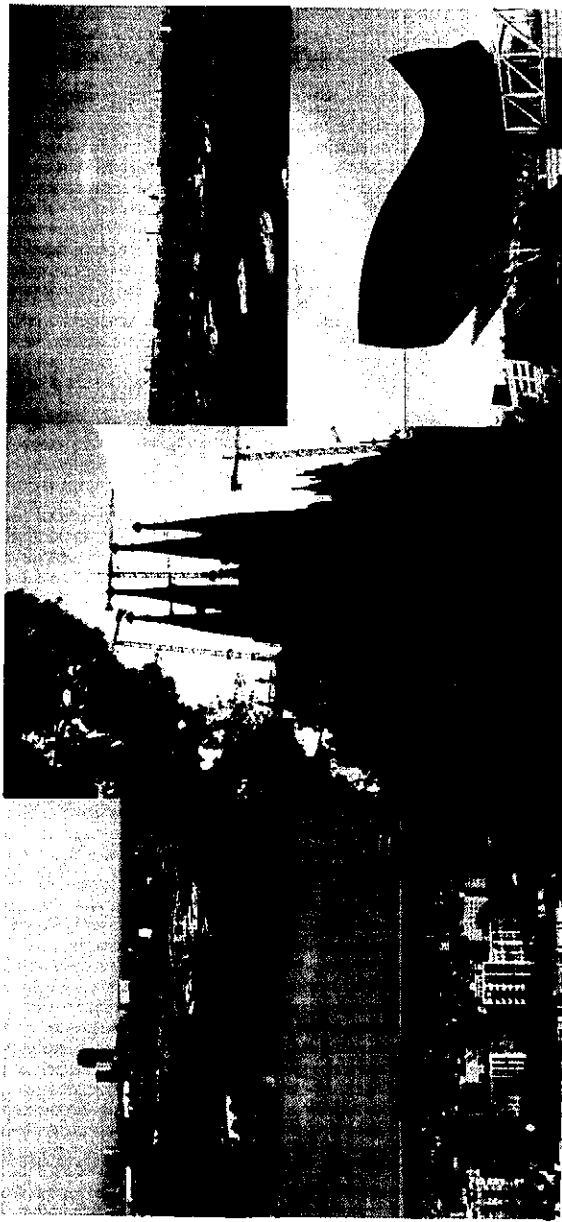
# ARES 2008

## The Third International Conference on Availability, Security and Reliability

### PROCEEDINGS

March 4-7, 2008

Barcelona, Spain



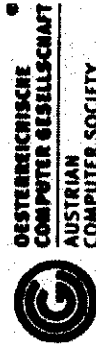
Edited by Stefan Jakoubi, Simon Tjoa, and Edgar R. Weippl

Organised by

**[SECURE]**  
Business Austria



In cooperation with



*Proceedings of the*

# The Third International Conference on Availability, Security, and Reliability

March 4-7, 2008, Barcelona, Spain



Los Alamitos, California  
Washington • Tokyo



All rights reserved.

*Copyright and Reprint Permissions:* Abstracting is permitted with credit to the source. Libraries may photocopy beyond the limits of US copyright law, for private use of patrons, those articles in this volume that carry a code at the bottom of the first page, provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

Other copying, reprint, or republication requests should be addressed to: IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, P.O. Box 133, Piscataway, NJ 08855-1331.

*The papers in this book comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interests of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors, the IEEE Computer Society, or the Institute of Electrical and Electronics Engineers, Inc.*

IEEE Computer Society Order Number P3102  
ISBN 0-7695-3102-4  
ISBN 978-0-7695-3102-1  
Library of Congress Number 2007909935

*Additional copies may be ordered from:*

IEEE Computer Society  
Customer Service Center  
10662 Los Vaqueros Circle  
P.O. Box 3014  
Los Alamitos, CA 90720-1314  
Tel: +1 800 272 6657  
Fax: +1 714 821 4641  
<http://computer.org/cspress>  
[csbooks@computer.org](mailto:csbooks@computer.org)

IEEE Computer Society  
Asia/Pacific Office  
Watanabe Bldg., 1-4-2  
Minami-Aoyama  
Minato-ku, Tokyo 107-0062  
JAPAN  
Tel: +81 3 3408 3118  
Fax: +81 3 3408 3553  
[tokyo.ofc@computer.org](mailto:tokyo.ofc@computer.org)

*Individual paper REPRINTS may be ordered at:* <[reprints@computer.org](mailto:reprints@computer.org)>

Editorial production by Bob Werner  
Cover art production by Joe Daigle/Studio Productions  
Printed in the United States of America by The Printing House



IEEE Computer Society  
Conference Publishing Services (CPS)

<http://www.computer.org/cps>

# Table of Contents

## The Third International Conference on Availability, Reliability and Security (ARES 2008)

Message from the General Chairs..... **xxi**  
Conference Officers..... **xxii**

### Keynotes

Security and Privacy Challenges in Location Based Service Environments..... **xxiii**  
*Vijayalakshmi Athuri*  
Infrastructure Support for Authorization, Access Control and Privilege Management..... **xxvi**  
*Günther Pernul*

The ASCAA Principles for Next-Generation Role-Based Access Control..... **xxvii**  
*Ravi Sandhu and Venkata Bhamidipati*

### ARES Full Paper Sessions

#### Session 1: Applications

Securing Telehealth Applications in a Web-Based e-Health Portal..... **3**  
*Qian Liu, Shuo Lu, Yuan Hong, Lingyu Wang, and Rachida Dssouli*  
Multi-Level Reputation-Based Greylisting..... **10**  
*Wilfried Gansterer, Andreas Janecek, and Ashwin Kumar*  
Hardening XDS-Based Architectures..... **18**  
*Kim Wuyts, Riccardo Scandariato, Geert Claeys, and Wouter Joosen*

#### Session 2: Miscellaneous

Finding Evidence of Antedating in Digital Investigations..... **26**  
*Svein Yngvar Willassen*  
FEDC: Control Flow Error Detection and Correction for Embedded Systems without Program Interruption..... **33**  
*Navid Farazmand, Mahdi Fazeli, and Seyyed Ghasem Miremadi*  
Economic and Security Aspects of Applying a Threshold Scheme in e-Health..... **39**  
*Bernhard Riedl, Veronika Grascher, Mathias Kolb, and Thomas Neubauer*  
Anomaly Based Character Distribution Modeling to Detect SQL Injection Attacks..... **47**  
*Mehdi Kiani, Andrew Clark, and George Mohay*  
On the Possibility of Small, Service-Free Disk Based Storage Systems..... **56**  
*Jehan-François Pâris and Thomas Schwarz*  
Efficient High Availability Commit Processing..... **64**  
*Heine Kollveit and Svein-Olaf Hvasshovd*

### Session 3: Models

- Soundness Conditions for Message Encoding Abstractions in Formal Security Protocol Models..... 72  
*Alfredo Pironi and Riccardo Sisto*
- Towards Formal Specification of Abstract Security Properties..... 80  
*Antonio Maña and Gimena Pujol*
- A Behavioral Model of Ideologically-motivated "Snowball" Attacks ..... 88  
*Natalia Stakhanova, Oleg Stakhanov, and Ali Ghorbani*
- Property Specification and Static Verification of UML Models ..... 96  
*Igor Siveroni, Andrea Zisman, and George Spanoudakis*

### Session 4: Database

- Towards Comprehensive Requirement Analysis for Data Warehouses:  
Considering Security Requirements ..... 104  
*Emilio Soler, Veronika Stefanov, Jose-Norberto Mazón, Juan Trujillo,  
Eduardo Fernandez-Medina, and Mario Piattini*
- A New Scheme for Distributed Density Estimation Based Privacy-Preserving Clustering ..... 112  
*Chunhua Su, Jianying Zhou, Feng Bao, Tsyvoshi Takagi, and Kouichi Sakurai*
- A Database Replication Protocol Where Multicast Writesets Are Always Committed ..... 120  
*José Ramón Juárez-Rodríguez, Enrique Armendáriz-Jitigo,  
José Ramón González de Mendivil, and Francesc Daniel Muñoz-Escó*

### Session 5: Mobile

- Matching Policies with Security Claims of Mobile Applications..... 128  
*Natalia Bielova, Marco Dalla Torre, Nicola Dragoni, and Ida Sahaan*
- PSecGCM: Process for the Development of Secure Grid Computing based  
Systems with Mobile Devices ..... 136  
*David G. Rosado, Eduardo Fernández-Medina, Javier López, and Mario Piattini*
- WATCHMAN: An Overlay Distributed AAA Architecture for Mobile Ad hoc Networks ..... 144  
*Amir Khakpour, Maryline Laurent-Maknawicus, and Hakima Chaouchi*

### Session 6: RBAC and Recommender

- Hierarchical Domains for Decentralized Administration of Spatially-Aware RBAC Systems ..... 153  
*Maria Luisa Damiani, Claudio Silvestri, and Elisa Bertino*
- Experimental Demonstration of a Hybrid Privacy-Preserving Recommender System ..... 161  
*Esmá Aïmeur, Gilles Brassard, José M. Fernandez,  
Flavien Serge Mani Onana, and Zbigniew Rakowski*
- Fast Qualitative Reasoning about Actions for Computing Anticipatory Systems ..... 171  
*Natsumi Kitajima, Yuichi Goto, and Jingde Cheng*

### Session 7: Risk Management

- Enhancing Business Impact Analysis and Risk Assessment Applying a  
Risk-Aware Business Process Modeling and Simulation Methodolog..... 179  
*Simon Tjoa, Stefan Jakoubi, and Gerald Quirchmayr*
- Defining Secure Business Processes with Respect to Multiple Objectives ..... 187  
*Thomas Neubauer and Johannes Heurix*
- Analysis and Component-based Realization of Security Requirements ..... 195  
*Denis Hatebur, Maritta Heisel, and Holger Schmidt*

### Session 8: Networks

- A Framework for Detecting Anomalies in VoIP Networks..... 204  
*Yacine Bouzida and Christophe Mangin*
- Rapid Detection of Constant-Packet-Rate Flows ..... 212  
*Kuan-Ta Chen and Jing-Kai Lou*
- Performance Analysis of Anonymous Communication Channels Provided by Tor..... 221  
*Andriy Panchenko, Lexi Pimenidis, and Johannes Renner*
- Fast Algorithms for Consistency-Based Diagnosis of Firewall Rule Sets ..... 229  
*Sergio Pozo Hidalgo, Rafael Ceballos, and Rafael Martínez Gasca*
- Privacy/Analysis Tradeoffs in Sharing Anonymized Packet Traces: Single-Field Case..... 237  
*William Yurcik, Clay Woolam, Greg Hellings, Latifur Khan, and Bhavani Thuraisingham*

### A Distributed Defense Framework for Flooding-Based DDoS Attacks..... 245

- Yonghua You, Mohammad Zulkernine, and Anwar Haque*
- Pure MPLS Technology ..... 253  
*Liwen He and Paul Boham*

### Symmetric Active/Active Replication for Dependent Services..... 260

- Christian Engelmann, Stephen L. Scott, Chokchai Leangsuksun, and Xubin He*

### Session 9: Software

- Statically Checking Confidentiality of Shared-Memory Programs with Dynamic Labels..... 268  
*Marcus Völz*
- A Cause-Based Approach to Preventing Software Vulnerabilities..... 276  
*David Byers and Nahid Shahmehri*
- Integrating a Security Plug-in with the OpenUP/Basic Development Process..... 284  
*Shanai Ardi and Nahid Shahmehri*
- A Novel Testbed for Detection of Malicious Software Functionality ..... 292  
*Jostein Jensen*
- Type and Effect Annotations for Safe Memory Access in C..... 302  
*Syrine Tlili and Mourad Debbabi*

### Session 10: IDS and Models

- Adaptability of a GP Based IDS on Wireless Networks..... 310  
*Adetokunbo Makanju, Nur Zincir-Heywood, and Evangelos Milios*
- An Intrusion-Tolerant Mechanism for Intrusion Detection Systems ..... 319  
*Liwei Kuang and Mohammad Zulkernine*
- Fuzzy Private Matching (Extended Abstract)..... 327  
*Lukasz Chmielewski and Jaap-Henk Hoepman*

### Session 11: Trust, Security and Economics

- Navigating in Webs of Trust: Finding Short Trust Chains in  
Unstructured Networks without Global Knowledge..... 335  
*Jens-Uwe Bußer, Steffen Fries, Martin Otto, and Peter Hartmann*
- Trust Modelling in E-Commerce through Fuzzy Cognitive Maps ..... 344  
*Christian Schlöger and Günther Pernul*
- Boosting Markov Reward Models for Probabilistic Security Evaluation by  
Characterizing Behaviors of Attacker and Defender ..... 352  
*Zonghua Zhang, Farid Nait-Abdesselam, and Pin-Han Ho*

### ARES Short Paper Sessions

#### Session 1: Applications

- CERTLOC: Implementation of a Spatial-Temporal Certification Service Compatible with  
Several Localization Technologies ..... 363  
*José María de Fuentes García-Romero de Tejada,  
Ana Isabel González-Tablas Ferreres, and Arturo Ribagorda Garnacho*
- Extending Mixed Serialisation Graphs to Replicated Environments ..... 369  
*Josep M. Bernabé-Gisbert and Francesc D. Muñoz-Escot*
- Towards Secure E-Commerce Based on Virtualization and Attestation Techniques ..... 376  
*Frederic Stumpf, Claudia Eckert, and Shane Balfé*
- Fuzzy Belief-Based Supervision..... 383  
*Alexandre Vorobiev and Rudolph Seviora*
- Ensuring Progress in Amnesiac Replicated Systems ..... 390  
*Rubén de Juan-Marín, Luis Irín-Briz, and Francesc D. Muñoz-Escot*
- Enhancing Face Recognition with Location Information ..... 397  
*R.J. Hulsebosch and P.W.G. Ebben*
- A Lazy Monitoring Approach for Heartbeat-Style Failure Detectors..... 404  
*Benjamin Satzger, Andreas Pietzowski, Wolfgang Trumler, and Theo Ungerer*
- Defending On-Line Web Application Security with User-Behavior Surveillance ..... 410  
*Yu-Chin Cheng, Chi-Sung Laih, Gu-Hsin Lai, Chia-Mei Chen, and Tzuhan Chen*

#### Session 2: Services and Trust

- A Pattern-Driven Security Process for SOA Applications ..... 416  
*Nelly A. Delessy and Eduardo B. Fernandez*
- Toward a Dependable Architecture for Highly Available Internet Services ..... 422  
*Ayari Narjess, Pablo Neira Ayuso, Laurent Lefevre, Denis Barbaron, and Rafael Gasca*
- Assessing the Reliability and Cost of Web and Grid Orchestration ..... 428  
*Alan Stewart, Maurice Clint, Terry Harmer, Peter Kilpatrick, Ron Perrott, and Joaquim Gabarro*
- Application-Oriented Trust in Distributed Computing..... 434  
*Riccardo Scandariato, Yoram Ofek, Paolo Falcarin, and Mario Baldi*
- BlueTrust in a Real World ..... 440  
*Bradley Markides and Marijke Coetzee*

#### Session 3: Privacy and Safety

- Privacy Preserving Shortest Path Computation in Presence of Convex Polygonal Obstacles ..... 446  
*Ananda Swarup Das, Jitu Kumar Keshri, Kannan Srinathan, and Vaibhav Srivastava*
- Privacy Protected ELF for Private Computing on Public Platforms..... 452  
*Thomas Morris and V.S.S. Nair*

haplog: A Hash-Only and Privacy-Preserved Secure Logging Mechanism <i>Chih-Yin Lin</i>	458
An Improved Zonal Safety Analysis Method and Its Application on Aircraft CRJ200 <i>Li Xiaolei, Tian Jin, and Zhao Tingdi</i>	461
<b>Session 4: Networks</b>	
A Model for Specification and Validation of Security Policies in Communication Networks: The Firewall Case <i>Ryma Abbassi and Sihem Guemara El Fatmi</i>	467
SPIT Detection and Prevention Method in VoIP Environment <i>He Guang-Yu, Wen Ying-You, and Zhao Hong</i>	473
A New Approach to Analysis of Interval Availability <i>Ezzat Kirmant and Cynthia Hood</i>	479
SFMD: A Secure Data Forwarding and Malicious Routers Detecting Protocol <i>Xiang-he Yang, Hua-ping Hu, and Xin Chen</i>	484
Fault Effects in FlexRay-Based Networks with Hybrid Topology <i>Mehdi Dehbashi, Yahid Lari, Seyed Ghassem Miremadi, and Mohammad Shokrolah-Shirazi</i>	491
Securing Wireless Sensor Networks <i>Xun Yi, Mike Faulkner, and Eiji Okamoto</i>	497
SEIF: Secure and Efficient Intrusion-Fault Tolerant Routing Protocol for Wireless Sensor Networks <i>Abdelraouf Ouadjaout, Yacine Challal, Nouredine Lasla, and Miloud Bagaa</i>	503
The Impact of Flooding Attacks on Network-based Services <i>Meiko Jensen, Nils Gruschka, and Norbert Luttenberger</i>	509
Managing Priorities in Atomic Multicast Protocols <i>Emili Miedes and Francesc D. Muñoz-Escot</i>	514
Beacon Frame Spoofing Attack Detection in IEEE 802.11 Networks <i>Asier Martínez, Urko Zurutuza, Roberto Uribeetxeberria, Miguel Fernández, Jesús Lizarraga, Ainhoa Serna, and Itzi Vález</i>	520
An End-to-End Security Solution for SCTP <i>Stefan Lindskog and Anna Brunstrom</i>	526
<b>Session 5: Crypto</b>	
An Identity-Based Group Key Agreement Protocol from Pairing <i>Hongji Wang, Gang Yao, and Qingshan Jiang</i>	532
An Authenticated 3-Round Identity-Based Group Key Agreement Protocol <i>Gang Yao, Hongji Wang, and Qingshan Jiang</i>	538
High Capacity Steganographic Method Based Upon JPEG <i>Adel Almohammad, Robert Hierons, and Gheorghita Ghinea</i>	544
Cluster-based Group Key Agreement for Wireless Ad hoc Networks <i>Elisavet Konstantinou</i>	550
<b>Session 6: Crypto and Health</b>	
A Statistical Algorithm for Linguistic Steganography Detection Based on Distribution of Words <i>Chen Zhi-li, Huang Liu-sheng, Yu Zhen-shan, Li Ling-jun, and Yang Wei</i>	558
RTQG: Real-Time Quorum-based Gossip Protocol for Unreliable Networks <i>Bo Zhang, Kai Han, Binoy Ravindran, and E.D. Jensen</i>	564
A Secure and Scalable Infrastructure for Inter-Organizational Data Exchange and eGovernment Applications <i>Jan Willemson and Arne Anspér</i>	572
A Security Model and its Application to a Distributed Decision Support System for Healthcare <i>Liang Xiao, Andrew Peet, Paul Lewis, Srimandan Dasmahapatra, Carlos Sáez, Madalina Croitoru, Javier Vicente, Horacio González-Vélez, Magi Lluch i Ariet, David Dupplaw, and Alex Gibb</i>	578
<b>Session 7: Models and Networks</b>	
Run-time Information Flow Monitoring based on Dynamic Dependence Graphs <i>Salvador Cavadini and Diego Cheda</i>	586
Automated Process Classification Framework using SELinux Security Context <i>Pravin Shinde, Priyanka Sharma, and Srinivas Guntupalli</i>	592
Using Composition Policies to Manage Authentication and Authorization Patterns and Services <i>Judith E. Y. Rossebo and Roh Bræk</i>	597
Providing Fault Tolerance in Wireless Backhaul Network Design with Path Restoration <i>Pakorn Leesuthipornchai, Naruemon Wattanapongsakorn, and Chalermpol Charmsripinyo</i>	604
<b>Session 8: IDS</b>	
Histogram Matrix: Log File Visualization for Anomaly Detection <i>Adrian Frei and Marc Rennhard</i>	610
Context-based Profiling for Anomaly Intrusion Detection with Diagnosis <i>Benferhat Salem and Tabia Karim</i>	618
A Revised Taxonomy of Data Collection Mechanisms with a Focus on Intrusion Detection <i>Ulf Larson, Erlend Jonsson and Stefan Lindskog</i>	624
IDRS: Combining File-level Intrusion Detection with Block-level Data Recovery based on iSCSI <i>Youhui Zhang, Hongyi Wang, Yu Gu, and Dongsheng Wang</i>	630
Intrusion Detection for Wormhole Attacks in Ad hoc Networks: A Survey and a Proposed Decentralized Scheme <i>Marianne Azer, Sherif El-Kassas, Abdel Wahab Hassan, and Magdy El-Soudani</i>	636

<b>Session 9: Hardware</b>	
NFC Devices: Security and Privacy <i>Gerald Madlmayr, Josef Langer, Christian Kamtner, and Josef Scharinger</i>	642
Analyzing Fault Effects in the 32-bit OpenRISC 1200 Microprocessor <i>Nima Mehdizadeh, Mohammad Shokrolah Shirazi, and Seyed Ghassem Miremadi</i>	648
Increasing the Performability of Computer Clusters Using RADIC II <i>Guna Santos, Angelo Duarte, Dolores Rexachs, and Emilio Luque</i>	653
A Framework for Proactive Fault Tolerance <i>Geoffroy Vallée, Kulathep Charoenpormwattana, Christian Engelmann, Anand Tikotekar, Chokchai Leangsuksun, Thomas Naughton, and Stephen Scott</i>	659
<b>Workshop FARES</b>	
<b>Session 1: Miscellaneous</b>	
Anti-DDoS Virtualized Operating System <i>Sanjiam Garg and Huzur Saran</i>	667
A Case for High Availability in a Virtualized Environment (HAVEN) <i>Erin Farr, Richard Harper, Lisa Spainhower, and Jimi Xenidis</i>	675
<b>Session 2: Access Control and Algorithms</b>	
A Federated Physical and Logical Access Control Enforcement Model <i>Stéphane Onno</i>	683
Fostering the Uptake of Secure Multiparty Computation in E-Commerce <i>Octavian Catrina and Florian Kerschbaum</i>	693
Efficient Certificate Path Validation and Its Application in Mobile Payment Protocols <i>Rafael Martínez-Peláez, Cristina Sotizábal, Francisco Rico-Novella, and Jordi Forné</i>	701
Avoiding Policy-based Deadlocks in Business Processes <i>Mathias Kohler and Andreas Schaad</i>	709
A Secure High-Speed Identification Scheme for RFID Using Bloom Filters <i>Yasunobu Nohara, Sozo Inoue, and Hiroto Yasuura</i>	717
<b>Session 3: Crypto</b>	
New Self Certified Proxy Digital Signature Scheme based on Elliptic Curve Cryptosystem <i>Youn Xiao</i>	723
Privacy-preserving Protocols for Finding the Convex Hulls <i>Qi Wang, Yonglong Luo and Liusheng Huang</i>	727
A Secure RFID Protocol based on Insubvertible Encryption Using Guardian Proxy <i>Kyosuke Osaka, Shuang Chang, Tsuyoshi Takagi, Kenichi Yamazaki, and Osamu Takahashi</i>	733
Cryptographic Properties of Second-Order Memory Elementary Cellular Automata <i>Ascension Hernández Encinas, Angel Martín del Rey, J.L. Pérez Iglesias, Gerardo Rodríguez Sánchez, and Araceli Queiruga Dios</i>	741
New Efficient and Authenticated Key Agreement Protocol in Dynamic Peer Group <i>Shengke Zeng, Mingxing He, and Weidong Luo</i>	746
<b>Session 4: Risk Management</b>	
Intensive Programme on Information and Communication Security <i>Christian Schläger, Ludwig Fuchs, and Günther Pernul</i>	752
Applications for IT-Risk Management—Requirements and Practical Evaluation <i>Heinz Lothar Grob, Gereon Strauch, and Christian Buddendick</i>	758
Security Analysis of Role-based Separation of Duty with Workflows <i>Rattikorn Hewett, Phongphun Kijsanayothin, and Ashay Thipse</i>	765

### Session 5: Databases and Models

- Detecting Suspicious Relational Database Queries ..... 771  
*Stefan Bötlicher, Rita Hartel, and Matthias Kirschner*
- Assessing the Value of Enterprise Identity Management (EIdM)—  
Towards a Generic Evaluation Approach ..... 779  
*Denis Royer*
- An Ontological Approach to Secure MANET Management ..... 787  
*Mark Orwat, Timothy Levin, and Cynthia Irvine*

### Session 6: Models

- Reliability Analysis using Graphical Duration Models ..... 795  
*Roland Donat, Laurent Bouillaut, Patrice Aknin, and Philippe Leray*
- From Omega to  $\Omega$ P in the Crash-Recovery Failure Model with Unknown Membership ..... 801  
*Mikel Larrea and Cristian Martin*
- Policy-based Group Organizational Structure Management using an Ontological Approach ..... 807  
*Mario Anzuarez-Garcia and Luz A. Sánchez-Gálvez*
- A Systematic Review and Comparison of Security Ontologies ..... 813  
*Carlos Blanco, Joaquín Lasheras, Rafael Valencia-García, Eduardo Fernández-Medina, Ambrosio Toval, and Mario Piattini*
- Context Ontology for Secure Interoperability ..... 821  
*Céline Coma, Nora Cuppens-Bouahia, Frédéric Cuppens, and Ana Rosa Cavalli*

### Session 7: Passwords and Services

- On the Security of VSH in Password Schemes ..... 828  
*Kimmo Halunen, Pauli Rikula, and Juha Rönning*
- Sustaining Web Services High-Availability Using Communities ..... 834  
*Zakaria Maamar, Quan Z. Sheng, and Djamal Benslimane*
- Distributed Information Retrieval Service for Ubiquitous Services ..... 842  
*Takeshi Tsuchiya, Marc Lihan, Hirokazu Yoshinaga, and Keiichi Koyanagi*

### Session 8: Software

- A Lightweight Security Analyzer inside GCC ..... 851  
*Davide Pozza and Riccardo Sisto*
- Dynamic Maintenance of Software Systems at Runtime ..... 859  
*Habib Seifzadeh, Mostafa Kermani, and Mohsen Sadighi*
- Software Security: A Vulnerability Activity Revisit ..... 866  
*Mohammad Ali Hadavi, Hossein Shirazi, Hasan Mokhtari Sangchi, and Valid Saber Hamishagi*

### Session 9: Trust

- Making Multi-Dimensional Trust Decisions on Inter-Enterprise Collaborations ..... 873  
*Sini Ruohomaa and Lea Kivronen*
- A Survey on Trust and Reputation Schemes in Ad Hoc Networks ..... 881  
*Mariamme Azer, Sherif El-Kassas, Abdel Wahab Hassan, and Magdy El-Soudani*

### Workshop WPA

- Privacy-Preserving Recommendation Systems for Consumer Healthcare Services ..... 889  
*Stefan Katzenbeisser and Milan Peirković*
- Detecting Bots Based on Keylogging Activities ..... 896  
*Yusuf Al-Hammadi and Uwe Aickelin*
- A Comprehensive Approach for Context-dependent Privacy Management ..... 903  
*Mike Bergmann, Thomas Springer, Elke Franz, and Christin Groba*
- Traceable Quantitative Risk Assessment Applied to Investment Decision for Local Backups ..... 911  
*Steffen Weiss, Martin Wahl, Michael Tieleman, and Klaus Meyer-Wegener*
- Quantitative Assessment of Enterprise Security System ..... 921  
*Ruth Breu, Frank Innerhofer-Oberperfer, and Artsiom Yautsiukhin*
- Clustering Oriented Architectures in Medical Sensor Environments ..... 929  
*Eleni Kladoulatou, Elisavet Konstantinou, Georgios Kambourakis, and Stefanos Gritzalis*
- An Initial Model and a Discussion of Access Control in Patient Controlled Health Records ..... 935  
*Lillian Røstad*
- Secure Team-Based EPR Access Acquisition in Wireless Networks ..... 943  
*Sigurd Eskeland and Vladimir Oleshchuk*
- VEA-bility Security Metric: A Network Security Analysis Tool ..... 950  
*Melanie Tupper and A. Nur Zimeir-Heywood*
- Towards an Architecture for Balancing Privacy and Traceability in Ubiquitous Computing Environments ..... 958  
*Stefan G. Weber, Andreas Heinemann, and Max Mühlhäuser*



## Workshop PSAI

GOST-28147 Encryption Implementation on Graphics Processing Units.....	967
<i>Victor Korobitsin and Sergey Ilyin</i>	
Intelligent Video Surveillance Networks: Data Protection Challenges.....	975
<i>Fanny Coudert and Jos Dumortier</i>	
Intrusion Detection with Data Correlation Relation Graph.....	982
<i>Amin Hassanzadeh and Babak Sadeghian</i>	
A Critique of <i>k</i> -Anonymity and Some of Its Enhancements.....	990
<i>Josep Domingo-Ferrer and Vicenç Torra</i>	
Cluster-Specific Information Loss Measures in Data Privacy: A Review.....	994
<i>Vicenç Torra and Susana Ladrá</i>	
Hierarchical Trust Architecture in a Mobile Ad-Hoc Network Using Ant Algorithms.....	1000
<i>Cristina Sattizábal, Jordi Forné, Rafael Martínez-Peláez, and Francisco J. Rico-Novella</i>	
Representation and Reasoning on ORBAC: Description Logic with Defaults and Exceptions Approach.....	1008
<i>Narhimene Boustia and Aicha Mokhtari</i>	
Using Non-Adaptive Group Testing to Construct Spy Agent Routes.....	1013
<i>Georgios Kalogridis and Chris Mitchell</i>	
A Bayesian Approach for on-Line Max Auditing.....	1020
<i>Gerardo Canfora and Bice Cavallo</i>	
Detection of Malcodes by Packet Classification.....	1028
<i>Irfan Ahmed and Kyung-suk Lee</i>	
Performance of a Strategy Based Packets Forwarding in Ad Hoc Networks.....	1036
<i>Marcin Serechynski, Pascal Bouvry, and Mieczysław Kłopotek</i>	
Bayesian Additive Regression Trees-Based Spam Detection for Enhanced Email Privacy.....	1044
<i>Saeed Abu-Nimeh, Dario Nappa, Xinlei Wang, and Suku Nair</i>	
AntTrust: A Novel Ant Routing Protocol for Wireless Ad-hoc Network Based on Trust between Nodes.....	1052
<i>Carlos Aguilar Melchor, Bousad Ait Salem, Philippe Gaborit, and Karim Tamime</i>	
A Post-processing Method to Lessen <i>k</i> -Anonymity Dissimilarities.....	1060
<i>Agusti Solanas, Glòria Pujol, Antoni Martínez-Ballesté, and Josep Maria Mateo-Sanz</i>	
Improving Techniques for Proving Undecidability of Checking Cryptographic Protocols.....	1067
<i>Zhiyao Liang and Rakesh Verma</i>	
A Preliminary Investigation of Skype Traffic Classification Using a Minimalist Feature Set.....	1075
<i>Duffy Angevine and A. Nur Zincir-Heywood</i>	

## Workshop APE

Partial Disclosure of Searchable Encrypted Data with Support for Boolean Queries.....	1083
<i>Yasuhiro Ohtaki</i>	
Secure and Privacy-Friendly Logging for eGovernment Services.....	1091
<i>Karel Wouters, Koen Simoens, Danny Lathouwers, and Bart Preneel</i>	
The REM Framework for Security Evaluation.....	1097
<i>Flora Amato, Valentina Casola, Antonino Mazzeo, and Valeria Vittorini</i>	
Static Validation of Licence Conformance Policies.....	1104
<i>René Rydhof Hansen, Flemming Nielson, Hanne Riis Nielson, and Christian W. Probst</i>	
Towards Practical Security Monitors of UML Policies for Mobile Applications.....	1112
<i>Fabio Massacci and Katsiaryna Naliuka</i>	
Synthesis of Local Controller Programs for Enforcing Global Security Properties.....	1120
<i>Fabio Martinelli and Ilaria Matteucci</i>	
Weighted Datalog and Levels of Trust.....	1128
<i>Stefano Bistarelli, Fabio Martinelli, and Francesco Santini</i>	
Negotiation of Usage Control Policies—Simply the Best?.....	1135
<i>Alexander Pretschner and Thomas Walter</i>	
<b>Workshop SECSE</b>	
Security Requirement Engineering at a Telecom Provider.....	1139
<i>Albin Zuccato, Viktor Endersz, and Nils Daniels</i>	
Identifying Security Aspects in Early Development Stages.....	1148
<i>Takao Okubo and Hidehiko Tanaka</i>	
Using Security Patterns to Combine Security Metrics.....	1156
<i>Thomas Heyman, Riccardo Scandariato, Christophe Huygens, and Wouter Joosen</i>	
Secure Software Design in Practice.....	1164
<i>Per Håkon Meland and Jostein Jensen</i>	
Covering Your Assets in Software Engineering.....	1172
<i>Martin Gilje Jaatun and Inger Anne Tøndel</i>	
A Non-Intrusive Approach to Enhance Legacy Embedded Control Systems with Cyber Protection Features.....	1180
<i>Shangping Ren and Kevin Kwiat</i>	
Towards Incorporating Discrete-Event Systems in Secure Software Development.....	1188
<i>Sarah Whittaker, Mohammad Zulkernine, and Karen Rudie</i>	
How to Open a File and Not Get Hacked.....	1196
<i>James Kupsch and Barton Miller</i>	

Rules of Thumb for Developing Secure Software: Analyzing and Consolidating Two Proposed Sets of Rules <i>Holger Peine</i>	1204
<b>Workshop DAWAM</b>	
Adaptive Data Integrity through Dynamically Redundant Data Structures <i>Vincenzo De Florio and Chris Blondia</i>	1213
ISEDS: An Information Security Engineering Database System Based on ISO Standards <i>Daisuke Horie, Shoichi Morimoto, Noor Azimah, Yuichi Goto, and Jingde Cheng</i>	1219
Privacy Aspects of eHealth <i>Daniel Slamang and Christian Stingl</i>	1226
Adaptive Voting Algorithms for Reliable Dissemination of Data in Sensor Networks <i>Kaliappa Ravindran, Jiang Wu, Kevin Kwiat, and Ali Sabbir</i>	1234
Risk as Dependability Metrics for the Evaluation of Business Solutions: A Model-driven Approach <i>Yudistira Asnar, Rocco Moretti, Maurizio Sebastianis, and Nicola Zannone</i>	1240
Implementing Multidimensional Security into OLAP Tools <i>Carlos Blanco, Eduardo Fernández-Medina, Juan Trujillo, and Mario Piattini</i>	1248
Detecting Key Players in 11-M Terrorist Network: A Case Study <i>Nasrullah Memon and David L. Hicks</i>	1254
Privacy Preserving Support Vector Machines in Wireless Sensor Networks <i>Dong Seong Kim, Muhammad Anwarul Azim, and Jong Sou Park</i>	1260
An Image Encryption System by Cellular Automata with Memory <i>Farhad Maleki, Ali Mohades, S. Mehdi Hashemi, and Mohammed Ebrahim Shiri</i>	1266
<b>Workshop WAIS</b>	
Insider-secure Signcryption KEM/Tag-KEM Schemes without Random Oracles <i>Chik How Tan</i>	1275
Internet Observation with ISDAS: How Long Does a Worm Perform Scanning? <i>Tomohiro Kobori, Hiroaki Kikuchi, and Masato Terada</i>	1282
Electronic Voting Scheme to Maintain Anonymity in Small-scale Election by Hiding the Number of Votes <i>Tsukasa Endo, Isao Echizen, and Hiroshi Yoshiura</i>	1287
Enocoro-80: A Hardware Oriented Stream Cipher <i>Dai Watanabe, Kota Ideguchi, Jun Kitahara, Kenichiro Muto, Hiroki Furuichi, and Toshinobu Kaneko</i>	1294
Cryptanalysis and Improvement of an 'Improved Remote Authentication Scheme with Smart Card' <i>Marko Hölbl and Tatjana Welzer</i>	1301
Effective Monitoring of a Survivable Distributed Networked Information System <i>Paul Rubel, Michael Atighetchi, Partha Pal, Martin Fong, and Richard O'Brien</i>	1306
Design of an FDB based Intra-domain Packet Traceback System <i>Hiroaki Hazezama, Yoshihide Matsumoto, and Youki Kadobayashi</i>	1313
An Independent Evaluation of Web Timing Attack and its Countermeasure <i>Yoshitaka Nagami, Daisuke Miyamoto, Hiroaki Hazezama, and Youki Kadobayashi</i>	1319
Secure Spatial Authentication for Mobile Stations in Hybrid 3G-WLAN Serving Networks <i>Arjan Durresi, Mimoza Durresi, and Leonard Barolli</i>	1325
Privacy-Preserving Distributed Set Intersection <i>Qingsong Ye, Huaxiong Wang, and Christophe Tartary</i>	1332
Examination of Forwarding Obstruction Attacks in Structured Overlay Networks <i>Yo Mashimo, Shintaro Ueda, Yasutaka Shinzaki, and Hiroshi Shigeno</i>	1340
A Novel Approach for Multiplication over GF(2 <sup>m</sup> ) in Polynomial Basis Representation <i>Abdulah Abdulah Zadeh</i>	1346
<b>Workshop WSDF</b>	
Wi-Fi Network Signals as a Source of Digital Evidence: Wireless Network Forensics <i>Benjamin Turnbull and Jill Slay</i>	1355
Improving the Analysis of Lawfully Intercepted Network Packet Data Captured for Forensic Analysis <i>Jill Slay, Benjamin Turnbull, and Joshua Broadway</i>	1361
Recovery of Encryption Keys from Memory Using a Linear Scan <i>Christopher Hargreaves and Howard Chivers</i>	1369
Proposal for Efficient Searching and Presentation in Digital Forensics <i>Jooyoung Lee</i>	1377
Secure Steganography in Compressed Video Bitstreams <i>Bin Liu, Fenlin Liu, Chunfang Yan, and Yifeng Sun</i>	1382
Considerations Towards a Cyber Crime Profiling System <i>Kweku Arthur, Martin Olivier, Hein Yenter, and Jan H.P. Eloff</i>	1388

## Workshop SREIS

Alignment of Misuse Cases with Security Risk Management.....	1397
<i>Raimundas Matulevičius, Nicolas Mayer, and Patrick Heymans</i>	
Information Stream Based Model for Organizing Security .....	1405
<i>Bernhard Thalheim, Sabah Al-Fedaghi, and Khaled Al-Sagabi</i>	
Security Requirements Variability for Software Product Lines .....	1413
<i>Daniel Mellado, Eduardo Fernandez-Medina, and Mario Piattini</i>	
Transforming Security Requirements into Architecture.....	1421
<i>Koen Yskout, Riccardo Scandariato, Bart De Win, and Wouter Joosen</i>	
Modelling Security Properties in a Grid-based Operating System with Anti-Goals .....	1429
<i>Alvaro Arenas, Benjamin Aziz, Juan Bicarregui, Brian Matthews, and Erica Y. Yang</i>	
Annotating Regulations Using Cerno: An Application to Italian Documents—Extended Abstract.....	1437
<i>Nicola Zeni, Nadzeya Kiyavitskaya, James R. Cordy, Luisa Mich, and John Mylopoulos</i>	
Goal-Oriented, B-Based Formal Derivation of Security Design Specifications from Security Requirements.....	1443
<i>Riham Hassan, Shawn Bohner, Sherif El-Kassas, and Mohamed Eltoweissy</i>	
Analysis of Security Requirements for Cryptographic Voting Protocols (Extended Abstract).....	1451
<i>Orhan Cetinkaya</i>	

**Author Index**..... **1457**

## Chair's Message

The Third International Conference on Availability, Reliability and Security (ARES 2008 – The International Dependability Conference) brings together researchers and practitioners in the area of dependability. ARES 2008 highlights the various aspects of dependability, with special focus on the crucial linkage between availability, reliability and security.

ARES aims at a full and detailed discussion of research issues in the field of dependability as an integrative concept that covers amongst others availability, safety, confidentiality, integrity, maintainability and security and their different areas of applications.

This conference emphasizes the interplay between foundations and practical issues of dependability in areas such as information systems, e-government, m-government, location-based services, ubiquitous computing, and autonomous computing.

This years ARES conference is devoted to the critical examination and research challenges of the various aspects of Dependable Computing and the definition of a future road map.

We are very happy to welcome three well-known keynote speakers:

- Prof. Ravi Sandhu (Executive Director, Institute for Cyber-Security Research (ICSR) and Latcher Brown Endowed Chair in Cyber-Security, University of Texas, San Antonio)
- Prof. Vijay Atluri (Management Science and Information Systems Department, Rutgers University)
- Prof. Günther Pernul (Department of Information Systems, University of Regensburg)

From over 200 submissions we have selected the 44 best for a presentation as full paper. In addition, several workshops and short papers show ongoing research projects and offer interesting starting points for discussions.

We wish all participants an enjoyable conference and interesting discussions.

**Edgar R. Weippl, Secure Business Austria, Vienna University of Technology**  
**Gerald Quirchmayr, University of Vienna and University of South Australia**

**Jill Slay, University of South Australia**

# Conference Officers

## **Honorary Co-Chairs**

Roland Wagner, University of Linz, Austria

## **General Co-Chairs**

Guenther Pernul, University of Regensburg, Germany  
Makoto Takizawa, Tokyo Denki University, Japan

## **Program Co-Chairs**

Gerald Quirchmayr, University of South Australia, Australia  
Jill Slay, University of South Australia, Australia  
Edgar Weippl, Vienna University of Technology / Secure Business Austria, Austria

## **Workshops Co-Chairs**

Leonard Barolli, Fukuoka Institute of Technology (FIT), Japan  
A Min Tjoa, Vienna University of Technology, Austria

## **Organizing Chair**

Fatos Xhafa, Technical University of Catalonia, Spain

## **International Liaison Co-Chairs**

Maria Wimmer, University of Koblenz-Landau, Germany  
Charles Shoniregun, University of East London, United Kingdom

## **Publicity Chair**

Vladimir Marik, Czech Technical University, Czech Republic

## A Systematic Review and Comparison of Security Ontologies

Carlos Blanco<sup>1</sup>, Joaquín Lasheras<sup>2</sup>, Rafael Valencia-García<sup>2</sup>, Eduardo Fernández-Medina<sup>1</sup>, Ambrosio Toval<sup>2</sup> and Mario Piattini<sup>1</sup>

<sup>1</sup>Department of Information Technologies and Systems. University of Castilla-La Mancha  
 Paseo de la Universidad, 4. 13071. Ciudad Real (Spain)

{Carlos.Blanco, Eduardo.Fdzmedina, Mario.Piattini}@uclm.es

<sup>2</sup>Department of Informatics and Systems. University of Murcia

Campus Universitario de Espinardo. 30011. Murcia (Spain)

{jtolave, valencia, atoval}@um.es

### Abstract

The use of ontologies for representing knowledge provides us with organization, communication and usability. Information security is a serious requirement which must be carefully considered. Concepts and relations managed by any scientific community need to be formally defined and ontological engineering supports their definition. In this paper, the method of systematic review is applied with the purpose of identifying, extracting and analyzing the main proposals for security ontologies. The main identified proposals are compared using a formal framework and we conclude by stating their early state of development and the need of additional research efforts.

### 1. Introduction

An ontology is a specification of a conceptualization [1]. It represents knowledge in a formal and structured form as well as provides a better communication, reusability and organization of knowledge and a better computational inference [2-4]. In this way, the main objective of ontologies is that of establishing ontological agreements not only to decrease language ambiguity but also to serve as a basis for communication between agents.

Information security is a serious requirement which must be carefully considered, not as an isolated aspect, but as an element presented in all stages of the development lifecycle, from requirement analysis to implementation and maintenance [5-7]. In this way, information assurance, security and privacy have moved from being considered by information systems

designers as narrow topics of interest to become critical issues of fundamental importance in our society [8]. Some authors indicate that the survival of organizations depends on the correct management of information security and confidentiality [9].

It is very important to have the concepts and relations shared by the community formally defined. Therefore, several authors have indicated that the security community needs an ontology [10, 11] and they have considered this need as an important challenge and a research branch [7].

In this paper, we will carry out a systematic review of the existing literature on ontological engineering applied to security with the objective of knowing, analyzing and comparing the most relevant proposals. To perform this systematic review, we rely on the guideline proposed by Kitchenham [12] that is appropriate for software engineering researchers. In addition, we use a review protocol template developed by Biolchini [13] which facilitates systematic reviews planning and execution in software engineering.

The rest of the paper is organized as follows: in section 2, we will plan the review by defining the research question. Section 3 will execute the review and the first studies will be explained. Next, in section 4 we will define the data to be extracted and a data synthesis of the most relevant studies will be presented. In section 5, we will compare the ontologies and the results will be stated. Lastly, our conclusions will be set out in section 6.

### 2. Review Planning

In this phase, we must define the research objectives and the way in which the review will be executed

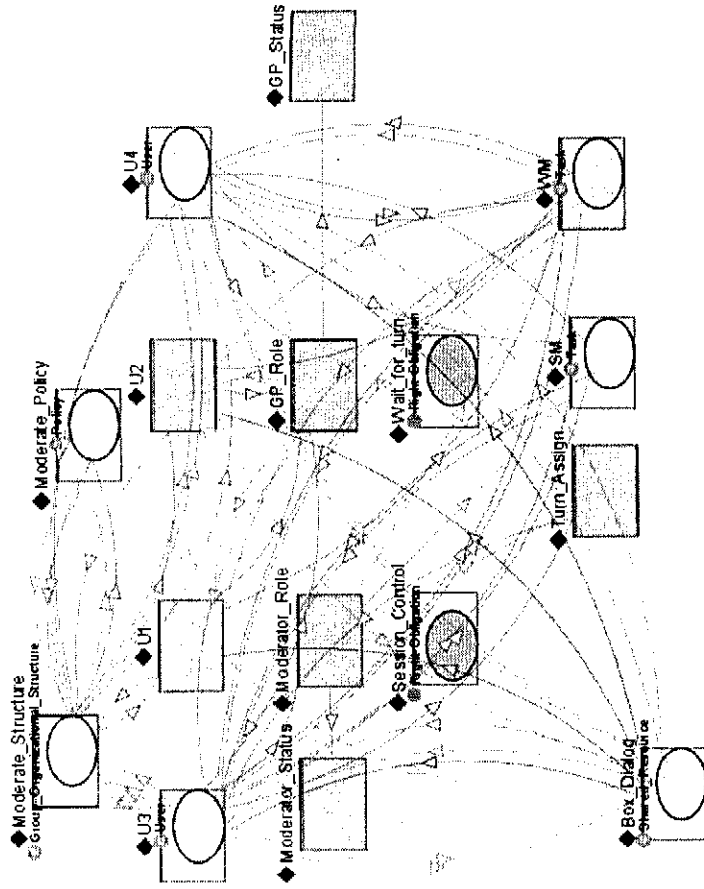


Figure 3. Ontology instances: Moderate policy. Figure generated by Jambalaya [13] plug-in for Protégé [14].

### 6. Conclusions

In this paper, we have presented policy-based group organizational structure management using an ontological approach. On the one hand, the policy-based approach dynamically adapts the behaviour of the group organizational structure without changing code and without requiring the consent or cooperation of the components being governed. On the other hand, the ontology-based policy specification, simplifies the access to policy information, with the possibility of dynamically calculating relations between policies and environment, or entities based on ontology relations.

### 7. References

- [1] S. Wright, R. Chadha, G. Lapiotis (eds.), "Special Issue on Policy based Networking". IEEE Network, Vol. 16-2, 2002, pp. 8-36.
- [2] N. Damianou, N. Dulay, E. Lupu, M. Sloman, "The Ponder Policy Specification Language", Springer-Verlag, LNCS Vol.1995, 2001, pp. 18-38.
- [3] J.M. Bradshaw, P. Beaulat, L. Bunch, S. V. Drakunov et al., "Making Agents Acceptable to People". In N. Zhong, J. Liu (eds): Handbook of Intelligent Information Technology. IOS Press, 2003.
- [4] G. Tomi, J.M. Bradshaw, R. Jeffers, R. Montanari, N. Suri, and A. Uszok, "Semantic Web Languages for Policy Representation and Reasoning: A Comparison of KAoS, Rei, and Ponder", Springer-Verlag, LNCS Vol. 2870, 2003, pp. 419-437.

- [5] T.R. Gruber, "Toward principles for the design of ontologies used for knowledge sharing", International Journal of Human Computer Studies Vol. 43(5/6), 1995, pp. 907-928.
- [6] M. Uschold, and M. Gruninger, "Ontologies and Semantics for Seamless Connectivity", In SIGMOD Record, Vol. 33-4, 2004, pp. 58-4.
- [7] <http://www.w3.org/2004/OWL/>. OWL Web Ontology Language Guide.
- [8] <http://www.w3.org/XML/>.
- [9] <http://www.w3.org/RDF/>.
- [10] Online at: <http://protege.stanford.edu/>
- [11] H. Shen, P. Dewan, "Access Control for Collaborative Environments", in Proceedings CSCW of ACM, ACM Press, 1992, pp. 51-58.
- [12] C.A. Ellis, and S.J. Gibbs, "Concurrency control in groupware systems", in proceedings ACM SIGMOD International Conference on Management of Data, 1989, pp. 399-407.
- [13] H.P. Donnel, J.J. Garcia-Luna-Aceves, "Floor Control for Multimedia Conferencing and Collaboration, ACM Multimedia, Vol. 5-1, 1997, pp. 23-38.
- [14] <http://www.thechiselgroup.org/jambalaya>

which includes, both the formulations of research questions and the planning of how the sources and studies selection will be carried out.

### 2.1. Question Formulation

In this section, the research objectives must be clearly defined. The *question focus* is to identify the most relevant works centered in the development of ontologies that deal with security issues.

In section 1, we have presented not only security as a relevant aspect to be taken into account in the development process but also the ontologies being considered as a tool that provides us with advantages such as concepts unification of a community. In this way, our *problem* is the study of the existing proposals in ontological engineering applied to information security.

The *research question* which will be addressed by our research is the following one: What initiatives have been carried out to develop security ontologies in the field of ontological engineering? The *keywords and related concepts* that make up this question and that will be used during the review execution are:

- Ontology (Ontological Engineering), OWL, RDF, DAML.
  - Security (Secure) and Privacy.
- In the context of the planned systematic review, the security ontologies proposals will be *observed*, analyzed and compared. And therefore, the *population* group that will be observed is formed by publications in the selected data sources.

The expected *result* at the end of this systematic review is the identification of initiatives related to security ontologies. Additionally, the *outcome measures* are the number of identified initiatives grouped by area and the main comparison proposal. The main *application* area that will benefit from the systematic review results is the ontological engineering applied to the security, specifically academics, researchers or professionals interested in this field.

### 2.2. Sources Selection

The objective of this section is to select the sources where searches for primary studies will be executed.

The *selection criteria* to evaluate studies sources are based on the opinion of the authors of this work as experts in both ontological and security engineering. Besides, these sources must be web available and must possess search engines using keywords. The studies must be written in English. The following list of *sources* has been considered: ScienceDirect, ACM

digital library, IEEE digital library, Scholar Google and DBLP. Later, the experts will refine the results and will include important works that had not been recovered in these sources.

### 2.3. Studies Selection

Once the sources are defined, it is necessary to describe the process and the criteria for studies selection and evaluation.

The *procedure* for studies selection consists of adapting our search chain to the syntax of each search engine and executing it. We then obtain a set of results to which the inclusion criteria is applied in order to obtain the relevant studies. Finally, the exclusion criteria is applied to the set of relevant studies in order to obtain our set of primary studies.

The studies *inclusion and exclusion criteria* are based on the research question, by finding proposals that make contributions to security ontological engineering. The inclusion criteria are focused on analyzing titles, keywords and abstracts of the studies, while the exclusion criteria mainly analyze abstracts, conclusions and other sections.

### 3. Review Execution

During this phase, the search in the defined sources must be executed and the obtained studies must be evaluated according to the established criteria. In next section, the information relevant to the research question must be extracted from the selected studies. The obtained studies which completely fit all previously defined inclusion and exclusion criteria are the following ones:

- Amaral et al. "An Ontology-based Approach to the Formalization of Information Security Policies" [14].
- Denker et al. "Security in the Semantic Web using OWL" [8].
- Denker et al. "Security for DAML Web Services: Annotation and Matchmaking" [15].
- Dobson et al. "Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web" [2].
- Donner. "Toward a Security Ontology" [10].
- Fenz et al. "Ontology based IT-security planning" [16].
- Firesmith. "A Taxonomy of safety-related requirements" [17].
- Geneiatakis et al. "An ontology description for SIP security flaws" [18].

- Giorgini et al. "Modelling Security and Trust with Secure Tropos" [19].

- Kagal et al. "Modeling conversation policies using permissions and obligations" [20].

- Karyda et al. "An ontology for secure e-government applications" [21].

- Kim et al. "Security Ontology for Annotating Resources" [22].

- Kwon et al. "Visual modelling and formal specification of constraints of RBAC using semantic web technology" [23].

- Lee et al. "Building Problem Domain Ontology from Security Requirements in Regulatory Documents" [24].

- Maamar et al. "Towards an ontology-based approach for specifying and securing Web services" [25].

- McGibney et al. "A service-centric model for intrusion detection in next-generation networks" [26].

- Mouratidis et al. "Integrating Security and Software Engineering: An Introduction" [7].

- Mouratidis et al. "An Ontology for Modelling Security: The Tropos Approach" [27].

- Raskin et al. "Ontology in information security: a useful theoretical foundation" [28].

- Tan et al. "Dynamic security reconfiguration for the semantic web" [29].

- Thuringham. "Security standards for the semantic web" [30].

- Tsoumas et al. "Towards an Ontology-based Security Management" [11].

- Undercoffer et al. "Modeling Computer Attacks: An Ontology for Intrusion Detection" [31].

- US Department of Defense. "Orange Book" [32].

- Vorobiev et al. "Security Attack Ontology for Web Services" [33].

- Yu et al. "A Social Ontology for Integrating Security and Software Engineering" [34].

- Zhou et al. "Ontology Based Software Reliability Modelling" [35].

- Zhou et al. "An Integrated QoS-Aware Service Development and Management Framework" [36].

### 4. Information Extraction

Once primary studies are selected, the extraction of relevant information begins. In this section, extraction criteria and results will be described.

To standardize the way that information will be represented we create forms to collect data from the selected studies. The information forms defined for this

review are composed of three components: basic information (title, publication, authors and reference in EndNote format), general description (study area and summary) and our general impressions and comments. The selected areas to classify studies are as follows: security ontologies (general and applied to specific domain), theoretical works and semantic web oriented.

Next, we will present a brief outline of each of the selected studies in the previous section according to the extracted information obtained through the information forms. We will only focus on security ontologies proposals due to space constraints.

Denker et al. "Security in the Semantic Web using OWL" [8] and "Security for DAML Web Services: Annotation and Matchmaking" [15].

Authors develop several ontologies for security annotations of agents and web services, in a first work using DAML (DARPA Agent Markup Language) [15] and later using OWL (Web Ontology Language) [8]. These ontologies represent well-known security concepts and enable us to interconnect security standards. The defined ontology is formed by two sub-ontologies: "security mechanisms" that captures high-level security notations and "credential" that defines authentication methods.

Dobson et al. "Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web" [2].

Due to the emergence of the semantic web, the interest in ontologies is increasing. In this work, authors focus on the field of dependability requirements and revise ontologies for Requirements Engineering. They also define in OWL a dependability ontology compliant with the IFIP Working Group 10.4 taxonomy that includes security issues such as "dependability", "reliability", "availability", "integrity", "confidentiality" or "safety".

Fenz et al. "Ontology based IT-security planning" [16].

In this proposal, authors study security in small and medium size enterprises (SMEs) and propose a holistic solution based on a security ontology that includes low-cost risk management and threat analysis. The security ontology consists of five sub-ontologies. "Threat" is the main sub-ontology and includes proper countermeasures, threatened infrastructures and proper evaluation methods. "Attribute" sub-ontology models the impact of threats, "Infrastructure" describes infrastructure elements, "Role" maps enterprise

hierarchies and "Person" represents natural persons who are relevant for security issues modelling.

Firesmith "A Taxonomy of safety-related requirements" [17].

Firesmith states that the main objective of a safety engineer is that of identifying the requirements to keep valuable assets (like staff, property or environment) off threats. Ontologies could be used due to the fact that safety-related requirements typically have reuse potentials. He presents the following taxonomy of safety-related requirements: "Safety requirements" are requirements obtained from threats analysis. "Safety-significant requirements" includes non-safety requirements that can cause hazards and safety incidents. "Safety constraints" are constraints that directly impact safety and are derived from laws, policies, standards and industrial practices. "Safety system requirements" specify aspects of the primary system.

Karyda et al. "An ontology for secure e-government applications" [21].

In this work, the authors use OWL to propose a security ontology with which to develop secure applications. It captures the security knowledge of experts to support the communication between security experts, users and developers and developers use it to include security requirements as well as to support design choices.

The proposed ontology is formed of "assets" (data asset, hardware data,...), "countermeasures" (identification and authentication, network management, auditing services, physical protection,...), "objectives", "persons" (insider stakeholder, attacker,...) and "threats" (errors, attacks, technical failures,...). They validate the defined ontology using nRQL queries and in order to demonstrate that their ontology can be used in various contexts they apply it to e-government scenarios: e-tax and e-voting.

Kim et al. "Security Ontology for Annotating Resources" [22].

Authors use OWL for developing the NRL security ontology focused on annotation of functional aspects of resources. This ontology is capable of representing security statements like mechanisms, protocols, algorithms and credentials and can be applied to any electronic resource.

NRL presents an architecture easy to use and easy to extend, and is composed of seven sub-ontologies. Three of them are based on existing ontologies in DAML: firstly, "Service security ontology" that

describes security annotation of semantic web services secondly, "Agent security ontology" that enables querying of security information and finally "Information object ontology" that describes security of input and output parameters of web services.

The four remaining ontologies are as follows: "Main security ontology" that describes security protocols, mechanisms and policies, "Credentials ontology" that specifies authentication credentials, "Security algorithms ontology" that describes various security algorithms and "Security assurance ontology" that specifies different assurance standards.

Lee et al. "Building Problem Domain Ontology from Security Requirements in Regulatory Documents" [24].

In this paper, authors identify security requirements for certification and accreditation activities which are expressed in regulatory documents. These requirements have a non-functional nature that imposes complex constraints on behaviour of software systems and makes them hard to understand, predict and control.

Authors present a framework that includes techniques extracted from software requirements engineering and knowledge engineering and they propose a common language for extracting concepts from regulatory documents. They apply this methodology to build problem domain ontology from regulatory documents enforced by the DITSCAP Department of Defense Information Technology Security Certification and Accreditation Process.

Mouratidis et al. "An Ontology for Modelling Security: The Tropos Approach" [27] and "Modelling Security and Trust with Secure Tropos" [19].

The Tropos methodology considers two approaches in software development: a security-oriented process and a management of the dependability-oriented process.

This methodology is based on social hierarchies and adapts components of the T\* framework [34]. Authors improve the social ontology created for T\* framework with new security concepts: constraints, secure entities (goals, tasks and secure resources) and secure dependences between actors.

Tsoumas et al. "Towards an Ontology-based Security Management" [11].

In this proposal, authors define security ontology in OWL and present a security framework of an arbitrary information system which provides security acquisition and knowledge management. They extend the DMJF Common Information Model (CIM) standard with

ontological semantics in order to use it as a container for IS security-related information.

Undercoffer et al. "Modeling Computer Attacks: An Ontology for Intrusion Detection" [31].

Here, first of all, authors analyzed around 4000 vulnerabilities and their exploit strategies and after that they created an ontology, in DAML+OIL and DAML+JessKB, for specifying computer attacks. In this paper, authors also summarize the main languages for specifying computer attacks: P-Best, STATL, LogWeaver, CISL, BRO, Snort Rules and IDMEF and present several use case scenarios with common attacks: "Denial of Service - Syn Flood", "The Classic Mitnick Type Attack" and "Buffer Overflow Attack".

Zhou et al. "An Integrated QoS-Aware Service Development and Management Framework" [36].

This work proposes a method for management and service quality assurance (QoS-aware) that consists of QoS-aware service management infrastructure, QoS ontology and QoS property ontology.

The QoS ontology provides us with a knowledge mapping with QoS concepts and relations that can be used for QoS-aware services communicating and exchanging. The QoS property ontology has two sub-ontologies: "Technical QoS property", that defines concepts and relations related to software development and "Managerial QoS property" focused on service providing.

Zhou et al. "Ontology Based Software Reliability Modelling" [35].

Authors propose an ontology-based method for software reliability modeling that includes a software reliability ontology developed in OWL together with an ontology-based software modeling system.

They describe reliability engineering as a series of interrelated processes by which reliability knowledge is reorganized with the support of methods, tools, models, organization, and the specifications of input and output. In future works, they will focus on extending reliability ontology and applying the method to software architecture design.

## 5. Result Analysis

After the systematic review execution, the results must be summarized and analyzed using the methods defined during the planning phase. In this section, we classify the primary studies into the above defined areas and compare the main proposals to an ontological framework.

In Table 1, we present the primary studies classified by area and we observe that the greater part of the studies are security ontologies applied to specific domains.

Next, we compare the ontologies using a framework presented in [37], which is based on comparing basic elements (concepts, relations, attributes, etc) and measures made with OntoMetric framework [38]. It has not been possible to accomplish the comparison taking into consideration all the identified security ontologies because some of them are not web available and when we have tried to obtain them, authors have communicated us that their ontologies are still under construction.

In the following subsections, we present comparison results together with the conclusions that we have obtained after analyzing the available ontologies. These conclusions are shown by comparing similar ontologies: Denker versus Kim, which are general ontologies that describe secure mechanisms, and Dobson versus Undercoffer, which are focused on specific domains.

Table 1. Primary studies classified by area

Area	References	N° of studies
Security ontologies (general)	[8, 15, 21, 22, 24, 11, 36]	7
Security ontologies (applied to a specific domain)	[14, 2, 16-19, 27, 31, 34, 35]	10
Theoretical Works	[32, 10, 7, 28]	4
Semantic web-oriented	[8, 15, 20, 23, 25, 26, 29, 30, 33]	9

## 5.1. General Comparison

In Table 2, we present general measures of the available ontologies obtained using an OWL ontology editor, SWOOP.

Table 2. General comparison

	Denker	Kim	Dobson	Undercoffer
Number of concepts	87	82	92	106
Root concepts	45	20	32	41
Instances	136	81	61	22
Avg depth of inheritance	1,9	2,19	2,26	1,8
Avg of rel. concepts	0,57	0,37	0,62	0,55
Avg of attributes	0,11	0,42	1,18	0
Avg of subclasses	0,44	0,65	0,65	0,61
Number of taxonomic relations	42	62	60	65
Number of no taxonomic relations	24	25	25	75

We can observe that Denker's ontology has a greater number of concepts and instances than Kim's

proposal. This fact indicates that Kim's ontology is more general and does not detail any concrete area.

Kim's ontology is composed of seven sub-ontologies; one of them is focused on authentication methods and Denker defines it in greater depth. Denker performs a great conceptualization of the domain but he uses less attributes to define concepts and he should assign more properties as Kim does.

On the other hand, Dobson and Undercoffer proposals present a greater number of concepts because they try to model specific domains (dependability and computer attacks). Undercoffer neither identifies attributes nor use them for defining concepts.

The rest of our measures of this general comparison will be useful for the OntoMetric comparison accomplished in the following subsection.

### 5.1. OntoMetric

OntoMetric [38] is a method for comparing ontologies that is composed of factors grouped into five dimensions: represented contents, language, methodology, software environment and cost of using the ontology in new systems.

We focus on contents dimension that presents four factors: concepts, relations, concepts taxonomy and axioms. In relation to language dimension, all studied ontologies use OWL as representation language.

Every factor has measurable characteristics scored from 1 to 5 according to their low or high degree of accomplishment. The considered values for each characteristic will be shown in tables 3, 4, 5 and 6.

In table 3, we show the values for the concepts factor and we observe how Kim poorly describes concepts and does not formally specify them in natural language. On the contrary, Denker defines the concepts of the domain properly. Therefore, Kim's ontology makes its reutilization difficult because he does not describe concepts in natural language. However, Denker should assign more properties to each concept to correctly define the attributes that the concepts instances have.

Undercoffer's proposal is more difficult to understand because it poorly describes concepts, it does not make use of attributes to describe them and the used concepts identifiers are not representative. Nevertheless, Dobson widely describes concepts in natural language and includes attributes for defining them; therefore Dobson's ontology is more reusable.

In Table 4, we specify the values for the relations factor. In general, although relationships have been properly defined in the domain, they are not properly specified in natural language and not all of the formal

properties of the relations are identified, in fact some authors such as Denker and Kim do not take them into account. They should specify relations in a formal way to obtain reusability and detection of incongruences.

In table 6, we show the axiom factor and its characteristics. Kim and Denker define few axioms and they cannot infer knowledge, only some restrictions to the value of the attributes of the concepts, while Dobson and Undercoffer use more constraints and can infer knowledge and verify consistency, but these are related to the concept of the ontology (they are not independent). It is advisable that authors include formal properties in the relations (reflexion, transitivity, asymmetry, symmetry and inverse function) which verify consistence.

## 6. Conclusions

In this section, we put forward our conclusions after planning the revision, executing it, analyzing primary studies and comparing the available proposals. We have observed that the greatest part of the identified works is focused on specific domains or the semantic web; therefore, we can affirm that so far, the scientific community has not accomplished a general security ontology but the need of security ontology has been identified as a branch of research.

Defining ontology is considered a main task within any scientific community; in this way, we give formal support and sharing capabilities to the managed knowledge. In the security field, it is impossible to formalize all existing concepts, so the definition of a complete security ontology is not an isolated task and the community should add efforts for joining and improving the developed ontologies. This complete security ontology should be flexible and easy to update for including changes along with new concepts that appear in the community.

In addition, we have observed how the greatest part of the selected works is still at the early stages of development and the source files of the security ontologies are not available yet for their study.

We have compared the available proposals and we have found out that not only include few attributes for defining concepts but also the natural language expressions used for describing them are not appropriate. They are not exhaustive because the ontologies do not define all possibilities of the studied domain, so we have identified this lack as a future work. These ontologies use few axioms and formal properties for inferring knowledge like reflexivity, transitivity, symmetry, asymmetry and inverse function.

We can conclude that the existing ontologies are not prepared for being reused and extended and that the security community still needs a complete security

ontology that solves these lacks and provides reusability, communication and knowledge sharing.

In this sense, we have tried to combine the ontologies identified in section 5 but we have had some problems such as common concepts have different terms applied to them: for example, Kim specifies the terms CryptographicKey and BiometricToken, while Denker uses Key and Biometric. Furthermore, we have identified deficiencies in the attributes associated to the ontology and in the use of some expressions in natural language for describing concepts so that to combine both ontologies has been impossible without being the creator of the ontologies and to know exactly what this term mean, although being a domain expert.

## Acknowledgements

This research is part of the Projects ESFINCE (TIN2006-15175-C05-05), DEDALO (TIC2006-15175-C05-03) and RETISTRUST (TIN2006-26885-E) financed by the "Ministerio de Educación y Ciencia", and the MISTICO (PBC-06-0082) financed by the FEDER and the "Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha (Spain)".

## References

- [1] Gruber, T., Towards Principles for the Design of Ontologies used for Knowledge Sharing. International Journal of Human-Computer Studies, 1995. 43(5/6): p. 907-928.
- [2] Dobson, G. and P. Sawyer, Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web. International Seminar on "Dependable Requirements Engineering of Computerised Systems at NPP's", Institute for Energy Technology (IFE), Halden, 2006.
- [3] Fernández-Breis, J.T. and R. Martínez-Béjar, A cooperative framework for integrating ontologies. International Journal of Human-Computer Studies, 2002. 56: p. 665-720.
- [4] Gruninger, M. and J. Lee, Ontology Applications and Design. Communications of the ACM, 2002. 45(2): p. 39-41.
- [5] Devanbu, P. and S. Stubblebine, Software engineering for security: a roadmap. ACM Press. Future of Software Engineering, 2000: p. 227-239.
- [6] Ferrari, E. and B. Thuraisingham. Secure Databases Systems. in Advanced Databases: Technology Design. 2000. Artech Huse: London.
- [7] Mouratidis, H. and P. Giorgini. An Introduction, in Integrating Security and Software Engineering: Advances and Future Visions. 2006. Idea Group Publishing.
- [8] Denker, G., L. Kagal, and T. Finin, Security in the Semantic Web using OWL. Information Security Technical Report, 2005. 10(1): p. 51-58.

Table 3. OntoMetric comparison: concepts factor

Concepts factor	Denker	Kim	Dobson	Undercoffer
Essential concepts	4	4	4	4
Essential concepts in superior levels	5	5	5	5
Concepts properly described in NL	2	1	3	1
Formal specification coincides with NL	4	4	4	4
Attributes describe concepts	1	1	2	2
Number of concepts	4	4	4	4

Table 4. OntoMetric comparison: relations factor

Relations factor	Denker	Kim	Dobson	Undercoffer
Essential relations	4	4	4	4
Relations relate appropriate concepts	5	5	5	4
Formal specification of relations coincides with naming	2	1	3	1
Any specified relations	2	2	3	3
Formal properties of relations	1	1	2	2
Number of relations	4	4	4	5

Table 5. OntoMetric comparison: taxonomy factor

Taxonomy factor	Denker	Kim	Dobson	Undercoffer
Several perspectives	2	2	4	2
Appropriate not subclass of	1	1	1	1
Appropriate exhaustive partitions	2	4	3	4
Appropriate disjoint partitions	2	4	4	1
Maximum depth	3	4	4	3
Average of subclasses	3	3	3	3

Table 6. OntoMetric comparison: axioms factor

Axioms factor	Denker	Kim	Dobson	Undercoffer
Solve queries	2	2	3	3
Infer knowledge	2	3	3	4
Verify consistency	3	3	3	3
Not linked to concepts	2	3	1	1
Nº of axioms	1	1	3	3

The values for the taxonomy factor are presented in table 5. Kim and Denker do not use either several perspectives to classify the concepts or do not use the relation "not\_subclass\_of" to break an inheritance relation between concepts. Moreover, they could improve the use of appropriate exhaustive partitions by revising all possible decomposition classes in the



## Context Ontology for Secure Interoperability

Céline Coma<sup>1</sup>, Nora Cuppens-Boulahia<sup>1</sup>, Frederic Cuppens<sup>1</sup>, Ana Rosa Cavalli<sup>2</sup>

<sup>1</sup> GET/ENST Bretagne, 2 rue de la chataigneraie, 35512 Cesson Sevigne Cedex, France

<sup>2</sup> GET/INT Evry-CNRS, 9, rue Charles Fourier, 91011 Evry, France

### Abstract

During interoperability exchanges, organizations are actively conducting computation and sharing tasks. How organizations can have different security policies. To guarantee good interoperability exchanges, organizations have to share with other participants information about the policies they provide. In addition, to be compliant with security requirements during interoperability, security policies have to be dynamic. One purpose of this paper is to provide this dynamic behavior by taking care about context of access parameters. The context-aware security elements may be met by using a contextual access control model to define the security policy of each party involved in the interaction, and OrBAC (Organization based Access Control) is an adequate model for this purpose. Elaborating an ontology based security model provides a mean to ensure a high level of understandable knowledge, in particular knowledge needed to derive the authorized accesses and usages during the interoperability sessions. In this paper, we thus present a context ontology to be combined with an ontology representation of the OrBAC model and show how it can be used to ease the security rules definition and derivation during interoperability sessions.

**Keywords:** Security model, Interoperability, Ontology, Context, OrBAC

### Introduction

The growth of the Internet has triggered opportunities for cooperative computation and electronic interoperation (interoperation), where enterprises are jointly conducting computation and sharing business tasks based on the classification of resources they each supply or authorize to use or to share. These e-interoperations generally occur between organizations having different security policies. To conduct interoperation, one organization must usually access resources of the other participants; however if no entity is trusted enough to access or modify all the resources whatever is the environment conditions (temporal, his-

Software engineering for secure systems. 2006, ACM Press: Shanghai, China.

[25] Maamar, Z., N.C. Narendra, and S. Sattanathan, Towards an ontology-based approach for specifying and securing Web services. *Information and Software Technology*, 2006. 48(7): p. 441-455.

[26] McGibney, J., N. Schmidt, and A. Patel, A service-centric model for intrusion detection in next-generation networks. *Computer Standards & Interfaces*, 2005. 27(5): p. 513-520.

[27] Mouratidis, H., P. Giorgini, and G. Manson, An Ontology for Modelling Security: The Tropos Approach, in *Knowledge-Based Intelligent Information and Engineering Systems*, 2003, Springer Berlin / Heidelberg. p. 1387-1394.

[28] Raskin, V., et al., Ontology in information security: a useful theoretical foundation. *Proceedings of the 2001 workshop on New security paradigms NSPW'01*. ACM Press, 2001.

[29] Tan, J.J. and S. Poslad, Dynamic security reconfiguration for the semantic web. *Engineering Applications of Artificial Intelligence*, 2004. 17(7): p. 783-797.

[30] Thraisingham, B., Security standards for the semantic web. *Computer Standards & Interfaces*, 2005. 27(3): p. 257-268.

[31] Undercoffer, J., A. Joshi, and J. Pinkston, Modeling Computer Attacks: An Ontology for Intrusion Detection, in *The Sixth International Symposium on Recent Advances in Intrusion Detection*, 2003: Springer.

[32] DOD, Orange Book. Estándar DOD 5200.58-STD., in [www.radium.ncsc.mil/txep/library/raibow/5200.28-STD.html](http://www.radium.ncsc.mil/txep/library/raibow/5200.28-STD.html), D.d.d.l. EEUU, Editor. 1970.

[33] Vorobiev, A. and J. Han, Security Attack Ontology for Web Services. *Proceedings of the Second International Conference on Semantics, Knowledge, and Grid SKG '06*. IEEE Computer Society, 2006: p. 42.

[34] Yu, E., L. Liu, and Mylopoulos, A Social Ontology for Integrating Security and Software Engineering, in *Integrating Security and Software Engineering: Advances and Future Visions*, 2006, Idea Group Publishing.

[35] Zhou, J., E. Niemelä, and A. Evesti, Ontology-based software reliability modelling. *Proceedings of Software and Services Variability Management Workshop - Concepts, Models and Tools*, Helsinki, Finland, 2007: p. 17-31.

[36] Zhou, J., E. Niemelä, and P. Savolainen, An Integrated QoS-Aware Service Development and Management Framework. *wicisa*, 2007: p. 13.

[37] Blomqvist, E., A. Öhrgren, and K. Sandkuhl, Ontology Construction in an Enterprise Context: Comparing and Evaluating Two Approaches. in *In Proceedings of the Eighth International Conference on Enterprise Information Systems: Databases and Information Systems Integration*, 2006, Paphos, Cyprus.

[38] Lozano-Tello, A. and A. Gómez-Pérez, ONTOMETRIC: A Method to Choose the Appropriate Ontology. *Journal of Database Management*, Special Issue on Ontological analysis, Evaluation, and Engineering of Business Systems Analysis Methods, 2004. 15(2).

[9] Dhillon, G. and J. Backhouse, Information system security management in the new millennium. *Communications of the ACM*, 2000. 43(7): p. 125-128.

[10] Donner, M., Toward a Security Ontology. *IEEE Security and Privacy*, 2003.

[11] Tsourmas, B. and D. Grizalis, Towards an Ontology-based Security Management. *Proceedings of the 20th International Conference on Advanced Information Networking and Applications*. IEEE Computer Society, 2006. Volume 1 (AINA'06) - Volume 01 AINA '06.

[12] Kitchenham, B., Procedures for performing systematic reviews (Joint Technical Report), in *TR/SE-0401*. 2004, Software Engineering Group, Department of Computer Science: Keele University. p. 33 p.

[13] Biolchini, J. and P. Gomes, Systematic Review in Software Engineering. 2005, Systems Engineering and Computer Science Department, UFRJ: Rio de Janeiro, Brazil.

[14] Amaral, F.N.d., et al., An Ontology-based Approach to the Formalization of Information Security Policies. *Proceedings of the 10th IEEE on International Enterprise Distributed Object Computing Conference Workshops EDOCW'06*. IEEE Computer Society, 2006.

[15] Denker, G., et al., Security for DAML Web Services. *ISWC 2003*, 2003, Springer Berlin / Heidelberg. p. 335-350.

[16] Fenz, S. and E. Weippl, Ontology based IT-security planning. *Proceedings of the 12th Pacific Rim International Symposium on Dependable Computing PRDC '06*. IEEE Computer Society, 2006: p. 389-390.

[17] Firesmith, D., Engineering safety-related requirements for software-intensive systems. in *Proceedings of the 27th international conference on Software engineering*, 2005, ACM Press: St. Louis, MO, USA.

[18] Geneiatakis, D. and C. Lambrinoukakis, An ontology description for SIP security flaws. *Computer Communications*, 2006. In Press, Corrected Proof.

[19] Giorgini, P., H. Mouratidis, and N. Zannone, Modelling Security and Trust with Secure Tropos, in *Integrating Security and Software Engineering: Advances and Future Visions*, 2006, Idea Group Publishing.

[20] Kagal, L. and T. Finin, Modeling conversation policies using permissions and obligations. *AAMAS workshop on Agent communication*, LNCS. Springer-Verlag, 2005.

[21] Karyda, M., et al., An ontology for secure e-government applications. *First International Conference on Availability, Reliability and Security (ARES'06)*. IEEE Computer Society, 2006: p. 1033-1037.

[22] Kim, A., J. Luo, and M. Kang, Security Ontology for Annotating Resources, in *4th International Conference on Ontologies, Databases, and Applications of Semantics (ODBASE'05)*, 2005, Agia Napa, Cyprus.

[23] Kwon, J. and C.-J. Moon, Visual modeling and formal specification of constraints of RBAC using semantic web technology. *Knowledge-Based Systems*, 2006. In Press, Corrected Proof.

[24] Lee, S.-W., et al., Building problem domain ontology from security requirements in regulatory documents, in *Proceedings of the 2006 international workshop on*

# Author Index

## The Third International Conference on Availability, Reliability and Security (ARES 2008)

Abbassi, Ryma.....	467	Blondia, Chris.....	1213
Abu-Nimeh, Saeed.....	1044	Bohner, Shawn.....	1443
Almed, Irfan.....	1028	Botham, Paul.....	253
Aickelin, Uwe.....	896	Böttcher, Stefan.....	771
Almeur, Esma.....	161	Bouillaut, Laurent.....	795
Aknin, Patrice.....	795	Boustia, Narhimene.....	1008
Al-Fedaghi, Sabah.....	1405	Bouvy, Pascal.....	1036
Al-Hammadi, Yousof.....	896	Bouzida, Yacine.....	204
Almohammad, Adel.....	544	Bræk, Rolv.....	597
Al-Saqabi, Khaled.....	1405	Brassard, Gilles.....	161
Amato, Flora.....	1097	Breu, Ruth.....	921
Angevine, Duff.....	1075	Broadway, Joshua.....	1361
Anspér, Arne.....	572	Brunstrom, Anna.....	526
Anzures-García, Mario.....	807	Buddendick, Christian.....	758
Ardi, Shanai.....	284	Bußer, Jens-Uwe.....	335
Arenas, Alvaro.....	1429	Byers, David.....	276
Ariet, Magi Lluch i.....	578	Canfora, Gerardo.....	1020
Armendáriz-Iñigo, Enrique.....	120	Casola, Valentina.....	1097
Arthur, Kweku.....	1388	Catrina, Octavian.....	693
Asnar, Yudistira.....	1240	Cavadini, Salvador.....	586
Atighetchi, Michael.....	1306	Cavalli, Ana Rosa.....	821
Ayuso, Pablo Neira.....	422	Cavallo, Bice.....	1020
Azer, Marianne.....	636, 881	Ceballos, Rafael.....	229
Azim, Muhammad Anwarul.....	1260	Cetinkaya, Orhan.....	1451
Azimah, Noor.....	1219	Challal, Yacine.....	503
Aziz, Benjamin.....	1429	Chang, Shuang.....	733
Bagaa, Miloud.....	503	Chaouchi, Hakima.....	144
Baldi, Mario.....	434	Charnsripinyo, Chalermpol.....	604
Balfe, Shane.....	376	Charoenpomwattana, Kulathap.....	659
Bao, Feng.....	112	Cheda, Diego.....	586
Barbaron, Denis.....	422	Chen, Chia-Mei.....	410
Barolli, Leonard.....	1325	Chen, Kuan-Ta.....	212
Benslimane, Djamel.....	834	Chen, Tsuhan.....	410
Bergmann, Mike.....	903	Chen, Xin.....	484
Bernabé-Gisbert, Josep M.....	369	Cheng, Jingde.....	171, 1219
Bertino, Elisa.....	153	Cheng, Yu-Chin.....	410
Bicarregui, Juan.....	1429	Chivers, Howard.....	1369
Bielova, Nataliia.....	128	Chmielewski, Łukasz.....	327
Bistarelli, Stefano.....	1128	Claeys, Geert.....	18
Blanco, Carlos.....	813, 1248	Clark, Andrew.....	47

Clint, Maurice ..... 428  
 Coetzee, Marijke ..... 440  
 Coma, Céline ..... 821  
 Cordy, James R. .... 1437  
 Coudert, Fanny ..... 975  
 Croitoru, Madalina ..... 578  
 Cuppens, Frédéric ..... 821  
 Cuppens-Boulahia, Nora ..... 821  
 Damiani, Maria Luisa ..... 153  
 Daniels, Nils ..... 1139  
 Das, Ananda Swarup ..... 446  
 Dasmahapatra, Srinandan ..... 578  
 Debbabi, Mourad ..... 302  
 Dehbashi, Mehdi ..... 491  
 Delessy, Nelly A. .... 416  
 Dios, Araceli Queiruga ..... 741  
 Domingo-Ferrer, Josep ..... 990  
 Donat, Roland ..... 795  
 Dragoni, Nicola ..... 128  
 Dssouli, Rachida ..... 3  
 Duarte, Angelo ..... 653  
 Dumortier, Jos ..... 975  
 Dupplaw, David ..... 578  
 Durrési, Arjan ..... 1325  
 Durrési, Mimoza ..... 1325  
 Ebben, P.W.G. .... 397  
 Echizen, Isao ..... 1287  
 Eckert, Claudia ..... 376  
 El-Kassas, Sherif ..... 636, 881, 1443  
 Eloff, Jan H.P. .... 1388  
 El-Soudani, Magdy ..... 636, 881  
 Eltoweissy, Mohamed ..... 1443  
 Encinas, Ascension Hernández ..... 741  
 Endersz, Viktor ..... 1139  
 Endo, Tsukasa ..... 1287  
 Engelmann, Christian ..... 260, 659  
 Eskeland, Sigurd ..... 943  
 Falcarin, Paolo ..... 434  
 Farazmand, Navid ..... 33  
 Farr, Erin ..... 675  
 Fatmi, Sihem Guemara El ..... 467  
 Faulkner, Mike ..... 497  
 Fazeli, Mahdi ..... 33  
 Fernandez, Eduardo B. .... 416  
 Fernandez, José M. .... 161  
 Fernández, Miguel ..... 520  
 Fernández-Medina, Eduardo ..... 104,  
 136, 813, 1248  
 Fernandez-Medina, Eduardo ..... 1413

Ferreres, Ana Isabel González-Tablas ..... 363  
 Florio, Vincenzo De ..... 1213  
 Fong, Martin ..... 1306  
 Formé, Jordi ..... 701, 1000  
 Franz, Elke ..... 903  
 Frei, Adrian ..... 610  
 Fries, Steffen ..... 335  
 Fuchs, Ludwig ..... 752  
 Furuichi, Hiroki ..... 1294  
 Gabarró, Joaquim ..... 428  
 Gaborit, Philippe ..... 1052  
 Gansterer, Wilfried ..... 10  
 Garg, Sanjam ..... 667  
 Garnacho, Arturo Ribagorda ..... 363  
 Gasca, Rafael Martínez ..... 229  
 Gasca, Rafael ..... 422  
 Ghinea, Gheorghita ..... 544  
 Ghorbani, Ali ..... 88  
 Gibb, Alex ..... 578  
 González-Vélez, Horacio ..... 578  
 Goto, Yuichi ..... 171, 1219  
 Grascsher, Veronika ..... 39  
 Gritzalis, Stefanos ..... 929  
 Grob, Heinz Lothar ..... 758  
 Groba, Christin ..... 903  
 Gruschka, Nils ..... 509  
 Gu, Yu ..... 630  
 Guang-Yu, He ..... 473  
 Guntupalli, Srinivas ..... 592  
 Hadavi, Mohammad Ali ..... 866  
 Halunen, Kimmo ..... 828  
 Hamishagi, Vahid Saber ..... 866  
 Han, Kai ..... 564  
 Hansen, René Rydhof ..... 1104  
 Haque, Anwar ..... 245  
 Hargreaves, Christopher ..... 1369  
 Harmer, Terry ..... 428  
 Harper, Richard ..... 675  
 Hartel, Rita ..... 771  
 Hartmann, Peter ..... 335  
 Hashemi, S. Mehdi ..... 1266  
 Hassan, Abdel Wahab ..... 636, 881  
 Hassan, Riham ..... 1443  
 Hassanzadeh, Amin ..... 982  
 Hatebur, Denis ..... 195  
 Hazeyama, Hiroaki ..... 1313, 1319  
 He, Liwen ..... 253  
 He, Mingxing ..... 746  
 He, Xubin ..... 260

Kerschbaum, Florian ..... 693  
 Keshri, Jitu Kumar ..... 446  
 Khakpour, Amir ..... 144  
 Khan, Latifur ..... 237  
 Kiani, Mehdi ..... 47  
 Kijisanayothin, Phongphun ..... 765  
 Kikuchi, Hiroaki ..... 1282  
 Kilpatrick, Peter ..... 428  
 Kim, Dong Seong ..... 1260  
 Kirmani, Ezzat ..... 479  
 Kirschner, Matthias ..... 771  
 Kitahara, Jun ..... 1294  
 Kitajima, Natsumi ..... 171  
 Kiyavitskaya, Nadzeya ..... 1437  
 Klaoudatou, Eleni ..... 929  
 Klopotek, Mieczyslaw ..... 1036  
 Kobori, Tomohiro ..... 1282  
 Kohler, Mathias ..... 709  
 Kolb, Mathias ..... 39  
 Kollveit, Heine ..... 64  
 Konstantinou, Elisavet ..... 550, 929  
 Korobitsin, Victor ..... 967  
 Koyanagi, Keiichi ..... 842  
 Kuang, Liwei ..... 319  
 Kumar, Ashwin ..... 10  
 Kupsch, James ..... 1196  
 Kutvonen, Lea ..... 873  
 Kwiat, Kevin ..... 1180, 1234  
 Ladra, Susana ..... 994  
 Lai, Gu-Hsin ..... 410  
 Laihi, Chi-Sung ..... 410  
 Langer, Josef ..... 642  
 Lari, Vahid ..... 491  
 Larrea, Mikel ..... 801  
 Larson, Ulf ..... 624  
 Lasheras, Joaquin ..... 813  
 Lasla, Noureddine ..... 503  
 Lathouwers, Danny ..... 1091  
 Laurent-Maknavicius, Maryline ..... 144  
 Leangsuksun, Chokchai ..... 260, 659  
 Lee, Jooyoung ..... 1377  
 Leesutthipornchai, Pakorn ..... 604  
 Lefevre, Laurent ..... 422  
 Leray, Philippe ..... 795  
 Levin, Timothy ..... 787  
 Lewis, Paul ..... 578  
 Lhee, Kyung-suk ..... 1028  
 Liang, Zhiyao ..... 1067  
 Lihan, Marc ..... 842

Lin, Chih-Yin	458	Miremedi, Seyed Ghassem	491, 648	Piattini, Mario	104, 136, 813, 1248, 1413	Schlager, Christian	344, 752
Linskog, Stefan	526, 624	Miremedi, Seyyed Ghassem	33	Pjetzowski, Andreas	404	Schmidt, Holger	195
Ling-jun, Li	558	Mitchell, Chris	1013	Pimenidis, Lexi	221	Schwarz, Thomas	56
Liu, Bin	1382	Miyamoto, Daisuke	1319	Pironti, Alfredo	72	Scott, Stephen L.	260
Liu, Fenlin	1382	Mohades, Ali	1266	Pozza, Davide	851	Scott, Stephen	659
Liu, Qian	3	Mohay, George	47	Preneel, Bart	1091	Sebastianis, Maurizio	1240
Liu-sheng, Huang	558	Mokhtari, Aicha	1008	Pretschner, Alexander	1135	Seifzadeh, Habib	859
Lizarraga, Jesus	520	Moretti, Rocco	1240	Probst, Christian W.	1104	Seredynski, Marcin	1036
López, Javier	136	Morimoto, Shoichi	1219	Pujol, Grimena	80	Serna, Ainhoa	520
Lou, Jing-Kai	212	Morris, Thomas	452	Pujol, Gloria	1060	Seviora, Rudolph	383
Lu, Shuo	3	Mühlhäuser, Max	958	Quirchmayr, Gerald	179	Shahmehri, Nahid	276, 284
Luo, Weidong	746	Muñoz-Escóí, Francesc D.	369, 390, 514	Rakowski, Zbigniew	161	Sharma, Priyanka	592
Luo, Yonglong	727	Muñoz-Escóí, Francesc Daniel	120	Ravindran, Binoy	564	Sheng, Quan Z.	834
Luque, Emilio	653	Muto, Kenichiro	1294	Ravindran, Kaliappa	1234	Shugeno, Hiroshi	1340
Luttenberger, Norbert	509	Mylopoulos, John	1437	Ren, Shangping	1180	Shinde, Pravin	592
Maamar, Zakaria	834	Nagami, Yoshitaka	1319	Renner, Johannes	221	Shinzaki, Yasutaka	1340
Madlmayr, Gerald	642	Nair, Suku	1044	Rennhard, Marc	610	Shirazi, Hossein	866
Makanju, Adetokunbo	310	Nair, V.S.S.	452	Rexachs, Dolores	653	Shirazi, Mohammad Shokrolah	648
Maleki, Farhad	1266	Nait-Abdesselam, Farid	352	Rey, Angel Martin del	741	Shiri, Mohammed Ebrahim	1266
Maña, Antonio	80	Nalinuka, Katsiaryna	1112	Rico-Novella, Francisco	701	Shokrolah-Shirazi, Mohammad	491
Mangin, Christophe	204	Nappa, Dario	1044	Rico-Novella, Francisco J.	1000	Siahaan, Ida	128
Markides, Bradley	440	Narjess, Ayari	422	Riedl, Bernhard	39	Silvestri, Claudio	153
Martin, Cristian	801	Naughton, Thomas	659	Rikula, Pauli	828	Simoens, Koen	1091
Martinelli, Fabio	1120, 1128	Neubauer, Thomas	39, 187	Röning, Juha	828	Sisto, Riccardo	72, 851
Martinez, Asier	520	Nielson, Fleming	1104	Rosado, David G.	136	Siveroni, Igor	96
Martinez-Ballesté, Antoni	1060	Nielson, Hanne Riis	1104	Rossebo, Judith E.Y.	597	Slamanig, Daniel	1226
Martinez-Peláez, Rafael	1000	Nohara, Yasunobu	717	Røstad, Lillian	935	Slay, Jill	1355, 1361
Martinez-Peláez, Rafael	701	O'Brien, Richard	1306	Royer, Denis	779	Solanas, Agusti	1060
Mashimo, Yo	1340	Ofek, Yoram	434	Rubel, Paul	1306	Soler, Emilio	104
Massacci, Fabio	1112	Ohtaki, Yasuhiro	1083	Rudie, Karen	1188	Spanhower, Lisa	675
Mateo-Sanz, Josep Maria	1060	Okamoto, Eiji	497	Ruohomaa, Simi	873	Spanoudakis, George	96
Matsumoto, Yoshihide	1313	Okubo, Takao	1148	Sabbir, Ali	1234	Springer, Thomas	903
Matteucci, Ilaria	1120	Oleshchuk, Vladimir	943	Sadeghian, Babak	982	Srinathan, Kannan	446
Matthews, Brian	1429	Olivier, Martin	1388	Sadighi, Mohsen	859	Srivastava, Vaibhav	446
Matulevičius, Raimundas	1397	Onana, Flavien Serge Mani	161	Sáez, Carlos	578	Stakhanov, Oleg	88
Mayer, Nicolas	1397	Onno, Stéphane	683	Sakurai, Kouichi	112	Stakhanova, Natalia	88
Mazón, Jose-Norberto	104	Orwat, Mark	787	Salem, Benferhat	618	Stefanov, Veronika	104
Mazzeo, Antonino	1097	Osaka, Kyosuke	733	Salem, Boussad Ait	1052	Stewart, Alan	428
Mehdizadeh, Nima	648	Otto, Martin	335	Sánchez, Gerardo Rodriguez	741	Stingl, Christian	1226
Meland, Per Håkon	1164	Ouadjaout, Abdelraouf	503	Sánchez-Gálvez, Luz A.	807	Strauch, Gereon	758
Melchor, Carlos Aguilar	1052	Pal, Partha	1306	Sangchi, Hasan Mokhtari	866	Stumpf, Frederic	376
Mellado, Daniel	1413	Panchenko, Andriy	221	Santini, Francesco	1128	Su, Chunhua	112
Memon, Nasrullah	1254	Páris, Jehan-François	56	Santos, Guna	653	Sun, Yifeng	1382
Mendivil, José Ramón González de	120	Park, Jong Sou	1260	Saran, Huzur	667	Takagi, Tsuyoshi	112, 733
Meyer-Wegener, Klaus	911	Peet, Andrew	578	Satizábal, Cristina	701, 1000	Takahashi, Osamu	733
Mích, Luísa	1437	Peine, Holger	1204	Satzger, Benjamin	404	Tamine, Karim	1052
Miedes, Emili	514	Pernul, Günther	344, 752	Scandariato, Riccardo	18, 434, 1156, 1421	Tan, Chik How	1275
Milios, Evangelos	310	Perrott, Ron	428	Schaad, Andreas	709	Tanaka, Hidehiko	1148
Miller, Barton	1196	Petković, Milan	889	Scharinger, Josef	642	Tartary, Christophe	1332

# Notes

Tejada, José María de Fuentes		
García-Romero de	363	911
Terada, Masato	1282	1301
Thalheim, Bernhard	1405	1188
Thipsc, Aashay	765	26
Thuraisingham, Bhavani	237	572
Tielemann, Michael	911	1421
Tikotekar, Anand	659	237
Tingdi, Zhao	461	1091
Tjoa, Simon	179	1234
Tlili, Syrène	302	18
Töndel, Inger Anne	1172	675
Torra, Vicenç	990, 994	578
Torre, Marco Dalla	128	723
Toval, Ambrosio	813	461
Trujillo, Juan	104, 1248	733
Trumler, Wolfgang	404	1382
Tsuchiya, Takeshi	842	1429
Tupper, Melanie	950	484
Turnbull, Benjamin	1355, 1361	532, 538
Ueda, Shintaro	1340	717
Ungerer, Theo	404	921
Uribeceberria, Roberto	520	1332
Valencia-García, Rafael	813	497
Vallée, Geoffroy	659	473
Vélez, Iñaki	520	842
Venter, Hein	1388	1287
Verma, Rakesh	1067	245
Vicente, Javier	578	1421
Vittorini, Valeria	1097	237
Völp, Marcus	268	1346
Vorobiev, Alexandre	383	1240
Wahl, Martin	911	746
Walter, Thomas	1135	1437
Wang, Dongsheng	630	564
Wang, Hongji	532, 538	630
Wang, Hongyi	630	352
Wang, Huaxiong	1332	558
Wang, Lingyu	3	558
Wang, Qi	727	112
Wang, Xinlei	1044	Zincir-Heywood, A. Nur 950, 1075
Watanabe, Dai	1294	Zincir-Heywood, Nur 310
Wattanapongsakorn, Naruemon	604	Zisman, Andrea 96
Weber, Stefan G.	958	Zuccato, Albin 1139
Wei, Yang	558	Zulkernine, Mohammad 245, 319, 1188
		Zurutuza, Urko 520

**CPOC Chair**

Chita R. Das  
*Professor, Penn State University*

**Board Members**

Mike Hinchey, *Director, Software Engineering Lab, NASA Goddard*  
Paolo Montuschi, *Professor, Politecnico di Torino*  
Jeffrey Voas, *Director, Systems Assurance Technologies, SAIC*  
Suzanne A. Wagner, *Manager, Conference Business Operations*  
Wenping Wang, *Associate Professor, University of Hong Kong*

**IEEE Computer Society Executive Staff**

Angela Burgess, *Executive Director*  
Alicia Stickley, *Senior Manager, Publishing Services*  
Thomas Baldwin, *Senior Manager, Meetings & Conferences*

**IEEE Computer Society Publications**

The world-renowned IEEE Computer Society publishes, promotes, and distributes a wide variety of authoritative computer science and engineering texts. These books are available from most retail outlets. Visit the CS Store at <http://www.computer.org/portal/site/store/index.jsp> for a list of products.

**IEEE Computer Society Conference Publishing Services (CPS)**

The IEEE Computer Society produces conference publications for more than 250 acclaimed international conferences each year in a variety of formats, including books, CD-ROMs, USB Drives, and on-line publications. For information about the IEEE Computer Society's *Conference Publishing Services (CPS)*, please e-mail: [cps@computer.org](mailto:cps@computer.org) or telephone +1-714-821-8380. Fax +1-714-761-1784. Additional information about *Conference Publishing Services (CPS)* can be accessed from our web site at: <http://www.computer.org/cps>

**IEEE Computer Society / Wiley Partnership**

The IEEE Computer Society and Wiley partnership allows the CS Press *Authored Book* program to produce a number of exciting new titles in areas of computer science and engineering with a special focus on software engineering. IEEE Computer Society members continue to receive a 15% discount on these titles when purchased through Wiley or at: <http://wiley.com/ieeecs>. To submit questions about the program or send proposals, please e-mail [jwilson@computer.org](mailto:jwilson@computer.org) or telephone +1-714-816-2112. Additional information regarding the Computer Society's authored book program can also be accessed from our web site at: <http://www.computer.org/portal/pages/ieeecs/publications/books/about.html>

*Revised: 21 January 2008*

**CPS Online** is our innovative online collaborative conference publishing system designed to speed the delivery of price quotations and provide conferences with real-time access to all of a project's publication materials during production, including the final papers. The **CPS Online** workspace gives a conference the opportunity to upload files through any Web browser, check status and scheduling on their project, make changes to the Table of Contents and Front Matter, approve editorial changes and proofs, and communicate with their CPS editor through discussion forums, chat tools, commenting tools and e-mail.

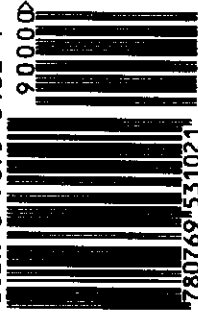
The following is the URL link to the **CPS Online** Publishing Inquiry Form:  
[http://www.ieeeconpublishing.org/cpir/inquiry/cps\\_inquiry.html](http://www.ieeeconpublishing.org/cpir/inquiry/cps_inquiry.html)



Published by the IEEE Computer Society  
10662 Los Vaqueros Circle  
P.O. Box 3014  
Los Alamitos, CA 90720-1314

IEEE Computer Society Order Number P3102  
Library of Congress Number 2007909935  
ISBN 0-7695-3102-4

ISBN 0-7695-3102-4



9 780769 531021