



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

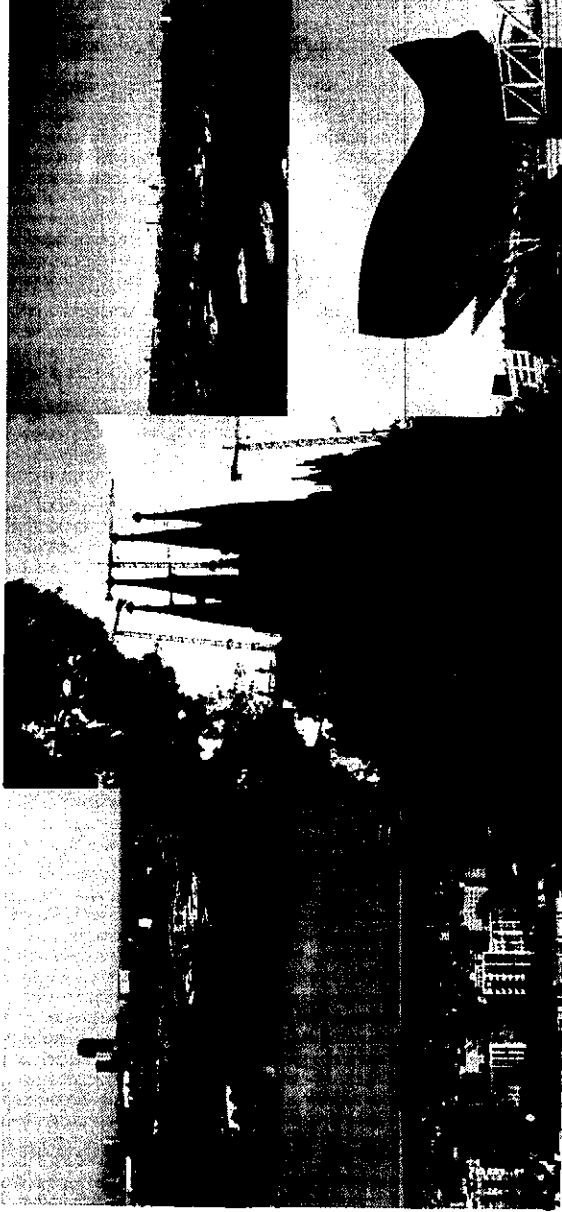
ARES 2008

The Third International Conference on Availability, Security and Reliability

PROCEEDINGS

March 4-7, 2008

Barcelona, Spain



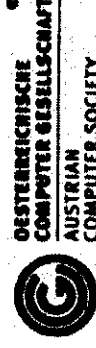
Edited by Stefan Jakoubi, Simon Tjoa, and Edgar R. Weippl

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

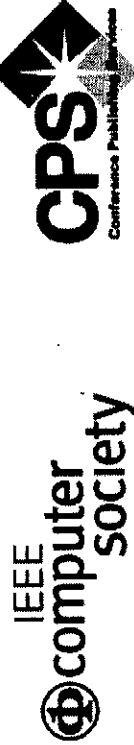
Additional copies may be ordered from:

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

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

Individual paper REPRINTS may be ordered at: <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 Fernández-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 Völp
- 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
Session 4: Networks	
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
Session 5: Crypto	
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
Session 6: Crypto and Health	
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
Session 7: Models and Networks	
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 Rohv Bræk</i>	597
Providing Fault Tolerance in Wireless Backhaul Network Design with Path Restoration <i>Pakorn Leesuthipornchai, Naruemon Wattanapongsakorn, and Chalermpol Charmsripinyo</i>	604
Session 8: IDS	
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

Session 9: Hardware	
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
Workshop FARES	
Session 1: Miscellaneous	
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
Session 2: Access Control and Algorithms	
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
Session 3: Crypto	
New Self Certified Proxy Digital Signature Scheme based on Elliptic Curve Cryptosystem <i>Youan 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
Session 4: Risk Management	
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 Böttcher, 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 Ω 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 Anzués-García 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-Boulahia, 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
Yousof 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, Bousaad 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>	
Workshop SECSE	
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
Workshop DAWAM	
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
Workshop WAIS	
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 ^m) in Polynomial Basis Representation <i>Abdulah Abdulah Zadeh</i>	1346
Workshop WSDF	
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

Implementing Multidimensional Security into OLAP Tools

Carlos Blanco¹, Eduardo Fernández-Medina¹, Juan Trujillo² and Mario Piattini¹
¹Dep. of Information Technologies and Systems. Escuela Superior de Informática
 University of Castilla-La Mancha. Ciudad Real, Spain
 {Carlos.Blanco, Eduardo.Fdzmedina, Mario.Piattini}@uclm.es

²Department of Information Languages and Systems. Facultad de Informática
 University of Alicante. Alicante, Spain
 jtrujillo@dlsi.ua.es

Abstract

Data Warehouses (DW) manage historical information for the decision making process and for enterprises, it is vitally important to consider security requirements from the earliest stages of the development process. OLAP tools are the most used tools for implementing and consulting DWs and it is necessary to define security measures to avoid that users can access unauthorized information by executing queries. We have created a MDA architecture for developing secure DW and in this paper, we will propose how to implement the security measures defined at upper abstraction levels using our approach into SQL Server Analysis Services 2008.

1. Introduction

Information security is a serious requirement that must be carefully taken into account, not as an isolated aspect, but as an element present in all stages of the development lifecycle, from requirement analysis to implementation and maintenance [1-3]. 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 [4]. Some authors indicate that the survival of organizations depends on the correct management of information security and confidentiality [5].

On the other hand, multidimensional modeling is the foundation of Data Warehouses (DW), MD Databases and On-Line Analytical Processing Applications (OLAP). Data Warehouses (DW) use enterprise information for the decision making process and a user can find out very important information by using

queries in OLAP tools. In this way, it is necessary that security measures defined in all early stages of the development process are applied in OLAP.

In addition, Model Driven Engineering (MDE) and the OMG Model Driven Architecture (MDA) [6] are model-oriented approaches for software development that are based on the separation between the specification of the system functionality and its implementation using specific platforms.

MDA defines a platform-independent model (PIM) that does not include information about specific platforms and technologies. This model (PIM) can be translated into one or more platform-specific models (PSM) with information about the used specific technology. Then, each PSM can be translated into a code that can be executed in the specific platform. There are several proposals for defining these translations between models [7], and OMG proposes to use Query/Views/Transformations (QVT) for defining transformations between models created by using Meta-Object Facility (MOF).

We have developed a proposal [8] for modeling secure Data Warehouses using a MDA approach that will be described in the following sections. This proposal does not deal with the implementation into OLAP tools. Therefore, in this paper we will analyze this problem and propose how security measures defined by using this approach can be finally implemented into OLAP tools. In future works, we will obtain this implementation in an automatic way following the MDA approach.

The rest of the paper is organized as follows: in Section 2 we will describe the background of this work; in Section 3 we will propose how to implement security requirements into OLAP tools. Finally, in Section 4 we will present our conclusions and future work.

2. Background

In this section, first of all, we will describe the Model Driven Architecture for developing secure Data Warehouses; then, the Access Control and Audit model and finally what OLAP tools offer for defining security measures.

2.1. Model Driven Architecture for developing secure Data Warehouses

We have developed a MDA architecture for developing secure Data Warehouses [8]. Security rules specified at the conceptual level in the multidimensional model are translated into logical level and code. Figure 1 illustrates our architecture: the upper section presents the SMD CIM (Secure Multidimensional CIM) which defines both functional and non functional requirements for DWs at the business level. Through T1 transformation, we will obtain the SMD PIM (Secure Multidimensional PIM) at the conceptual level and through T2 transformation, we will obtain the SMD PSM (Secure Multidimensional PSM) at the logical level. Finally, through T3 we will obtain specific SMD code.

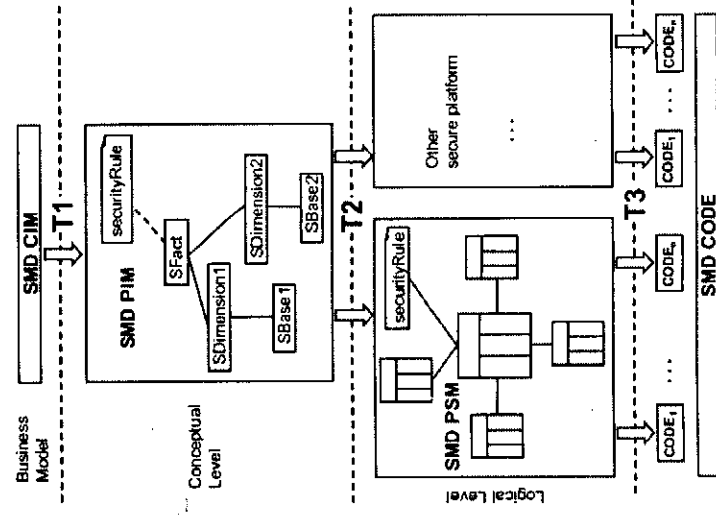


Figure 1. Model Driven Architecture for secure DW

The SMD PIM is defined by using an extension of the UML profile called Secure Data Warehouse (SECDW) [9] and it allows us to represent the main security requirements for DW conceptual modeling (an example is shown in Figure 2). This metamodel includes the main characteristics of Data Warehouses and security aspects defined according to our Access Control and Audit model. We can define security levels, user categories, user roles and security constraints for each element of the metamodel and we can define security rules (SIAR), authorization rules (AUR) and audit rules (AU) by using OCL expressions and UML notes associated with the corresponding class.

The specification of a platform-specific model is designed according to the specific properties of the Database Management Systems (DBMS). Our metamodel at the logical level for Secure Multidimensional PSM (SMD PSM) is a ROLAP approach called Secure Relational Data Warehouse (SECRDW) [10]. It extends the Relational Warehouse Metamodel (CWM) with security and audit capabilities.

In order to complete the MDA architecture, it is necessary to define the transformation between models. The transformation between conceptual and logical levels using SMD PIM (SECDW) and SMD PSM (SECRDW) has already been defined [11]. Furthermore, the transformation from SMD PSM to SMD code in a DBMS using Oracle Label Security has been defined too. Due to the fact that in Data Warehouses OLAP tools are more used than DBMS, our research effort is focused on developing secure code in OLAP tools according to the above-defined security requirements at conceptual and logical levels.

2.2. Access Control and Audit Model (ACA)

The ACA model [12] is an access control and audit model defined for DWs. Traditional access control models are based on relational concepts (tables, columns, rows, etc) and they are not appropriate for the multidimensional modeling used in data warehouses.

The ACA model is based on the conceptual model using our UML profile for DW [13] and allows us to specify security constraints in DW's multidimensional models. This model considers a combination of mandatory and role based access control which is based on the classification of subjects and objects in the system.

We can use levels, roles, compartments and security constraints to classify users. So, an *authorization subject* is an identity composed of: userID, user roles,

user compartments, security level or a levels interval and subjectExpression in OCL.

According to MD models, we can identify the main *authorization objects* as follows: facts, dimension, classification, hierarchy levels, measures, dimension attributes and instances. The authorization object component is composed of an identity (class name or attribute name) and an objectExpression in OCL.

Sensitive Information Assignment Rules (SIAR) specify multilevel security policies and allow us to define sensitivity information for each element in the MD model. The information we need for defining these rules is: objects, sensitivity information (security levels, user roles and user compartments), involved classes (some information can be confidential associated with other data) and a condition specified with OCL.

Authorization Rules (AUR) specify the subject which the rule applies to, the object which the authorization refers to, the action which the rule refers to (in this approach, we will only consider read operations) and the sign describing whether the rule permits or denies access. In Table 2, the syntax for authorization rules is shown.

Auditing rules (AR) help us ensure that authorized users do not misuse their privileges defining objects, log types (access to be recorded), log conditions and information to be logged.

2.3. Implementing security requirements into OLAP tools

Data Warehouses (DW) are usually implemented into OLAP tools. The main OLAP tools offer possibilities to define security measures but we can not define them at upper abstract levels in the multidimensional model. Our MDA architecture for developing secure DW includes security measures at CIM, PIM and PSM levels. In order to complete our architecture, we need to obtain secure code in OLAP tools that it is defined at business, conceptual and logic levels according to the security measures.

These OLAP tools work with operations that are usually the following ones: roll-up (increasing the level of aggregation) and drill-down (decreasing the level of aggregation) along one or more classification hierarchies, slice-dice (selection and projection) and pivoting (re-orienting the MD view of data which also allows us to exchange dimensions for facts; i.e., symmetric treatment of facts and dimensions).

For developing secure code, it is necessary to take into account how these OLAP operations work with information. Users can use these operations to obtain unauthorized information by using navigations or

aggregations with operations or by inferring information with chained queries.

Current OLAP tools do not allow us to represent in a direct way all security measures that we can define by using our ACA model. On the one hand, Oracle Label Security 11g provides us with the possibility of defining security constraints by using levels, compartments and roles. We can grant and revoke permissions but not over multidimensional elements at upper abstraction levels as cubes or dimensions.

On the other hand, SQL Server Analysis Services (SSAS) 2008 offers us the possibility of working with multidimensional models as well as that of defining security measures over multidimensional elements. SSAS uses a role-based access control policy (RBAC) that is supposed to translate our measures defined according to our ACA model into role approach.

3. Implementing security requirements into Microsoft Analysis Services 2008

In this section, our security model will be implemented into an OLAP tool. SQL Server Analysis Services 2008 (SSAS) has been selected as the OLAP tool to be used for our implementation because it allows defining security measures in multidimensional structures.

3.1. Description of SASS 2008 security

Analysis Services security uses a role-based policy and each role contains one or more specific user accounts or user groups that we can use to establish restriction access measures for metadata and multidimensional elements such as cubes, dimension or stored values.

It lets us define security measures to establish administrative authorizations for processing a database, cube, dimension or mining structure and to establish read authorizations on metadata for showing or hiding definitions. We can to grant or revoke users access to data sources, cubes, cell data, dimensions, dimension data, and mining structures and define access control at the cell level by establishing allowed and denied sets using MDX queries.

Another interesting characteristic are the "Visual Totals" property that filters the aggregate values to calculate those using only the visible elements for the role considering the defined security measures; contingence permissions for read accesses to control inferences on derived cells and auditing capabilities that include audit objects, auditing DDL commands and support for multiple logging targets.

3.2. Methodology

As previously stated, SSAS offers us the possibility of defining security measures over multidimensional elements but it considers a role-based control access policy and establishes for each role which elements we can see. Next, we will analyze how to represent the security constraints defined using our ACA model in SSAS. According to our ACA model, subjects can be classified into levels, compartments and roles, and security constraints can be defined. As SSAS's policy is role-based we have to translate this security information by creating new roles for each possible classification as shown in Table 4.

ACA Model	SSAS 2008
Security Roles	For each security role "r" we create a "SR" role.
Security Compartments	For each security compartment "c" we create a "SCc" role.
Security Levels	For each security level "l" we create a "SL" role that contains users with this security level.
Security Constraints	Security constraints are specified when possible by defining denied sets using MDX queries. If it is necessary we will create a specific role "SCTx" that contains the unauthorized users.

Table 1. Role definition

In addition, we have to consider Sensitivity Information Assignment Rules (SIAR) and Authorization Rules (AUR) that have been defined in our model. We use an open policy with specific denials and these rules define multidimensional elements that are hidden for certain roles.

For each sensitivity information assignment rule (SIAR) we have to detect the involved roles as well as configure them by hiding certain DW elements that are denied for the considered rule. Each rule represents explicit denials for each role with certain security constraints and as we consider an open world policy, we will implement these constraints into SSAS by establishing MDX queries which hide these involved elements for certain roles.

We follow the same procedure for each authorization rules (AUR), detecting involved roles along with the multidimensional elements that have to be hidden for these roles by defining MDX queries.

3.3. Example

In this subsection, we will describe a complete example from its definition at upper abstract levels using our model to its implementation into SSAS.

Figure 2 shows our example at the conceptual level, modelled with our SECDW approach including sensitivity information assignment rules (SIAR) and authorization rules (AUR). In this example, we will define an enumeration with security levels: unclassified, confidential, secret and top secret. User roles follow the simplified hierarchy shown in Figure 3 and compartments have not been defined as they depend on organization policies.

3.3.1. Defining security roles. Firstly, we have to define roles for each possible security classification of the subjects. In this way, we will create in SSAS a specific role for each role of the hierarchy shown in Figure 3 (SRDoctor, SRNurse, SRHealth, etc) as well as for each security level (SLUnclassified, SLConfidential, SLSecret and SLTopsecret).

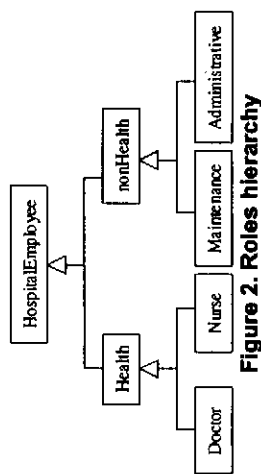


Figure 2. Roles hierarchy

3.3.2. Defining SIAR rules. Once the necessary roles have been defined, we have to translate the security rules.

The sensitivity information assignment rules (SIAR) defined as tagged values of classes or attributes are easy to translate because they do not present conditions and can be implemented by detecting involved roles and hiding affected DW elements.

SIAR titled "1" (Figure 2) specifies that "admission" class and involved classes have a top secret security level if the disease is "cancer" or "AIDS". Then, if the condition is satisfied we have the following explicit denial for each security level lower than top secret and for each involved class:

```
[-, SLSecret, CLAdmission)
```

In SSAS, for each role that represents a security level lower than top secret (SLSecret, SLConfidential and SLUnclassified) we will hide all involved classes using the following MDX expression as denied set for each one:

```
Admission.Diagnosis.[Diagnosis_Group].&[cancer] or Admission.Diagnosis.[Diagnosis_Group].&[AIDS]
```

SIAR titled "2" (Figure 2) defines that the "admission" class together with the "patient" involved

class have a top secret security level if the cost is higher than 10000. Then, if the condition is satisfied we will have the following denial for each involved role (with SL lower than secret) and class ("admission" and "patient"):

```
(-, SL_Secret, CL_Patient)
```

In SSAS, for each role that represents a security level lower than secret we will hide the involved classes using the following expression:

```
Admission.cost > 10000
```

3.3.3. Defining AUR rules. Now, we will translate the authorization rules (AUR).

AUR titled "4" (Figure 2) defines that queries involving "Diagnosis", "Diagnosis_Group" and "Patient" corresponding to a particular health area will be accessible to members of the user role Health only if their working area is the same as that health area. Note that this authorization rule is propagated up. It is necessary to define security constraints on SRHealth

role including the following MDX expression as denied set for each involved classes:

```
Diagnosis.healthArea<>currentUser.userProfile.WorkingArea
```

AUR titled "5" (Figure 2) defines that Patients will be special users of the system as we would like them to have access to their own data. Each patient will therefore have permission to access his/her own data (not to other patients' data) when querying classes Patient, Admission, and Diagnosis.

As this authorization rule is positive, it is propagated down. In this case it is better to define just one positive rule for all users using "SRHospitalEmployee" role. We will establish the following expression as allowed set in this role:

```
currentUser.UserProfile.name = Patient.name
```

3.3.4. Defining AR rules. SSAS allows us to audit activity on our data including information about when data has been read and modified. To establish these rules we can define audit specification in data warehouses with SQL Server 2008.

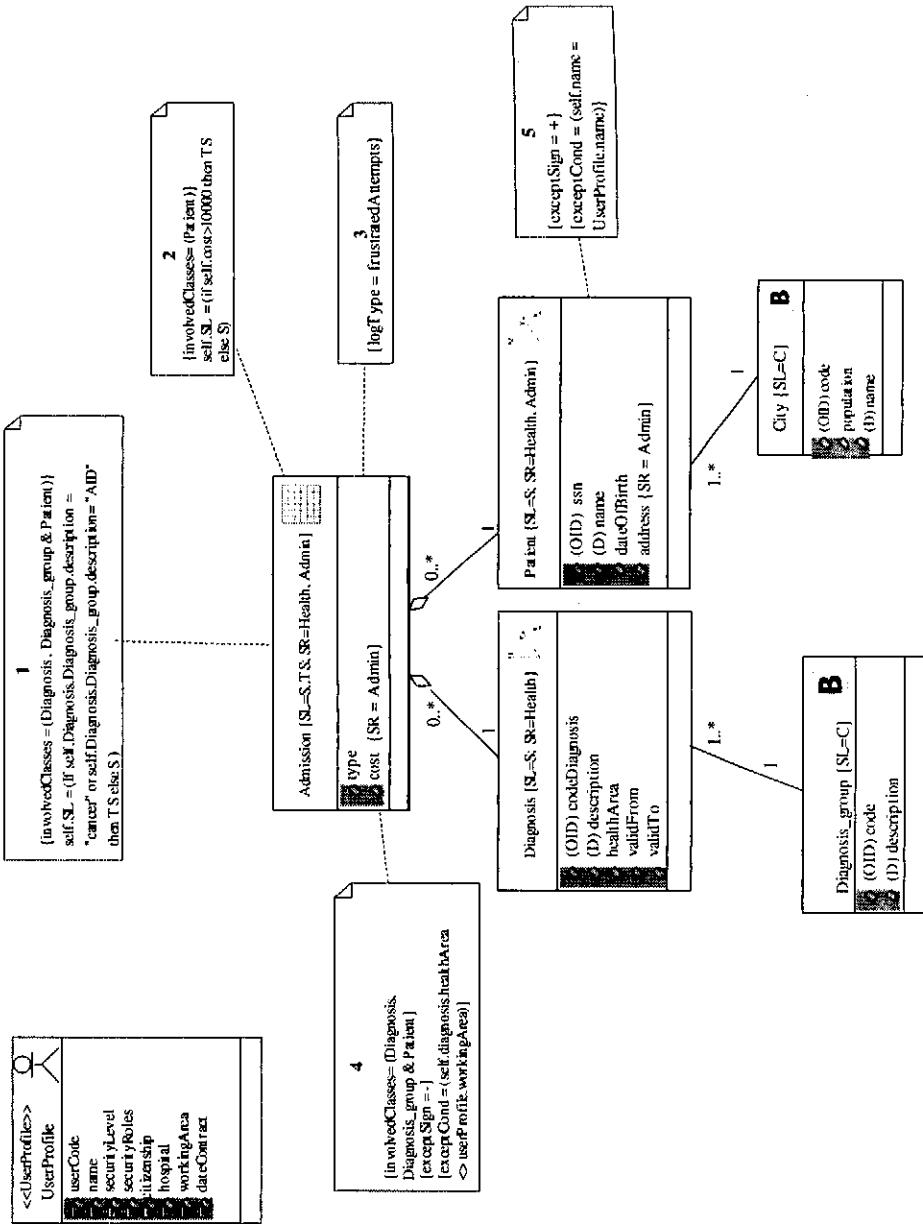


Figure 3. Example of SMD PIM (SECDW)

4. Conclusions

The first conclusion of our work is that OLAP tools do not support the complete security requirements definition over the multidimensional model at upper abstraction levels. These tools deal with partial security establishment, i.e. SSAS uses RBAC as access control policy, but they do not consider how OLAP operations affect to the defined security constraints. Users could access unauthorized information by using operations that navigate over the multidimensional structures.

These tools allow us to set security constraints over data or users but not over OLAP operations at upper abstraction levels. It is necessary that navigability constraints can be represented at the conceptual levels and finally respected in OLAP tools. Another problem is the hiding of the existence of determinate hide data. SSAS gives us null or N/A values but we know that this information exists and we have tips to obtain it.

In addition, the inference problem is not completely supported and requires a lot of computational effort to control. There are some strategies to control inferences; for instance, to limit the maximum number of sub queries or to include perturbations in the data. SSAS allows us to control inferences over derivative data but not other that involving queries. We can define contingency chains that represent dependencies between data to denied data access if you do not have permissions over all data of which it is derived from.

When we have translated the security requirements defined at the conceptual level into OLAP code, we have found that our security model is richer than the security capabilities that OLAP tools offer. To define security in SSAS we have to adapt our security information in a role-based approach and to represent rules we have to hide multidimensional elements for each involved role. This is an iterative and tedious process and it would be interesting that OLAP tools allow us to define security constraints over multidimensional elements. However, the biggest detected problem is the impossibility of representing security constraints on OLAP operations at upper abstraction levels. These constraints would allow us to avoid the access to unauthorized information by using navigations or inferences.

Our MDA architecture for developing secure DW allows us to define security requirements but should be extended with the possibility of establishing navigations and inferences constraints that can be translated into OLAP code. In the same way, tools should be extended to give us control over navigations and inferences that can find out unauthorized enterprise information.

Acknowledgment

This research is part of the Projects ESFINGE (TIN2006-15175-C05-05) financed by the Spanish Ministry of Education and Science, and the MISTICO (PBC-06-0082), DADS (PBC-05-012-2) and DIMENSIONS (PBC-05-012-2) financed by the FEDER and the Regional Science and Technology Ministry of Castilla-La Mancha (Spain).

References

- [1] Devanbu, P. and S. Stubblebine, *Software engineering for security: a roadmap*. ACM Press. Future of Software Engineering, 2000: p. 227-239.
- [2] Ferrai, E. and B. Thuraisingham. *Secure Databases Systems in Advanced Databases: Technology Design*. 2000. Artech Huse: London.
- [3] Mouratidis, H. and P. Giorgini, *An Introduction, in Integrating Security and Software Engineering: Advances and Future Visions*. 2006, Idea Group Publishing.
- [4] Denker, G., L. Kagal, and T. Finin, *Security in the Semantic Web using OWL*. Information Security Technical Report, 2005. 10(1): p. 51-58.
- [5] Dhillon, G. and J. Backhouse, *Information system security management in the new millennium*. Communications of the ACM, 2000. 43(7): p. 125-128.
- [6] MDA, O.M.G., *Model Driven Architecture Guide*. 2003.
- [7] Czamecki, K. and S. Helsen, *Classification of model transformation approaches*, in *2nd OOPSLA Workshop on Generative Techniques in the Context of the Model Driven Architecture*. 2003.
- [8] Fernández-Medina, E., J. Trujillo, and M. Piattini, *Model Driven Multidimensional Modeling of Secure Data Warehouses*. European Journal of Information Systems, 2007. 16: p. 374-389.
- [9] Fernandez-Medina, E., et al., *Developing secure data warehouses with a UML extension*. Information Systems, 2007. 32(6): p. 826-856.
- [10] Soler, E., et al. *Representing Security and Audit Rules for Data Warehouses at the Logical Level by using the Common Warehouse Metamodel*. in *1st Int. Conference on Availability, Reliability and Security*. 2006. Vienna, Austria.
- [11] Soler, E., et al. *A Set of QVT relations to Transform PIM to PSM in the Design of Secure Data Warehouses*. in *IEEE International Symposium on Frontiers on Availability, Reliability and Security (FARES 2007)*. 2007. Vienna, Austria.
- [12] Fernandez-Medina, E., et al., *Access control and audit model for the multidimensional modeling of data warehouses*. Decision Support Systems, 2006. 42(3): p. 1270-1289.
- [13] Lujan-Mora, S., J. Trujillo, and I.-Y. Song, *A UML profile for multidimensional modeling in data warehouses*. Data & Knowledge Engineering, 2006. 59(3): p. 725-769.

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
Ahmed, Irfan	1028	Botham, Paul	253
Aickelin, Uwe.....	896	Bötcher, Stefan	771
Ahneur, Esma	161	Bouillaut, Laurent.....	795
Aknuin, Patrice.....	795	Boustia, Nathimene	1008
Al-Fedaghi, Sabah	1405	Bouvy, Pascal	1036
Al-Hammadi, Yousof	896	Bouzida, Yacine.....	204
Almohammad, Adel	544	Braek, Rolv.....	597
Al-Sagabi, Khaled	1405	Brassard, Gilles.....	161
Amato, Flora.....	1097	Breu, Ruth.....	921
Angevine, Duffy.....	1075	Broadway, Joshua	1361
Ansper, Arne	572	Brunstrom, Anna	526
Anzures-Garcia, Mario.....	807	Buddendick, Christian	758
Ardi, Shama.....	284	Buder, Jens-Uwe.....	335
Arenas, Alvaro.....	1429	Byers, David.....	276
Arret, Magi Lluçh i.....	578	Canfora, Gerardo	1020
Armendáriz-Iñigo, Enrique.....	120	Casola, Valentina	1097
Arthur, Kweku.....	1388	Cartrina, Octavian	693
Asnar, Yudistira.....	1240	Cavadini, Salvador.....	586
Atigbetchi, Michael	1306	Cavalli, Ana Rosa	821
Ayuso, Pablo Neira.....	422	Cavallo, Bice	1020
Azer, Marianne.....	636, 881	Ceballos, Rafael.....	229
Aziz, Muhammad Anwarul	1260	Cetinkaya, Orhan.....	1451
Azimah, Noor	1219	Challal, Yacine.....	503
Aziz, Benjamin.....	1429	Chang, Shuang	733
Bagaa, Mlioud	503	Chaouchi, Hakima	144
Baldi, Mario.....	434	Charnstripiyo, Chalernpol.....	604
Balfé, Shane.....	376	Charoempornwattana, Kulathop	659
Bao, Feng.....	112	Cheda, Diego	586
Bararon, Denis.....	422	Chen, Chia-Mei	410
Barolli, Leonard.....	1325	Chen, Kuan-Ta	212
Benslimane, Djamel	834	Chen, Tszhan	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, Lukasz.....	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
Croitori, Madalina 578
Cuppens, Frédéric 821
Cuppens-Boulahia, Nora 821
Darnani, Maria Luisa 153
Dantels, Nils 1139
Das, Ananda Swarup 446
Dasmahapatra, Srinandan 578
Debbabi, Mourad 302
Debbashi, 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
Durrezi, Arjan 1325
Durrezi, 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-Molina, Eduardo 104,
136, 813, 1248
Fernandez-Molina, 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
Gabarro, Joaquin 428
Gaborit, Philippe 1052
Gansterer, Wilfried 10
Garg, Sanjan 667
Garnacho, Arturo Ribagorda 363
Gasca, Rafael Martínez 229
Gasca, Rafael 422
Ghinea, Gheorghita 544
Ghortani, Ali 88
Gibb, Alex 578
González-Vélez, Horacio 578
Goto, Yuichi 171, 1219
Grascher, 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
Hannishagi, Vahid Saber 866
Han, Kai 564
Hansen, René Rydhoj 1104
Haque, Anwar 245
Hargreaves, Christopher 1369
Harner, 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

Heinemann, Andreas 958
Heisel, Marita 195
Hellings, Greg 237
Heurix, Johannes 187
Hewett, Rattkorn 765
Heyman, Thomas 1156
Heymans, Patrick 1397
Hicks, David L. 1254
Hidalgo, Sergio Pozo 229
Hierons, Robert 544
Ho, Pin-Han 352
Hoepman, Jaap-Henk 327
Hölbl, Marko 1301
Hong, Yuan 3
Hong, Zhao 473
Hood, Cynthia 479
Horie, Daisuke 1219
Hu, Hua-ping 484
Huang, Liusheng 727
Hulsbosch, R. J. 397
Huygens, Christophe 1156
Hvasshovd, Svein-Olaf 64
Ideguchi, Kota 1294
Iglesias, J. L. Pérez 741
Ilyin, Sergey 967
Innrhofer-Oberperfler, Frank 921
Inoue, Sozo 717
Irún-Briz, Luis 390
Irvine, Cynthia 787
Jaatun, Martin Gilje 1172
Jakoubi, Stefan 179
Janecek, Andreas 10
Jensen, E. D. 564
Jensen, Jostein 292, 1164
Jensen, Meiko 509
Jiang, Qingshan 532, 538
Jin, Tian 461
Jonsson, Erlend 624
Joosen, Wouter 18, 1156, 1421
Juan-Martin, Rubén de 390
Juárez-Rodríguez, José Ramón 120
Kadobayashi, Youki 1313, 1319
Kalogridis, Georgios 1013
Kambourakis, Georgios 929
Kaneko, Toshinobu 1294
Kantner, Christian 642
Karin, Tabia 618
Katzenbeisser, Stefan 889
Kermani, Mostafa 859

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, Mathias 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, Keichi 842
Kuang, Liwei 319
Kumar, Ashwin 10
Kupsch, James 1196
Kutvonen, Lea 873
Kwiat, Kevin 1180, 1234
Ladra, Susana 994
Lai, Gu-Hsin 410
Laih, 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-Makravičius, Maryline 144
Leangsuksun, Chokchai 260, 659
Lee, Jooyoung 1377
Leesuthipornchai, Pakorn 604
Lefèvre, Laurent 422
Leray, Philippe 795
Levin, Timothy 787
Lewis, Paul 578
Lhee, Kyung-suk 1028
Liang, Zhuyao 1067
Lihan, Marc 842

Lin, Chih-Yin	458	Miremadi, Seyed Ghassem	491, 648
Lindskog, Stefan	526, 624	Miremadi, Seyyed Ghassem	33
Ling-jun, Li	558	Mitchell, Chris	1013
Liu, Bin	1382	Miyamoto, Daisuke	1319
Liu, Fenlin	1382	Mohades, Ali	1266
Liu, Qian	3	Mohay, George	47
Liu-sheng, Huang	558	Mokhari, Aicha	1008
Lizarraga, Jesus	520	Moretti, Rocco	1240
López, Javier	136	Morimoto, Shoichi	1219
Lou, Jing-Kai	212	Morris, Thomas	452
Lu, Shuo	3	Mühlhäuser, Max	958
Luo, Weidong	746	Muñoz-Escobí, Francesc D.	369, 390, 514
Luo, Yonglong	727	Muñoz-Escobí, Francesc Daniel	120
Luque, Emilio	653	Muto, Kenichiro	1294
Luttenberger, Norbert	509	Mylopoulos, John	1437
Maamar, Zakaria	834	Nagami, Yoshiyaka	1319
Madhavar, Gerald	642	Nair, Suku	1044
Makanju, Adetokunbo	310	Nair, V.S.S.	452
Maleki, Parhad	1266	Nar-Abdesselam, Farid	352
Maña, Antonio	80	Naluka, Katsiaryna	1112
Mangin, Christophe	204	Nappa, Dario	1044
Markides, Bradley	440	Narjess, Ayari	422
Martin, Cristian	801	Naughton, Thomas	659
Martinelli, Fabio	1120, 1128	Neubauer, Thomas	39, 187
Martinez, Asier	520	Nielson, Flemming	1104
Martinez-Ballesté, Antoni	1060	Nielson, Hanne Rits	1104
Martinez-Peláez, Rafael	1000	Nohara, Yasunobu	717
Martinez-Peláez, Rafael	701	O'Brien, Richard	1306
Mashimo, Yo	1340	Ofek, Yoram	434
Massacci, Fabio	1112	Ohtaki, Yasuhito	1083
Mateo-Sanz, Josep Maria	1060	Okamoto, Eiji	497
Matsumoto, Yoshhide	1313	Okubo, Takao	1148
Matteucci, Ilaria	1120	Oleshchuk, Vladimir	943
Mathews, Brian	1429	Olivier, Martin	1388
Mathievičius, Raimundas	1397	Onana, Flavien Serge Mani	161
Mayer, Nicolas	1397	Onno, Stéphane	683
Mazón, Jose-Norberto	104	Orwat, Mark	787
Mazzeo, Antonino	1097	Osaka, Kyosuke	733
Mehdizadeh, Nima	648	Otto, Martin	335
Meland, Per Håkon	1164	Quadjout, Abdelraouf	503
Melchor, Carlos Aguilar	1052	Pal, Partha	1306
Mellado, Daniel	1413	Panchenko, Andriy	221
Memon, Nasrullah	1254	Páris, Jehan-François	56
Mendivil, José Ramón González de	120	Park, Jong Sou	1260
Meyer-Wegener, Klaus	911	Peet, Andrew	578
Mich, Luisa	1437	Peine, Holger	1204
Miedes, Emili	514	Pernul, Günther	344, 752
Milos, Evangelos	310	Perron, Ron	428
Miller, Barton	1196	Petković, Milan	889

Piattini, Mario	104, 136, 813, 1248, 1413	Schläger, Christian	344, 752
Pietrowski, Andreas	404	Schmidt, Holger	195
Pimenidis, Lexi	221	Schwarz, Thomas	56
Pironi, Alfredo	72	Scott, Stephen L.	260
Pozza, Davide	851	Scott, Stephen	659
Prenel, Bart	1091	Sebastianis, Maurizio	1240
Pretschner, Alexander	1135	Seifzadeh, Habib	859
Probst, Christian W.	1104	Seredynski, Marcin	1036
Pujol, Gimena	80	Serna, Ainhoa	520
Pujol, Gloria	1060	Sevióra, Rudolph	383
Quirchmayr, Gerald	179	Shahmehri, Nahid	276, 284
Rakowski, Zbigniew	161	Sharma, Priyanka	592
Ravindran, Binoy	564	Sheng, Quan Z.	834
Ravindran, Kalappa	1234	Shigeno, Hiroshi	1340
Ren, Shangping	1180	Shinde, Pravin	592
Renner, Johannes	221	Shinzaki, Yasutaka	1340
Renhard, Marc	610	Shirazi, Hossein	866
Rexachs, Dolores	653	Shirazi, Mohammad Shokrolah	648
Rey, Angel Martin del	741	Shiri, Mohammed Ebrahim	1266
Rico-Novella, Francisco	701	Shokrolah-Shirazi, Mohammad	491
Rico-Novella, Francisco J.	1000	Siahbaan, Ida	128
Riedl, Bernhard	39	Silvestri, Claudio	153
Rikula, Pauli	828	Simons, Koen	1091
Röning, Juha	828	Sisto, Riccardo	72, 851
Rosado, David G.	136	Siveroni, Igor	96
Rossebo, Judith E.Y.	597	Sلمانج, Daniel	1226
Røstad, Lillian	935	Slay, Jill	1355, 1361
Royer, Denis	779	Solanas, Agustí	1060
Rubel, Paul	1306	Soler, Emilio	104
Rudie, Karen	1188	Spainhower, Lisa	675
Ruohomaa, Sini	873	Spanoudakis, George	96
Sabbir, Ali	1234	Springer, Thomas	903
Sadeghian, Babak	982	Srinathan, Kannan	446
Sadighi, Mohsen	859	Srivastava, Vaibhav	446
Sáez, Carlos	578	Stakhanov, Oleg	88
Sakurai, Kouichi	112	Stakhanova, Natalia	88
Salem, Benferhat	618	Stefanov, Veronika	104
Salem, Boussad Ait	1052	Stewart, Alan	428
Sanchez, Gerardo Rodriguez	741	Stingl, Christian	1226
Sanchez-Gálvez, Luz A.	807	Strauch, Gereon	758
Sangchi, Hasan Mokhtari	866	Stumpf, Frederic	376
Santini, Francesco	1128	Su, Chunhua	112
Santos, Guna	653	Sun, Yifeng	1382
Saran, Huzur	667	Takagi, Tsuyoshi	112, 733
Satizábal, Cristina	701, 1000	Takahashi, Osamu	733
Satzger, Benjamin	404	Tamine, Karim	1052
Scandariato, Riccardo	18, 434, 1156, 1421	Tan, Chik How	1275
Schaad, Andreas	709	Tanka, Hidehiko	1148
Scharinger, Josef	642	Tartary, Christophe	1332

Tejada, José María de Fuentes	363	Weiss, Steffen	911
García-Romero de	1282	Welzer, Tajana	1301
Terada, Masato	1405	Whittaker, Sarah	1188
Thalheim, Bernhard	765	Willassen, Svein Yngvar	26
Thipse, Aashay	237	Willemsen, Jan	572
Thuraisingham, Bhavani	911	Win, Bart De	1421
Tielemann, Michael	659	Woolam, Clay	237
Tikotekar, Anand	461	Wouters, Karel	1091
Tingdi, Zhao	179	Wu, Jiang	1234
Tjoa, Simon	302	Wuyts, Kim	18
Tlili, Syrine	1172	Xenidis, Jimi	675
Tøndel, Inger Anne	990, 994	Xiao, Liang	578
Torra, Vicenç	128	Xiao, Youan	723
Torre, Marco Dalla	813	Xiao, Li	461
Toral, Ambrosio	104, 1248	Xiaolei, Li	733
Trujillo, Juan	404	Yamazaki, Kenichi	1382
Trunler, Wolfgang	842	Yan, Chunfang	1429
Tsuchiya, Takeshi	950	Yang, Erica Y.	484
Tupper, Melanie	1355, 1361	Yang, Xiang-he	532, 538
Turnbull, Benjamin	404	Yao, Gang	717
Ueda, Shintaro	520	Yasunura, Hiroto	921
Ungerer, Theo	813	Yausiukhin, Artsiom	1332
Uribecheberria, Roberto	659	Ye, Qingsong	497
Valencia-García, Rafael	520	Yi, Xun	473
Vallée, Geoffroy	520	Ying-You, Wen	842
Vélez, Iñaki	1388	Yoshinaga, Hirokazu	1287
Venter, Hein	1067	Yoshinaga, Hiroshi	245
Verna, Rakesh	578	You, Yonghua	1421
Vicente, Javier	1097	Yskout, Koen	237
Vitorini, Valeria	268	Yurcik, William	1346
Völp, Marcus	383	Zadeh, Abdulah Abdulah	1240
Vorobiev, Alexandre	911	Zannone, Nicola	746
Wahl, Martin	1135	Zeng, Shengke	1437
Walter, Thomas	630	Zeni, Nicola	564
Wang, Dongsheng	532, 538	Zhang, Bo	630
Wang, Hongli	630	Zhang, Youhui	352
Wang, Hongyi	1332	Zhang, Zonghua	558
Wang, Huaxiong	727	Zhen-shan, Yu	112
Wang, Lingyu	1044	Zhi-li, Chen	950, 1075
Wang, Qi	1294	Zhou, Jianying	310
Wang, Xinlei	604	Zincir-Heywood, A. Nur	1139
Watanapongsakorn, Naruemon	958	Zisman, Andrea	245, 319, 1188
Weber, Stefan G.	558	Zuccato, Albin	520
Wei, Yang		Zulkernine, Mohammad	
		Zurubzu, Urko	



**IEEE Computer Society
Conference Publications
Operations Committee**



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 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/ieecs>. To submit questions about the program or send proposals, please e-mail 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/ieecs/publications/books/about.html>

Revised: 21 January 2008



Conference Publishing Services

IEEE Online Collaborative Publishing Environment

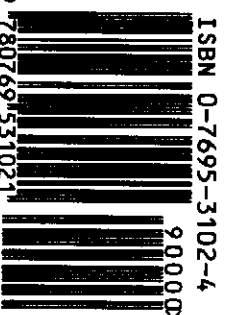
CPS Online is our innovative online collaborative conference publishing system designed to speed the delivery of price quotations and provide conferences with real-time access to all of a project's publication materials during production, including the final papers. The **CPS Online** workspace gives 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.ieeeconfpublishing.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 00000

9 780769 531021