Lecture Notes in Computer Science

The LNCS series reports state-of-the-art results in computer science research, development, and education, at a high level and in both printed and electronic form. Enjoying tight cooperation with the R&D community, with numerous individuals, as well as with prestigious organizations and societies, LNCS has grown into the most comprehensive computer science research forum available.

The scope of LNCS, including its subseries LNAI and LNBI, spans the whole range of computer science and information technology including interdisciplinary topics in a variety of application fields. The type of material published traditionally includes

- proceedings (published in time for the respective conference)
- post-proceedings (consisting of thoroughly revised final full papers)
- research monographs (which may be based on outstanding PhD work, research projects, technical reports, etc.)

More recently, several color-cover sublines have been added featuring, beyond a collection of papers, various added-value components; these sublines include

- tutorials (textbook-like monographs or collections of lectures given at advanced courses)
- state-of-the-art surveys (offering complete and mediated coverage of a topic)
- hot topics (introducing emergent topics to the broader community)

In parallel to the printed book, each new volume is published electronically in LNCS Online.

Detailed information on LNCS can be found at
www.springer.com/lncs

Proposals for publication should be sent to
LNCS Editorial, Tiergartenstr. 17, 69121 Heidelberg, Germany
E-mail: lncs@springer.com

ISSN 0302-9743

ISBN 978-3-540-88872-7

9 783540 888727

Lecture Notes in Computer Science

LNCS LNAI LNBI

springer.com

Meersman • Tari (Eds.)

LNCS 5332

Internet Systems: OTM 2008

LNCS 5332

e Move to Meaningful
net Systems: OTM 2008

OTM 2008 Confederated International Conferences
CoopIS, DOA, GADA, IS, and ODBASE 2008
Monterrey, Mexico, November 2008
Proceedings, Part II

Part II

CoopIS DOA

INFORMATION SECURITY

ODBASE

Springer

Lecture Notes in Computer Science 5332

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

Robert Meersman Zahir Tari (Eds.)

On the Move to Meaningful Internet Systems: OTM 2008

OTM 2008 Confederated International Conferences
CoopIS, DOA, GADA, IS, and ODBASE 2008
Monterrey, Mexico, November 9-14, 2008
Proceedings, Part II

Springer

Volume Editors

Robert Meersman
Vrije Universiteit Brussel (VUB), STARLab
Bldg G/10, Pleinlaan 2, 1050, Brussels, Belgium
E-mail: meersman@vub.ac.be

Zahir Tari
RMIT University, School of Computer Science and Information Technology
Bld 10.10, 376-392 Swanston Street, VIC 3001, Melbourne, Australia
E-mail: zahir.tari@rmit.edu.au

Library of Congress Control Number: 2008938070

CR Subject Classification (1998): H.2, H.3, H.4, C.2, H.5, D.2.12, I.2, K.4

LNCS Sublibrary: SL 3 – Information Systems and Application, incl. Internet/Web and HCI

ISSN 0302-9743
ISBN-10 3-540-88872-1 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-88872-7 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2008
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12558315 06/3180 5 4 3 2 1 0

Volume Editors

Robert Meersman
Zahir Tari

CoopIS

Johann Eder
Masaru Kitsuregawa
Ling Liu

DOA

Mark Little
Alberto Montresor
Greg Pavlik

ODBASE

Malu Castellanos
Fausto Giunchiglia
Feng Ling

GADA

Dennis Gannon
Pilar Herrero
Daniel S. Katz
María S. Pérez

IS

Jong Hyuk Park
Bart Preneel
Ravi Sandhu
André Zúquete

OTM 2008 General Co-chairs' Message

Dear OnTheMove Participant, or Reader of these Proceedings,

The OnTheMove 2008 event in Monterrey, Mexico, 9–14 November, further consolidated the growth of the conference series that was started in Irvine, California in 2002, and held in Catania, Sicily in 2003, in Cyprus in 2004 and 2005, in Montpellier in 2006, and in Vilamoura in 2007. The event continues to attract a diversifying and representative selection of today's worldwide research on the scientific concepts underlying new computing paradigms, which, of necessity, must be distributed, heterogeneous and autonomous yet meaningfully collaborative.

Indeed, as such large, complex and networked intelligent information systems become the focus and norm for computing, there continues to be an acute and increasing need to address and discuss in an integrated forum the implied software, system and enterprise issues as well as methodological, semantical, theoretical and applicational issues. As we all know, email, the Internet, and even video conferences are not sufficient for effective and efficient scientific exchange. The OnTheMove (OTM) Federated Conferences series has been created to cover the scientific exchange needs of the community/ies that work in the broad yet closely connected fundamental technological spectrum of data and web semantics, distributed objects, web services, databases, information systems, enterprise workflow and collaboration, ubiquity, interoperability, mobility, grid and high-performance computing.

OnTheMove aspires to be a primary scientific meeting place where all aspects for the development of such Internet- and Intranet-based systems in organizations and for e-business are discussed in a scientifically motivated way. This sixth edition of the OTM Federated Conferences event again provided an opportunity for researchers and practitioners to understand and publish these developments within their individual as well as within their broader contexts.

Originally the federative structure of OTM was formed by the co-location of three related, complementary and successful main conference series: DOA (Distributed Objects and Applications, since 1999), covering the relevant infrastructure-enabling technologies, ODBASE (Ontologies, DataBases and Applications of SEmantics, since 2002) covering Web semantics, XML databases and ontologies, and CoopIS (Cooperative Information Systems, since 1993) covering the application of these technologies in an enterprise context through e.g., workflow systems and knowledge management. In 2006 a fourth conference, GADA (Grid computing, high-performAnce and Distributed Applications) was added to this as a main symposium, and last year the same happened with IS (Information Security). Both of these started as successful workshops at OTM, the first covering the large-scale integration of heterogeneous computing systems and data resources with the aim of providing a global computing space, the second covering the issues of security in complex Internet-based information systems.

Each of these five conferences encourages researchers to treat their respective topics within a framework that incorporates jointly (a) theory, (b) conceptual design and development, and (c) applications, in particular case studies and industrial solutions.

Following and expanding the model created in 2003, we again solicited and selected quality workshop proposals to complement the more "archival" nature of the main conferences with research results in a number of selected and more "avant-garde" areas related to the general topic of distributed computing. For instance, the so-called Semantic Web has given rise to several novel research areas combining linguistics, information systems technology, and artificial intelligence, such as the modeling of (legal) regulatory systems and the ubiquitous nature of their usage. We were glad to see that in spite of OnTheMove switching sides of the Atlantic, seven of our earlier successful workshops (notably AweSOMe, SWWS, ORM, OnToContent, MONET, PerSys, RDDS) re-appeared in 2008 with a third or even fourth edition, sometimes by alliance with other newly emerging workshops, and that no fewer than seven brand-new independent workshops could be selected from proposals and hosted: ADI, COMBEK, DiSCo, IWSSA, QSI and SEMELS. Workshop audiences productively mingled with each other and with those of the main conferences, and there was considerable overlap in authors. The OTM organizers are especially grateful for the leadership, diplomacy and competence of Dr. Pilar Herrero in managing this complex and delicate process for the fifth consecutive year.

Unfortunately however in 2008 the number of quality submissions for the OnTheMove Academy (formerly called Doctoral Consortium Workshop), our "vision for the future" in research in the areas covered by OTM, proved too low to justify a 2008 edition in the eyes of the organizing faculty. We must however thank Antonia Albani, Sonja Zaplata and Johannes Maria Zaha, three young and active researchers, for their efforts in implementing our interactive formula to bring PhD students together: research proposals are submitted for evaluation; selected submissions and their approaches are (eventually) to be presented by the students in front of a wider audience at the conference, and intended to be independently and extensively analyzed and discussed in public by a panel of senior professors. Prof. Em. Jan Dietz, the Dean of the OnTheMove Academy, also is stepping down this year, but OnTheMove is committed to continuing this formula with a new Dean and peripatetic faculty.

All five main conferences and the associated workshops shared the distributed aspects of modern computing systems, and the resulting application-pull created by the Internet and the so-called Semantic Web. For DOA 2008, the primary emphasis stayed on the distributed object infrastructure; for ODBASE 2008, it has become the knowledge bases and methods required for enabling the use of formal semantics; for CoopIS 2008, the focus as usual was on the interaction of such technologies and methods with management issues, such as occur in networked organizations, for GADA 2008, the main topic was again the scalable integration of heterogeneous computing systems and data resources with the aim of providing a global computing space, and in IS 2008 the emphasis was on information security in the networked society. These subject areas overlapped in a scientifically natural fashion and many submissions in fact also treated an envisaged mutual impact among them. As for the earlier editions, the organizers wanted to stimulate this cross-pollination by a *shared* program of famous keynote speakers: this year we were proud to announce Dan Atkins of the U.S. National Science Foundation and the University of Michigan, Hector Garcia-Molina of Stanford, Rick Hull of IBM T.J. Watson Lab, Ted Goranson of Sirius-Beta and of Paradigm Shift, and last but not least Cristina Martinez-Gonzalez of the European Commission with a special interest in more future scientific collaboration between the EU and Latin America, as well as emphasizing the concrete outreach potential of new Internet technologies for enterprises anywhere.

This year the registration fee structure strongly encouraged multiple event attendance by providing *all* main conference authors with free access or discounts to *all* other conferences or workshops (workshop authors paid a small extra fee to attend the main conferences). In both cases the price for these combo tickets was made lower than in 2007 in spite of the higher organization costs and risks!

We received a total of 292 submissions for the five main conferences and 171 submissions in total for the 14 workshops. The numbers are about 30% lower than for 2007, which was not unexpected because of the transatlantic move of course, and the emergent need to establish the OnTheMove brand in the Americas, a process that will continue as we proceed in the coming years. But, not only may we indeed again claim success in attracting an increasingly representative volume of scientific papers, many from US, Central and South America already, but these numbers of course allow the program committees to compose a high-quality cross-section of current research in the areas covered by OTM. In fact, in spite of the larger number of submissions, the Program Chairs of each of the three main conferences decided to accept only approximately the same number of papers for presentation and publication as in 2006 and 2007 (i.e., average 1 paper out of 3-4 submitted, not counting posters). For the workshops, the acceptance rate varies but the aim was to stay as strict as before, consistently about 1 accepted paper for 2-3 submitted. We have separated the proceedings into three books with their own titles, two for the main conferences and one for the workshops, and we are grateful to Springer for their suggestions and collaboration in producing these books and CDROMs. The reviewing process by the respective program committees was again performed very professionally, and each paper in the main conferences was reviewed by at least three referees, with arbitrated email discussions in the case of strongly diverging evaluations. It may be worthwhile emphasizing that it is an explicit OnTheMove policy that all conference program committees and chairs make their selections completely autonomously from the OTM organization itself. The OnTheMove Federated Event organizers again made all proceedings available on a CDROM to all participants of conferences resp. workshops, independently of their registration to a specific conference resp. workshop. Paper proceedings were on request this year, and incurred an extra charge.

The General Chairs were once more especially grateful to the many people directly or indirectly involved in the setup of these federated conferences. Few people realize what a large number of people have to be involved, and what a huge amount of work, and in 2008 certainly also financial risk, the organization of an event like OTM entails. Apart from the persons in their roles mentioned above, we therefore in particular wish to thank our 17 main conference PC co-chairs:

GADA 2008	Dennis Gannon, Pilar Herrero, Daniel Katz, María S. Pérez
DOA 2008	Mark Little, Alberto Montresor, Greg Pavlik
ODBASE 2008	Malu Castellanos, Fausto Giunchiglia, Feng Ling
CoopIS 2008	Johann Eder, Masaru Kitsuregawa, Ling Liu
IS 2008	Jong Hyuk Park, Bart Preneel, Ravi Sandhu, André Zúquete
50 Workshop PC Co-chairs	Stefan Jablonski, Olivier Curé, Christoph Bussler, Jörg Denzinger, Pilar Herrero, Gonzalo Méndez, Rainer Unland, Pieter De Leenheer, Martin Hepp, Amit Sheth, Stefan Decker, Ling Liu, James Caverlee, Ying Ding, Yihong Ding, Arturo Molina, Andrew Kusiak, Hervé Panetto, Peter Bernus, Lawrence Chung, José Luis Garrido, Nary Subramanian, Manuel Noguera, Fernando Ferri, Irina Kondratova, Arianna D'ulizia, Patrizia Grifoni, Andreas Schmidt, Mustafa Jarrar, Terry Halpin, Sjir Nijssen, Skevos Evripidou, Roy Campbell, Anja Schanzenberger, Ramon F. Brena, Hector Ceballos, Yolanda Castillo, Achour Mostefaoui, Eiko Yoneki, Elena Simperl, Reto Krummenacher, Lyndon Nixon, Emanuele Della Valle, Ronaldo Menezes, Tharam S. Dillon, Ernesto Damiani, Elizabeth Chang, Paolo Ceravolo, Amandeep S. Sidhu

All, together with their many PC members, did a superb and professional job in selecting the best papers from the large harvest of submissions.

We must all be grateful to Ana Cecilia Martinez-Barbosa for researching and securing the local and sponsoring arrangements on-site, to Josefa Kumpfmüller for many useful scientific insights in the dynamics of our transatlantic move, and to our extremely competent and experienced Conference Secretariat and technical support staff in Antwerp, Daniel Meersman, Ana-Cecilia (again), and Jan Demey, and last but not least to our apparently never-sleeping Melbourne Program Committee Support Team, Vidura Gamini Abhaya and Anshuman Mukherjee.

The General Chairs gratefully acknowledge the academic freedom, logistic support and facilities they enjoy from their respective institutions, Vrije Universiteit Brussel (VUB) and RMIT University, Melbourne, without which such an enterprise would not be feasible.

We do hope that the results of this federated scientific enterprise contribute to your research and your place in the scientific network... We look forward to seeing you again at next year's event!

August 2008

Robert Meersman
Zahir Tari

Organization Committee

OTM (On The Move) is a federated event involving a series of major international conferences and workshops. These proceedings contain the papers presented at the OTM 2008 Federated Conferences, consisting of five conferences, namely CoopIS (Cooperative Information Systems), DOA (Distributed Objects and Applications), GADA (Grid computing, high-performAnce and Distributed Applications), IS (Information Security) and ODBASE (Ontologies, Databases and Applications of Semantics).

Executive Committee

OTM 2008 General Co-chairs	Robert Meersman (Vrije Universiteit Brussel, Belgium) and Zahir Tari (RMIT University, Australia)
GADA 2008 PC Co-chairs	Pilar Herrero (Universidad Politécnica de Madrid, Spain), Daniel Katz (Louisiana State University, USA), María S. Pérez (Universidad Politécnica de Madrid, Spain), and Dennis Gannon (Indiana University, USA)
CoopIS 2008 PC Co-chairs	Johann Eder (University of Klagenfurt, Austria), Masaru Kitsuregawa (University of Tokyo, Japan), and Ling Liu (Georgia Institute of Technology, USA)
DOA 2008 PC Co-chairs	Mark Little (Red Hat, UK), Alberto Montresor (University of Trento, Italy), and Greg Pavlik (Oracle, USA)
IS 2008 PC Co-chairs	Jong Hyuk Park (Kyungnam University, Korea), Bart Preneel (Katholieke Universiteit Leuven, Belgium), Ravi Sandhu (University of Texas at San Antonio, USA), and André Zúquete (University of Aveiro, Portugal)
ODBASE 2008 PC Co-chairs	Malu Castellanos (HP, USA), Fausto Giunchiglia (University of Trento, Italy), and Feng Ling (Tsinghua University, China)
Publication Co-chairs	Vidura Gamini Abhaya (RMIT University, Australia) and Anshuman Mukherjee (RMIT University, Australia)
Local Organizing Chair	Lorena G. Gómez Martínez (Tecnológico de Monterrey, Mexico)
Conferences Publicity Chair	Keke Chen (Yahoo!, USA)

Workshops Publicity Chair	Gonzalo Mendez (Universidad Complutense de Madrid, Spain)
Secretariat	Ana-Cecilia Martinez Barbosa, Jan Demey, and Daniel Meersman

CoopIS 2008 Program Committee

Ghaleb Abdulla
Marco Aiello
Joonsoo Bae
Alistair Barros
Zohra Bellahsene
Boualem Benatallah
Salima Benbernou
Djamal Benslimane
M. Brian Blake
Laura Bright
Christoph Bussler
David Buttler
Klemens Böhm
Ying Cai
James Caverlee
Keke Chen
Francisco Curbera
Vincenzo D'Andrea
Umesh Dayal
Xiaoyong Du
Marlon Dumas
Schahram Dustdar
Rik Eshuis
Opher Etzion
Renato Fileto
Klaus Fischer
Avigdor Gal
Bugra Gedik
Dimitrios Georgakopoulos
Paul Grefen
Amarnath Gupta
Mohand-Said Hacid
Thorsten Hampel
Geert-Jan Houben
Richard Hull
Patrick Hung
Paul Johannesson
Dimka Karastoyanova

Rania Khalaf
Hiroyuki Kitagawa
Akhil Kumar
Shim Kyusock
Wang-Chien Lee
Frank Leymann
Chen Li
Sanjay K. Madria
Tiziana Margaria
Leo Mark
Maristella Matera
Massimo Mecella
Ingo Melzer
Mohamed Mokbel
Nirmal Mukhi
Jörg Müller
Miyuki Nakano
Wolfgang Nejdl
Moira Norrie
Werner Nutt
Andreas Oberweis
Tadashi Ohmori
Cesare Pautasso
Barbara Pernici
Beth Plale
Frank Puhlmann
Lakshmish Ramaswamy
Manfred Reichert
Stefanie Rinderle-Ma
Rainer Ruggaber
Duncan Ruiz
Kai-Uwe Sattler
Ralf Schenkel
Jialie Shen
Aameek Singh
Mudhakar Srivatsa
Jianwen Su
Wei Tang

Anthony Tung
Susan Urban
Willem-Jan Van den Heuvel
Wil Van der Aalst
Maria Esther Vidal
Shan Wang
X. Sean Wang
Mathias Weske

Li Xiong
Jian Yang
Masatoshi Yoshikawa
Jeffrey Yu
Leon Zhao
Aoying Zhou
Xiaofang Zhou
Michael zur Muehlen

DOA 2008 Program Committee

Mark Baker
Judith Bishop
Gordon Blair
Barret Bryant
Harold Carr
Gregory Chockler
Geoff Coulson
Frank Eliassen
Patrick Eugster
Pascal Felber
Benoit Garbinato
Jeff Gray
Medhi Jazayeri
Eric Jul
Nick Kavantzas
Fabio Kon
Joe Loyall
Frank Manola
Nikola Milanovic
Graham Morgan
Gero Mühl

Rui Oliveira
Jose Orlando Pereira
François Pacull
Fernando Pedone
Gian Pietro Picco
Calton Pu
Arno Puder
Michel Riveill
Luis Rodrigues
Isabelle Rouvellou
Aniruddha S. Gokhale
Santosh Shrivastava
Richard Soley
Michael Stal
Jean-Bernard Stefani
Hong Va Leong
Aad van Moorsel
Andrew Watson
Stuart Wheater
Shalini Yajnik

GADA 2008 Program Committee

Juan A. Botía Blaya
Jemal Abawajy
Akshai Aggarwal
Artur Andrzejak
Oscar Ardaiz
Sattar B. Sadkhan Almaliky
Costin Badica
Mark Baker
Pascal Bouvry

Rajkumar Buyya
Santi Caballé Llobet
Blanca Caminero Herraez
Mario Cannataro
Jess Carretero
Jinjun Chen
Carmela Comito
Toni Cortes
Geoff Coulson

Jose Cunha
Alfredo Cuzzocrea
Ewa Deelman
Beniamino Di Martino
Marios Dikaiakos
Markus Endler
Geoffrey Fox
Maria Ganzha
Felix García
Antonio Garcia Dopico
Anastasios Gounaris
Eduardo Huedo
Félix J. García Clemente
Shantenu Jha
Liviu Joita
Francisco José da Silva e Silva
Kostas Karasavvas
Kamil Kuliberda
Jose L. Bosque
Laurent Lefevre
Ángel Lucas González Martínez
José Luis Vázquez Poletti
Francisco Luna
Rosa M. Badia
Ignacio M. Llorente

Jose M. Pea
Edgar Magana
Gregorio Martinez
Reagan Moore
Mirela Notare
Hong Ong
Neil P Chue Hong
Marcin Paprzycki
Manish Parashar
Dana Petcu
Bhanu Prasad
Víctor Robles
Ruben S. Montero
Rizos Sakellariou
Manuel Salvadores
Alberto Sanchez
Hamid Sarbazi-Azad
Heinz Stockinger
Alan Sussman
Elghazali Talbi
Jordi Torres
Cho-Li Wang
Adam Wierzbicki
Fatos Xhafa

IS 2008 Program Committee

J.H. Abbawajy
Gail Ahn
Vijay Atluri
Manuel Bernardo Barbosa
Ezedin Barka
Elisa Bertino
Bruno Crispo
Gwenal Dorr
Huirong Fu
Clemente Galdi
Luis Javier Garcia Villalba
Helena Handschuh
Sheikh Iqbal Ahamed
James Joshi
Stefan Katzenbeisser
Hiroaki Kikuchi

Byoung-soo Koh
Klaus Kursawe
Kwok-Yan Lam
Deok Gyu Lee
Javier Lopez
Evangelos Markatos
Sjouke Mauw
Chris Mitchell
Yi Mu
Nuno Ferreira Neves
Giuseppe Persiano
Milan Petkovic
Frank Piessens
Bhanu Prasad
Carlos Ribeiro
Pierangela Samarati

Biplab K. Sarker
Diomidis D. Spinellis
Avinash Srinivasan
Umberto Villano
Liudong Xing

Shouhuai Xu
Sang-Soo Yeo
Xinwen Zhang
Deqing Zou

ODBASE 2008 Program Committee

Harith Alani
Jon Atle Gulla
María Auxilio Medina
Franz Baader
Renato Barrera
Sonia Bergamaschi
Leopoldo Bertossi
Mohand Boughanem
Francisco Cantu-Ortiz
Edgar Chavez
Oscar Corcho
Umesh Dayal
Benjamin Habegger
Bin He
Andreas Hotho
Jingshan Huang
Farookh Hussain
Vipul Kashyap
Uladzimir Kharkevich
Phokion Kolaitis
Manolis Koubarakis
Maurizio Lenzerini
Juanzi Li
Alexander Löser
Lois M. L. Delcambre
Li Ma
Enzo Maltese
Maurizio Marchese

Riichiro Mizoguchi
Peter Mork
Wolfgang Nejdl
Erich Neuhold
Matthew Perry
Wenny Rahayu
Rajugan Rajagopalapillai
Sudha Ram
Arnon Rosenthal
Satya Sahoo
Pavel Shvaiko
Il-Yeol Song
Stefano Spaccapietra
Veda C. Storey
Umberto Straccia
Eleni Stroulia
Heiner Stuckenschmidt
Vijayan Sugumaran
York Sure
Octavian Udrea
Michael Uschold
Yannis Velegrakis
Guido Vetere
Kevin Wilkinson
Baoshi Yan
Laura Zavala
Jose Luis Zechinelli
Yanchun Zhang

OTM Conferences 2008 Additional Reviewers

Aditya Bagchi
Adrian Holzer
Agnes Koschmider
Ahlem Bouchahda
Akshai Aggarwal

Alexander Behm
Alexander Hornung
Alexandros Kapravelos
Alfranio Correia Jr.
Aliaksandr Birukou

Alvin Chan
Anh Tuan Ngyuen
Anirban Mondal
Antonio Garcia Dopico
Aries Tao
Arnd Schroeter
Bing-rong Lin
Boris Motik
Carlos Baquero
Chen Wang
Christian Meilicke
Christoph Gerdes
Cinzia Cappiello
Daniel Eichhorn
Daniel Ried
Darrell Woelk
Deok Gyu Lee
Di Wu
Dimitris Mitropoulos
Dominic Mueller
Don Baker
Eirini Kaldeli
Ela Hunt
Eli Gjørven
Elie el Khoury
Evandro Bacarin
Evgeny Kharlamov
Evi Syukur
Ezedin Barka Barka
Ezedin Barka
Fabien Duchateau
Farouk Toumani
Feng Cao
Fernando Castor Filho
Francesco Guerra
Francesco Lelli
Francisco Cantu
Frithjof Dau
G.R. Gangadharan
Gabriela Montiel-Moreno
Gail Mitchell
Genoveva Vargas-Solar
George Vasiliadis
Gero Decker
Giorgos Stoilos

Graham Morgan
Guandong Xu
Haiyang Sun
Hajo Reijers
Hakim Hacid
Hamid Motahari
Hamid Sarbazi-Azad
Harald Gjermundrod
Harald Meyer
Harry Wang
He Hu
Hideyuki Kawashima
Hiroyuki KASAI
Hong-Hai Do
Huajing Li
Jan Schönherr
Jesus Carretero
Jiangang Ma
Jianxia Chen
Jilian Zhang
Jochem Vonk
Jonas Schulte
Joonsoo Bae
Josh Benaloh
Jutta Mlle
Kai Eckert
Kamil Kuliberda
Karen Sauvagnat
Ken. C.K. Lee
Ki Jung Lee
Konstantinos Karasavvas
Ladjel Bellatreche
Larry Moss
Laura Po
Lin Hao Xu
Linh Thao Ly
Liudong Xing
Lourdes-Angélica Martinez-Medina
Manuel Salvadores
Mao Ye
Marcin Wieloch
Marcus Schramm
Maria Auxilio Medina
María del Carmen
Suárez de Figueroa Baonza

Mariagrazia Fugini
Massimo Benerecetti
Maurizio Vincini
Meng Ge
Michael Uschold
Mikaél Beauvois
Minqi Zhou
Mirko Orsini
Mona Allani
Nick Nikiforakis
Nickolas Kavantzas
Nicolas Schiper
Noyan Ilk
Oliver Kutz
Ornsiri Thongoom
Paul Khoury (El)
Peter Graubmann
Peter McBrien
Pierluigi Plebani
Ralph Bobrik
Rares Vernica
Raymond Pon
Reagan Moore
Ritu Khare
Robert Jäschke
Rochat Denis
Romain Rouvoy
Rui Joaquim
Sasa Radomirovic
Sattar B. Sadkhan

Serena Sorrentino
Shantenu Jha
Shaokun Fan
Shengyue Ji
Sherry Sun
Shih-Hsi Liu
Siang Song
Siim Karus
Simon Woodman
Stefan Schlobach
Stephan Neuhaus
Stephanos Androutsellis-Theotokis
Thomas Wächter
Ton van Deursen
Toshiyuki Amagasa
Toumani, McBrien
Vasileios Vlachos
Vincenzo Maltese
Wenjuan Xu
Wojciech Barczynski
Xiao Yuan Wang
Xing Zhi Sun
Xingjie Liu
Yacine Sam
Yiming Lu
Yuan Tian
Yue Zhang
Yujin Tang
Yves Younan
Zhebglu Yang

Sponsoring Institutions

OTM 2008 was proudly sponsored by BN (Bauch & Navratil, Czech Republic), Nuevo Leon, and the City of Monterrey.

Supporting Institutions

OTM 2008 was proudly supported by RMIT University (School of Computer Science and Information Technology), Vrije Universiteit Brussel (Department of Computer Science), Technical University of Monterrey and Universidad Politécnica de Madrid.

Table of Contents – Part II

Information Security (IS) 2008 International Conference

Intrusion Detection

Information Hiding

Data and Risk Management

Access Control

Evaluation and Implementation

Ontologies, Databases and Applications of Semantics (ODBASE) 2008 International Conference

Keynote

Invited Papers

Semantic Matching and Similarity Measuring

Semantic Searching

Ontology Development

Ontology Maintenence and Evaluation

Ontology Applications I

Ontology Applications II

Semantic Query Processing

Automatic Generation of Secure Multidimensional Code for Data Warehouses: An MDA Approach

Carlos Blanco[1], Ignacio García-Rodríguez de Guzmán[1],
Eduardo Fernández-Medina[1], Juan Trujillo[2], and Mario Piattini[1]

[1] Dep. of Information Technologies and Systems. Escuela Superior de Informática
Alarcos Research Group – Institute of Information Technologies and Systems
Univ. of Castilla-La Mancha. Paseo de la Universidad, 4. 13071. Ciudad Real. Spain
{Carlos.Blanco,Ignacio.GRodriguez,Eduardo.Fdezmedina,
Mario.Piattini}@uclm.es

[2] Department of Information Languages and Systems. Facultad de Informática
University of Alicante. San Vicente s/n. 03690. Alicante. Spain
jtrujillo@dlsi.ua.es

Abstract. Data Warehouses (DW) manage enterprise information for the decision making process, and the establishment of security measures at all stages of the DW development process is also highly important as unauthorized users may discover vital business information. Model Driven Architecture (MDA) based approaches allow us to define models at different abstraction levels, along with the automatic transformations between them. This has thus led to the definition of an MDA architecture for the development of secure DWs. This paper uses an example of a hospital to show the benefits of applying the MDA approach to the development of secure DWs. The paper is focused on transforming secure multidimensional Platform Independent Models (PIM) at the conceptual level into Platform Specific Models (PSM) at the logical level by defining the necessary set of Query/Views/Transformations (QVT) rules. This PSM model is therefore used to obtain the corresponding secure multidimensional code for a specific On-Line Analytical Processing (OLAP) platform such as SQL Server Analysis Services (SSAS).

Keywords: Data Warehouses, Security, MDA, QVT, OLAP, SQL Server Analysis Services.

1 Introduction

The survival of organizations depends on the correct management of information security and confidentiality [1], and DWs manage enterprises' historical information which is used to support the decision making process and must be ensured by establishing security measures from the early stages of the development lifecycle [2]. Therefore, it is necessary to consider security constraints in models at all abstraction levels and to ultimately take these security issues into account in the final tools in order to avoid the situation of users being able to access unauthorized information by using operations.

R. Meersman and Z. Tari (Eds.): OTM 2008, Part II, LNCS 5332, pp. 1052–1068, 2008.

Furthermore, MDA [3] is the Object Management Group (OMG) standard approach for model driven software development based on the separation of the specification of the system functionality and its implementation. MDA allows us to define models at different abstraction levels: computer-independent models (CIM) at business level and platform-independent models (PIM) at conceptual level which do not include information about specific platforms and technologies, and platform-specific models at logical level (PSM) with information about the specific technology used. Moreover, MDA proposes the use of *model transformations* as a mechanism with which to move from one level of abstraction to another, by transforming input models into new models or searching for matchings, among the other models involved. Many languages for model transformations exist. Nonetheless, the OMG proposes Query / Views / Transformations (QVT) [4] as a new standard for model transformation based on the Meta-Object Facility (MOF) standard [5] through which to define model transformation in an intuitive manner. Supporting the development of DWs with an MDA approach provides many advantages such a better separation of models including security requirements from the first stages of the DWs lifecycle and automatic translations through which to obtain other models and final code for different target platforms.

An architecture for developing secure DWs by using MDA and QVT transformations has been proposed in [6]. This architecture supports the modeling of secure DWs at different abstraction levels: CIM (specifying goals and subgoals), PIM (a multidimensional model), PSM (a relational model) and the final implementation in a database management system (DBMS). However, these aforementioned works are focused on a relational approach and the greatest part of DW is managed by OLAP tools over a multidimensional approach. We have therefore deployed a specialization of this architecture which defines a secure multidimensional PSM and implements secure DWs in SQL Server Analysis Services (SSAS) as a specific OLAP platform. In this architecture, we have decided to specify those QVT rules which directly transform our secure multidimensional PIM into a secure multidimensional PSM, and to then use this PSM to obtain secure multidimensional code for this OLAP platform (SSAS). In this paper we show the benefits of our approach through its application to an example. We show the steps involved in a conceptual model (PIM), a logical model (PSM), multidimensional secure code and the application of a set of QVT rules which transform the concepts of our secure multidimensional model at the conceptual level (PIM) into a logical model (PSM) which is used to obtain pieces of the code of our target platform (both the structural and security aspects of the final DW).

The remainder of the paper is organised as follows: Section 2 will present related work. Section 3 will introduce our MDA architecture for the development of secure DWs, and will be focused both on our source and target metamodels (PIM, PSM and code), and on the transformations which are necessary to obtain PSM from PIM and code from PSM. Section 4 will introduce our example regarding the admission system of a hospital. We will present models at the conceptual (PIM), logical (PSM) and code levels and will show how the proposed QVT transformations have been applied to obtain PSM from PIM. We will then demonstrate how to obtain the final code from PSM. Finally, Section 5 will present our conclusions and future work.

2 Related Work

OLAP systems are mechanisms with which to discover business information and use a multidimensional analysis of data to make strategic decisions. This information is organized according to the business parameters, and users can discover unauthorized data by applying a set of OLAP operations to the multidimensional view. Therefore, it is of vital importance for the organization to protect its data from unauthorized accesses. Several works attempting to include security issues in OLAP tools by implementing the previously defined security rules at a conceptual level have been proposed, but these works focus solely upon Discretional Access Control (DAC) policy and use a simplified role concept implemented as a subject. For instance, Katic et al. [7] proposed a DWs security model based on metamodels which provides us with views for each user group and uses DAC with classification and access rules for security objects and subjects. However, this model does not allow us to define complex confidentiality constraints. Kirkgöze et al. [8] defined a role-based security concept for OLAP by using a "constraints list" for each role, and this concept is implemented through the use of a discretional system in which roles are defined as subjects.

Priebe and Pernul later proposed a security design methodology, analyzed security requirements, classifying them into basic and advanced, and dealt with their implementation in commercial tools. Firstly, in [9] they used ADAPTed UML to define a DAC system with roles defined as subjects at a conceptual level. They then went on to implement this in SQL Server Analysis Servicies 2000 by using Multidimensional Expressions (MDX). They created a Multidimensional Security Constraint Language (MDSCL) based on MDX and put forward HIDE statements with which to represent negative authorization constraints on certain multidimensional elements: cube, measure, slice and level.

Our proposal uses an access control and audit model specifically designed for DWs to define security constraints in early stages of the development lifecycle. By using an MDA approach we consider security issues in all stages of the development process and automatically transform models at upper abstraction level towards logical models over a relational or multidimensional approach and finally obtain from these models secure code for DBMS or OLAP tools.

3 An MDA Approach for Developing Secure DWs

Our MDA architecture [6] is an adaptation of an MDA architecture for developing DWs [10] which has been improved with security capabilities. Our approach is made up of several models which allow us to model the DW at different abstraction levels (see Figure 1): at the business level (CIM) with a UML profile [11] based on the i* framework [12], which is an agent orientated approach towards requirement engineering centering on the intentional characteristics of the agent; at the conceptual level (PIM) with a UML profile called SECDW [13]; and at the logical level (PSM) with an extension of the relational package of Common Warehouse Metamodel (CWM) called SECRDW [14]. As has previously been mentioned, this paper considers a specialization of this architecture (represented in grey in Figure 1) focused on defining a PSM metamodel over a multidimensional approach and transforming structural and security issues from PIM into this multidimensional PSM which allows us to obtain final multidimensional code for OLAP tools. The transformation from PSM models into secure multidimensional code for a specific OLAP platform (SSAS) is also treated in this paper. The source (PIM) and target (PSM) metamodels are briefly described in the following subsections, and an overview of the QVT rules defined to support this transformation will be presented.

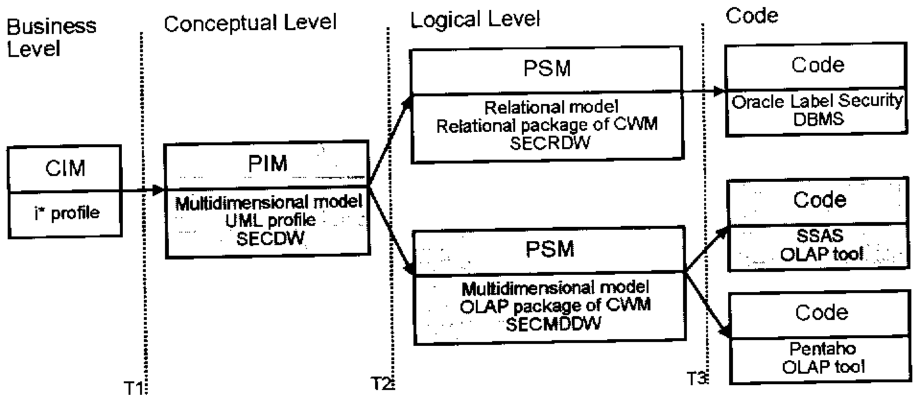


Fig. 1. MDA architecture for developing secure DWs

3.1 Secure Multidimensional PIM

A secure multidimensional conceptual metamodel called SECDW, has been defined in [13] by using a UML profile. This metamodel is shown in Figure 2 and is based on a UML profile for the conceptual design of DWs [15] which allows us to define fact, dimension and base classes, and considers specific aspects of DWs such as many-to-many relations, degenerated dimensions, multiple classifications or alternative paths of hierarchies. SECDW is enriched with security capabilities through the use of an access control and audit model (ACA) [16], which was specifically designed to consider security in DWs.

ACA allows us to define secure classes (SecureClass) and properties (SecureProperty), to classify authorization subjects and objects into security roles (SecurityRole) which organize users into a hierarchical role structure according to the responsibilities of each type of work, levels (SecurityLevel) which indicate the clearance level of the user, and compartments (SecurityCompartment) which classify users into a set of horizontal compartments or groups.

ACA also considers the definition of security rules over multidimensional elements of DWs by using stereotypes and Object Constraints Language (OCL) notes (Constraint). Three kinds of security rules are permitted: sensitive information assignment rules (SIAR) which specify multilevel security policies and allow us to define sensitivity information for each element in the multidimensional model; authorization rules (AUR) which permit or deny access to certain objects by defining the subject that the rule applies to, the object that the authorization refers to, the action that the rule refers to and the sign describing whether the rule permits or denies access; and audit rules (AR) to ensure that authorized users do not misuse their privileges.

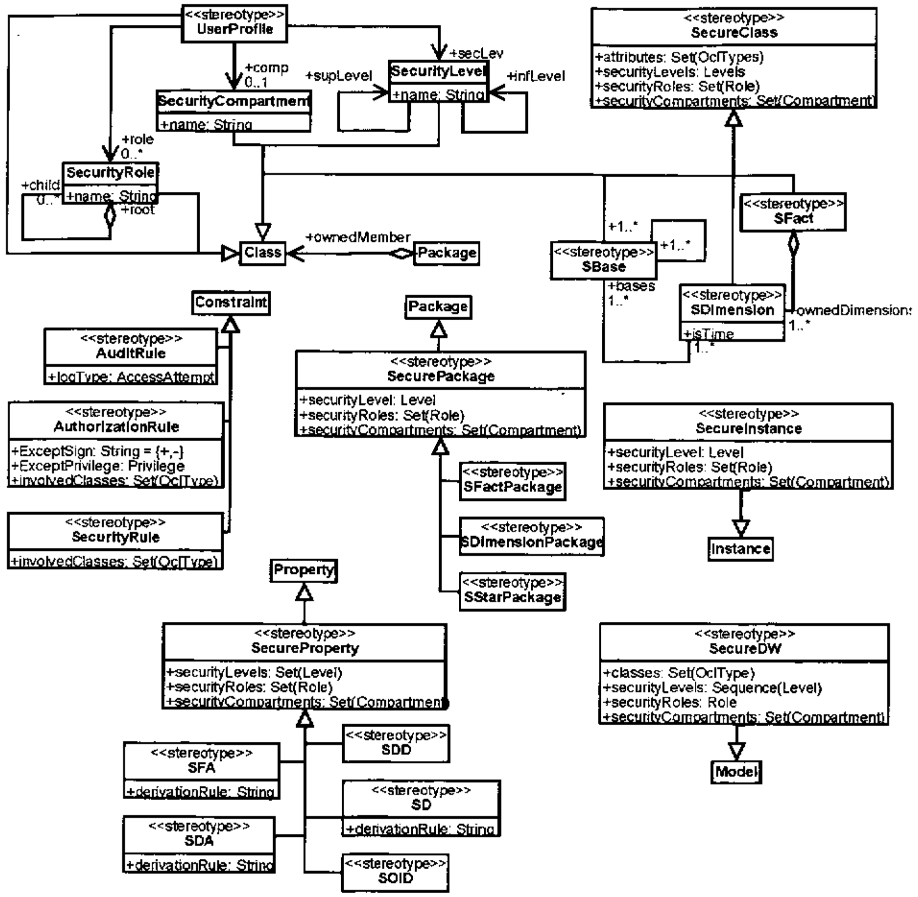

<<stereotype>> UserProfile
+comp 0..1
+secLev
+supLevel
+infLevel
SecurityCompartment
+name: String
SecurityLevel
+name: String
+role 0..*
SecurityRole
+name: String
+child 0..*
+root
Class
+ownedMember
Package
Constraint
<<stereotype>> AuditRule
+logType: AccessAttempt
<<stereotype>> AuthorizationRule
+ExceptSign: String = {+,-}
+ExceptPrivilege: Privilege
+involvedClasses: Set(OclType)
<<stereotype>> SecurityRule
+involvedClasses: Set(OclType)
Package
<<stereotype>> SecurePackage
+securityLevel: Level
+securityRoles: Set(Role)
+securityCompartments: Set(Compartment)
<<stereotype>> SFactPackage
<<stereotype>> SDimensionPackage
<<stereotype>> SStarPackage
Property
<<stereotype>> SecureProperty
+securityLevels: Set(Level)
+securityRoles: Set(Role)
+securityCompartments: Set(Compartment)
<<stereotype>> SFA
+derivationRule: String
<<stereotype>> SDA
+derivationRule: String
<<stereotype>> SDD
<<stereotype>> SD
+derivationRule: String
<<stereotype>> SOID
<<stereotype>> SecureClass
+attributes: Set(OclTypes)
+securityLevels: Levels
+securityRoles: Set(Role)
+securityCompartments: Set(Compartment)
+1..*
<<stereotype>> SBase
+1..*
+bases 1..*
<<stereotype>> SFact
<<stereotype>> SDimension
+isTime
1..*
+ownedDimensions
1..*
<<stereotype>> SecureInstance
+securityLevel: Level
+securityRoles: Set(Role)
+securityCompartments: Set(Compartment)
Instance
<<stereotype>> SecureDW
+classes: Set(OclType)
+securityLevels: Sequence(Level)
+securityRoles: Role
+securityCompartments: Set(Compartment)
Model

Fig. 2. Secure multidimensional PIM (SECDW)

3.2 Secure Multidimensional PSM

A secure multidimensional metamodel at the logical level (PSM), called SECMDDW, has been defined in this work by extending the OLAP package of CWM. This metamodel represents the intermediate step between conceptual and code levels, that is, our multidimensional PSM is obtained from PIM and can be used to obtain code towards different OLAP tools. Our PSM uses a multidimensional approach and considers the *security configuration* of the system, *structural* elements of the DW's and *security* constraints defined at class (fact, dimension or base) or attribute levels. Figure 3 shows the *security configuration* metamodel obtained. Our logical metamodel (PSM) only considers a role-based access control policy (RBAC) because the vast majority of OLAP tools use this policy and the PSM metamodel is closer to the final platform than the PIM metamodel. However, at the conceptual level we have considered security roles, levels and compartments defined by using our ACA model which have to be translated into roles. To accomplish this process we will follow the methodology to implement secure DWs into OLAP tools presented in [17]. Furthermore, we have defined two metamodels to support the definition of the *structural* and *security* issues of cubes and dimensions.

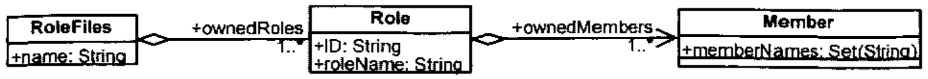


Fig. 3. Secure multidimensional PSM (SECMDDW): security configuration

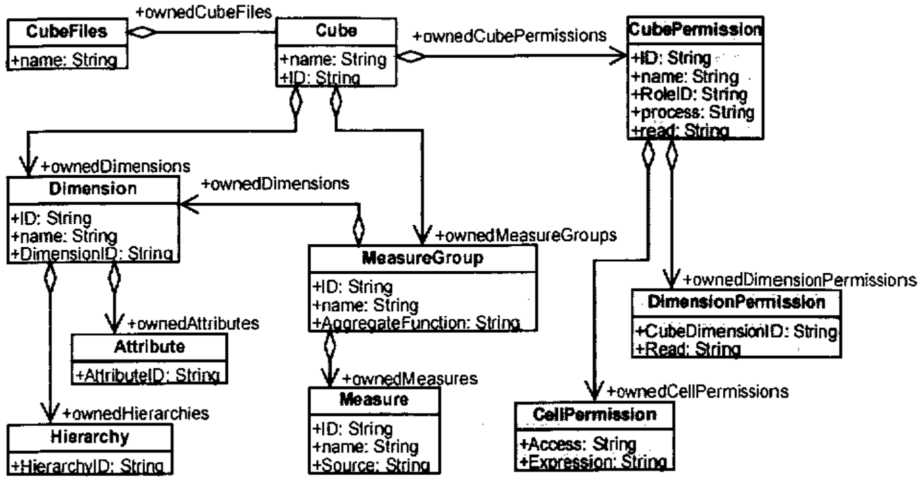


Fig. 4. Secure multidimensional PSM (SECMDDW): cubes

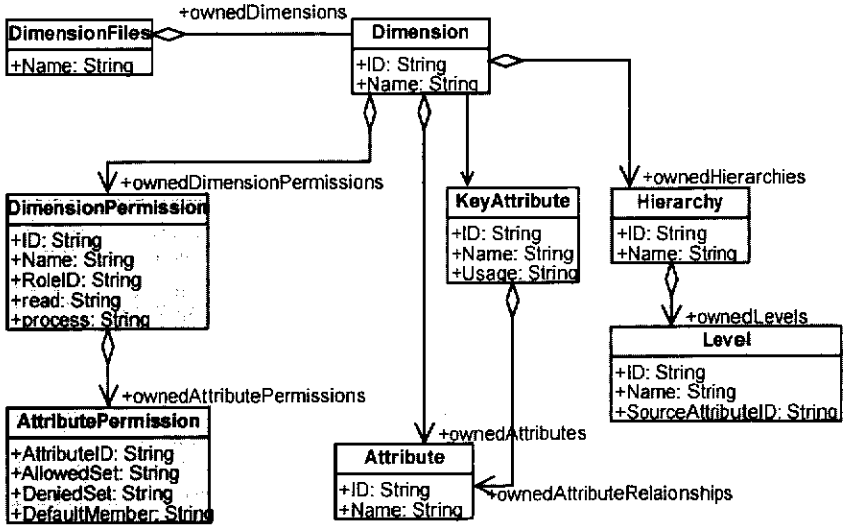


Fig. 5. Secure multidimensional PSM (SECMDDW): dimensions

Figures 4 and 5 show metamodels for cubes and dimensions which allow us to define facts classes (Cube), measures (MeasureGroup, Measure), dimension classes (Dimension), attributes (Attribute), hierarchies (Hierarchy) and base classes as attributes of the related dimension, and which also allow us to define security constraints over these multidimensional elements by using permissions over cubes (CubePermission), dimensions (DimensionPermission), cells (CellPermission) or attributes (AttributePermission). In these figures, the security-related aspects are represented in grey.

PIM to PSM transformation. A set of QVT transformations has been developed to automatically obtain secure multidimensional logical models, defined according to our PSM metamodel (SECMDDW), from conceptual models defined according to our PIM metamodel (SECDW). In order to develop these rules we have followed a methodology to implement multidimensional security in OLAP tools presented in [17]. These proposed transformations are made up of three main transformations which obtain our various kinds of target models from source conceptual models: *SECDW2Role*, *SECDW2Cube* and *SECDW2Dimension*.

SECDW2Role deals with the security configuration of the system. As our ACA model is richer than our PSM, which only considers roles, this transformation generates a new role for each security role (SR), level (SL) and compartment (SC) defined in our source model (PIM); *SECDW2Cube* generates the cube files that represent cubes, measures, dimensions, and cube permissions from the SECDW model; and *SECDW2Dimension* generates the dimension files that represent dimensions, bases, attributes, hierarchies and security permissions defined over dimensions and attributes. The security measures defined at the conceptual level (PIM) over classes or attributes by using SC, SR and SL, are translated into a set of permissions for involved roles (SC, SR and SL are translated into roles). As the transformations are quite verbose and the available space is limited, Section 4 will show some examples of complete rules and this section only presents the signatures of the developed rules.

SECDW2Role is composed of a top relation "*Package2RoleFiles* {…}" and relations "*SCompartment2Role* {…}", "*SRole2Role* {…}" and "*SLevel2Role* {…}". The signatures for the remainder of the developed rules are shown in Table 1.

Table 1. PIM to PSM transformations (signatures)

SECDW2Cube	**SECDW2Dimension**
top relation *Package2CubeFiles* {…}	top relation *Package2DimensionFiles* {…}

relation *SFact2Cube* {…}
relation *CreateMeasureGroups* {…}
relation *SProperty2Measure* {…}
relation *SDimension2Dimension* {…}
relation *ProcessSBase* {…}
relation *CreateOwnedHierarchies* {…}
relation *SProperty2Property* {…}
	relation *SDimension2Dimension* {…}
	relation *KeyProperty2KeyAttribute* {…}
	relation *NonKeyProperty2Attribute* {…}
	relation *SBase2Attribute* {…}

relation *SCompartmentClass2CubePermission*{}
relation *SRoleClass2CubePermission* {…}
relation *SLevelClass2CubePermission* {…}
relation *SCompartmentAtt2CellPermission* {…}
relation *SRoleAtt2CellPermission* {…}
relation *SLevelAtt2CellPermission* {…}
	relation *createDimensionSIARForSCompartment* {…}
	relation *createDimensionSIARForSRole* {…}
	relation *createDimensionSIARForSLevel* {…}
	relation *authorizeSCompartment* {…}
	relation *authorizeSRole* {…}
	relation *authorizeSLevel* {…}
	relation *processSecureProperty* {…}
	relation *createPositiveAttributePermission* {…}
	relation *createNegativeAttributePermission* {…}

3.3 Secure Multidimensional Code

As a target OLAP platform we have selected SQL Server Analysis Services (SSAS), which deals with multidimensional elements and allows us to establish security measures over them. Furthermore, SSAS uses several kinds of XML files to manage this information, the most important of which are role, cubes and dimension files. We have analyzed this OLAP tool by studying how structural and security information could be implemented in this platform, in order to obtain secure multidimensional code from PSM.

PSM to Code Transformation. Obtaining secure multidimensional code from our secure multidimensional PSM is a simple task since both consider structural and security issues by using a multidimensional approach and the vast majority of the destination concepts are defined in our source metamodel. This paper is focused on obtaining PSM from PIM, but also deals with the transformation of PSM into a specific OLAP platform, SSAS. In order to obtain code for the security measures defined in the conceptual models we have followed the methodology to implement multidimensional security in SSAS which is presented in [17]. The presentation of our example will show a portion of code in SSAS and screenshots of the final implementation in SSAS.

4 Applying MDA for Developing Secure DWs

This section presents the application of our MDA architecture to an example of a hospital that wishes to automate its admission process and requires confidentiality for the information involved. This example will be used to show the application of the transformations to obtain a logical model (PSM) according to our target metamodel and to obtain secure multidimensional code in SSAS from PSM.

4.1 Secure Multidimensional PIM

Figure 6 shows the conceptual model (defined as an instance of the SECDW model) for our hospital which is required to resolve the aforementioned problem. The security configuration of the hospital uses a classification of users and objects in security roles (SR) and security levels (SL). Security compartments have not been defined since they depend on organization policies. The user roles (SR) might be "HospitalEmployee", "Health" (including "Doctor" and "Nurse" roles) and "NonHealth" (including "Admin" and "Maintance" roles). The levels of security (SL) used are top secret (TS), secret (S), confidential (C) and undefined (U). The secure fact class "Admission" contains two secure dimension classes ("Diagnosis" and "Patient"). The "UserProfile" metaclass contains information about all the users who will have access to this secure multidimensional model. This information can also define characteristics of users such us age, citizenship, etc. which can be used to establish complex security constraints. We have also defined a set of sensitive information assignment rules (SIAR) over classes and attributes: instances of "Admission" fact class or "Patient" dimension can be accessed by the "Admin" or "Health" roles and the Secret (or upper) security level; the "Diagnosis" dimension can be accessed by the "Health" role and the Secret (or upper) security level; the bases "City" and "DiagnosisGroup" can be accessed by the Confidential (or upper) security level; and attributes "Admission.cost" and "Patient.address" can be accessed by the "Admin" role.

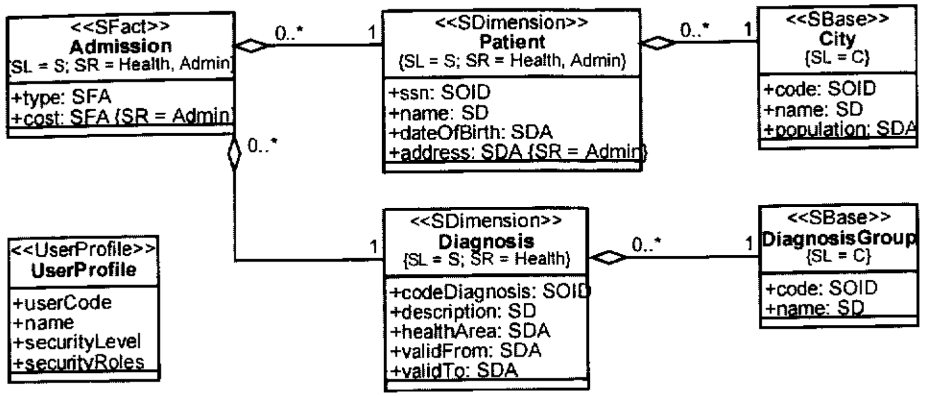


Fig. 6. Secure multidimensional PIM for hospital

4.2 Secure Multidimensional PSM

In this section we obtain a logical model (PSM) from the conceptual model defined above for a hospital according to the SECDW metamodel by using a set of QVT transformations (see Table 1). We have applied our three main defined transformations (SECDW2Role, SECDW2Cube and SECDW2Dimension) and we present the resulting logical models according to our PSM metamodel. These were obtained from conceptual models according to our PIM metamodel.

SECDW2Role. Table 2 shows the application of the *SECDW2Role* transformation to the hospital. The *SRole2Role* rule creates for each security role "r" detected in the source model a new role called "SRr". The QVT code for the rule SLevel2Role is shown in Table 3 and also creates a new role called "SLn" for each security level "n" defined at conceptual level, that is, in this example creates "SLTS", "SLS", "SLC" and "SLU" roles. *SCompartment2Role* has not been shown because security compartments have not been defined in the hospital.

Table 2. SECDW2Role transformation for hospital

top relation **Package2RoleFiles:** Hospital
relation **SRole2Role:** HospitalEmployee, Health, Doctor, Nurse, NonHealth, Admin, Maintenance relation **SLevel2Role:** TS, S, C, U relation **SCompartment2Role:** not thrown

Table 3. Relation SLevel2Role

```
relation SLevel2Role
checkonly domain psm sl:SRole{
   name = n;  }
enforce domain pim r:Role{
   fileName = "SL"+n+".role";
   ID = "SL"+n;
   roleName = "SL"+n;
   ownedMembers = OWNEDMEMBS:Set(Member);  }
```

The target model with the security configuration for the hospital has been represented in Figure 7 according to PSM metamodel (SECMDDW). This model defines roles at logical level for each security role and security level detected at conceptual level.

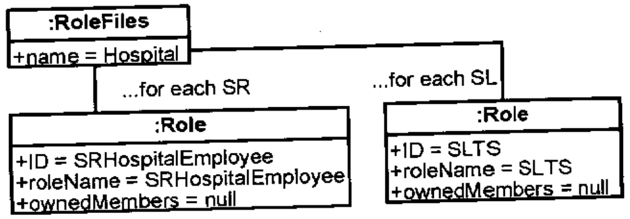


Fig. 7. Secure multidimensional PSM for hospital: security configuration

SECDW2Cube. Next, the *SECDW2Cube* transformation obtains the structure and security of cubes defined in the hospital. Table 4 shows the process: *SFact2Cube* rule creates the "Admission" cube; then the *CreateMeasuresGroups* and *SProperty2Measure* rules create measures and the remainder of the structural rules create dimensions, attributes and hierarchies for dimensions and bases related to the "Admission" cube. Finally, security rules analyze the security constraints defined over the fact class and its attributes, and define cube and cell permissions for involved security roles (which represent the SR, SL and SC of the source model).

Table 4. SECDW2Cube transformation for hospital

top relation **Package2RoleFiles:** Hospital
relation **SFact2Cube:** Admission relation **CreateMeasureGroups:** Admission relation **SProperty2Measure:** type, cost relation **SDimension2Dimension:** Patient, Diagnosis relation **ProcessSBase:** City, DiagnosisGroup relation **CreateOwnedHierarchies:** City-Patient, DiagnosisGroup-Diagnosis relation **SProperty2Attribute:** (for Patient) ssn, name, dateOfBirth, address (for Diagnosis) codeDiagnosis, description, healthArea, validFrom, validTo (for City) code, name, population (for DiagnosisGroup) code, name
relation **SCompartmentClass2CubePermission:** Not thrown relation **SRoleClass2CubePermission:** (for Admission) Health, Admin relation **SLevelClass2CubePermission:** (for Admission) S relation **SCompartmentAtt2CellPermission:** Not thrown relation **SRoleAtt2CellPermission:** (for Admission.address) Admin relation **SLevelAtt2CellPermission:** Not thrown

Table 5 shows the code for "SLevelClass2CubePermission" rule which permits accesses to cube by creating cube permissions for each authorized role that represent allowed security levels. In this example, cube permissions allowing access to security level secret "S" (SLS role) and its upper security levels (SLTS role) are defined in "Admission" class.

Figure 8 shows the model obtained from SECDW2Cube transformation in which has been created an "Admission" cube with its measure groups (including "type" and "cost" measures), related dimensions ("Patient" and "Diagnosis"), cube permissions

Table 5. Relation SLevelClass2CubePermission

```
relation SLevelClass2CubePermission
checkonly domain psm sl:SLevel {
    name = n; }
enforce domain pim c:Cube {
    name = cubeName;
    ID = cubeName;
    ownedCubePermissions = OWNCUBEPERMS:Set(CubePermission); }
enforce domain pim cp:CubePermission {
    ID = "CubePermission"+n;
    name = "CubePermission"+n;
    RoleID = n;
    Process = "true";
    Read = "Allowed"; }
where{ OWNCUBEPERMS->including(cp); }
```

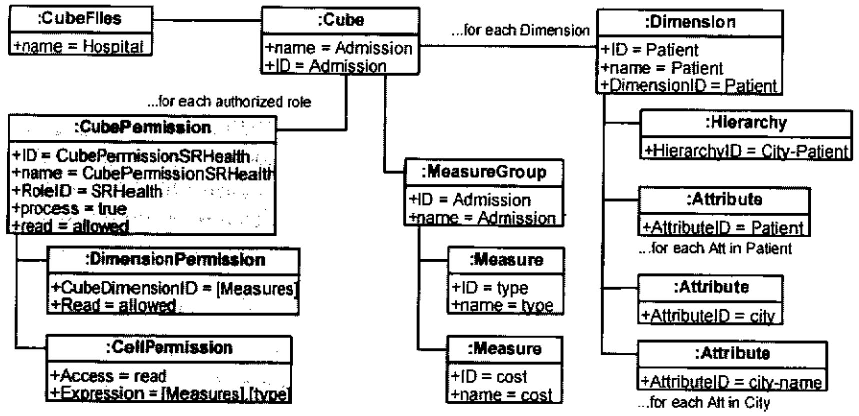


Fig. 8. Secure multidimensional PSM for hospital: cube

over "Admission" cube allowing accesses to authorized roles ("SRHealth", "SRAdmin" and its descendants, and "SLS" and upper levels) and cell permissions allowing accesses to each allowed measure ("SRAdmin" cannot access "cost" measure) .

SECDW2Dimension. Finally, the *SECDW2Dimension* transformation obtains the structure and security of dimensions and bases by following the process shown in Table 6. Firstly, structural rules obtain dimensions, hierarchies and attributes for the dimensions and bases defined in our SECDW model. Each attribute of the base classes is added as an attribute of its related dimension in our target model. Next, the security rules are applied. These are composed of several rules which obtain security constraints defined over classes (dimension or base classes) and their attributes, and they then analyze the security roles which are involved to obtain dimension and attribute permissions. Security constraints detected at the class level generate dimension permissions for each authorized role, allowing access to this class. Attribute permissions are also created for the security constraints defined at the attribute level, defining positive attribute permissions for each authorized role and negative attribute permissions to avoid access to unauthorized users.

Table 6. SECDW2Dimension transformation for hospital

top relation **Package2Dimension:** Hospital
relation **SDimension2Dimension:** Patient, Diagnosis relation **KeyProperty2KeyAttribute:** (for Patient) ssn (for Diagnosis) codediagnosis relation **NonKeyProperty2Attribute:** (for Patient) name, dateOfBirth, address (for Diagnosis) description, healthArea, validFrom, validTo relation **SBase2Attributes:** City, DiagnosisGroup
relation **createDimensionSIARForSCompartment:** Not thrown relation **createDimensionSIARForSRole:** (for Patient) Health, Admin (for Diagnosis) Health relation **createDimensionSIARForLevel:** (for Patient) S (for Diagnosis) S (for City) C (for DiagnosisGroup) C relation **authorizeSCompartment:** Not thrown relation **authorizeSRole:** (for Patient) Health, Admin and their descendants (for Diagnosis) Health and its descendants relation **authorizeSLevel:** (for Patient) S, TS (for Diagnosis) S, TS (for City) C, S, TS (for DiagnosisGroup) C, S, TS relation **processSecureProperty:** (for Patient) address relation **createPossitiveAttributePermission:** allowed roles (Admin and its descendants) relation **createNegativeAttributePermission:** denied roles (distinct to allowed roles)

Table 7 shows a piece of source code for one rule of our developed set of QVT transformation which obtains security constraints defined at the conceptual level over attributes and establishes this constraint by using an attribute permission with an explicit denial over this attribute for the involved roles. In this example, a security constraint over "address" attribute of "Patient" dimension allowing access to security role "Admin" was defined. This rule creates attribute permissions for each unauthorized roles (roles distinct to "SRAdmin" and its descendants) with a denied set over "address" attribute of "Patient" dimension.

Table 7. Relation createNegativeAttributePermissions

```
relation createNegativeAttributePermissions
checkonly domain pim sp:SecureProperty {
    name = spName; }
enforce domain psm dp:DimensionPermission {
    ID = "DimensionPermission"+ID;
    Name = "DimensionPermission"+ID;
    ownedAttributePermissions= OWNATTPERMS:Set(AttributePermission);}
enforce domain psm at:AttributePermission {
    AttributeID = spName;
    DeniedSet = "["+sp.class.name+"].["+sp.name+"]"; }
```

Figure 9 shows the model obtained from SECDW2Dimension transformation in which are defined each dimension ("Patient" and "Diagnosis"), attributes (key attributes, non key attributes and attributes derived from its related bases), hierarchies and security permissions over dimensions and attributes (positive and negative permissions).

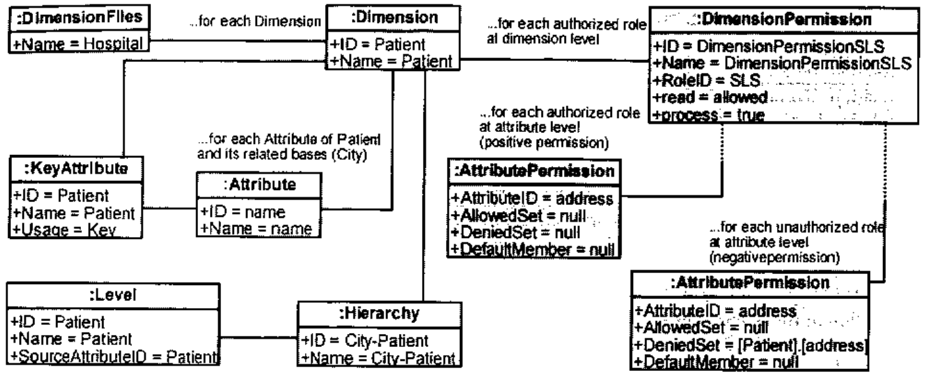


Fig. 9. Secure multidimensional PSM for hospital: dimensions

4.3 Secure Multidimensional Code

Finally, the security multidimensional code for SSAS is obtained from the logical model (PSM). Although SSAS has some particularities, this model, with which to text transformation, is easy to obtain. SSAS manages multidimensional elements (such as cubes, dimensions, hierarchies or measures) and also considers the establishment of security measures over these multidimensional elements with security permissions over cubes, dimensions, cells and attributes.

Table 8. Secure multidimensional Code for hospital: Admission cube

```
<Cube>
  <ID>Admission</ID>
  <Name>Admission</Name>

  <Dimensions>...</Dimensions>
  <MeasureGroups>...</MeasureGroups>

  <CubePermissions>
   <CubePermission>
     <ID>CubePermissionSLS</ID>
     <Name>CubePermissionSLS</Name>
     <RoleID>SLS</RoleID>
     <Process>true</Process>
     <Read>Allowed</Read>
     <CellPermissions>
       <CellPermission>
         <Access>Read</Access>
         <Expression>[Measures].[type]</Expression>
       </CellPermission>
     </CellPermissions>
   </CubePermission>
   ...(cube permissions for each authorized role)

  </CubePermissions>
</Cube>
```

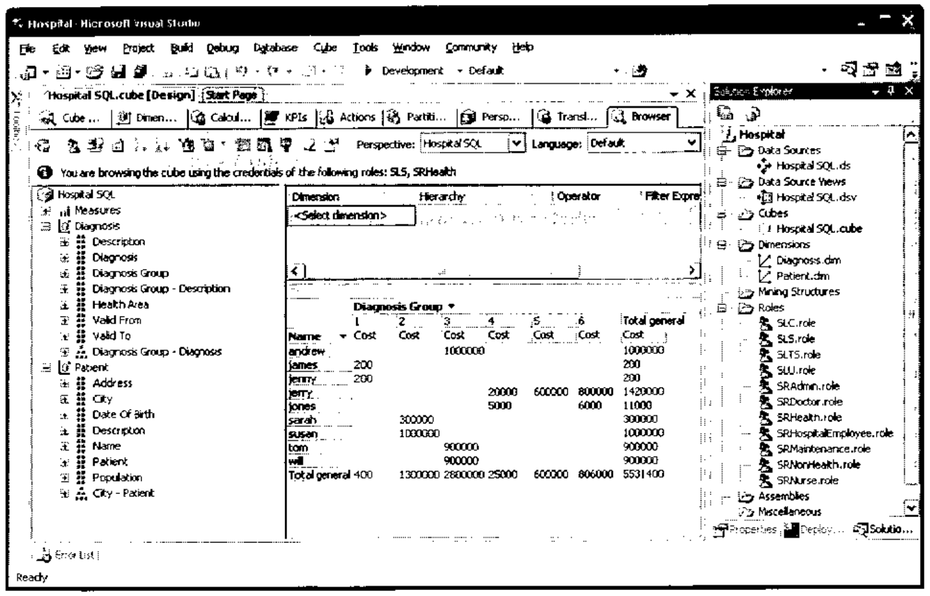
The first example correspond to a security rule defined at conceptual level that allows accesses to "Admission" measures for security level secret or upper and security roles "Health", "Admin" and their descendants. Table 8 shows a piece of the final code for SSAS with a cell permission over attribute "type" that allows access to security level secret (role "SLS"). In this example we have used a positive permission to allow access to "type" and we have thus denied access to the remaining cube measures (attributes of the "Measures" dimension).

At conceptual level we have defined a rule that hides the "Diagnosis" dimension from users with a security level which is lower than "Secret" ("SLC" and "SLU" at the logical level) and with a security role which is not "Health" or "Admin" or their descendents ("SRMaintance" at the logical level). Table 9 shows secure multidimensional code obtained from PSM for the "Diagnosis" dimension which hides all its attributes from unauthorized roles. Due to space constraints, this table only shows a piece of the code in which the "DiagnosisGroup" attribute is hidden from users with the "Confidential" security level ("SLC" role). The rest of the code similarly defines attribute permissions for each attribute of the "Diagnosis" dimension and dimension permission for each unauthorized role.

Table 9. Secure multidimensional Code for hospital: Diagnosis dimension

```
<Dimension>
  <ID>Diagnosis</ID>
  <Name>Diagnosis</Name>

  <Attributes>...</Attributes>

  <DimensionPermissions>

    <DimensionPermission>
      <ID>DimensionPermissionSLC</ID>
      <Name>DimensionPermissionSLC</Name>
      <RoleID>SLC</RoleID>
      <Read>Allowed</Read>

      <AttributePermissions>
        <AttributePermission>
          <AttributeID>DiagnosisGroup</AttributeID>
          <DeniedSet>[Diagnosis].[DiagnosisGroup]</DeniedSet>
        </AttributePermission>
        ...(attribute permissions for each attribute of Diagnosis)
      </AttributePermissions>

    </DimensionPermission>
    ...(dimension permissions for each unauthorized role)

  </DimensionPermissions>
</Dimension>
```

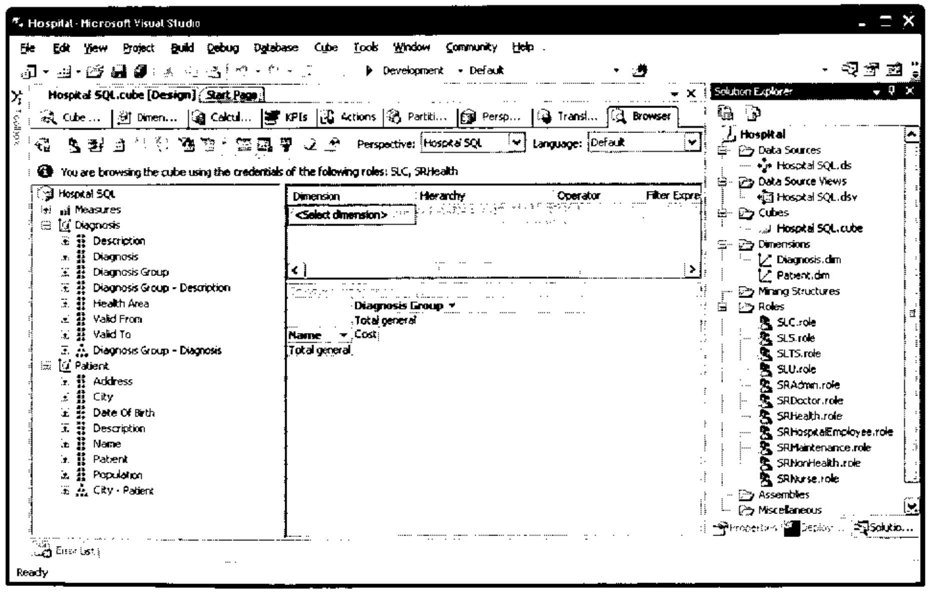
Figures 10 and 11 show screenshots of the code generated for this example by working with SSAS in which we can see the result of executing two queries that check a security rule defined at conceptual level that has been automatically translated at logical level by using the set of QVT rules defined and has been finally implemented in SSAS by obtaining the corresponding secure multidimensional code from this logical model. At conceptual level, in our PIM model (Figure 6), we have define a security constraint over "Patient" dimension that permits accesses to security level secret and upper and security roles "Health", "Admin" and their descendants. When logical models are obtained from this conceptual model by applying our set of QVT rules (see Figure 9), this security constraint is transformed into dimension permissions that deny accesses to unauthorized roles (security levels "SLC" and "SLU", and security roles distinct to authorized roles).



You are browsing the cube using the credentials of the following roles: SLS, SRHealth

	Diagnosis Group						
	1	2	3	4	5	6	Total general
Name	Cost	Cost	Cost	Cost	Cost	Cost	Cost
andrew			1000000				1000000
james	200						200
jenny	200						200
jerry				20000	600000	800000	1420000
jones				5000		6000	11000
sarah		300000					300000
susan		1000000					1000000
tom			900000				900000
will			900000				900000
Total general	400	1300000	2800000	25000	600000	806000	5531400

Fig. 10. SSAS implementation for hospital: authorized query



You are browsing the cube using the credentials of the following roles: SLC, SRHealth

	Diagnosis Group
	Total general
Name	Cost
Total general	

Fig. 11. SSAS implementation for hospital: unauthorized query

Firstly, an authorized user with the security level "Secret" ("SLS" role at the logical level) and the security role "Health" ("SRHealth" role at the logical level) makes a query involving attributes from the "Diagnosis" and "Patient" dimensions. Figure 10 shows the result of this query. Next, an unauthorized user with a lower security level, "Confidential" ("SLC" role at the logical level) and the same security role, "Health", makes the same query, but in this case it is an unauthorized query and the requested information is hidden. Figure 11 shows the result of this unauthorized query.

5 Conclusions

This work shows the advantages of applying an MDA approach to the development of DWs by analyzing PIM to PSM and PSM to code transformations, which is then applied to an example. This approach allows us to automatically develop DWs, thus saving time and money and obtaining better quality and security by translating the requirements identified at early stages of development into the final implementation.

We have defined the necessary metamodels at the logical level (PSM), multidimensional secure code for a specific OLAP platform (SSAS) and the transformations to obtain PSM from conceptual models defined according to our SECDW metamodel and secure multidimensional code in SSAS from PSM. Furthermore, we have analyzed an example in which we have obtained secure multidimensional PSM and code from a conceptual model of a hospital.

In future works, we intend to improve our MDA architecture for the development of secure DWs in several ways. New security rules and constraints will be included in our ACA model in order to consider the security threats related to specific OLAP operations such as navigations or inferences. These transformations from PIM with which to include the advanced security rules defined in SECDW will be extended by using OCL notes, and we shall also define the transformation from PSM to code for other OLAP tools such as Pentaho and Oracle, and the inverse transformations from code to PSM and PIM.

Acknowledgments. This research is part of the ESFINGE (TIN2006-15175-C05-05) and METASIGN (TIN2004-00779) Projects financed by the Spanish Ministry of Education and Science, and of the MISTICO (PBC-06-0082) Project financed by the FEDER and the Regional Science and Technology Ministry of Castilla-La Mancha (Spain).

References

1. Dhillon, G., Backhouse, y.J.: Information system security management in the new millennium. Communications of the ACM 43(7), 125–128 (2000)
2. Mouratidis, H., Giorgini, y.P.: An Introduction. In: Integrating Security and Software Engineering: Advances and Future Visions. Idea Group Publishing (2006)
3. MDA, O.M.G., Model Driven Architecture Guide (2003)
4. OMG, MOF QVT final adopted specification (2005)
5. OMG, Meta Object Facility (MOF) specification (2002)
6. Fernández-Medina, E., Trujillo, J., Piattini, y.M.: Model Driven Multidimensional Modeling of Secure Data Warehouses. European Journal of Information Systems 16, 374–389 (2007)

7. Katic, N., Quirchmayr, G., Schiefer, J., Stolba, M., Tjoa, y.A.: A Prototype Model for DW Security Based on Metadata. In: en 9th Int. Workshop on DB and Expert Systems Applications, Vienna, Austria (1998)
8. Kirkgöze, R., Katic, N., Stolda, M., Tjoa, y.A.: A Security Concept for OLAP. In: en 8th Int. Workshop on Database and Expert System Applications, Toulouse, France (1997)
9. Priebe, T., Pernul, y.G.: A Pragmatic Approach to Conceptual Modeling of OLAP Security. In: en 20th Int. Conference on Conceptual Modeling, Yokohama, Japan (2001)
10. Mazón, J.-N., Trujillo, y.J.: An MDA approach for the development of data warehouses. Decision Support Systems 45(1), 41–58 (2008)
11. Soler, E., Stefanov, V., Mazón, J.-N., Trujillo, J., Fernández-Medina, E., Piattini, y.M.: Towards Comprehensive Requirement Analysis for Data Warehouses: Considering Security Requirements. In: en Proccedings of The Third International Conference on Availability, Reliability and Security (ARES). IEEE Computer Society, Barcelona (2008)
12. Yu, E.: Towards modelling and reasoning support for early-phase requirements engineering. In: en 3rd IEEE International Symposium on Requirements Engineering (RE 1997), Washington, DC (1997)
13. Fernández-Medina, E., Trujillo, J., Villarroel, R., Piattini, y.M.: Developing secure data warehouses with a UML extension. Information Systems 32(6), 826–856 (2007)
14. Soler, E., Trujillo, J., Fernández-Medina, E., Piattini, y.M.: SECRDW: An Extension of the Relational Package from CWM for Representing Secure Data Warehouses at the Logical Level. In: en International Workshop on Security in Information Systems, Funchal, Madeira, Portugal (2007)
15. Luján-Mora, S., Trujillo, J., Song, y.I.-Y.: A UML profile for multidimensional modeling in data warehouses. Data & Knowledge Engineering 59(3), 725–769 (2006)
16. Fernández-Medina, E., Trujillo, J., Villarroel, R., Piattini, y.M.: Access control and audit model for the multidimensional modeling of data warehouses. Decision Support Systems 42(3), 1270–1289 (2006)
17. Blanco, C., Fernández-Medina, E., Trujillo, J., Piattini, y.M.: Implementing Multidimensional Security into OLAP Tools. In: en Third International Workshop Dependability Aspects on Data WArehousing and Mining applications (DAWAM 2008). IEEE Computer Society, Barcelona (2008)

Appendix A: Acronyms

ACA: Access Control and Audit model
AR: Audit Rule
AUR: Authorization Rule
C: Confidential
CIM: Computer Independent Model
CWM: Common Warehouse Metamodel
DAC: Discretional Access Control
DBMS: Database Management System
DW: Data Warehouse
MDA: Model Driven Architecture
MDSCL: Multidimensional Security Constraint Language
MDX: Multidimensional Expressions
MOF: Meta-Object Facility
OCL: Object Constraints Language
OLAP: On-Line Analytical Processing
OMG: Object Management Group
PIM: Platform Independent Model
PSM: Platform Specific Model
QVT: Query / Views / Transformations
RBAC: Role-Based Access Control
S: Secret
SC: Security Compartment
SIAR: Sensitive Information Assignment Rule
SL: Security Level
SR: Security Role
SSAS: SQL Server Analysis Services
TS: Top Secret
U: Undefined

Trusted Reputation Management Service for Peer-to-Peer Collaboration*

Lingli Deng, Yeping He, and Ziyao Xu

Institute of Software, Chinese Academy of Sciences
No.4 NanSi Street, ZhongGuanCun, Beijing, 100190, P.R. China
{denglingli,yphe,ccxu}@ercist.iscas.ac.cn

Abstract. The open and autonomous nature of peer-to-peer (P2P) systems invites the phenomenon of widespread decoys and free-riding. Reputation systems are constructed to ensure file authenticity and stimulate collaboration. We identify the authenticity, availability and privacy issues concerning the previous reputation management schemes. We propose to add integrity control for the reputation storage/computation processing in order to enhance the authenticity of the resultant reputation values; and present an integrity model to articulate necessary mechanisms and rules for integrity protection in a P2P reputation system. We design a fully-distributed and secure reputation management scheme, Trusted Reputation Management Service (TRMS). Employing Trusted Computing and Virtual Machine Technologies, a peer's reputation values and specific transaction records can be stored, accessed and updated in a tamper-proof way by the Trusted Reputation Agent (TRA) on the same platform, which guarantees the authenticity of reputation values. Transaction partners exchange directly with each other for reputation values, services and transaction comments with no reliance on a remote third party, ensuring the availability of reputation and peers' privacy.

Keywords: P2P, reputation management, data integrity, trusted computing, virtual machine.

1 Introduction

The open and autonomous nature of peer-to-peer systems invites the phenomenon of inauthentic files and free-riding. Since anyone can freely join and leave the system, it is easy to inject undesirable data, ranging from decoy files (that are tampered with or do not work)[1] to malware[2], without the fear of being punished. The prevalence of free-riders, peers who attempt to use the resources of others without sharing with them their own resources, has been reported to degrade system performance in popular P2P networks [3][4][5][6]. Reputation systems are constructed in P2P systems to prevent the spread of malicious data and to stimulate collaboration of selfish peers. A reputation system collects, distributes, and

* Supported by the National High Technology Research and Development Program ("863" Program) of China under grants No.2007AA010601 and No.2006AA010201.

R. Meersman and Z. Tari (Eds.): OTM 2008, Part II, LNCS 5332, pp. 1069–1086, 2008.