ARES Conference

The International Dependability Conference

CONFERENCE INFORMATION

PAPERS BY SESSION

PAPERS BY AUTHOR

GETTING STARTED

TRADEMARKS

SEARCH

ARES 2009

16-19 March 2009

Fukuoka Institute of Technology
Fukuoka, Japan

Published by

IEEE computer society

CPS Conference Publishing Services

Message from ARES General Co-chairs

The Fourth International Conference on Availability, Reliability and Security (ARES 2009 – The International Dependability Conference) brings together researchers and practitioners in the area of dependability. ARES 2009 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 establishing collaborations between different sub-disciplines and building a strong community for further research.

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

- Elisa Bertino (Purdue University),
- Sushil Jajodia (George Mason University Fairfax)
- Eiji Okamoto (Tsukuba University).

From many submissions we have selected the 40 best for a presentation as full paper. The quality and quantity of submissions have improved considerably over the last years and the conference officers sometimes faced a difficult decision when selecting which papers should be accepted. This year's acceptance rate has decreased to 25% for full papers. 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.

General Co-chairs
Makoto Takizawa, *Sekei University, Japan*
A Min Tjoa, *Vienna University of Technology, Austria*

Message from ARES Workshops’ Co-chairs

Welcome to the Workshops of the 4th International Conference on Availability, Reliability and Security (ARES) which is held at the Fukuoka Institute of Technology, Fukuoka, Japan from March 16 -19, 2009.

The workshops are very important events for ARES as they provide an essential platform for researchers of various domains to present and discuss their current results. This year we can offer the conference attendees’ 10 workshops which range from “start-ups” to well-established ones supporting ARES the fourth year.

The succeeding listing comprises the workshops of ARES 2009:

1. The Forth International Workshop on Dependability Aspects on Data Warehousing and Mining applications (DAWAM-2009)
2. The Fourth International Workshop on Frontiers in Availability, Reliability and Security (FARES 2009)
3. The Third International Workshop on Secure Software Engineering (SecSE-2009)
4. The Third Workshop on Advances in Information Security (WAIS-2009)
5. The Second International Workshop on Digital Forensics (WSDF-2009)
6. The First International Workshop on Global Information Security for an Inclusive Information Society (GloSec-2009)
7. The First International Workshop on Sensor Security (IWSS-2009)
8. The First International Workshop on Organizational Security Aspects (OSA-2009)
9. The First International Workshop on Recent Innovations and Breakthroughs in Cryptography (RIBC-2009)
10. The First International Workshop on Security and Usability (SecUSAB-2009)

These workshops are organized each on specific topics and thus offer researchers the opportunity to learn from this rich multi-disciplinary experience. The Workshop Chairs would like to thank the workshop organizers for their great efforts and hard work in proposing the workshop, selecting the papers, the interesting programs and for the arrangements of the workshops during the conference days.

We are grateful to Amin Anjomshoaa for his excellent work and support with the Confdriver system. We also would like to thank the support of the webmasters’ team of ARES-2009 and CISIS-2009 conferences and the local organization team at Fukuoka Institute of Technology.

We would like to give special thanks to Mr. Yoji Unoki, Chairman of Board of Trustees of FIT for hosting CISIS-2009, providing the university facilities and his continuous support. We would like to thank Fukuoka Convention Bureau for their great support, help, advices and local arrangement. We are grateful to Fukuoka City and Human Line Corporation (HLC) for the financial support. We also thank Fukuoka Institute of Technology and Secure Business Austria as sponsors of our conference.

We hope you enjoy the workshops programs and proceedings.

ARES International Conference Workshops’ Co-chairs
Leonard Barolli, *Fukuoka Institute of Technology, Japan*
Stefan Jakoubi, *Secure Business Austria, Austria*
Simon Tjoa, *Secure Business Austria, Austria*

Conference Officers

General Co-chairs

Makoto Takizawa, *Sekei University, Japan*
A Min Tjoa, *Vienna University of Technology, Austria*

Program Committee Co-chairs

Arjan Durresi, *Indiana University Purdue University Indianapolis, USA*
Hiroaki Kikuchi, *Tokai University, Japan*
Edgar Weippl, *Vienna University of Technology, Austria*

Workshops Co-chairs

Leonard Barolli, *Fukuoka Institute of Technology, Japan*
Stefan Jakoubi, *Secure Business Austria, Austria*
Simon Tjoa, *Secure Business Austria, Austria*

ARES Program Committee

Jemal H. Abawajy, *Deakin University, Australia*
Rafael Accorsi*, University of Freiburg, Germany*
Andre Adelsbach, *Telindus PSF S.A., Luxembourg*
Vasilis Aggelis, *Piraeus Bank SA, Greece*
John Andrews, *Loughborough, University, United Kingdom*
Amin Anjomshoaa, *Secure Business Austria, Vienna*
Davide Balzarotti, *Eurecom - Sophia Antipolis, France*
Lisa Bartlett, *Loughborough University, United Kingdom*
Massimo Bartoletti, *Universita' di Pisa, Italy*
Bharat Bhargava, *Purdue University, USA*
Christophe Blanchet, *Centre National de la Recherche Scientifique Institut de Biologie et Chimie des Protéines, France*
Benjamin Böck, *Secure Business Austria, Vienna*
Stephane Bressan, *National University of Singapore, Singapore*
Luciano Burgazzi, *Ente per le Nuove tecnologie, l'Energia e l'Ambiente, Italy*
Kevin Butler, *Pennsylvania State University, USA*
Alexander Böhm, *University of Mannheim, Germany*
Francesco Cadini, *Polytechnic of Milan, Italy*
Lasaro Camargos, *Microsoft, USA*
Jan Camenisch, *IBM Research, Zurich*
Jiannong Cao, *Hong Kong Polytechnic University, China*
Barbara Carminati, *University of Insubria, Italy*
Jordi Castellà-Roca, *Rovira i Virgili University of Tarragona, Spain*
David Chadwick, *University of Kent, United Kingdom*
Surendar Chandra, *University of Notre Dame, USA*
Simon Christophe, *Nancy University, France*
Soon Ae Chun, *College of Staten Island/City University of New York, USA*
Nathan Clarke, *University of Plymouth, United Kingdom*
Ricardo Corin, *Microsoft Cambridge, United Kingdom*
George Davida, *University of Wisconsin at Milwaukee, USA*
Jacques Demerjian, *Communication & Systems, Homeland Security, France*
Beniamino Di Martino, *Second University of Naples, Italy*
Jochen Dinger, *Universitaet Karlsruhe, Germany*
Schahram Dustdar, *Vienna University of Technology, Austria*
Andreas Ekelhart, *Secure Business Austria, Vienna*
Christian Engelmann, *Oak Ridge National Laboratory, USA*
Yung-Chin Fang, *Dell Inc., USA*
Hannes Federrath, *University of Regensburg, Germany*
Christophe Feltus, *Centre de Recherche Public Henri Tudor, Luxembourg*
Stefan Fenz, *Secure Business Austria, Vienna*
Eduardo Fernandez Medina, *University of Castilla-La Mancha, Spain*
Vincenzo De Florio, *University of Antwerp, Belgium*
Vladimir Fomichov, *K.E. Tsiolkovsky Russian State Technological University, Russia*
Jordi Forné, *Universitat Politècnica de Catalunya, Spain*
Huirong Fu, *Oakland University, Michigan, USA*
Steven Furnell, *University of Plymouth, United Kingdom*
Javier Garcia-Villalba, *Complutense University of Madrid, Spain*
Karl Goeschka, *Vienna University of Technology, Austria*

Swapna Gokhale, *University of Connecticut, USA*
Gernot Goluch, *Secure Business Austria, Vienna*
Marcin Gorawski, *Silesian University of Technology, Poland*
Daniel Grosu, *Wayne State University, USA*
Michael Grottke, *University of Erlangen-Nuremberg, Germany*
Stephan Groß, *Technische Universität Dresden, Germany*
Le Gruenwald, *University of Oklahoma, USA*
Abdelkader Hameurlain, *Paul Sabatier University, France*
Marit Hansen, *Independent Centre for Privacy Protection, Kiel, Germany*
Yanxiang He, *Wuhan University, China*
Rattikorn Hewett, *Texas Tech University, USA*
Jimmy Huang, *York University, Canada*
Martin Gilje Jaatun, *SINTEF Information and Communication Technology, Norway*
Stefan Jakoubi, *Secure Business Austria, Austria*
Hai Jin, *Huazhong University of Science and Technology, China*
Jan Jurjens, *Munich University of Technology, Germany*
Kresimir Kasal, *Secure Business Austria, Vienna*
Stefan Katzenbeisser, *Technische Universität Darmstadt, Germany*
Holger Kenn, *University of Bremen, Germany*
Dong Seong Kim, *Duke University, USA*
Raphael Kunis, *Technische Universität Chemnitz, Germany*
Yih-Jiun Lee, *Department of Information Management, CTU, Taiwan*
Jun Li, *University of Oregon, USA*
Chae-Hoon Lim, *Sejong University, Korea*
Man Lin, St. Francis *Xavier University, Canada*
Hua Liu, *Xerox Labs, USA*
Jianhua Ma, *Hosei University, Japan*
Josef Makolm, *Federal Ministry of Finance, Austria*
Carsten Maple, *University of Luton, United Kingdom*
Keith Martin, *Royal Holloway, University of London, United Kingdom*
Rivalino Matias Jr., *Duke Electrical and Computer Engineering, USA*
Nasrullah Memon, *Aalborg University Esbjerg, Denmark*
Florian Michahelles, *ETH Zurich, Department of Management, Technology*
Geyong Min, *University of Bradford, United Kingdom*
George Mohay, *Queensland University of Technology, Australia*
Mattia Monga, *Universita` degli Studi di Milano, Italy*
Marina Mongiello, *Technical University of Bari, Italy*
Yi Mu, *University of Wollongong, Australia*
Thomas Neubauer, *Secure Business Austria, Vienna*
Jesper Buus Nielsen, *University of Aarhus, Denmark*
Thomas Nowey, *University of Regensburg, Germany*
Hong Ong, Oak, *Ridge National Laboratory, USA*
Jose A. Onieva, *Universidad de Málaga, Spain*
Maria Papadaki, *University of Plymouth, United Kingdom*
Lucia Draque Penso, *University of Mannheim, Germany*
Günther Pernul, *University of Regensburg, Germany*
Makan Pourzandi, *Ericsson Canada, Canada*
Gerald Quirchmayr, *University of Vienna, Austria*
Jean-Jacques Quisquater, *Universite Catholique de Louvain, Belgium*
Raghav Rao, *State University of New York at Buffalo, USA*
Indrajit Ray, *Colorado State University, USA*

Domenico Rosaci, *University "Mediterranea" of Reggio Calabria, Italy*
Bimal Roy, *Indian Statistical Institute, India*
Kouichi Sakurai, *Kyushu University, Japan*
Biplab Sarker, *Primal Fusion, Waterloo, Canada*
Christian Schläger, *Ernst & Young, Germany*
Rodrigo Schmidt, *École Polytechnique Fédérale de Lausanne, Switzerland*
Tony Shan, *Bank of America, USA*
Richard Sinnott, *University of Glasgow, United Kingdom*
Jill Slay, *University of South Australia, Australia*
Jon A. Solworth, *University of Illinois at Chicago*
Dieter Sommer, *IBM Research, Zurich*
Aaron Striegel, *University of Notre Dame, USA*
Tsuyoshi Takagi, *Future University, Hakodate, Japan*
Oliver Theel, *University of Oldenburg, Germany*
Marco Thorbruegge, *European Network and Information Security Agency, Greece*
Simon Tjoa, *Secure Business Austria, Vienna*
Juan-Carlos Trujillo Mondéjar, *University of Alicante, Spain*
Kalyan Vaidyanathan, *Sun Microsystems, USA*
Luca Vigano, *University of Verona, Italy*
Umberto Villano, *Universita' del Sannio, Italy*
Melanie Volkamer, *Institute of IT-Security and Security, University of Passau, Germany*
Carine Webber, *Universidade de Caxias do Sul, Brazil*
Yawen Wei, *Iowa State University, USA*
Edgar Weippl, *Secure Business Austria, Vienna*
Severin Winkler, *Secure Business Austria, Vienna*
Liudong Xing, *University of Massachusetts, USA*
Mariemma Yagüe, *University of Malaga, Spain*
Jeff Yan, *Newcastle University, United Kingdom*
Laurence T. Yang, *Saint Francis Xavier University, Canada*
Alec Yasinsac, *University of South Alabama, USA*
George Yee, *National Research Council, Canada*
Meng Yu, *Western Illinois University, Illinois*
Nicola Zannone, *University of Trento, Italy*
Jianhong Zhang, *North China University of Technology, China*
Liqiang Zhang, *Indiana University South Bend, USA*
Jianying Zhou, *Institute for Infocomm Research, Singapore*
Bo Zhu, *Concordia University, Canada*

2009 International Conference on Availability, Reliability and Security

ARES 2009

Table of Contents

Distributed Systems and Grid (ARES Full Papers)

SOA Security (ARES Full Papers)

Enterprise Security 1 (ARES Full Papers)

Intrusion and Fraud Detection (ARES Full Papers)

Enterprise Security 2 (ARES Full Papers)

Digital Forensics and Security in Communication (ARES Full Papers)

Availability and Reliability 1 (ARES Full Papers)

Cryptography (ARES Full Papers)

Software Security 1 (ARES Full Papers)

Software Security 2 (ARES Full Papers)

Availability and Reliability 2 (ARES Full Papers)

Privacy and Trust (ARES Full Papers)

Dependable Systems and Trusted Computing 1 (ARES Short Papers)

Dependable Systems and Trusted Computing 2 (ARES Short Papers)

Software Security (ARES Short Papers)

Privacy and Trust (ARES Short Papers)

Enterprise Security and Security Evaluation 1 (ARES Short Papers)

Enterprise Security and Security Evaluation 2 (ARES Short Papers)

Availability and Reliability (ARES Short Papers)

Authentication and Authorization (ARES Short Papers)

Cryptography 1 (ARES Short Papers)

Cryptography 2 (ARES Short Papers)

DAWAM 2009 - Security & Privacy Enhancement in DWHs

DAWAM 2009 - Intrusion and Network Attack Prevention

2009 International Conference on Availability, Reliability and Security

Applying an MDA-based approach to consider security rules in the development of Secure DWs

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
University of Castilla-La Mancha. Paseo de la Universidad, 4. 13071. Ciudad Real, Spain
{Carlos.Blanco, Ignacio.GRodriguez, Eduardo.Fdezmedina, Mario.Piattini}@uclm.es
[2] Dep. of Information Languages and Systems. Facultad de Informática
LUCENTIA Research Group. University of Alicante. San Vicente s/n. 03690. Alicante, Spain
jtrujillo@dlsi.ua.es

Abstract

Data Warehouses (DWs) manage crucial information for enterprises which must be protected from unauthorized accesses. The question of which security issues are present in all stages of the DW design is therefore of great importance when considering these security constraints in design decisions. We have used the Model Driven Architecture (MDA) approach to propose an MDA architecture with which to develop secure DWs, which defines secure models at different abstraction levels along with their automatic transformation between models. Our approach considers a multidimensional path towards On-Line Analytical Processing (OLAP) tools, but did not, until now, support the transformation of complex security rules from conceptual models. After carrying out a modification of our conceptual metamodel to support a better representation of security rules and to define several sets of transformation rules, this paper shows how to transform these security rules through an example.

1. Introduction

The correct management of confidentiality is a crucial aspect for the survival of enterprises which has been traditionally considered as an added value in the final stages of development. However, an early detection of security requirements affects design decisions, thus providing a greater assurance of information and a saving of time. Within the development of secure information systems it is therefore necessary to consider security in all stages of the development process [1], from early stages as a strong requirement to a final secure implementation.

Furthermore, Data Warehouses (DWs) store historical information for the decision making process which is very important for enterprises. Security constraints must therefore be defined in order to protect this information from unauthorized users who could access it by querying the DW in final tools.

Our proposal [2] thus develops secure DWs, including security issues, in all stages of the development process. It considers the special characteristics of DWs and security aspects on the basis of an Access Control and Audit (ACA) model [3] specifically developed for DWs in which the security classification of subjects and objects and the definition of several kinds of security rules is supported.

This proposal has also been aligned with a Model Driven Architecture (MDA) [4] and defines extensions of models at different abstraction levels. MDA provides a model driven software development based on the separation of the specification of the system functionality and its implementation. It permits the model to be defined at different abstraction levels (business, conceptual and logical levels) and the automatic transformation between models through the definition of transformations rules.

Our architecture was originally focused on a relational approach towards Data Base Management Systems (DBMS), providing a logical relational model. However, since the majority of DWs are managed by On-Line Analytical Processing (OLAP) tools over a

978-0-7695-3564-7/09 $25.00 © 2009 IEEE
DOI 10.1109/ARES.2009.68

multidimensional approach, our most recent research efforts have been focused on a logical multidimensional model which leads to eventual secure implementation in OLAP tools [5]. We have defined a multidimensional logical metamodel and transformation rules from conceptual models, considering some security issues, but our proposal did not until now completely support the transformation of all the types of security rules that can be defined with our ACA model.

Thus, this paper completes our work dealing with the automatic transformation of security rules from conceptual models to multidimensional logical models.

The remainder of this paper is organized as follows: Section 2 will present the research background on secure DW development; Section 3 will briefly introduce our complete MDA approach through which to develop secure DWs and upon which this work is focused; Section 4 will show how security rules defined in conceptual models are transformed into a multidimensional logical model; and finally, Section 5 will present our conclusions and future work.

2. Background

Within the field of information systems, one of the first and most relevant proposals that integrates security through the use of UML is UMLsec [6] which can be used to specify and evaluate UML security specifications using formal semantics.

Furthermore, Model Driven Security (MDS) [7] extends MDA in order to build secure information systems. Its designers specify the inclusion of security properties in high-level system models and use tools to automatically generate secure system architectures. Within the context of MDS, the same authors propose an extension of UML for modeling a generalized role based access control called SecureUML [8]. These proposals are interesting contributions for information systems but do not deal with DWs in the context of taking their specific security issues into consideration.

Traditionally, security in DWs was taken into account in the final stage of development. Several works [9-11] exist which deal with a secure implementation in OLAP tools by using a discretional access control (DAC) security policy and a simplified concept of user role defined as subject. The most interesting proposal is [11] which is based on a representation of DWs at the conceptual level with ADAPTed UML, and in which the authors analyze security requirements and their implementation in SQL Server Analysis Services (SSAS). They extend multidimensional expressions (MDX) with hide statements (for cubes, dimensions, etc.), to create a Multidimensional Security Constraint Language (MDSCL). These works do not include security in the entire development process and are focused on the last stages. Although other interesting proposals through which to model DWs at conceptual and logical levels and which consider special characteristics of DWs also exist, they do not support security issues.

In order to early detect security requirements and to consider them in all DW's development stages, Fernández-Medina et al. propose an MDA approach with which to develop secure DWs [2]. This allows us to define models and security constraints at different abstraction levels, and to support the automatic transformation between models and the generation of secure code for final tools.

3. Developing Secure DWs with an MDA approach

This section briefly presents our MDA architecture with which to develop secure DWs [2]. It is composed of several models at different abstraction levels (business, conceptual and logical), and the automatic transformation between them (see Figure 1).

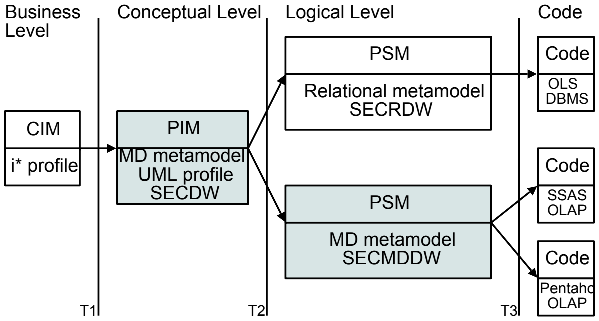

Fig. 1 MDA architecture for secure DWs

In order to include security requirements in a Computational Independent Metamodel (CIM) at the business level from an early stage, we have defined a UML profile [12] which extends i*, a requirement engineering framework centered on agents and their intentional characteristics. Moreover, in order to conceptually design the DW we have defined a Platform Independent Metamodel (PIM) called SECDW [13], a UML profile for DWs which has been improved with an access control and audit model (ACA) [3].

At the logical level, two Platform Specific Metamodels (PSM) have been proposed as extensions of Common Warehouse Metamodel (CWM) packages, and the corresponding transformations from the conceptual level have also been defined by using Query / View / Transformation (QVT) rules. On the one hand we have a relational path composed of a logical relational metamodel called SECRDW [14] and the final implementation into DBMS by using Oracle Label Security.

On the other hand, a multidimensional path improves this architecture, providing a logical multidimensional metamodel called SECMDDW and dealing with the final implementation in a certain OLAP tool, SQL Server Analysis Services [5]. This is an interesting improvement since the majority of DWs are managed with OLAP tools over a multidimensional approach. However, although our proposal considers structural aspects and security constraints, the transformation of security rules has not, until now, been completely supported. This paper fulfills the transformation from conceptual models to multidimensional logical models supporting the different kinds of security rules which can be defined using our ACA model [3]. Next, the final implementation in OLAP tools can be easily obtained from this multidimensional logical model. This implementation has been studied in [15] for a certain OLAP tool, SQL Server Analysis Services (SSAS).

4. Supporting security rules

Our ACA model [3] was specifically designed for DWs and allows us to classify subjects and objects in three ways: in security levels (SL) which represent user's clearance levels; in security roles (SR) of a hierarchical role structure; and in horizontal groups called security compartments (SC).

It also specifies three kinds of security rules: Sensitive Information Assignment Rules (SIAR) which allow us to define sensitivity information for each element in the multidimensional model over a multilevel security policy; 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.

The automatic transformation of security rules from conceptual models is not a trivial task. Complex security rules can be expressed by using Object Constraint Language (OCL) expressions which are difficult to analyze and which include information about subjects, objects, conditions, security information, privileges, log types, etc.

In order to include security rules support in our approach we have improved our conceptual metamodel to include the security information from OCL expressions in the model. Moreover, in order to obtain secure multidimensional logical models automatically, the set of transformation rules has been completed with a new set of QVT transformations for security rules. In this section, the generation of security rules at the logical multidimensional level is shown by using an application example of a web store sales service.

4.1. Secure conceptual model

Figure 2 shows the conceptual model of our example, defined according to the SECDW profile (further details can be found in [13]). The DW manages sales (secure fact class "Sale") with information concerning their cost and whether the delivery is confidential or not. Furthermore, sales information is classified in two dimensions: "Product" with information relating to identification, name and base cost of products, and "Customer", which contains clients' information regarding identification, postal address and bank account. Customers are additionally aggregated by distribution zones through the use of a "Distribution Network" base class.

The security classification used in this example is as follows: two security levels, top secret (TS) and secret (S); and one security compartment for each delivery zone (USA, Europe and Asia). The security roles have not been defined in this example because the DW is only queried by one user role: web store administrators.

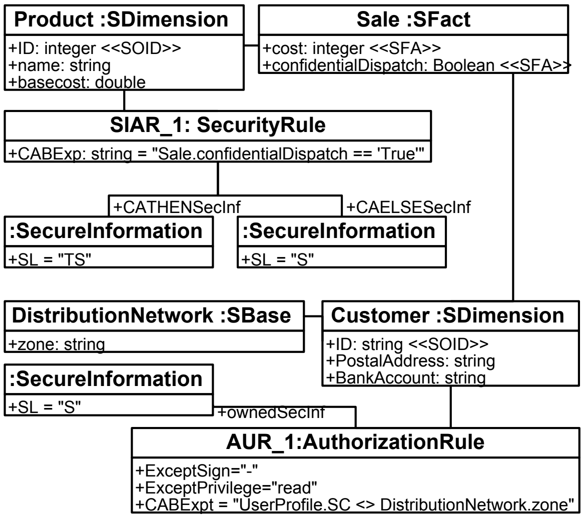

Fig. 2 Conceptual model

Various security rules have also been defined. There is one sensitive information assignment rule (SIAR) which establishes a “Top Secret” security level for information concerning products if the delivery is confidential (confidentialDispatch == true) or a “Secret” security level if it is a normal delivery.

Moreover, a negative authorization security rule (AUR) hides customers’ information from users with a low security level (Secret) according to the distribution areas (”Zone” attribute of “DistributionNetwork”). That is, users with the security level “Secret” can read customers’ data from the same distribution zone (for instance, USA), but not the remaining information (for instance, Europe and Asia).

4.2. Secure multidimensional logical model

Once the conceptual model has been defined, QVT transformation rules are applied to generate a multidimensional logical model according to the SECMDDW metamodel [16]. This metamodel is composed of three metamodels: a “security configuration metamodel” which represents the roles of a role based access control (RBAC) policy; a “cube metamodel” which defines the structural aspects of cubes, measures and hierarchies and security constraints with cube and cell permissions; and finally, a “dimension metamodel” with structural information concerning dimensions, attributes and base classes, and security issues which use permissions over dimensions and attributes.

Transformations are composed of several sets of rules (see Figure 3) which obtain a DW security configuration (SECDW2Role), structural aspects and security constraints related to cubes (SECDW2Cube) and dimensions (SECDW2Dimension).

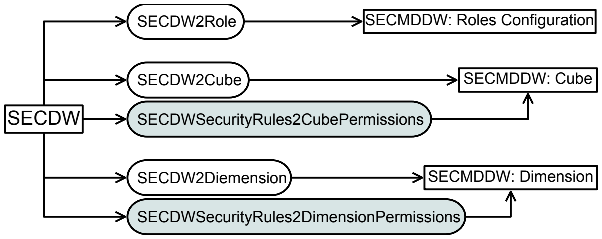
SECDW
SECDW2Role
SECMDDW: Roles Configuration
SECDW2Cube
SECMDDW: Cube
SECDWSecurityRules2CubePermissions
SECDW2Diemension
SECMDDW: Dimension
SECDWSecurityRules2DimensionPermissions

Fig. 3 Transformation rules

These transformations have been improved with two new sets which deal with security rules (SECDWSecurityRules2CubePermissions and SECDWSecurityRules2DimensionPermissions). This section shows how transformations are applied to our example, generating multidimensional logical models, focuses on security rules and briefly comments on the remaining transformations.

Firstly, **SECDW2Role** creates a role based security configuration at the logical level (see Figure 4). That is, it transforms each security level, compartment and role defined at the conceptual level into roles at the logical level in order to prepare the DW for the use of a role based access control policy. In our example the roles “SLTS” and “SLS” are generated for security levels “TS” and “S”, and “SCUSA”, “SCEurope” and “SCAsia” are generated for security compartments “USA”, “Europe” and “Asia”.

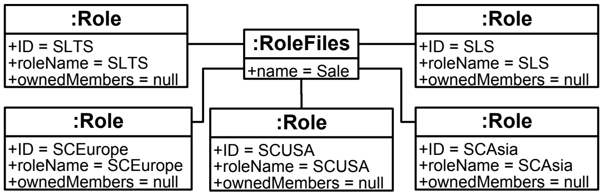

Fig. 4 MD logical model: security configuration

Next, structural aspects and some security issues for cubes and dimensions are generated by the **SECDW2Cube** transformation which creates the “Sales” cube and its associated measures and dimensions (see Figure 5), and by the **SECDW2Dimension** transformation which creates “Product” and “Customer” dimensions and the “DistributionNetwork” base with their related attributes (see Figure 6).

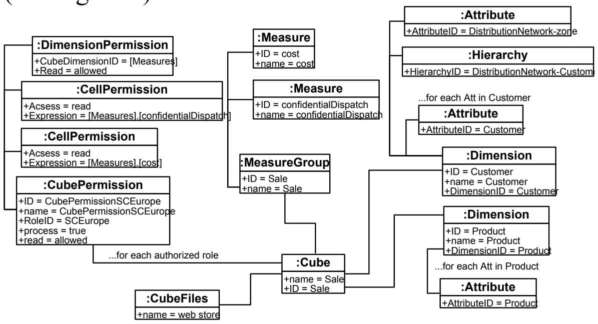

Fig. 5 MD logical model: cubes

The security rules are now analyzed and permissions at cube and dimension levels are defined. Firstly, the **SECDWSecurityRules2CubePermissions** transformation processes the SIAR and AUR security rules expressed respectively in the “SecurityRule” and“AuthorizationRule” of the PIM. Since, Fig. 2 includes neither SIAR nor AUR rules at cube level, this transformation is not activated, and therefore the cube logical model (and thus the PSM) is not modified with such security rules.

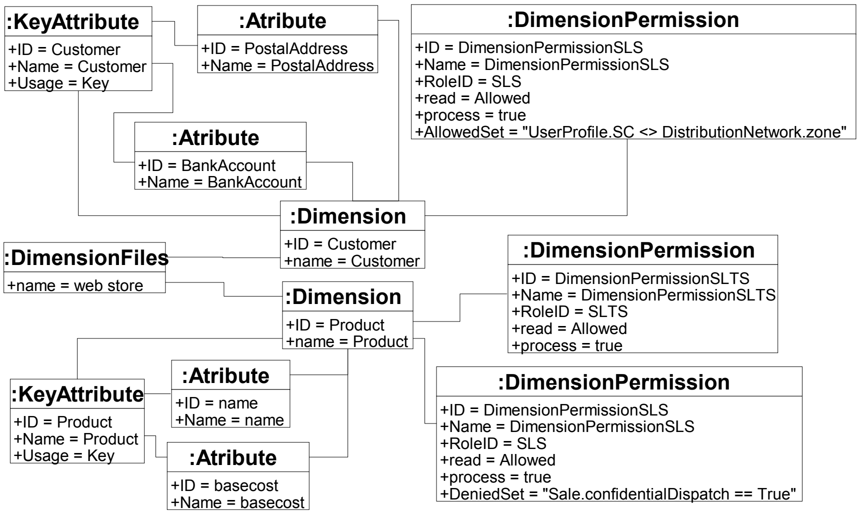

Fig. 6 MD logical model: dimensions

SECDWSecurityRules2DimensionPermissions This transformation processes the aforesaid SIAR and AUR rules from the PIM. In the example shown in Fig. 2 the "Product" dimension and the "Customer" dimension have a SIAR and an AUR rule respectively. This transformation has two main relations *processDimensionSIAR* and *processDimensionAUR,* each of which is intended to deal with the different kinds of security rules. For a better understanding, Table 1 and Table 2 show the flow of the execution for these relations. The rules of Table 1 are executed for the security rule SIAR_1 (which establishes a security level of Top Secret to read products' data).

The classes from the PIM which throw the rule have been included for each relation in the table. After executing the whole "processDimensionSIAR", the model shown in Fig. 6 is produced.

relation **processDimensionSIAR:** WebStore

relation **processDimensionSIAR:** SIAR_1
//authorizing
relation **createDimensionSIARForSLevel:** TS, Product
relation **authorizeSLevel:** TS, Product
//denying
relation **createDimensionSIARForSLevel:** S, Product
relation **denySLevel:** S, Product

Table 1 Flow of relations to process SIAR Rules

The AUR_1 authorization rule denies users with the security level "S" access to customers' data from a distribution zone which is different from that of the user compartment. Furthermore, in order to process the AUR_1 security rule the "processDimensionAUR" relation is thrown. Table 2 depicts the relations which are in turn executed to process the whole rule.

relation **processDimensionAUR:** WebStore
relation **processDimensionAUR:** AUR_1 relation **createDimensionAURForSLevel**: S, Customer relation **authorizeSLevelForAUR**: Customer, S, "UserProfile.SC <> DistributionNetwork.zone", "-"

Table 2 Flow of relations to process AUR Rules

After executing all the transformations, the MD logic model for Dimensions includes 2 "DimensionPermission" classes attached to the Product dimension (created from the SIAR_1 rule) and 1 "DimensionPermission" (created from the AUR_1 rule). These new classes place the semantic of the security rules from the PIM in the different PSMs.

5. Conclusions

An early detection of security requirements and the inclusion of security issues in all stages of the development process are crucial for the survival of enterprises, and our MDA approach supports a secure development of DWs.

This architecture initially only supported a relational path towards DBMS, but since the majority of DWs are managed over a multidimensional approach, it was recently improved with a multidimensional path towards OLAP tools. However, this improvement did not deal with complex security rules defined in conceptual models by using OCL expressions.

This work includes support for security rules in our MDA architecture, by modifying our conceptual metamodel to represent these security rules and defining sets of QVT transformations which automatically generate multidimensional logical models from conceptual models.

In future works, we intend to study the security problems related to OLAP operations and to improve our proposal with dynamic security models. We shall also define transformation rules from multidimensional logical models to other OLAP platforms such as Pentaho, and inverse transformations to support reengineering.

Acknowledges

This research is part of the ESFINGE (TIN2006-15175-C05-05) Project financed by the Spanish Ministry of Education and Science, and of the MISTICO (PBC-06-0082) and QUASIMODO (PAC08-0157-0668) Projects financed by the FEDER and the Regional Science and Technology Ministry of Castilla-La Mancha (Spain).

References

1. Mouratidis, H. and P. Giorgini, *An Introduction*, in *Integrating Security and Software Engineering: Advances and Future Visions*. 2006, Idea Group Publishing.
2. 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.
3. Fernández-Medina, E., et al., *Access Control and Audit Model for the Multidimensional Modeling of Data Warehouses.* Decision Support Systems, 2006. **42**: p. 1270-1289.
4. MDA, O.M.G., *Model Driven Architecture Guide.* 2003.
5. Blanco, C., et al., *Applying QVT in order to implement Secure Data Warehouses in SQL Server Analysis Services.* Journal of Research and Practice in Information Technology, 2008. **In Press**.
6. Jürjens, J., *Secure Systems Development with UML*. 2004: Springer-Verlag.
7. Basin, D., J. Doser, and T. Lodderstedt, *Model Driven Security: from UML Models to Access Control Infrastructures.* ACM Transactions on Software Engineering and Methodology, 2006. **15**(1): p. 39-91.
8. Lodderstedt, T., D. Basin, and J. Doser. *SecureUML: A UML-based modeling language for model-driven security*. in *UML 2002. The Unified Modeling Language. Model Engineering, Languages Concepts, and Tools. 5th International Conference*. 2002. Dresden, Germany: Springer.
9. Katic, N., et al. *A Prototype Model for Data Warehouse Security Based on Metadata*. in *9th International Workshop on Database and Expert Systems Applications (DEXA'98)*. 1998. Vienna, Austria.: IEEE Computer Society.
10. Kirkgöze, R., et al. *A Security Concept for OLAP*. in *8th International Workshop on Database and Expert System Applications (DEXA'97)*. 1997. Toulouse, France: IEEE Computer Society.
11. Priebe, T. and G. Pernul. *A Pragmatic Approach to Conceptual Modeling of OLAP Security*. in *20th International Conference on Conceptual Modeling (ER 2001)*. 2001. Yokohama, Japan: Springer-Verlag.
12. Soler, E., et al. *Towards Comprehensive Requirement Analysis for Data Warehouses: Considering Security Requirements*. in *Proccedings of The Third International Conference on Availability, Reliability and Security (ARES)* 2008. Barcelona, Spain: IEEE Computer Society.
13. Fernández-Medina, E., et al., *Developing Secure Data Warehouses with a UML extension.* Information Systems, 2007. **32**(6): p. 826-856.
14. Soler, E., et al., *Building a secure star schema in data warehouses by an extension of the relational package from CWM.* Computer Standard and Interfaces, 2008. **30**(2008): p. 341-350.
15. Blanco, C., et al., *How to Implement Multidimensional Security into OLAP Tools.* Int. J. of Business Intelligence and Data Mining - IJBIDM, 2008. **3**(3): p. 255.
16. Blanco, C., et al. *Obtaining secure code in SQL Server Analysis Services by using MDA and QVT*. in *6th International Workshop on Security in Information Systems, WOSIS 2008*. 2008. Barcelona. Spain.