Proceedings

DEXA

ARES 2007

In Cooperation with

enisa European Network and Information Security Agency

TU WIEN Technische Universität Wien Vienna University of Technology

[SECURE] Business Austria

Oesterreichische Computer Gesellschaft Austrian Computer Society

IEEE Computer Society Conference Publications Operations Committee

CPOC Chair

Phillip Laplante
Professor, Penn State University

Board Members

Mike Hinchey, *Director, Software Engineering Lab, NASA Goddard*
Linda Shafer, *Professor Emeritus, University of Texas at Austin*
Jeffrey Voas, *Director, Systems Assurance Technologies, SAIC*
Thomas Baldwin, *Manager, Conference Publishing Services* (CPS)

IEEE Computer Society Executive Staff

David Hennage, *Executive Director*
Angela Burgess, *Publisher*

IEEE Computer Society Publications

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

IEEE Computer Society *Conference Publishing Services* (CPS)

The IEEE Computer Society produces conference publications for more than 200 acclaimed international conferences each year in a variety of formats, including books, CD-ROMs, USB Drives, and on-line publications. For information about the IEEE Computer Society's *Conference Publishing Services* (CPS), please e-mail: tbaldwin@computer or telephone +1-714-821-8380. Fax +1-714-761-1784. Additional information about the IEEE Computer Society's *Conference Publishing Services* (CPS) can be accessed from our web site at: *http://www.computer.org/cps.*

IEEE Computer Society / Wiley Partnership

The IEEE Computer Society and Wiley partnership allows the CS Press *Authored Book* program to produce a number of exciting new titles in areas of computer science and engineering with a special focus on software engineering. IEEE Computer Society members continue to receive a 15% discount on these titles when purchased through Wiley or at: *http://wiley.com/ieeecs*. To submit questions about the program or send proposals, please e-mail: dplummer@computer.org or telephone +1-714-821-8380. Additional information regarding the Computer Society's authored book program can also be accessed from our web site at: *http://www.computer.org/portal/pages/ieeecs/publications/books/about.html.*

Revised: 17 August 2006

New *CPS Online* Workspace

An IEEE Online Collaborative Publishing Environment

We're proud to announce the launch of ***CPS Online***, a new IEEE online collaborative conference publishing environment designed to speed the delivery of price quotations and provide conferences with anytime access to all of a project's publication materials during production, including the final papers. **CPS Online**'s workspace gives a conference the opportunity to upload files through any Web browser, check status and scheduling on a project, make changes to the Table of Contents and Front Matter, approve editorial changes and proofs, and communicate with a CPS editor through discussion forums, chat tools, commenting tools and e-mail.

The following is the URL link to the CPS Online Publishing Inquiry Form:
http://www.ieeeconfpublishing.org/cpir/inquiry/cps_inquiry.html

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

IEEE Computer Society Order Number P2775
Library of Congress Number 2007922437
ISBN 0-7695-2775-2

The Second International Conference on Availability, Reliability and Security

DEXA

ARES 2007

10 - 13 April 2007

Vienna, Austria

In Cooperation with

enisa European Network and Information Security Agency

TU WIEN Technische Universität Wien Vienna University of Technology

[SECURE] Business Austria

Österreichische Computer Gesellschaft Austrian Computer Society

IEEE Computer Society

IEEE

Los Alamitos, California

Washington • Tokyo

CPS Conference Publishing Services

IEEE Computer Society Order Number P2775
ISBN 0-7695-2775-2
ISBN 978-0-7695-2775-8
Library of Congress Number 2007922437

Additional copies may be ordered from:

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

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: + 1 732 981 0060
Fax: + 1 732 981 9667
http://shop.ieee.org/store/
customer-service@ieee.org

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

Individual paper REPRINTS may be ordered at: <reprints@computer.org>

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

Conference Publishing Services
http://www.computer.org/proceedings/

Table of Contents

Second International Conference on Availability, Reliability and Security (ARES 2007)

Session 1: Trust Model & Trust Management

Session 2: Availability, Fault-Tolerant & Recovery

Session 3: Reputation Management & Trust

Session 4: Privacy & Access Control

Session 5: Failure Detection & Attack Prevention

Session 6: Authentication & Authorisation

Session 7: Security Algorithm & Framework

Session 8: Software Security

Session 9: Security Models

Session 10: Miscellaneous Security Techniques

Session 11: eAuction & eVoting Protocol

Session 12: Dependability in Distributed & Ubiquitous Computing

Session 13: Anomaly & Intrusion Detection

International Symposium on Frontiers in Availability, Reliability and Security (FARES)

Session 1: Fault-Tolerant & Availability

Session 2: Access Control

Session 3: Authentication

Session 4: Real-Time System & Sensor Network

Session 5: RFID Techniques & Applications

Session 6: Secure Solution & Applications

Session 7: Security Issue in Business Management

Session 8: Web, XML, Content Management

Session 9: Security Policies & Techniques

Session 10: Trust Management & Trust Model

Session 11: Miscellaneous Applications

Second International Workshop Dependability Aspects on Data Warehousing and Mining Applications (DAWAM 2007)

2nd International Workshop Dependability and Security in e-Government (DeSeGov 2007)

Workshop on Foundations of Fault-tolerant Distributed Computing (FOFDC 2007)

First International Workshop on Secure Software Engineering (SecSE 2007)

Workshop on "Modeling, Designing, and Testing Correct, Secure, and Dependable Event-Based System" (EBITS 2007)

First International Workshop on Advances in Information Security (WAIS 2007)

Workshop on "Security in E-Learning" (SEL)

Message from the Organizing Committee

Security, Reliability and Availability of IT systems and infrastructures have for over two decades been core research areas in the field of IT Security. Recent strategic research foci, especially in the European Union, have renewed the interest in the area and are setting the stage for very interesting and challenging developments, in areas ranging from the use of IT for increasing security in general, to the security of critical IT infrastructures and legal, economic and social issues. That is why ARES 2007, like ARES 2006 before, is again designed to serve as a bridge and discussion forum for researchers and practitioners.

We are therefore very pleased to have this conference for a second time organised in cooperation with ENISA (The European Network and Information Security Agency). ENISA supports the idea of this conference due to the urgent need of scientific research and the dissemination of new techniques in these areas.

We hope that this years ARES conference will again have a significant benefit for innovative applications which have to consider the various dependability issues and furthermore will build a platform for in-depth discussions between researchers in the different areas of Dependability, such as Availability, Reliability, and Security.

We have received 212 competed, on time submitted papers amongst over 250 abstract submissions from 43 countries for ARES 2007 and the Program Committee eventually selected 59 papers, making an acceptance rate of 27,83 % of submitted papers.

Seven workshops are organised on special topics of ARES, i.e.-

- Workshop "Dependability Aspects on Data Warehousing and Mining applications" (DAWAM 2007)
- Workshop "Dependability and Security in e-Government" (DeSeGov 2007)
- Workshop "Foundations of Fault-tolerant Distributed Computing" (FOFDC 2007)
- Workshop "Secure Software Engineering" (SecSE 2007)
- Workshop "Modeling, Designing, and Testing Correct, Secure, and Dependable Event-Based System" (EBITS 2007).
- Workshop "Advances in Information Security" (WAIS 2007)
- Workshop: Security in E-Learning (SEL 2007)

As an additional feature of ARES we have invited distinguished scientists for the International Symposium on Frontiers in Availability, Reliability and Security (FARES) to present and discuss special aspects relevant for future applications and research. We would like to express our gratitude to all program committee members, workshop organisers and committee members and all the external referees who reviewed the papers very profoundly and in a timely manner. Due to the high number of submissions and the high quality of the submitted papers, the reviewing, and discussion process was an extraordinarily challenging task.

Special thanks must be given to Dr. Tho Manh Nguyen for all his essential support in the organization of the PC-tasks of ARES 2007. We would also like to thank all the authors who submitted their papers to *ARES 2007* as their contributions built the basis of this year's excellent technical program. Many thanks go to Ms. Gabriela Wagner for her invaluable support with administrative issues.

Norman Revell, *Middlesex University, United Kingdom*

Roland Wagner, *University of Linz, Austria*

Honorary Co-Chairs

Günther Pernul, *University of Regensburg, Germany*

Makoto Takizawa, *Tokyo Denki University, Japan*

General Co-Chairs

Gerald Quirchmayr, *University of Southern Australia, Australia*

A Min Tjoa, *Vienna University of Technology, Austria*

Program Co-Chairs

A Framework for the Development of Secure Data Warehouses based on MDA and QVT

Emilio Soler[1], Juan Trujillo[2], Eduardo Fernández-Medina[3] and Mario Piattini[3]
(1) Departamento de Informática. University of Matanzas,Cuba
Autopista de Varadero km 3. Matanzas. Cuba.
esolercu@yahoo.es, http://www.umcc.cu
(2) Departamento de Lenguajes y Sistemas Informáticos. University of Alicante, Spain
C/ San Vicente S/N 03690 Alicante, Spain
jtrujillo@dlsi.ua.es, http://www.dlsi.ua.es
(3) Grupo ALARCOS, Departamento de Tecnologías y Sistemas de Información
Centro Mixto de Investigación y Desarrollo de Software UCLM-Soluziona
University of Castilla-La Mancha
Paseo de la Universidad, 4 – 13071 Ciudad Real, Spain
{eduardo.fdezmedina, mario.piattini}@uclm.es, http://www.uclm.es

Abstract

Data warehouses (DWs) store historical and aggregated information, extracted from multiple heterogeneous, autonomous and distributed sources of information, therefore it is essential to specify security measures from early stages of DW design and to enforce them. Several proposals on DW development have arised in the last couple of years. However, few approaches represent security measures in the DW conceptual model starting from early stages of development of a DW project. In addition, these security measures cannot be automatically represented at logical level, so heuristic design guides for such transformations have appeared. This paper presents a framework based on Model Driven Architecture (MDA) for the development of secure data warehouses that covers all the phases of design (conceptual, logical and physical) and embeds security measures in all of them. Moreover, transformations between models are clearly and formally established by using Query/View/Transformation (QVT), to obtain consequently a traceability of the security rules from the early stages of development to the final implementation.

1. Introduction

In the last years, there have been several initiatives to include security in the DW design [1-4], many of them being focused on specific aspects related to access control, multilevel security, federated databas applications, commercial tools applications, e However, [5, 6] propose an access and audit cont model integrated with an Unified Modeling Langua (UML) extension, this allowing the developmen secure multidimensional models at conceptual lev This proposal is promising, but still it does not cov all the stages of a DW development cycle.

The new standard that addresses the complete li cycle of developing applications by using models software development is arising: Model Drive Architecture (MDA) [7]. In the MDA technolog the standard for defining transformations is Meta Object Facility (MOF) 2.0 Query /View Transformations (QVT) [8].

Current specialized literature comprises seven proposals to integrate security with the MDA technology [9-12], but all of them are related wit information systems, access control, securit services and secure distributed applications, so non of them, is related with the design of secure DWs.

This article proposes a methodological approximation for the development of secure dat warehouses using MDA and QVT. This proposal is natural continuation of our previous work [13] an of the results presented in [5, 6, 14]. Our mai objective is the proposal of an architecture tha transforms security requirements from the conceptual level up to the logical level.

The rest of this article is structured as follow Section 2 presents the main aspects related to the MDA

0-7695-2775-2/07 $25.00 ©2007 IEEE

chnology and the QVT transformations. Section 3 sents a framework for the development of secure ata warehouses, by employing MDA and QVT. Finally, section 4 presents the main conclusions and outlines immediate future work.

2 MDA-QVT: an overview

This section summarizes the main characteristics of MDA and of QVT transformations.

MDA promotes the specification of a Platform Independent Model (PIM) that does not contain information specific to the platform or to the technology to be used to develop it. This PIM can be transformed into one or several Platform Specific Models (PSMs) by including platform and development technology specific information. Later, each PSM is implemented into code to be executed on a platform in order to obtain the final software product.

Besides these models, a Computation Independent Model (CIM) is provided by MDA as means of modeling requirements.

QVT specification has a hybrid declarative / imperative nature, with the declarative part being split into two-level architecture [8]: Relations and Core metamodels. In the relations metamodel, the model transformation between model candidates is specified as a set of relations. These relations must hold for a successful model transformation. In the imperative style, a Black-box implementation of operations can also be used to allow reuse of existing algorithms or domain specific libraries in certain model transformations. In this paper we focus on the QVT relations.

3 A framework for the development of secure data warehouses

This section integrates MDA and QVT with the multidimensional modeling of secure data warehouses. Subsections 3.1 and 3.2 introduce an Secure Multidimensional PIM (SMD PIM) and an Secure Multidimensional PSM (SMD PSM). In subsection 3.3 we define QVT relations that allow us to represent at logical level all security and audit requirements captured at the stage of conceptual modeling of the secure data warehouses. We do not comment on the way the code is obtained, as it is out of our scope.

Figure 1 illustrates through a diagram the Secure Multidimensional MDA architecture for the development of secure data warehouses. The upper part presents the CIM that defines the requirements for the DW. It represents a perspective on the DW within its business environment, so it plays an important role in reducing the gap between those who are experts in the domain and their requirements and those who are experts in the design and development of the DW which needs to satisfy the requirements.

By means of the transformation T_1 in Figure 1 we obtain the Secure Multidimensional PIM, which is located at conceptual level. The T_2 transformation derives the Secure Multidimensional PSM (SMD PSM). This transformation is not unique, as other secure PSMs are possible. This is why on the left hand side of the area corresponding to the logical level a secure relational platform is represented, while on the right hand side of the same area any other secure platform is represented.

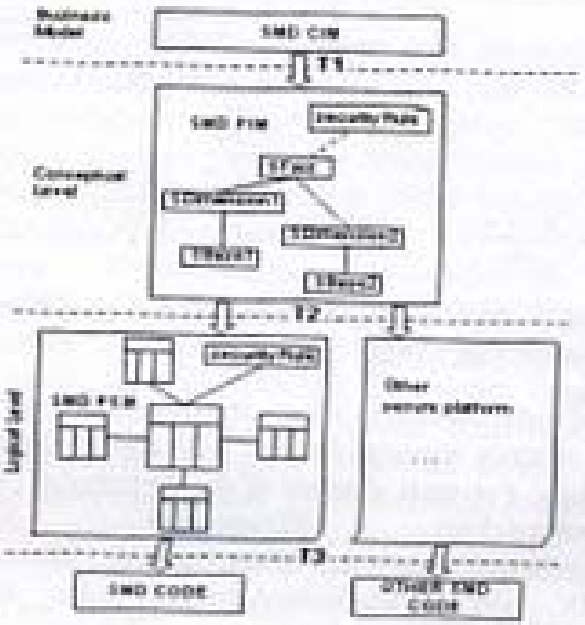

Figure 1. A framework for the development of secure data warehouses

Starting from each SMD PSM code is derived for the target platform. This code is called Secure Multidimensional Code, (SMD Code) and is represented in the lower part of Figure 1. It is to be noted how the security restriction defined using OCL (represented as an UML note) is transformed from the conceptual level to the logical level by means of T_2, and later transformed in code by means of T_3.

3.1 Definition of the SMD PIM

The UML profile presented in [6], called Secure Data Warehouse (SECDW), allows us to represent the main security requirements for the conceptual modeling of the DW. Figure 2 represents the SECDW metamodel, while omitting certain attributes to make the metamodel more comprehensible.

As security requirements are modeled in this PIM, it is therefore denominated as SMD PIM (Secure Multidimensional PIM). The main characteristics of this metamodel are the many-to-many relations between facts and specific dimensions, degenerated dimensions, the multiple classifications and the alternative path of hierarchy, as well as non-strict and complete hierarchies. The UserProfile metaclass contains information on each user's right of access to the multidimensional model.

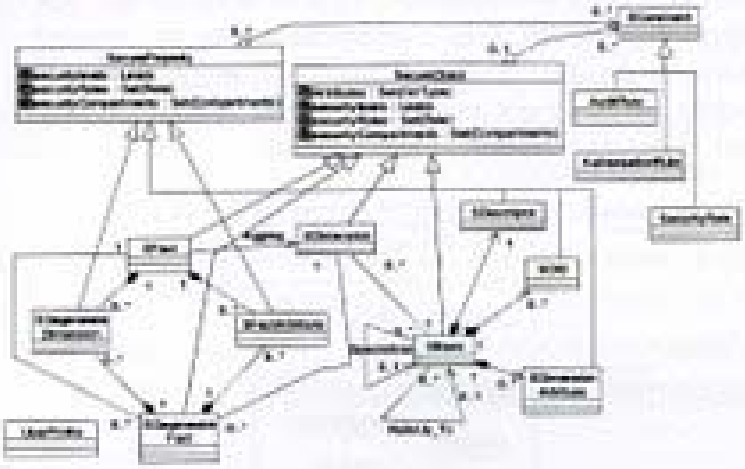

Figure 2. The SECDW metamodel used in the design of SMD PIM

The metamodel also allows the representation of the main security aspects for the DW multidimensional modeling. For each element of the metamodel (SFact, SDegenerateFact, SDimension, SBase, SDegenerateDimension, SFactAttribute, SDescriptor, SOID and SDimensionAttribute), its security information is defined by means of a sequence of security levels (SecurityLevels), a set of user categories (SecurityCompartment) and a set of user roles (SecurityRoles). Additionally these classes have security constraints (SConstraint) to indicate the security level and the rights conceded to a user to accede to certain information. For example, an authorization rule (AuthorizationRule) can represent an interdiction to specific users to access certain information. The access type can depend on the value of certain attributes contained in several classes. This fact can be captured in the model by means of a security rule (SecurityRule). If a user tries to accede to information for which his access is denied, then this fact can be modeled with an audit rule (AuditRule). These restrictions are defined using an Object Constraint Language (OCL) extension [15] and represented at model level with an UML note associated to the corresponding class.

More details on this profile can be found in [5, 6].

3.2 Definition of the SMD PSM

In the design of databases and data warehouse, t conceptual modeling provides the PIM, and the logi modeling the PSM. In multidimensional modeling, t logical level is designed according to the specific properties of the SGBD (Relational Online Analyti Processing, ROLAP, Multidimensional Onli Analytical Processing, MOLAP or Hybrid Onli Analytical Processing, HOLAP). Still, Kimball [9 assures that the most common representation is a relational platforms, i.e., on ROLAP systems.

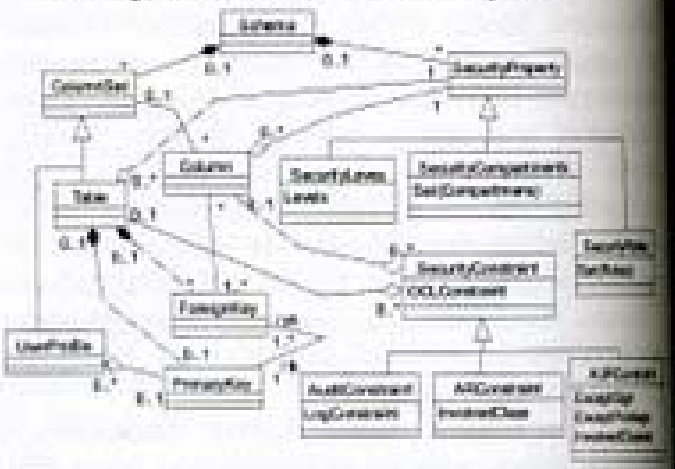

Figure 3. The SECDW metamodel used in the design of the SMD PSM

Our PSM is described in [17], starting from th relational Common Warehouse Metamodel (CWM, that allows us to model the security and aud aspects represented at logical level in DW modeling. This metamodel is called the Secure Relational Data Warehouse (SECRDW).

Figure 3 presents the SECRDW metamodel th will be designated in the following as PSM. In order to distinguish the security aspects it comprises, it will b called the Secure Multidimensional PSM (SMD PSM). With this metamodel we can represent Table, Columns, primary and foreign keys, etc. The Schem container allows the security at model level. Th SecurityProperty and SecurityConstraint metaclass are associated with the Table and Column metaclass respectively, and they establish security for attribute and tables. In addition SecurityConstraint allows us to express the constraints (AuditRule, AuthorizationRul and SecurityRule) modelled through the UML notes o the Secure DW (SECDW) metamodel, i.e., in PIM. The userProfile metaclass specifies restrictions on particular information corresponding to a user or use group.

3.3 QVT transformations of the SMD PIM to SMD PSM

Figure 4 employs the textual notation to establish main transformations, i.e., the SMD PIM to SMD transformation. The keyword *top* preceding the relations specifies that those relations will never be called by other relations throughout the transformation. Each one of these relations has its own domain and where clauses corresponding pre and post-conditions to be satisfied.

```
Transformation SMD To SREL(SMD: SECDW)
    SREL: SECRDW)
key Table(name, Schema);
key Column (name, owner);
key UserProfile(name, Schema);
key PrimaryKey(name, owner);
key ForeignKey(name, owner);
key SecurityProperty(name, owner);
key SecurityConstrain(name, owner);
top relation SecureDW2Schema()
top relation UserProfile2RUserProfile()
top relation SFact2Table ()
top relation SDegenerateFact2Table()
top relation SDimension2Table()
 //Association SFact with SDimension
top relation AssocSF_D2FKey()
 //Association SDegenerateFact with SDimension
top relation Assoc SDF_SD2FKeyFKey
} Association SDegenerateFact with SFact
top relation AssocSDF_SF2FKey()
```

Figure 4. Textual notation for the SMDPIM to SMDPSM transformation

3.3.1. The SFact to Table transformation

Figure 5 illustrates the SFact2Table relation in its graphical notation. There is a table corresponding to SFact and having the same name. This table has a column with a name (specified in the where clause), which is also the primary key of the table. The security information represented with tagged values in the SFact is transformed into objects associated to the table. This security information is modeled at logical [illegible] of the SFact table. The SFact2Table relation is satisfied only when the SecureDW2Schema pre-condition is satisfied, therefore ensuring that the table will be contained in Schema.

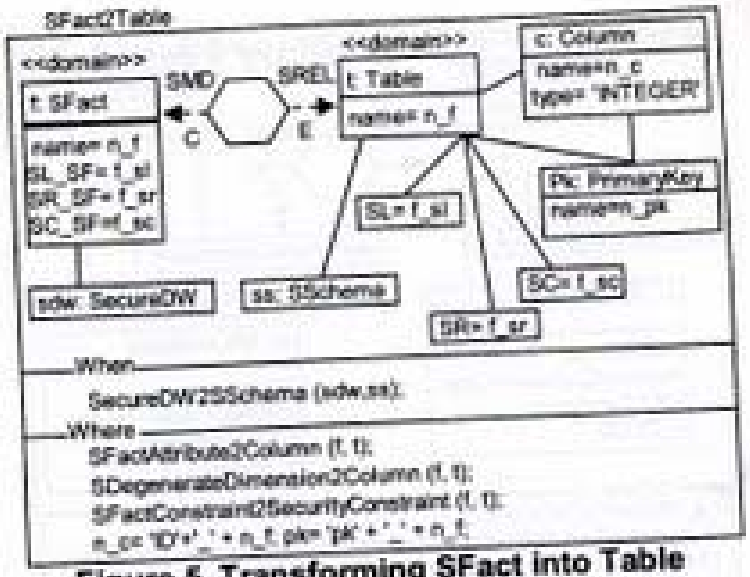

Figure 5. Transforming SFact into Table

The SFact attributes together with their security information and constrains are transformed according to the relations SFactAttribute2Column (if the attribute's type is FactAttribute) or SDegenerateDimension2Column (if the attribute is of type SDegenerateDimension).

Every SFactAttribute involved in the SFactAttribute2Column relation inherits security information and restrictions from the SecureProperty class, as the latter contains the SConstraint class. For this reason SFactAttribute2Column transforms not only attributes into columns, but also all the associated security information that SFActAttribute contains at conceptual level.

3.3.2. The SFactConstraint to Security Constraint transformation

SFact contains tagged values that inherit security restrictions of SecureClass. These security restrictions are transformed in table security restrictions by SFactConstraint2SecurityConstraint (see Figure 6), the resulting restrictions being modeled as UML[illegible]

Figure 6 illustrates the graphical notation provided by QVT to define the SFactConstraint2SecurityConstraint relation, certain attributes are omitted to make it more comprehensible. When the relation is applied, the constraints AuditRule, AuthorizationRule and SecurityRule transform themselves into AuditConstraint, ARConstraint and AURConstraint respectively, but associated to the table that represents the SFact. It is to be noted that this relation's where clause employs OCL to ensure that the "s_icsr" attribute corresponds to the tables that represent the involvedTables attribute of the ARConstraint restriction.

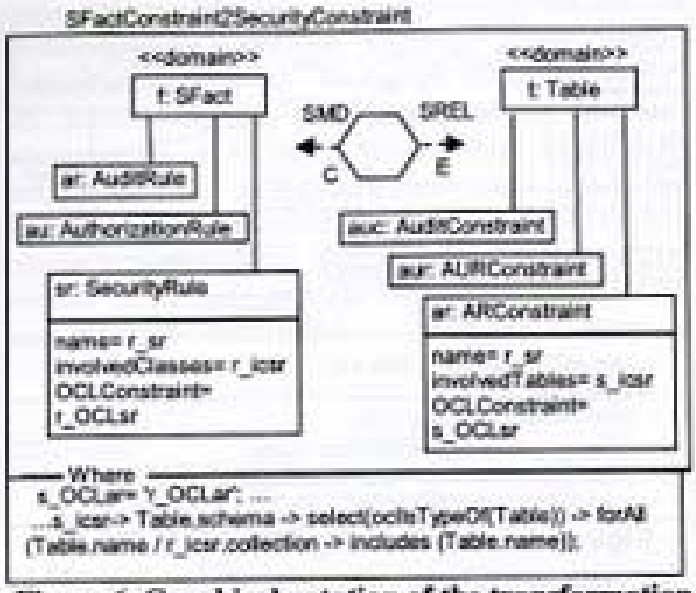

Figure 6. Graphical notation of the transformation of SFactConstraint into SecurityConstraint

4. Conclusions and Future Work

This paper introduces a new framework for the development of secure data warehouses based on MDA and QVT. The application of QVT transformation rules to the SMD PIM allows the development of different SMD PSMs, thus facilitating the representation at a logical level of all security and audit requirements captured at earlier stages of DW design. Afterwards, each SMD PSM can be directly converted into code.

The main contributions of this paper are: the development of DWs is reduced to creating an SMD PIM starting from an SMD CIM and its corresponding QVT relations, the time and effort invested in the development of DWs are shortened, the transition between different models and the final implementation is guaranteed, we reach interoperability, portability, adaptability and reusability by employing MDA technology.

Our immediate future work consists in studying the possibility to represent security requirements for Data Warehouses, and establish a transformation between secure CIM and SMD PIM.

Acknowledgements

This work has been partially supported by the METASIGN project (TIN2004-00779) from the Spanish Ministry of Education and Science, by the DADASMECA project (GV05/220) from the Regional Government of Valencia, and by the DADS project (PBC-05-012-2) from the Regional Science and Technology Ministry of Castilla -La Mancha (Spain).

References

[1] R. Kirkgöze, N. Katic, M. Stolda, and A. M. Tjoa, "A Security Concept for OLAP. (DEXA'97)," Toulouse, France.
[2] N. Katic, G. Quirchmayr, J. Schiefer, M. Stolba, and A. M. Tjoa, "A Prototype Model for DW Security Based on Metadata," (DEXA'98), Vienna, Austria, 1998.
[3] T. Priebe and G. Pernul, "Towards OLAP Security Design - Survey and Research Issues," (DMDW'0), Sweden.
[4] A. Rosenthal and E. Sciore, "View Security as the Basis for DW Security," (DMDW'00), Sweden, 2000.
[5] E. Fernandez-Medina, J. Trujillo, R. Villarroel, and M. Piattini, "Access control and audit model for the multidimensional modeling of data warehouses," *DSS*, vol. 42, pp. 1270-1289, 2006.
[6] R. Villarroel, E. Fernández-Medina, and M. Piattini, "A UML 2.0/OCL Extension for Designing Secure DW," *Journal of Research and Practice in IT*, vol. 38, 2006.
[7] J. Miller and J. Mukerji, "MDA Guide Version 1.0.1," 2003.
[8] OMG, "MOF 2.0 Query/View/Transformation."
[9] C.C. Burt, B.R. Bryant, R.R. Raje, A.M. Olson, and M. Auguston, "Model Driven Security: Unification of Authorization Models for Fine-Grain Access Control," (EDOC'03), 2003.
[10] D. Basin, J. Doser, and T. Lodderstedt, "Model Driven Security: From UML models to access control infrastructures," ETH, Zürich 4 - September 2003.
[11] S.N. Sivanandam and G.R. Karpagam, "A Novel approach for Implementing Security services," *Academic Open Internet Journal*, vol. 13, 2004.
[12] U. Lang and R. Schreiner, "OpenPMF: a Model-Driven Security Framework for Distributed Systems," (ISSE'04), Berlin, Germany, 2004.
[13] J.-N. Mazon, J. Trujillo, M. Serrano, and M. Piattini, "Applying MDA to the development of data warehouses," (DOLAP'05), Bremen, Germany, 2005.
[14] E. Fernández-Medina, JuanTrujillo, RodolfoVillarroel, and M. Piattini, "Developing secure DW with a UML extension," *IS*, vol. Article In Press, Corrected Proof.
[15] E. Fernández-Medina and M. Piattini, "Extending OCL for Secure Database Design," (UML'04), Lisboa, Portugal.
[16] R. Kimball and M. Ross, *The Data Warehouse Toolkit*, 2 edition ed: John Wiley, 2002.
[17] E. Soler, R. Villarroel, J. Trujillo, E. Fernández-Medina, and M. Piattini, "Representing security and audit rules for DW at the logical level by using the CWM", (ARES'06), Vienna, Austria, 2006.