ARES Conference

The International Dependability Conference

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

Including Security Rules support in an MDA approach for 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

Information security is a crucial aspect for enterprises that has to be considered as a strong requirement from the early stages of the development process and Data Warehouses (DWs) manage highly important information used to make strategic decisions which has to be protected from unauthorized users. In order to develop secure DWs we have proposed a Model Driven Architecture (MDA) composed of several secure metamodels at different abstraction levels and transformations between them. Lately, a specialization of this architecture considering a multidimensional approach towards On-Line Analytical Processing (OLAP) tools has been defined, but the support to automatically transform complex security rules has not been dealt with so far. This paper analyzes this lack and defines improvements in our metamodels and a set of transformations between models in order to fulfill our MDA approach.

1. Introduction

Information security is a critical issue for information systems that must be considered from the early stages of development as a strong requirement [1] and must be integrated into the whole development process [2] in order to take into account these security constraints for design decisions. Therefore, some research efforts have been made in the field of designing secure information systems. One of the most relevant proposal is UMLsec [3] which specifies and evaluates UML security specifications using formal semantics.

On the other hand, the Model Driven Architecture (MDA) [4], provides a model driven software development based on the separation of the specification of the system functionality and its implementation by defining models at different abstraction levels and transformations between them.

The Model Driven Security (MDS) [5] uses an MDA approach to build secure information systems in which designers specify high-level system models along with their security properties and use tools to automatically generate systems architectures from the models, including security infrastructures. Within the context of MDS the same authors propose SecureUML for modeling a generalized role based access control.

This is an interesting background, but Data Warehouses (DWs) are different from information systems. They have special characteristics and use a multidimensional model to integrate historical data from heterogeneous sources as well as to analyze this information in order to make strategic decisions. Thus, this information must be protected from malicious users who can discover unauthorized information by using queries if security constraints have not been defined.

There are some works considering security in DWs which deal with On-Line Analytical Processing (OLAP) tools but are solely focused upon the Discretional Access Control (DAC) policy and use a simplified role concept implemented as a subject. The most interesting proposal is Priebe and Pernul's design methodology [6] in which the authors use ADAPTed UML to define a DAC system and deal with the final implementation in a commercial tool.

978-0-7695-3564-7/09 $25.00 © 2009 IEEE
DOI 10.1109/ARES.2009.67

These previous works are focused on DAC and do not consider security issues at all stages of the development process: from early stages to final tools. In order to fulfill this research branch, Fernández-Medina et al. propose an MDA approach to develop secure DWs [7] which allows us to define models and security constraints at different abstraction levels supporting transformations between models and semiautomatic generation of secure code for final tools. This proposal is focused on a relational path towards final code in Data Base Management Systems (DBMS), but DWs are usually managed by On-Line Analytical Processing (OLAP) tools under a multidimensional approach. Thus, this architecture has been lately specialized with a new multidimensional path towards OLAP tools by defining a secure multidimensional model at logical level and automatic transformations from conceptual models.

The proposed transformation rules consider structural aspects and the set of security constraints which can be defined by using stereotypes in the conceptual model. However, our conceptual metamodel also allows us to define advanced security rules by using Object Constraint Language (OCL) notes, but their automatic transformation has not been dealt with so far. This paper analyzes this problem and provides a solution composed of: (1) an improvement of our conceptual metamodel with new features which support these advanced security rules and (2) a set of transformation which translate these rules from the conceptual level into a secure multidimensional model at logical level.

The remainder of this paper is organized as follows: Section 2 will briefly introduce our MDA approach to develop secure DWs; Section 3 will deal with security rules showing the improvements done in metamodels and the new set of rules defined to automatically support their transformation; and finally, Section 4 will present our conclusions and future work.

2. MDA architecture for Secure DWs

An MDA architecture is composed of several models at different abstraction levels and automatic transformations between them. Our MDA approach to develop secure DWs [7] considers security issues at all stages of the development process defining metamodels at business, conceptual and logical levels. At business level, a UML profile [8] has been defined to include security requirements in a Computational Independent Metamodel (CIM). This profile extends i*, which is a requirement engineering framework centered in agents and their intentional characteristics.

At conceptual level, a Platform Independent Metamodel (PIM) defined by a UML profile, called SECDW [9], extends with security capabilities an existing proposal for conceptual modeling of DWs which considers fact, dimension and base classes and specific aspects of DWs such as many-to-many relations, degenerated dimensions, multiple classifications or alternative paths of hierarchies.

SECDW metamodel is improved with an access control and audit model (ACA) [10] which classifies subjects and objects in three ways, defines secure classes and properties, and permits several kinds of security rules over the multidimensional elements of DWs which will be analyzed in next section. To classify subjects and objects, clearance levels (Security Levels), hierarchical role structures (Security Roles) and horizontal compartment or groups (Security Compartments) can be used.

Our proposal considers two Platform Specific Metamodels (PSM) at logical level. One of them is a relational approach and defines a metamodel, called SECRDW, extending the relational package from the Common Warehouse Metamodel (CWM). In this context, the transformation rules from PIM to relational PSM have been also defined by using Query / View / Transformation (QVT) and the final implementation in a DBMS, Oracle Label Security, has been dealt.

This architecture has been specialized with a multidimensional path due to fact that the majority of DWs are managed by OLAP tools within a multidimensional approach. This specialization [11] is composed of: (1) a multidimensional secure metamodel at logical level, called SECMDDW, which is based on the OLAP package of CWM; (2) a set of QVT rules from PIM; and (3) the final implementation in a certain OLAP tool, SQL Server Analysis Services (SSAS).

This specialization is focused on structural aspects and security constraints, but did not until now deal with more complex security rules which can be established in our conceptual models by using OCL expressions. This paper fulfills our proposal improving the metamodels to include information of security rules and defines new sets of QVT rules for their automatic transformation towards logical models.

3. Including Security Rules in our MDA approach for Secure DWs

This section presents the improvements carried out in metamodels and QVT rules in order to fulfill our approach to support the security rules defined at conceptual level by using our Access Control and Audit model [10].

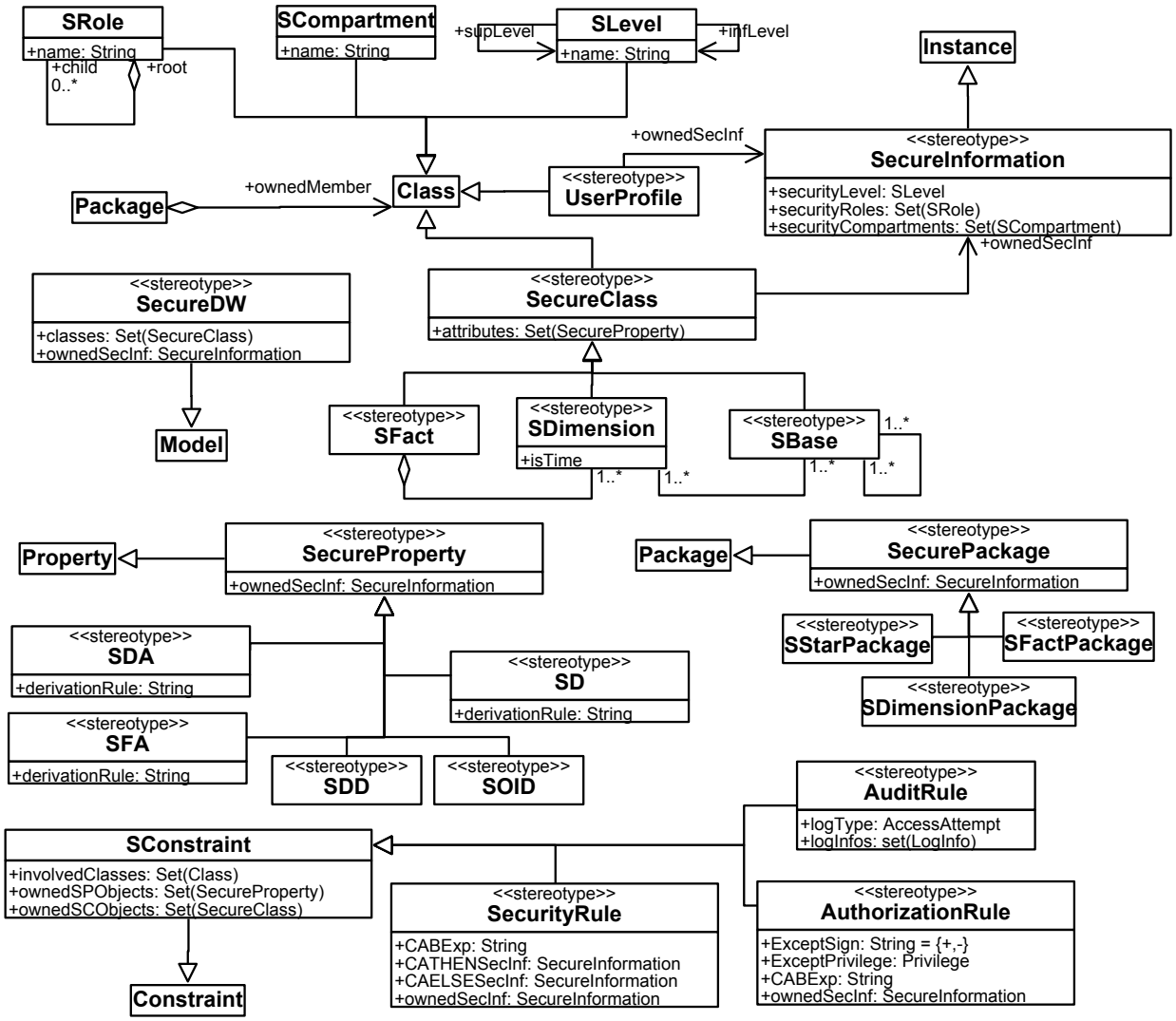

Figure 1 Conceptual metamodel (SECDW)

3.1. Conceptual metamodel (SECDW)

This section is focused on the improvements made in the conceptual metamodel (SECDW) to include security rules support. Due to space constraints, further details of another metamodel aspects are not provided in this paper, but can be found in [9].

The security classification of objects and subjects into security roles, compartments and levels is defined by using "SRole", "SCompartment" and "SLevel" metaclasses which allow us to specify a role hierarchy, a set of compartments and a list of levels. The "SecureInformation" metaclass has been also added to the metamodel in order to clearly define the security information (security roles, compartments and level) associated with a specific multidimensional element.

Our ACA model allows us to specify three kinds of security rules in conceptual models by using OCL expressions in notes associated with the corresponding classes. Sensitive Information Assignment Rules (SIAR) which let us 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.

Security rules usually include information about subjects, objects, conditions, security information, privileges, log types, etc. which is very difficult to directly analyze over the OCL expression. Therefore, our conceptual metamodel has been improved to manage this information. The three kinds of security

rules manage a list of multidimensional objects (secure properties and classes) where, with the purpose of applying the rule and defining this information, we have defined sets of secure classes and properties in a metaclass called "SContraint" which is specialized into one specific metaclass for each kind of security rule. SIAR rules are specified by the "SecurityRule" metaclass which considers conditions with a boolean expression and the secure information that will be assigned whether the condition is satisfied or not. AUR rules use the "AuthorizationRule" metaclass in which information about the security information associated the sign of the authorization (positive or negative), the privilege (read, insert, update, delete, all) and a boolean expression condition to establish a condition are included. Finally, AR rules are specified by the "AuditRule" metaclass which defines the access attempt and the information (subject, object, action, time and response) that will be logged.

3.2. Logical multidimensional metamodel (SECMDDW)

SECMDDW metamodel [11] uses a multidimensional approach to define secure models at logical level. This metamodel is composed of three metamodels: a security configuration metamodel which represents roles of a role based access control (RBAC) policy; a cube metamodel which defines structural aspects of cubes, measures and hierarchies and security constraints with cube and cell permissions; and finally, a dimension metamodel with structural information of dimensions, attributes and base classes, and security issues by using permissions over dimensions and attributes. Due to space constraints, figures of these metamodels are not shown.

3.3. Transformation SECDW to SECMDDW

Up to now, the following issues have been addressed: (1) existing *Security Rules* have been presented and (2) involved metamodels have been improved for a suitable representation of the mentioned rules (see Section 3.1, Figure 1). Two new rule sets have been defined in order to automatically transform security rules from conceptual models into multidimensional logical models. In a few words, these transformations extract the SIAR and AUR rules from the conceptual model and introduce their semantics into the *Cubes*, *Dimensions* and *Attributes* of the logic models of DW. Due to lack of space, these transformations have not been fully included.

SECDWSecurityRules2CubePermissions (Table 1) processes all the SIAR and AUR rules included in the PIM which are related with *Fact* classes. These security rules are expressed as a specialization of the *SConstraint* metaclass which in turn is a specialization of the UML 2.0 *Constraint* metaclass.

Transformation **SECDWSecurityRules2CubePermissions**
top relation processSecurityRules {…}
relation processCubeSIAR {…}
relation processCubeAUR {…}
relation denySLevelAtt2CellPermissionForSIAR {…}
relation denySRoleClass2CubePermission {…}
relation SCompartmentClass2CubePermission {…}
relation SRoleClass2CubePermission {…}
relation SLevelClass2CubePermission {…}
relation denySRoleAtt2CellPermissionForSIAR {…}
relation denySCompartmentAtt2CellPermissionForSIAR {…}
relation denySCompartmentClass2CubePermission {…}
relation denySLevelClass2CubePermission {…}
relation SCompartmentClass2CubePermissionForAUR {…}
relation SRoleClass2CubePermissionForAUR {…}
relation SLevelClass2CubePermissionForAUR {…}
relation SLevelAtt2CellPermissionForAUR {…}
relation SRoleAtt2CellPermissionForAUR {…}
relation SCompartmentAtt2CellPermissionForAUR {…}

Table 1. SECDWSecurityRules2CubePermission

To reflect the SIAR rules in the PSM, the transformation executes its *processCubeSIAR* relation (see Figure 2). The *processCubeSIAR* relation modifies the existing PSM and establishes certain values in properties of the PSM classes to implement the semantics of the SIAR rules included in the PIM. In the same way, the *processCubeAUR* (see Figure 3) deals with the representation of the *AuthorizationRules* in the PIM and processes it to produce the required security aspects depicted by these rules in the PSM.

The QVT relations to process the *AUR* rules produce positive and negative authorizations for the information of the *levels*, *roles* and *compartments* specified by the *SecureInformation* classes referenced by the AUR rules. Since both the SIAR and AUR rules accept Boolean expressions to be evaluated and applied over the content of the aforementioned *SecureInformation*, the transformations also propagate these boolean expressions to the PSM. Thus, the positive or negative authorization (when AUR) depends on the boolean expressions.

When the AUR is a positive one, the QVT rules authorize the given level (in the *SecureInformation*) and the upper ones, the given role and its descendants, and the specified compartments. On the other hand, when the authorization is negative, the QVT rules deny the given level and the lower ones, the given role and its descendants, and the specified compartments.

```
relation processCubeSIAR{
…CLASSES:Sequence(Class); SLEVS:Set(SLevel);
SROLES:Set(SRole); SCOMPS:Set(SCompartment);
  checkonly domain pim sr:SecurityRule{
     involvedClasses = INVCLASS:Set(Class),
     ownedSPObjects = OWNSPO:Set(SecureProperty),
     ownedSCObjects = OWNSCO:Set(SecureClass),
     ownedSecInf = secinf,      CABExp = cabexp,
     CATHENSecInf = catSecInf,   CAELSESecInf = caeSecInf }
  where{
     INVCLASS->forAll(cTmp:Class |CLASSES.append(cTmp));
     OWNSCO->forAll(cTmp:Class | CLASSES.append(cTmp));
     Let FACTS:Sequence(SFact) =
      CLASSES->select(cFact:Class |cFact.oclIsKindOf(SFact)) in
     Let PROPERTIES:Sequence(SecureProperty) =
      CLASSES->select(cProp:Class|
         sProp.oclIsKindOf(SecureProperty)) in
     SLEVS = getUpperSecurityLevels(catSecInf.securityLevel);
     catSecInf.securityRoles->forAll(sr:SRole |
         getLeafSRoles(st)->forAll(srTmp:SRole|
         SROLES.append(srTmp)))
     SCOMPS = catSecInf.securityCompartments;
     FACTS->forAll(sf:SFact | SLEVS->forAll(sl:SLevel|
         SLevelClass2CubePermission(sl, sf));
     SROLES->forAll(sr:SRole |
         SRoleClass2CubePermission(sr,sf));
     SCOMPS->forAll(sc:SCompartment |
         SCompartment2CubePermission(sc,sf)));
     PROPERTIES->forAll(sp:SecureProperty |
  SLEVS->forAll(sl:SLevel | SLevelAtt2CellPermission (sl, sp));
    SROLES->forAll(sr:SRole | SRoleAtt2CellPermission(sr,sp));
    SCOMPS->forAll(sc:SCompartment|
         SCompartmentAtt2CellPermission(sc,sp)));
    SLEVS = getLowerSecurityLevels(caeSecInf.securityLevel);
     caeSecInf.securityRoles->forAll(sr:SRole |
     getNotLeafSRoles(st)->forAll(srTmp:SRole|
       SROLES.append(srTmp)))
     SCOMPS = getNotIncludedCompartments
        (caeSecInf.securityCompartments);
     FACTS->forAll( SLEVS->forAll(sl:SLevel|
denySLevelClass2CubePermission(sl, sf, cabexp));
        SROLES->forAll(sr:SRole|
denySRoleClass2CubePermission(sr,sf, cabexp));
        SCOMPS->forAll(sc:SCompartment|
denySCompartment2CubePermission(sc,sf, cabexp)));
     //Denying SecureProperties
     PROPERTIES->forAll(sp:SecureProperty |
       SLEVS->forAll(sl:SLevel|
denySLevelAtt2CellPermissionForS (sl, sp, cabexp));
        SROLES->forAll(sr:SRole|
denySLevelAtt2CellPermission (sr,sp, cabexp));
        SCOMPS->forAll(sc:SCompartment|
denySLevelAtt2CellPermission (sc,sp, cabexp)));}
```

Figure 2. processCubeSIAR relation

SECDWSecurityRules2DimensionPermissions (Table 2) includes relations such as *processDimensionSIAR* and *processDimensionAUR* which work following a similar manner to the previous transformations for cubes performing the same functionalities over the *Dimension* classes in the PSM. Thus, no further explanation will be provided. As noted in this section have been included the transformations which drive the required actions to include the semantics of the

```
relation processCubeAUR{
…CLASSES:Sequence(Class);   SLEVS:Set(SLevel);
  SROLES:Set(SRole);   SCOMPS:Set(SCompartment);
checkonly domain pim ar:AuthorizationRule{
     involvedClasses = INVCLASS:Set(Class),
     ownedSPObjects = OWNSPO:Set(SecureProperty),
     ownedSCObjects = OWNSCO:Set(SecureClass),
     ownedSecInf = secinf,      ExceptionSign =es,
     ExceptPrivilege = ep,
     involvedClasses = INVCLASS:Set(Class),
     CABExp = exp   }
where{
     //Firstly, prepare a set of classes
  INVCLASS->forAll(cTmp:Class| CLASSES.append(cTmp));
  OWNSCO->forAll(cTmp:Class| CLASSES.append(cTmp));
     //Prepare the set of SFact Classes
Let FACTS:Sequence(SFact) = CLASSES->select(cFact:Class |
     cFact.oclIsKindOf(SFact)) in
Let PROPERTIES:Sequence(SecureProperty) = CLASSES
->select(cProp:Class | sProp.oclIsKindOf(SecureProperty)) in
     //Process ownedSecInf
     secInf.securityRoles->forAll(sr:SRole | getLeafSRoles(st)
->forAll(srTmp:SRole | SROLES.append(srTmp)))
     SCOMPS = secInf.securityCompartments;
     if (es = "+") then
  SLEVS = getUpperSecurityLevels(catSecInf.securityLevel);
     else
  SLEVS = getLowerSecurityLevels(catSecInf.securityLevel);
     //Process AUR for SFACTS according to the sign
     FACTS->forAll(sf:SFact |
       SLEVS->forAll(sl:SLevel|
SLevelClass2CubePermissionForAUR(sl, sf, exp,es));
        SROLES->forAll(sr:SRole|
SRoleClass2CubePermissionForAUR(sr, sf, exp, ex));
        SCOMPS->forAll(sc:SCompartment|
SCompartment2CubePermissionForAUR(sc,sf, exp, es)));
     PROPERTIES->forAll( sp:SecureProperty |
        SLEVS->forAll(sl:SLevel|
SLevelClass2CubePermissionForAUR(sl, sf, exp,es));
        SROLES->forAll(sr:SRole|
SRoleClass2CubePermissionForAUR(sr, sf, exp, ex));
        SCOMPS->forAll(sc:SCompartment}
```

Figure 3. processCubeAUR relation

Transformation **SECDWSecurityRules2DimensionPermissions**
top relation processDimensionSecurityRules {…}
relation processDimensionSIAR {...}
relation processDimensionAUR {...}
relation authorizeSCompartment {…}
relation authorizeSRole {…}
relation authorizeSLevel {…}
relation createDimensionSIARForSCompartment {…}
relation createDimensionSIARForSRole {…}
relation createDimensionSIARForSLevel {…}
relation createNegativeSIARAttributePermissionsForSLevel {…}
relation createNegativeSIARAttributePermissionsForSRole {…}
relation createNegativeSIARAttributePermissionsForSCompartment {...}
relation createDimensionAURForSLevel {…}
relation createDimensionAURForSRole {…}
relation createDimensionAURForSCompartment {…}
relation authorizeSLevelForAUR {…}
relation authorizeSCompartmentForAUR {…}
relation createAttributePermisionForAUR {…}
relation authorizeSRoleForAUR {…}

Table 2. SECDWSecurityRules2DimenssionPermission

Security Rules in the logic models (*processCubeSIAR, processDimensionSIAR, processCubeAUR* and *processDimensionAUR*).

Audit Rules (AR) have not been considered when developing the QVT transformations. Despite these rules are also considered as *Security Rules,* the OLAP tools do not implement *audit rules* defining permissions for cubes, dimensions or attributes, as the other kinds of rules do. The DW administrator is now in charge of defining which elements and information must be audited. To such an end, the DW administrator uses special auditing tools which are frequently provided by the OLAP tools.

Once we have obtained logical models, the next step is to generate the final implementation. In previous works [11] we have dealt with the implementation in a specific OLAP platform, SQL Server Analysis Services (SSAS).

4. Conclusions

The development of secure DWs by using an MDA approach provides us with a better quality and security by translating the requirements identified at early stages of development into the final implementation.

In previous works, due to the fact that the greatest part of DWs are managed by OLAP tools using a multidimensional approach, the architecture has been specialized with a multidimensional path towards OLAP by defining a secure multidimensional metamodel at logical level (SECMDDW) and a set of QVT rules to automatically obtain multidimensional logical models from conceptual models. However, the proposed transformation rules considered structural issues and some security constraints, but they did not support more complex security rules (SIAR, AUR and AR) that can be established in the conceptual model by using OCL expressions. This work deals with security rules and fulfills this multidimensional specialization improving metamodels to provide a better definition of security rules and defining a new set of QVT rules to support the automatic generation of multidimensional logical models.

In further works, in order to achieve a better evaluation of our proposal, an application to a large case-study in industrial environments will be carried out. Our MDA approach will be also improved with support to several platforms (Oracle and Pentaho) and reengineering features permitting inverse transformations from final code to logical and conceptual level, so that DWs migration can be supported.

Acknowledgments

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. Fink, T., M. Koch, and K. Pauls, *An MDA approach to Access Control Specifications Using MOF and UML Profiles.* Electronic Notes in Theoretical Computer Science, 2006. **142**: p. 161-179.
3. Jürjens, J., *Secure Systems Development with UML*. 2004: Springer-Verlag.
4. MDA, O.M.G., *Model Driven Architecture Guide.* 2003.
5. 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.
6. 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.
7. 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.
8. 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.
9. Fernández-Medina, E., et al., *Developing Secure Data Warehouses with a UML extension.* Information Systems, 2007. **32**(6): p. 826-856.
10. 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.
11. 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**.