IADIS International Conference

e-Society 2004

Proceedings of the IADIS International Conference

[illegible]

Ávila, Spain, 16 - 19 July 2004

[illegible]

Edited by

[illegible]

[illegible]

[illegible]

iadis

international association for development of the information society

IADIS INTERNATIONAL CONFERENCE

e-Society 2004

PROCEEDINGS OF THE IADIS INTERNATIONAL CONFERENCE
e-Society 2004

Volume I

ÁVILA, SPAIN

JULY 16-19, 2004

Organised by
IADIS
International Association for Development of the Information Society

Edited by
Pedro Isaías
Piet Kommers
Maggie McPherson

Associate Editors: Luís Rodrigues, and Patrícia Barbosa

ISBN: 972-98947-5-2

Depósito Legal N.º 214025/04

TABLE OF CONTENTS

VOLUME I

FULL PAPERS

SECURE MULTIDIMENSIONAL CONCEPTUAL MODELING

Rodolfo Villarroel[1], Eduardo Fernández-Medina[2], Juan Trujillo[3], Mario Piattini[2]

[1]*Departamento de Computación e Informática, Universidad Católica del Maule*
Avenida San Miguel 3605. Talca (Chile)
rvillarr@spock.ucm.cl

[2]*Departamento de Informática, Universidad de Castilla-La Mancha*
Paseo de la Universidad, 4. 13071 Ciudad Real (Spain)
{Eduardo.FdezMedina, Mario.Piattini}@uclm.es

[3]*Departamento de Lenguajes y Sistemas Informáticos, Universidad de Alicante*
Apartado de correos, 99. 03080 Alicante (Spain)
jtrujillo@dlsi.ua.es

ABSTRACT

Generally, Information Systems security is taken into consideration once the system has been built, it is in operation and security problems have already arisen. This kind of approach, called "penetrate and patch" is being shifted by methodologies that introduce security in the systems development process. This is an important advance but, unfortunately, methodologies incorporating security are based on an operational environment and not on an analytical one. Therefore, they do not include multidimensional modeling approaches to work with Data Warehouses (DW), Multidimensional Databases and On-Line Analytical Processing (OLAP) applications. This paper makes a comparison of secure information systems design methodologies and puts forward an extension based on the Unified Modeling Language (UML) for multidimensional modeling. Besides, an example of the application of the extension proposed is shown. Neither of the studied methodologies address the security aspect comprising all stages of the system development cycle nor considers the introduction of security in multidimensional modeling. We propose an extension which tackles these problems and allows us to introduce security elements into a multidimensional application through the standard mechanisms of UML extension. As a result, it avoids developers to waste time to adapt themselves to a new methodology and achieves a more robust specification.

KEYWORDS

Security, confidentiality, security design, multidimensional modeling, UML, secure information systems development.

1. INTRODUCTION

According to ISO/IEC 15408-1 (ISO/IEC, 1999) and Castano *et al.* (1995), security is defined as the capability of a software product to protect data and information in order to avoid that, unauthorized individuals or systems, are able to read and modify them and not to deny access to authorized staff. The above mentioned characteristics should be taken into account in every Information Systems (IS) development. However, solutions are mainly focused on providing security defences instead of solving one of the main reasons of security problems that refers to an appropriate software design (Ghosh *et al.*, 2002).

Fortunately, there have been developed new methodologies incorporating security in their development processes, such as Marks. *et al.* (1996), Jürgens (2001), Fernández-Medina and Piattini (2003), Liu *et al.* (2003). Each one of these methodologies comprises very important aspects concerning security that can be used as a basis to study aspects that new methodologies or extensions that may be developed do not cover. At the same time, these methodologies have a series of limitations that we have to take into account. One of their main limitations refers to the fact that they only study security in systems working in an operational

environment and not in an analytical one. To solve this problem, we must work in an analytical environment strongly supported by the use of multidimensional models. In the literature, we can find several initiatives to include security in DW, multidimensional databases and OLAP applications (Kirkgoze *et al.*, 1997, Priebe and Pernul, 2000, Rosenthal and Sciore, 2000). Many of them focus on interesting aspects related to access control, multilevel security, its application to federated databases, applications using commercial tools, etc. However, neither of them studies the security aspect comprising all stages of the system development cycle nor considers the introduction of security in multidimensional design. As there is not a methodological approach integrating security in multidimensional design, we can state that the problem of security in multidimensional design remains unsolved.

In the following section, we will describe four proposals incorporating security in the systems development stages, we will show the comparison framework that we have used and we will make the comparison in order to highlight the lack of security in the information systems development. Later on, in section 3, we will make a proposal of a security extension, based on UML, for multidimensional conceptual modeling. This proposal will be described together with an example. At last, we will explain our conclusions and future work lines arising from this paper.

2. PROPOSALS OF METHODOLOGIES INCORPORATING SECURITY

The proposals that will be analyzed in our comparison are as follows:

- MOMT: Multilevel Object Modeling Technique
- UMLSec: Secure Systems Development Methodology using UML
- Secure Database Design Methodology
- Security and Privacy Requirements Analysis Methodology within a Social Setting

We have chosen these four methodologies because all of them try to solve the problem of security from the earliest stages of the ISs development, emphasize security modeling aspects and use modeling languages that make it easier the security design process. However, we must highlight the fact that there are not methodologies incorporating security in multidimensional modeling.

2.1 General Description of each Proposal

MOMT (Multilevel Object Modeling Technique) is a methodology to develop secure databases (Marks et al., 1996) which extend OMT in order to be able to design multilevel databases providing the elements with a security level and establishing interaction rules among the elements of the model. MOMT is mainly composed of three stages: Analysis stage: It allows us to analyse the requirements to detect potential system vulnerabilities, System Design Stage. It allows us to design multilevel databases, Object Design Stage: It allows us to design the modules of the automated system.

Jürgens (2001) proposes a methodology to specify requirements regarding confidentiality and integrity in analysis models based on UML. Multilevel security and Mandatory Access Control are the security models highlighted in this proposal called UMLSec. This approach considers an UML extension to develop secure systems. In order to analyse security of a subsystem specification, the behaviour of the potential attacker is modelled; hence, specific types of attackers, that can attack different parts of the system in a specific way, are modelled.

Fernández-Medina and Piattini (2003) propose a methodology to design multilevel databases by integrating security in each one of the stages of the databases life cycle. This methodology includes the following aspects: A specification language of multilevel security constraints about the conceptual and logical models; a technique to the early gathering of multilevel security requirements; a technique to represent multilevel databases conceptual models; a logical model to specify the different multilevel relationships, the metainformation of databases and constraints; a methodology based upon the Unified Process, with different stages that allow us to design multilevel databases; a CASE tool that helps to automate multilevel databases analysis and design process.

Liu *et al.* (2003) define a methodological framework to deal with security and privacy requirements based on i*, which is an agent-oriented requirements modeling language. This framework is formed by a set of analysis techniques: Attacker analysis, it helps to identify system potential attackers and their malicious intents; Dependency vulnerability analysis, it helps to detect vulnerabilities in terms of organizational relationships among stakeholders; Countermeasure Analysis, the necessary factors for a successful attack are the attacker motivation, the system vulnerabilities and the attackers' capabilities to carry out the attack; Access control analysis, it establishes a link between security requirements models and security implementation models.

2.2 Comparison Framework

The comparison framework that we have used is that proposed by Khwaja *et al.* (2002). There are other comparison frameworks but this is one of the most recent and it solves the problem that many authors intermingle the concepts of specification and specification technique. The criteria used for one of these concepts should not be applied to others. For instance, a specification can be complete and consistent regardless of the way used to represent the specification, the process used in its construction, the degree/extent of tools and automation used or whether it is formal or informal. The criteria should be separated but it should exist a mapping between them, which means that the specification technique features help us to achieve certain features in a specification.

The specification criteria and the specification technique criteria are shown in the respective column in table 1. Due to space restrictions, we suggest readers to look up Khwaja and Urban (2002) to get an explanation of each criterion and subcriterion.

2.3 Comparison

Table 1 allows us to relate specification and specification technique criteria. We can see, for instance, that the fulfilment of a technical criterion must generate the fulfilment of all specification criteria related to that criterion. The degree of fulfilment will be "Y" (Yes), "N" (No) or "P" (Partial).

Table 1. Evaluation criteria for software specifications and specification techniques

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Expressive adequacy	Understandable	Y	Y	Y	Y
	Appropriate	P	P	Y	P
	Minimal	Y	Y	Y	P
Constructibility		Y	Y	Y	P
Scope of Specifications	Complete	P	P	P	P
Level of Formality	Unambiguous	Y	Y	Y	Y
	Consistent	Y	Y	Y	Y
	Complete	Y	Y	P	Y
	Verifiable	Y	Y	Y	Y
	Validateable	Y	Y	Y	Y
Formal Foundation	Unambiguous	Y	Y	Y	Y
	Consistent	Y	Y	Y	Y
	Complete	Y	Y	P	Y
	Verifiable	Y	Y	Y	Y
	Validateable	Y	Y	Y	Y
Extent of Applicability		P	P	Y	P
Easy to Use		Y	Y	Y	P
Help Support		N	P	P	N
Integrated Environment & Tool Support		N	P	P	N
Specification Organization Support	Understandable	Y	Y	Y	Y
	Modifiable	Y	Y	Y	Y
Support for Maintainability	Modifiable	Y	Y	Y	Y
	Traceable	P	Y	P	Y
Executable	Understandable	P	N	Y	P
	Unambiguous	P	N	Y	Y
	Consistent	P	N	Y	Y

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
	Complete	P	N	P	P
	Correct	P	N	Y	Y
	Verifiable	P	N	Y	Y
	Validateable	P	N	Y	P
Tolerance for Incompleteness	Verifiable	Y	Y	P	Y
	Validateable	Y	Y	P	Y
Multiple views	Understandable	Y	Y	Y	Y
Flexibility & Notational Simplicity	Understable	Y	Y	Y	P
Internal Verification Support	Unambiguous	N	N	N	N
	Complete	N	N	N	N
	Consistent	N	N	N	N
	Verifiable	N	N	N	N
External validation Support	Correct	Y	P	P	Y
	Validateable	P	P	P	Y
Support for other Development Phases	Traceable	N	P	P	N
Support for Documentation Generation	Understandable	P	P	P	N

All the proposed ideas are very interesting and they provide important contributions to solve the security problem in a methodological approach. Nevertheless, they have a series of limitations. For instance, one of the main deficiencies of these proposals is the automated support that each one of these methodologies need, specifically, it can be mentioned the lack of an automatic instrument of internal verification. Moreover, none of them considers security aspects in multidimensional modeling. As there is not a proposal to model security problems in the systems development in an analytical environment, a solution is required to be provided. This solution can be the definition of a new methodology or an extension of an already existing methodology.

3. MULTIDIMENSIONAL SECURITY MODELING PROPOSAL

In this section, we will describe the UML extension for multidimensional modeling. Later on, we will describe extensions for security in multidimensional modeling. Finally, we will provide an example to clarify the concepts dealt with in our proposal.

3.1 Object-oriented Multidimensional Conceptual Modeling

There is a mature field in relation to methodologies and techniques associated to multidimensional modeling, such as Golfarelli *et al.* (1998), Kimball *et al.* (1998), Trujillo *et al.* (2001), Sapia *et al.* (1999). However, there is an immature field regarding to the fact of taking into account security aspects in these methodologies and techniques. Some security proposals associated to multidimensional modeling have been developed but they are punctual solutions that partially comprise the necessary security requirements. Furthermore, none of these proposals considers a methodological approach formally including security in the process of multidimensional design.

Our conceptual modeling approach, based on UML to represent the structural properties of multidimensional modeling, has been specified through an UML profile that includes the necessary stereotypes to carry out multidimensional modeling successfully (Luján-Mora *et al.*, 2002). In table 2, we can see a summary of class and attribute stereotypes, defined together with a brief description and the respective icon to make their use and interpretation easier.

Table 2. Stereotypes for classes and attributes

Name	Type	Description	Icon
Fact	Class	Classes of this stereotype represent facts in a MD model.	
Dimension	Class	Classes of this stereotype represent dimensions in a MD model.	
Base	Class	Classes of this stereotype represent dimension hierarchy levels in a MD model.	B
OID	Attribute	Attributes of this stereotype represent OID attributes of Fact, Dimension or Base classes in a MD model.	OID
FactAttribute	Attribute	Attributes of this stereotype represent attributes of Fact classes in a MD model.	FA
Descriptor	Attribute	Attributes of this stereotype represent descriptor attributes of Dimension or Base classes in a MD model.	D
DimensionAttribute	Attribute	Attributes of this stereotype represent attributes of Dimension or Base classes in a MD model.	DA

The main structural properties of multidimensional modeling are specified by means of a UML class diagram in which the information is clearly separated into facts and dimensions. Dimensions and facts are represented by *dimension clases and fact classes*, respectively. Derived measured can also be explicitly considered (indicated by /) and their derivation rules are placed between braces near the fact classes, as shown in Fig. 1 (a). With respect to dimensions, every *classification hierarchy* level is specified by a class (called a *base class*). An association of classes specifies the relationships between two levels of a classification hierarchy. The constraint {dag} may represent both alternative path and multiple classification hierarchies. Every classification hierarchy level must have an *identifying* attribute (constraint {OID}) and a *descriptor attribute* (constraint {D}).

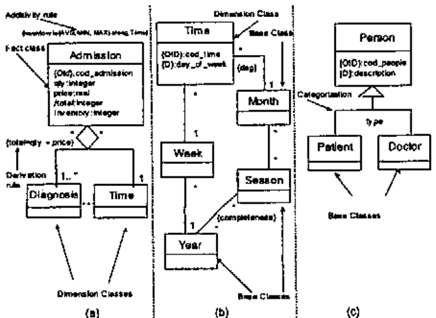

Figure 1. Multidimensional modeling using UML

Defining the {completeness} constraint in the target associated class role addresses the completeness of a classification hierarchy (see an example in Fig. 1 (b)). This approach assumes all classification hierarchies are non-complete by default. The *categorization of dimensions*, used to model additional features for a class's subtypes, is represented by means of generalization–specialization relationships. An example of categorization for the Person dimension is shown in Fig. 1 (c).

3.2 Security Extension for Multidimensional Modeling

Based on the multidimensional modeling stated in this paper, we propose the following extension mechanisms for secure multidimensional conceptual modeling:

- Labeled values: This kind of extension will allow us to indicate the security level of information in a fact class, dimension class or base class. Each security label will be able to store information related to the level of sensitiveness of information, user roles and different information organizational compartments. The higher the level of security, the higher the level of sensitiveness. User roles will be necessary when the organization in which DW is implemented is too big and requires the grouping of DW users in hierarchically organized groups (that will be called "roles") that have different functions within the organization and therefore have access to specific data. Compartments will allow us to identify areas that will describe the sensitiveness of a labeled data and associate this data to one or several security areas.
- Constraints: Constraints are specified by using OSCL language (Piattini and Fernández-Medina, 2001), that was specially designed to specify security constraints. Using this constraint language, it is possible to specify in the model not only inherent constraints but also all the rest of constraints (except for those ones based on events that should be managed from an extended dynamic model).

We can identify, and specify with complex OCL constraints many well-formedness rules. These rules are grouped as follows:

- The security information of instances. For example, the security level of the instance of a class has to be included in the ranking of security levels that has been defined for the class.
- Relationship between the security information of classes, and its attributes. The security levels defined for an attribute have to be equal or more restricted that the security levels defined for its class. The same rule is applicable for the role hierarchies and user compartments.
- Categorization of dimensions. When a dimension class is specialized in several base classes, the security levels of the subclasses have to be equal or more restrictive that the security levels of the superclase. The same rule is applicable for role hierarchies and user compartments.
- Classification hierarchies. As a general rule, we can consider that the more specific the information is, the more restricted its access is.
- Derived attributes. The security levels of a derived attribute has to be equal or more restricted than the attribute which it is derived. The same rule is applicable for user roles and compartments. By default, the derived attributed inherit the security information of the attribute it proceed.
- Combination of dimensions. For example, a query that involves the combination of a dimension class and the fact class has to consider the combination of the security information of the dimension class and of the fact class. The security levels of the combination will be the most restrictive from the security levels of the dimension class and the fact class.

3.3 Example of the Modeling of a Security MD Model

The case study that we consider here is related to a hospital patient admission. The example shown is an adaptation of examples shown by Golfarelli *et al.* (1998) and Bach and Jensen (1998). Patient admission is composed of a fact class called Admission, several dimension classes called Diagnosis, Person, Time and Age and the Base Classes that can be seen in Figure 2.

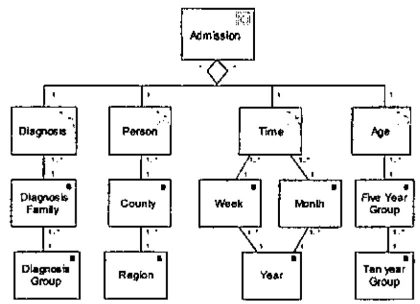

Figure 2. Multidimensional modeling using UML

With the objective of showing the problem we are dealing with in a more detailed way, we can see figure 3 as well.

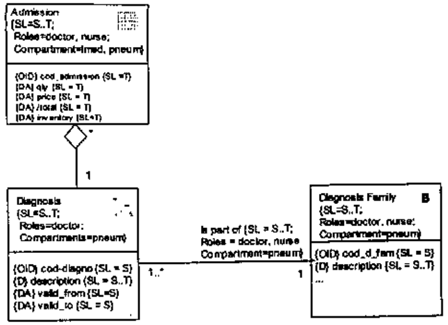

Figure 3. Multidimensional modeling security constraints

Figure 3 shows us security constraints for Admission fact class, *Diagnosis* dimension class and *Diagnosis Family* base class. We can see that the most restrictive constraint must be in the Fact class since it is the one that has the lowest level of granularity. Furthermore, it contains the confidential measures that must not be acceded by any user. The level of sensitiveness applied in this example considers the following values: T= Top Secret, S=Secret, C=Confidential and U=Unclassified. In this example, we can see that there are some attributes that have a range of levels (for example, description attribute has the S..T range of levels, which means that OSCL must specify a constraint when S or T levels are obtained. Let us consider, for instance, the setting up of a constraint in OSCL for Diagnosis dimension class.

```
Context Diagnosis inv:
self.level=if self.description='aids' or
            self.description='cancer'then T else S
```

This constraint allows us to specify that patients with certain diseases will have their data more protected so that their privacy cannot be violated. As information regarding aids or cancer is denied in this dimension, it will not be possible to have access to the fact class which would allow not only to obtain the stored measures but also to access to the rest of dimensions through the facts (such as personal data).

Moreover, in this example, we can see that a user fulfilling all the requirements to access to Diagnosis Dimension Class has not access to Admission fact class; because this access is restricted by the compartment (the user should have privileges in the compartments imed (Internal Medicine) and *pneum* (pneumatology). One of the inherent constraints is that user should have privileges in all compartments of the class.

4. CONCLUSION AND FUTURE WORK

Many of the existing methodologies that incorporate security in the information systems development process do not take into account the own features of the analytical environment, in which DW, multidimensional databases and OLAP applications work. At the same time, methodologies considering multidimensional modeling do not incorporate security aspects in their stages. Therefore, we have made a comparison of methodologies incorporating security in the development of their information systems in order to detect their limitations and to take them as a basis for the incorporation of security in the uncovered aspects. In this way, we have put forward, as a solution, an extension based on UML to incorporate security in multidimensional modeling. We provide UML, with the advantages that it carries out, with security features to be able to develop modeling including, on the one hand, the UML syntax and power and on the other hand, the new security features, ready to be used, when the application includes security requirements that need these features. The application of this extension has made it possible to generate a more robust specification that it was not considered in multidimensional modeling. Besides, the use of this extension will make it easier the implementation of secure multidimensional models with some of the DBMS that are able to implement multilevel databases, such as Oracle Label Security OLS (Levinger, 2002).

The short-term future work will focus on polishing and widening the constraint language in order to cope with other kind of security constraints related to information access control depending on certain roles of the organization or certain timetable, exceptions, etc. At a short and medium term, future work will focus on the definition of an UML profile for multidimensional modeling and the development of a more complete methodology based on UML and the Unified Process, in order to develop secure DW that grant information security and help us to fulfil the existing legislation on data protection.

ACKNOWLEDGEMENT

This research is part of the CALIPO (TIC2003-07804-C05-03) and RETISTIC (TIC2002-12487-E) projects, supported by the Dirección General de Investigación of the Ministerio de Ciencia y Tecnología.

REFERENCES

Adamson, C. And Venerable, M., 1998. *Data Warehouse Design Solutions*. John Wiley & Sons, USA.

Bach, T. and Jensen, C., 1999. Multidimensional Data Modeling for Complex Data. *Proceedings of the 15th International Conference on Data Engineering ICDE'99*, Sydney, Australia, pp. 336-345.

Castano, S. *et al.*, 1995. *Database Security*. Addison-Wesley.

Fernández-Medina, E., and Piattini, M.,2003, Designing Secure Databases for OLS. *In Proceedings of Database and Expert Systems Applications: 14th International Conference DEXA*, Praga, República Checa, Lecture Notes in Computer Science, Vol 2736, Springer-Verlag, Berlin Heidelberg, pp. 886-899.

Golfarelli, M. *et al.*,1998. *Conceptual Design of Data Warehouses from E/R Schemes, Proceedings of International Conference on System Science HICCS'98*, IEEE, Hawai, USA, pp. 334-343.

Ghosh, A. *et al.*, 2002, Building Software Securely from the Ground Up. *In IEEE Software*, January/February, pp. 14-16.

ISO/IEC, 1999. *Information Technology. Security Techniques. Evaluation Criteria for TI Security. Part I: Introduction and General Mode*, Switzerland.

Jürgens, J., 2001, Towards development of Secure Systems using UML. *Proceedings of the International Conference on the Fundamental Approaches to Software Engineering FASEiTAPS*, Lecture Notes in Computer Science, Springer-Verlag, Berlin Heidelberg.

Khwaja, A. And Urban, J., 2002, A Synthesis of Evaluation Criteria for Software Specifications and Specification Techniques. *In International Journal of Software Engineering and Knowledge Engineering*, Vol 12, Nº 5.

Kimball, R. *et al.*, 1998. *The Data Warehouse Lifecycle Toolkit*. John Wiley & Sons, USA.

Kirkgoze, R. *et al.*, 1997. A Security Concept for OLAP. *Proceedings of the 8th. International Workshop on Database an Expert System Applications DEXA '97*. IEEE Computer Society.

Levinger, J., 2002. *Oracle Label Security. Administrator's guide*. Release 2(9.2). Retrieved from http://www..csis.gvsu.edu/GeneralInfo/Oracle/network.920/a96578.pdf.

Liu, L. *et al.*, 2003. Security and Privacy Requirements Analysis within a Social Setting. *Proceedings of the 11th IEEE International Requirements Engineering Conference*, IEEE Computer Society.

Luján-Mora, S. *et al.*, 2002. Extending the UML for Multidimensional Modeling. *Proceedings of the 5th International Conference on the Unified Modeling Language*, Dresden, Germani, LNCS 2460, Springer-Verlag, pp. 290-304.

Marks, D. *et al.*, 1996. MOMT: A Multilevel Object Modeling Technique for Designing Secure Database Applications. *In Object-Oriented Programming*, Vol. 9, Nº 4, pp. 22-29.

Piattini, M. and Fernández-Medina, E., 2001. Specification of Security Constraints in UML. *Proceedings of the 35th Annual 2001 IEEE International Carnahan Conference on Security Technology ICCST 2001*, London, United Kingdom, pp. 163-171.

Priebe, T. and Pernul, G., 2000. Towards OLAP Security Design – Survey and Research Issues. *Proceedings of the 3rd ACM International Workshop on Data Warehousing and OLAP DOLAP 2000*, Washington DC.

Rosenthal, A. and Sciore, E., 2000. View Security as the Basic for Data Warehouse Security. *Proceedings of the International Workshop on Design and Management of Data Warehouse (DMDW'2000)*, Sweden.

Sapia, C. *et al.*, 1999. Extending the E/R Model for the Multidimensional Paradigm. *Proceedings of Advances in Database Technologies*, LNCS 1552, Springer-Verlag.

Trujillo, J. *et al.*, 2001. Designing Data Warehouses with OO Conceptual Models. *In IEEE Computer*, Vol 34, Nº 12, pp. 66-75.