Volume 30, Issue 6, August 2008

ISSN: 0920-5489

ELSEVIER

COMPUTER STANDARDS & INTERFACES

SPECIAL ISSUE

State of Standards in the Information Systems Security Area

Guest Editors: Eduardo Fernández-Medina and Mariemma I. Yagüe

The International Journal on the Development and Application of Standards for Computers, Software Quality, Data Communications, E-topics, Interfaces and Measurement

COMPUTER STANDARDS & INTERFACES (CS&I)

The International Journal on the Development and Application of Standards for Computers, Software Quality, Data Communications, Interfaces and Measurement

---

Aims and scope

The quality of software, well-defined interfaces (hardware and software), the process of digitalisation, and accepted standards in these fields are essential for building and exploiting complex computing, communication, multimedia and measuring systems. Standards can simplify the design and construction of individual hardware and software components and help to ensure satisfactory interworking.

COMPUTER STANDARDS & INTERFACES is an international journal dealing specifically with the topics below.

The journal:

- provides information about activities and progress on the definition of computer standards, software quality, interfaces and methods, at national, European and international levels
- publishes critical comments on standards and standards activities
- disseminates user's experiences and case studies in the application and exploitation of established or emerging standards, interfaces and methods
- offers a forum for discussion on actual projects, standards, interfaces and methods
- stimulates relevant research by providing a specialized refereed medium.

COMPUTER STANDARDS & INTERFACES is concerned with the specification, development and application of standards and with high-level publications of developments and methods in the following areas:

- ***Standards, Information Management, Formal Methods*** - Computers, Processors, Storage, Operating systems, Languages, Databases, Graphics, User interface, Multimedia, Information security, Office automation, Development of standards and instruments, Applications
- ***Software Quality, Software Process*** - Languages, Operating systems, Programming, Requirements specification, Design & implementation, Inspection & test, Maintenance, Product and process evaluation, Performance, Tools, Metrics, Embedded systems, Software in measurement and technical systems including real-time aspects, Development of International Standards in Software Engineering
- ***Distributed Systems, Open Systems, E-Topics*** - Digital interfaces, System and device buses, Fieldbuses, Data communication, Distributed computing, Protocols, Open systems interconnection, Local and wide area networks, Internet, Worldwide Web, Network security, Cryptology, E-services, E-business, E-commerce
- ***Data Acquisition*** - Analog-to-digital conversion, Specification, Modelling, Industrial electronics, Real-time systems, Laboratory automation, Automatic measurement, Process control, Electromagnetic compatibility
- ***Digital Instruments Standardization*** - Forum of EUPAS, European Project for ADC-based devices Standardisation (IMEKO TC-4 Working Group on A/D and D/A Converter Metrology), IEEE TC-10, IEC TC-42/WG8, IEC TC-85/WG16; Standardisation of specifications, modelling, testing, and analog and digital processing for digital instruments

The last issue of a volume includes an Author index and a Subject index.

CS&I also covers general topics concerning the standardization process, such as technical, political and commercial aspects of standards, their impact on the marketplace, cost/benefit analyses, legislative issues, and relationships among national and international standards bodies.

COMPUTER STANDARDS & INTERFACES
Volume 30/6

ELSEVIER

Amsterdam • Boston • Jena • London • New York • Oxford • Paris •
Philadelphia • San Diego • St. Louis

Printed in Printforce, Alphen a/d Rijn, The Netherlands

♾ The paper used in this publication meets the requirements of ANSI/NISO 239.48-1992 (Permanence of Paper)

COMPUTER STANDARDS & INTERFACES

Special Issue:

State of standards in the information systems security area

Guest Editors:

Eduardo Fernández-Medina
Mariemma I. Yagüe

Available online at www.sciencedirect.com
ScienceDirect
Computer Standards & Interfaces 30 (2008) 339–340
COMPUTER STANDARDS & INTERFACES
www.elsevier.com/locate/csi

Guest Editorial

State of standards in the information systems security area

The development and use of standards in information technologies, and in particular, in the area of security, have grown up in the last years. The main reason is the increasing need for interoperability due to the new scenarios (e.g. collaborative work, heterogeneous IT processes and systems) that have emerged on the Web.

As standards represent an important means of achieving interoperability on the WWW and the Web has become a new global platform, the scientific community focuses its attention on the different international standards bodies and organizations, such as the National Institute of Standards and Technology (NIST), the International Standard Organization (ISO), the International Electrotechnical Commission (IEC), the Institute of Electrical and Electronics Engineers (IEEE), the International Telecommunication Union (standardization section — ITU-T), the Organization for the Advancement of Structured Information Standards (OASIS), the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), etc. Not only specifications from these organisms become standards but also recommendations from very representative consortiums, such as the Object Management Group (OMG) become de facto standards as well.

These standards and specifications are crucial in many areas related to security in information systems. First of all, standards are important for unifying security techniques in different aspects, such as security protocols, cryptography, access control, authentication, privacy, integrity, attack detection, availability, personal data protection, etc. Secondly, an organizational view of security is very relevant too. Therefore, standards also reach this approach through the definition of security management systems, security maturity models, risk management guidelines, and so on. Nevertheless, standards are intensively considered in software engineering processes for developing information systems, and these standards are constantly redefined and extended in order to incorporate security into the software development. In this sense, standards and specifications define software modeling techniques, requirement engineering techniques, architecture languages and specifications, pattern definitions, life cycles models, software development methodologies, metamodeling techniques, etc., and also many specific technologies, with specific security requirements, such as Web services, grid computing, mobile devices, etc.

This Special Issue of the International Journal of Computer Standards and Interfaces includes a selection of the most representative papers presented at the Fifth International Workshop on Security in Information Systems (WOSIS 2007), which was held in Funchal, Madeira — Portugal, June 12–13, 2007. This edition of the workshop has been specially oriented to standards for security in information systems, obtaining a representative sample of the existing papers dealing with security and where standards fulfill a relevant role.

Our workshop has matured year by year, and it is established as a forum for high quality research papers in the area of security in information systems. The most valuable assets of this workshop to be attractive for authors are a very exclusive set of program committee members, along with the invitation of exceptional speakers, highly relevant in this scientific area. Among them, we can mention, for example, Yvo Desmedt, Sushil Jajodia, Ernesto Damiani, Leonardo Chiariglione, and Ruth Breu. Additionally, selections of the best papers of past editions of the workshop have been published in international journals such as Information Systems Security, Journal of Research and Practice in Information Technology, and Internet Research.

In the following paragraphs, a brief introduction to each selected paper will be stated.

The first contribution by Soler et al., presents an extension to the CWM (Common Warehouse Metamodel) specification developed by the OMG (Object Management Group) with the aim of specifying security in data warehouse models at the PSM (Platform Independent Model) level of the Model Driven Architecture. In this paper, standards such as UML, CWM, MOF, QVT, MDA are intensively used in the area of software engineering, with the purpose of integrating security into the development of data warehouses.

The second contribution by Tafreschi et al., deals with a reputation system, which, on the one hand, facilitates trust building among business partners who interact in an ad hoc manner with each other, and on the other hand enables market participants to rate the business performance of their partners as well as the quality of the offered goods. In this proposal, many types of standards and specifications, such as HTTP, XML, SOAP and WSDL are directly and indirectly used for the definition of the system architecture.

The third paper by Mellado et al., states a security standard-based process for software product line development. The proposal is a contribution in the area of security requirements engineering for software product lines, but providing its integration

0920-5489/$ - see front matter
doi:10.1016/j.csi.2008.03.001

with the Common Criteria (ISO/IEC 15408), as well as with some of the most relevant standards related to security management, such as ISO/IEC 17799 and ISO/IEC 27001. This proposal also conforms to IEEE 830-1998, regarding software requirements specification.

The fourth manuscript by Agreiter et al., puts forward a framework that provides fair non-repudiation for Web services messages, since there is not any sophisticated standard specifying this requirement for this environment. However, the paper deals with several standards, specifications, and protocols, such as UML, XML, SOAP, SSL, WSS, TTP, XACML, etc.

The fifth contribution, by Damiani et al., specifies a general query rewriting technique to securely query XML, the standard for data interchange. The proposed model is described by a Deterministic Finite Automata and is able to rewrite unsafe queries into safe ones, avoiding the many backtrackings inherent to non-deterministic finite automata. The proposed technique is linear with the size and depth of the repository schema.

The sixth contribution, by Plößl and Federrath, deals with security requirements of vehicular ad hoc networks (VANET). Nodes (mainly vehicles) are expected to communicate by means of the North American DSRC standard that makes use of the IEEE 802.11p standard for wireless communication. Authors evaluate some requirements such as message integrity and non-repudiation as well as propose a security infrastructure meeting all requirements, specially designed to protect privacy of the VANET users and efficient in terms of computational needs and bandwidth overhead.

The seventh contribution, by Canfora and Visaggio, refers to privacy preservation in highly dynamic, untrustworthy and scalable contexts, implementing the paradigm of front end trust filter. Therefore, the proposed solution makes the assumption that a privacy policy can be expressed at least at three different levels of detail, so-called layers, in other words, the statement of the policy, the strategies for realizing such policy and the implementation, which applies the strategy at the level of applications and database. This three-layered structure confers a high degree of flexibility.

The eighth contribution, by Zych, et al., studies the key management problem of the data-centric protection model, where data is cryptographically protected and allowed to be outsourced or even freely float on the network. Namely, when data is encrypted, the access control policies have to be taken into account so that control regulating what users are allowed to access to what data is maintained. Authors propose an efficient method that eliminates, as compared to broadcast encryption methods, the need for multiple copies of data keys and reduces to a single key the storage required per user. The solution is based on the Diffie–Hellman Key Exchange protocol, standardized by the RSA Laboratories as the Diffie–Hellman Key Agreement Standard.

The ninth contribution, by Sánchez, et al., is focused on the authorization problem. It shows how the eduroam user federation for an inter-NREN network roaming service based on AAA servers and the IEEE 802.1X standard can take advantage of the use of authorization services with the objective of offering a more grained network access control process. For that purpose, this work presents how eduroam can be extended with the NAS-SAML infrastructure and eduGAIN. The first is a network access control approach based on the AAA architecture and authorization attributes and the SAML and XACML standards. Secondly, the main goal of eduGAIN is to build an interoperable authentication and authorization infrastructure to interconnect different existing federations.

The tenth paper by Prandini and Ramilli proposes a communication scheme for remote system administration aimed at overcoming some intrinsic security issues of the traditional client–server models. While the subject of system administration has not been the subject of a comprehensive standardization activity, this proposal provides a viable alternative to de facto standards in the area of remote access such as SSH (RFC4250–4254), IPSec (RFC4301–4303 and related ones). Furthermore, it is related to the general problem of authentication and access control as defined in ISO/IEC 10181-2/3. The proposed system is based on human-oriented meeting places such as IRC (RFC2810–2813), but future extensions can foresee the design of more structured distributed meeting places, for instance, those in accordance with the CORBA Security Service definition.

This Special Issue does not try to cover all applications of security standards in information systems, since it would be impossible. However, we hope to offer a good sample of papers to show how important the use and development of standards for information technologies, and particularly to security are.

We would like to gratefully acknowledge the hard work and kindness of all members of our international program committee when performing their timely, complete and professional reviews. We would like to thank Sabrina De Capitani di Vimercati (Italy), Ernesto Damiani (Italy), Csilla Farkas (USA), Eduardo B. Fernández (USA), Steven Furnell (UK), Christian Geuer-Pollmann (Germany), Paolo Giorgini (Italy), Ehud Gudes (Israel), Carlos Gutiérrez (Spain), Haralambos Mouratidis (England), Jan Jürjens (Germany), Stamatis Karnouskos (Germany), Antonio Maña (Spain), Martin Olivier (South Africa), Brajendra Panda (USA), Günther Pernul (Gerrmany), Mario Piattini (Spain), Joachim Posegga (Germany), Indrajit Ray (USA), Indrakshi Ray (USA), Damian Sauveron (France), Ambrosio Toval (Spain), Rodolfo Villarroel (Chile), and Duminda Wijesekera (USA).

Finally, we would like to thank Computer Standards & Interfaces and Elsevier, and particularly Professor Bhavani Thuraisingham for giving us the opportunity to publish this Special Issue.

Eduardo Fernández-Medina
ALARCOS Research Group,
Information Systems and Technologies Department,
University of Castilla-La Mancha, Paseo de la Universidad 4,
13071 Ciudad Real, Spain
Corresponding author.
E-mail address: Eduardo.FdezMedina@uclm.es.

Mariemma I. Yagüe
GISUM Research Group, Department of Computer Science
Málaga University Campus Universitario de Teatinos,
s/n 29071 Málaga, Spain
E-mail address: mariemma@lcc.uma.es.

Computer Standards & Interfaces 30 (2008) 341–350

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Building a secure star schema in data warehouses by an extension of the relational package from CWM

Emilio Soler [a,*], Juan Trujillo [b], Eduardo Fernández-Medina [c], Mario Piattini [c]

[a] Department of Computer Science, University of Matanzas, Autopista de Varadero km 3, Matanzas, Cuba
[b] Department of Software and Computing Systems, University of Alicante, C/San Vicente S/N 03690 Alicante, Spain
[c] ALARCOS Research Group, Information Systems and Technologies Department, UCLM-Soluziona Research and Development Institute, University of Castilla-La Mancha, Paseo de la Universidad 4, 13071 Ciudad Real, Spain

ARTICLE INFO

Available online 10 March 2008

Keywords:
Security
Star scheme
CWM
Data Warehouses

ABSTRACT

Data Warehouses (DWs) are widely accepted as the core of current decision support systems. Therefore, it is vital to incorporate security requirements from the early stages of the DWs projects and enforce them in the further design phases. Very few approaches specify security and audit measures in the conceptual modeling of DWs. Furthermore, these security measures are specified in the final implementation on top of commercial systems as there is not a standard relational representation of security measures for DWs (i.e. the well-known star schema does not allow us to specify security and audit measures on its multidimensional representation of data; instead, they must be specified on top of the implemented relational tables). On the other hand, the Common Warehouse Metamodel (CWM) has been accepted as the standard for the exchange and the interoperability of metadata. Nevertheless, it does not allow us to specify security measures for DWs. In this paper, we make use of the own extension mechanisms provided by the CWM to extend the relational package in order to build a star schema that represents the security and audit rules captured during the conceptual modeling phase of DWs. Finally, in order to show the benefits of our extension, we apply it to a case study related to the management of the pharmacy consortium business.

1. Introduction

Data Warehouses (DWs) play a central role in current decision support systems because they provide crucial business information through which to improve strategic decision-making processes [8]. Organizations have begun to adopt more and more computerized information systems, which rely upon databases and DWs that require more security, because the very survival of the organization depends on the appropriate manipulation, security and confidentiality of information [4]. On the other hand, it is widely accepted that the design of DWs is based on multidimensional (MD) modeling which structures the information into facts and dimensions.

As for traditional databases, we follow the three design phases proposed by ANSI/SPARC [2] in the design of data warehouses from user requirements to the final implementation, i.e. the business (requirement analysis), conceptual, logical and physical levels.

Following this procedure, we align the design of DWs with the Model Driven Architecture (MDA) [21]. MDA allows us to achieve the portability and interoperability of software systems by means of transformations between models. To help us with these transformations, the Query/View/Transformation (QVT) Language [22] is proposed in order to allow us to accomplish automatic transformations between models. MDA proposes several models at different levels: Computation Independent Model (CIM), Platform Independent Model (PIM), Platform Specific Model (PSM) and Code. In our context, the CIM corresponds with the work [15], which is based on an extension of the i* framework considered [36]. The proposal will be extended to consider security at the business level (see 7: Future work section). The PIM corresponds with an extension of the Unified Modeling Language (UML) profile [11] presented in [34] which allows us to consider the main properties of secure MD modeling at this stage. The PSM corresponds with our extension of the Common Warehouse Metamodel (CWM) at the logical level and the Code with implementation at the physical level, i.e. with a Database Management System (DBMS). Fig. 1 shows the relationship between MDA and the DWs lifecycle in detail. In this paper, we focus on the logical level. It is out of the scope of this paper to consider the business and physical levels. See, the 7: Future work section.

As we will describe in the related work section, security has hardly been contemplated in literature. Normally in DWs projects, security aspects are implemented in the final stages of the design. However, information security is a serious requirement which must be given careful thought, not as an isolated aspect, but as an element which is

* Corresponding author.
E-mail addresses: emilio.soler@umcc.cu (E. Soler), jtrujillo@dlsi.ua.es (J. Trujillo), eduardo.fdezmedina@uclm.es (E. Fernández-Medina), mario.piattini@uclm.es (M. Piattini).

0920-5489/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2008.03.002

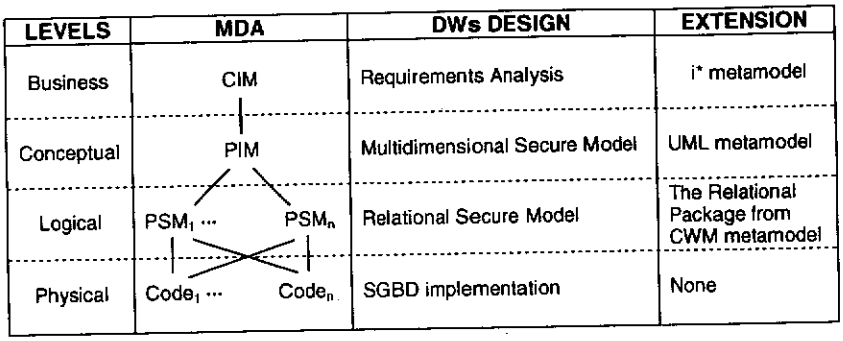


Fig. 1. Aligning the design of DWs with MDA.

in all development lifecycle stages, from requirement analysis to implementation and maintenance [3].

The works [6,7,34] extend the proposal presented in [11] to incorporate security aspects to the DWs design at the conceptual level. In order to align our architecture with MDA we need to build a secure PSM that allows us to represent security and auditing aspects. On the other hand, MDA does not provide security specific modeling facilities and its general modeling facilities fail to satisfy one or more of the security protocol modeling aspects [16].

The previous work presented in [14] employs MDA for DWs development, choosing the relational metamodel from CWM [19]. The relational package of CWM enables mediated interchange between relational databases from the majority of relational commercial systems [26]. CWM also offers the On-Line Analytical Processing (OLAP) package for the essential OLAP concepts common to most OLAP systems. However, the OLAP package is a general metamodel with which to exchange metadata information, and therefore, it only considers general aspects of multidimensional modeling. Thus, we do not consider it to be appropriate for the conceptual modeling of complex and real case DWs. For the conceptual modeling phase, we have based our proposal on UML [11], which offers a greater level of expressiveness of MD modeling at the conceptual level. The CWM offers facilities through which to access and exchange data warehouse metadata. However, security and audit measures cannot be modeled in the CWM because it does not provide the modeling constructors through which to represent data security related to issues such as access rights, users or roles [18]. Most data access control approaches are based on the proprietary metadata structures of specific software products [25]. Thus, integrating security related to metadata into the CWM improves the security support and facilitates the establishment of a standardized access control mechanism for data warehouses [18]. According to the MDA we do not need the metadata of a DBMS; we need a metamodel that allows us to represent security and audit measures at the logical level, i.e., a PSM which in our case corresponds with a relational platform. In order to achieve this goal we have extended the relational package from the CWM.

Hence, in this paper we present an extension of the relational metamodel from CWM by using its own extension mechanisms. By using QVT, we automatically transform all the security and audit measures captured from the conceptual modeling phase of the DWs design at the logical level. Our main contribution is that the proposed extension allows us to represent all the requirements of security and audit captured during the conceptual modeling phase at the logical level.

The remainder of this paper is structured as follows. The works related to our proposal are discussed in Section 2. Secure MD modeling is introduced in Section 3. Section 4 shows an overview of the CWM. Section 5 presents our extension of the relational metamodel from CWM. Then, in Section 6, we develop a case study in order to build a secure star scheme using our extension in the design of secure DWs. Finally, Section 7 draws the main conclusions and outlines our immediate future work.

2. Related work

Relevant literature on this subject comprises several initiatives to include security in the DW design. In [9] the authors describe a prototype model for DWs security based on metadata, which enables the definition of views of data for each group of users. However, this does not permit the specification of complex restrictions of confidentiality. Rosenthal and Sciore [27] extend SQL grants and create a mechanism of inferences through which to establish security. Another attempt is the architecture for both Federated Information Systems (FIS) and DWs that preserve MultiLevel security integration between FIS and DWs [28]. These approaches [9,27,28] are attractive but only focus on practical issues such as acquisition, storage and access control on the OLAP side. None of them examine the representation of security at both a conceptual and a logical stage.

On the other hand, there are more elaborate initiatives that propose authorization models for the design of DWs. For instance, in [10], the authors propose a security concept for OLAP, which is a role based security model for data warehouses. Priebe and Pernul [25] propose a security design methodology similar to that of the classical database design (requirement analysis, conceptual, logical, and physical design) which covers requirements and concrete implementations in commercial systems. The same authors extend the ADAPTed UML model for the previous conceptual phase [24], specifying a methodology and a MD security constraint language for the conceptual modeling of OLAP security. In [5], the authors show that access privileges for DWs and OLAP can be expressed more intuitively than by using SQLs grant statements. Their access control model focuses specifically on expressiveness and usability. These proposals [10,25,24] offer security models at the conceptual level by means of security constraints, but basically deal with OLAP operations. These proposals [25,24] are one of the best references in this area. As a summary, these works implement the security rules considered in their conceptual approach to commercial database systems. On the other hand, we base our approach on the works of [6,7,34] in which the authors call for the design of the security rules at all stages of the DWs design, from requirement analysis to final implementation. Therefore, in this paper, we formally extend the CWM in order to allow us to automatically transform the security rules considered at the conceptual level in the logical representation of the DW.

Some proposals related to the access and preservation of the confidential information in the analysis at the data cube level have recently appeared. In [35] the authors proposed a method for protecting sensitive data in OLAP cubes from unauthorized access and malicious inferences of sensitive values. Other proposals for preserving data privacy and range queries in data cubes in DWs are the zero-sum and the cubic-wise balance methods (respectively)

which can be found in [12,32]. These works ascertain that security in DWs is of ever-increasing interest, especially in areas where data are sold in pieces to third parties for data-mining practices. None of these proposals attempt to define security in all of the DWs development stages.

Numerous proposals exist that extend CWM with different objectives for: the modeling of logical object-orientated relational data storage and the corresponding Extract, Transform and Load (ETL) processes [13], a universal data-mining library that implements data-mining methods and algorithms [33], recording the trace information of metadata evolution and maintaining consistency during metaclass evolution [37], representing and integrating the metadata generated by data and metadata lineage implementation [29], providing quality information to DW client tools [1], and the construction of a conceptual model for data quality and cleaning, both of which are applicable to the operational and data warehousing context. However, none of the aforementioned proposals extend the relational metamodel from CWM with security aspects. Only the work presented in [31] shows how the CWM might be adequate for representing security issues for DWs at the logical level. In this paper the CWM is not formally extended through formal extension mechanisms.

3. Secure Multidimensional Modeling

The main properties of multidimensional modeling are represented by a UML profile [11], which is based on Object-Orientated (OO) conceptual modeling. In [7], the aforementioned profile is reused in order to be able to design an MD conceptual model. The profile allows us to classify both information and users in order to represent the main security aspects in the conceptual modeling of DWs. Therefore, we can classify the security information that will be used in our conceptual modeling of data warehouses. Security information is defined for each element of the model (Fact, Dimension, FactAttribute, etc.), specifying a sequence of security levels, a set of user compartments and user roles. Security constraint is considered to specify security in attributes and classes. The security information and these constraints indicate the security properties that users have to be able to access in order to access information. The description of the profile is represented as a UML package [34].

The main feature of the Secure Multidimensional Modeling (SMD modeling) considered are the many-to-many relationships between facts and one specific dimension, degenerated dimensions, multiple classification and alternative path hierarchies, and the non-strict and complete hierarchies. In this approach, the structural properties of MD modeling are represented by means of a UML class diagram in which the information is clearly organized into Fact and Dimension. These facts and dimensions are represented by SFact and SDimension classes respectively, in which S is an abbreviation for secure.

SFact classes are defined as composite classes in shared aggregation relationships of SDimension classes. The minimum cardinality in the role of the SDimension classes is 1 to indicate that every fact must always be related to all the dimensions. The many-to-many relationships between a SFact and a specific SDimension are established by means of the cardinality 1...* in the role of the corresponding dimension class. A SFact is composed of measures or SFactAttributes. By default, all measures in the SFact class are considered to be additive. For non-additive measures, additive rules are defined as constraints and are included in the SFact class. Furthermore, derived measures can also be explicitly represented (indicated by /) and their derivation rules are placed between braces near the fact class.

With respect to SDimensions, each level of a classification hierarchy is specified by a SBase class. An association of SBase classes specifies the relationship between two levels of a classification hierarchy. The only prerequisite is that these classes must define a Directed Acyclic Graph (DAG) rooted in the SDimension class (DAG restriction is defined in the stereotype SDimension). The DAG structure can represent both multiple and alternative path hierarchies. Every SBase class must also contain an identifying SAttribute OID (SOID) and a SDescriptor attribute (SD). All constraints (AuditRule, AuthorizationRule and SecurityRule) are modeled by using UML notes. The class called UserProfile will contain information about all users who are entitled to access the multidimensional model.

Fig. 2 shows an example of the MD modeling of a hotel. Booking represents a Fact (customers that book a room). This Fact contains several measures (FactAttributes) to be analyzed (Price, Quantity, Discount, and Total). Furthermore, we specify an invoice number (invoiceN) as a Degenerate dimension. On the other hand, we also consider the following dimensions as contexts through which to analyze measures: Customer, Check in date (i.e. the date when the customer checks in), Check out date (i.e. the date when the customer checks out), and Room. Customer dimension, with the following bases or hierarchy levels: Customer data, City, and Country. Each of these levels may have a Descriptor or Dimension attributes.

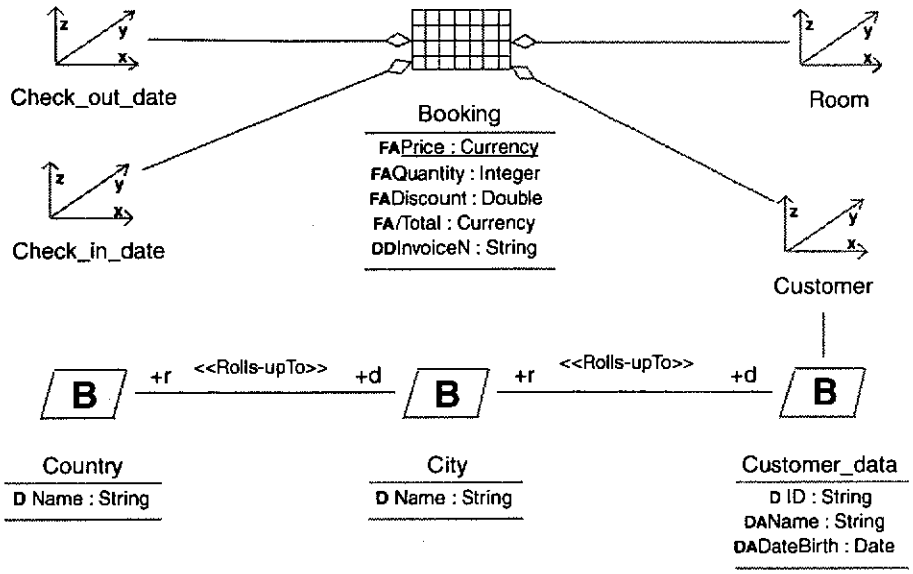


Fig. 2. An example of MD modeling without considering security.

In the following section, we present a general description of the CWM, emphasizing its structure and the different extension mechanisms.

4. An overview of the CWM

The main purpose of the CWM [19] is to enable the easy interchange of warehouse and business intelligence metadata between warehouse tools, warehouse platforms and warehouse metadata repositories in distributed heterogeneous environments. CWM is based on three key industry standards:

- UML (Unified Modeling Language), an OMG standard specification language for object modeling.
- MOF (Meta Object Facility), an OMG metamodeling and metadata repository standard.
- XMI (XML Metadata Interchange), an OMG metadata interchange standard.

The UML standard defines a rich, object-orientated modeling language that is supported by a range of graphical design tools. The MOF standard defines an extensible framework for defining models for metadata, and providing tools with programmatic interfaces with which to store and access metadata in a repository. The XMI standard allows metadata to be interchanged as streams or files with a standard format based on XML. CWM has been designed to conform to the "MOF model". It belongs to the M2 layer metamodel, and we refer the reader to [19,23,26] for further details on the different metamodel layers of the CWM.

4.1. Organization of the CWM

In [17] the authors showed the organization of CWM in detail. CWM is organized into 21 separate packages which are grouped into five stackable layers by means of similar roles. See Fig. 3.

From the organization represented in Fig. 3, we will mainly focus our work on the Resource layer and, more precisely, on the relational package as a relational metamodel that describes the corresponding metadata of the relational data resources. The Resource layer describes the structure of data resources that act as either sources or targets of a CWM mediated interchange. The relational package describes data which are accessible through a relational interface such as a native Relational Database Management System (RDBMS), Object Database Connectivity (ODBC), or Java Database Connectivity (JDBC).

The relational package depends on the following:

- org.omg::OMG::ObjectModel::Behavioral
- org.omg::OMG::ObjectModel::Core
- org.omg::OMG::ObjectModel::Instance
- org.omg::OMG::Foundation::DataTypes
- org.omg::OMG::Foundation::KeysIndexes

The relational package, as do the other data packages, defines top level containers (Catalog, Schema), that extend the ObjectModel Package class. Schema is a collection of tables. A ColumnSet represents any form of relational data. A Table is a cataloged version of a ColumnSet, which contains Columns. A ForeignKey associates columns from one table with columns from another table. The PrimaryKey class inherits from the UniqueConstraint. The PrimaryKey and ForeignKey metaclasses are owned by the Table metaclass [19].

4.2. CWM extensibility mechanism

CWM provides extension mechanisms with which to build specific metamodels. According to [20], there are two general techniques through which to extend CWM:

- Use of the general extension mechanisms provided by the UML Object Model, by means of tagged values and stereotypes. This approach is usually used for minor extensions (for example additional attributes to objects model) that are not significant enough to require the creation of a specific model.
- Non-normative model extensions or modeled extensions (sometimes called subclass or modeled extensions [26]) documented as additional metamodel packages that extend the CWM metamodel. This proposal is used for more complex extensions, and the CWM itself is built by following this extension type.

An additional extension technique is available to the CWM developer-XMI extension [23]. However, using XMI extensions might be best left as a technique intended for professional programmers who are interested in building tool-specific CWM interchange definitions. To represent security aspects at the logical level we need to introduce new classes and associations, hence, the non-normative extension is the preferred mechanism, because it is not a simple extension [26].

In the following section, we use the non-normative extension mechanism to extend the relational package, in order to represent security and audit rules at the logical level.

5. The SECRDW extension

The extension of the relational package from CWM defines new classes which will permit the representation of all the security and audit requirements captured during the conceptual modeling phase of DWs design at the logical level. This extension will be called the SECure Relational Data Warehouses (SECRDW) metamodel, which depends on the following packages: Relational, Core and Data Types.

5.1. Inheritance

In Fig. 4 the new classes that conform to the SECRDW package are shown in grey, whereas classes from the CWM metamodel remain in white. The SSchema (SCatalog) classes specialize in the schema (catalog) classes to allow a secure schema (catalog). STable and the UserProfile specializes in the Table metaclass. The SColumn specializes in the Column metaclass. The UserProfile table is a special table that stores information about users who have access to the systems,

Management	Warehouse Process				Warehouse Operation			
Analysis	Transformation		OLAP		Data Mining	Information Visualization		Business Nomenclature
Resource	Object		Relational		Record	Multidimensional		XML
Foundation	Business Information	Data Types		Expressions	Keys and Indexes		Software Deployment	Type Mapping
Object Model	Core		Behavioral		Relationships		Instance	

Fig. 3. CWM metamodel layering and its packages.

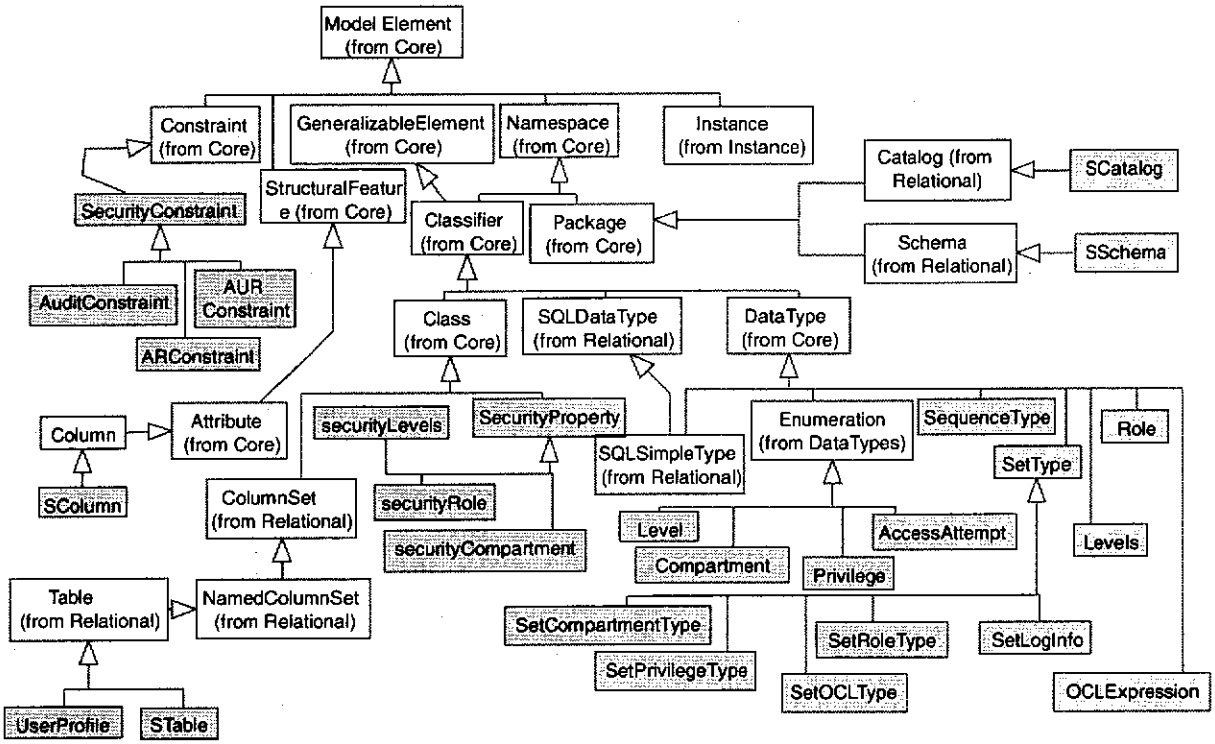


Fig. 4. SECRDW Package Inheritance.

and these rights are specified by SecurityProperty (securityLevel, securityCompartment and securityRole). STable and SColumn have associated security information by means of SecurityProperty (securityLevel, securityCompartment and securityRole). SecurityProperty specializes in the Class (from Core) metaclass and with it we establish, by means of securityLevel, securityCompartment and securityRole, access properties over tables and columns that the user must fulfill if s/he is to access them.

AuditConstraint is useful both as a deterrent against misbehavior and as a means by which to analyze user behavior by employing the system to find out possible attempted or actual violations. AuditConstraint is essential to record the accesses to tables and columns which are performed by users. ARConstraint allows us to define rules for specifying multilevel security policies in tables and columns. AURConstraint, may coexist with ARConstraint, and enable us to specify access to the tables and columns, thus permitting us to specify much more elaborate security models. The SecurityConstraint class logically inherits properties of the Constraint class from Core. The data types are studied in greater depth in the following section.

5.2. New data types

In general, the CWM packages only support data type attributes that are considered necessary for information interchange between systems [19]. If we are to represent security and audit information at the logical level then we need new data types. In Fig. 5 new classes

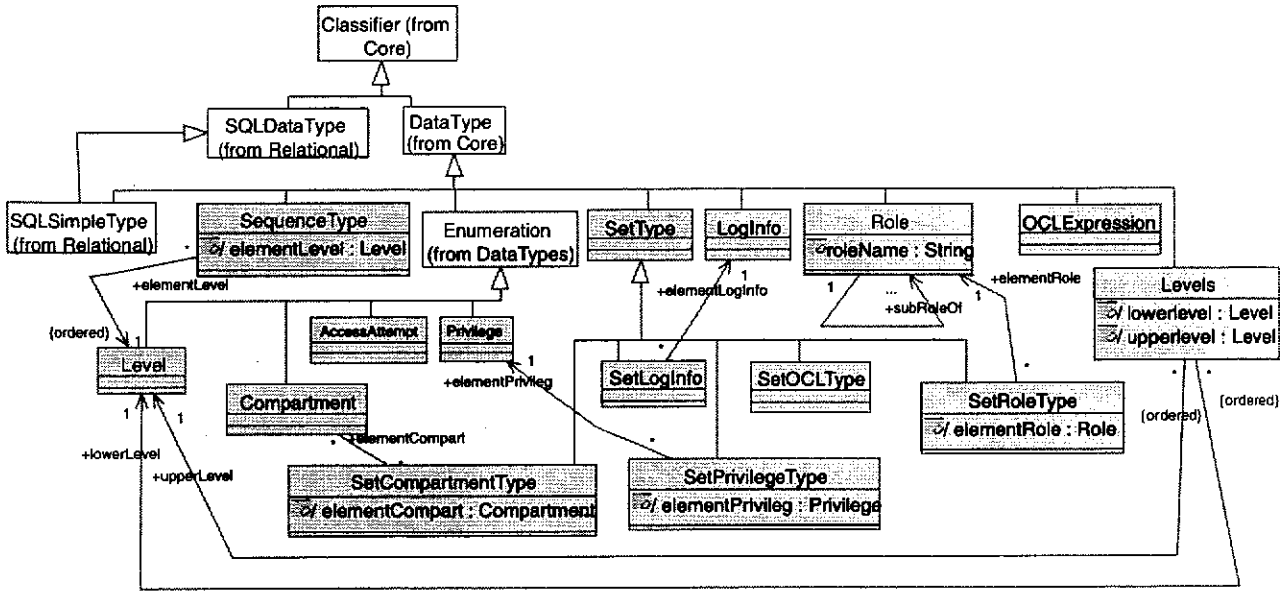


Fig. 5. New data types for SECRDW package.

appear that inherit from DataType or from Enumeration classes. The new classes that represent new data types appear in grey in Fig. 5. These new data types are necessary to model the access properties (SecurityProperty) and the constraints (SConstraint) to STable, UserProfile and SColumn.

The SequenceType class represents a data type that allows the specification of all the levels of security that can be used by the elements of the model (ordered from minor to the most restrictive). Level is an ordered enumeration composed of all the security levels that have been considered (unclassified, confidential, secret and top Secret). Compartment is the enumeration composed of all the user compartments that have been considered. Privilege will be an ordered enumeration composed of all the different privileges that have been considered (read, insert, delete, update, all). Attempt will be an ordered enumeration composed of all the different access attempts that have been considered (all, frustratedAttempt, successfullAccess, none). Levels will be an interval of levels composed of a lower level and an upper level. If the upper and lower security levels coincide, all instances will have the same security level; otherwise, the specific level will be defined according to a SecurityConstraint. OCLExpression specifies an Object Constraint Language (OCL) expression that fulfils some conditions for the users of the system. Role will represent the hierarchy of user roles that can be defined. SetRoleType specifies a set of users; each role is the root of a subtree of the hierarchy of user roles considered. SetCompartmentType represents a set of compartments. SetPrivilegeType specifies the privileges the user can receive or remove. SetOCLType specifies the tables involved in a query performed by the user, in order to establish a new requirement for tables or columns by means of SecurityConstraint (ARConstraint or AURConstraint). SetLogInfo specifies the elements that we wish to register for a future audit, and usually refers to the subject requesting access (subjectID), tables or columns to be accessed (objectID), the operation requested (action), the time of the request (time) and the access control response (response).

5.3. New secure classes and main association

The SECRDW package defines a container SCatalog and SSchema which are inherited from Schema and Catalog respectively. SCatalog is a local repository of meta data which describes all the databases maintained by the relational database engine. SSchema is a collection of STables and securityProperties and is aimed at security at the model level. A ColumnSet represents any form of relational data. A STable and UserProfile are inherited from Table, which contains Columns. Note that in Fig. 6 the table UserProfile contains columns through which to specify the access properties (SecurityProperty) that the user has. UserProfile, unlike STable, is unique and has no association with the rest of the tables of the system. A ForeignKey associates columns from one table with columns from another table. The PrimaryKey class inherits from the UniqueConstraint. The PrimaryKey and ForeignKey metaclasses are owned by the STable metaclass (see Fig. 6).

In order to represent security and audit measures in the new metamodel, we have added some metaclasses.

The SecurityProperty metaclass inherits from the Class (from Core) metaclass and specializes in securityLevels, securityCompartments and securityRoles metaclasses. Furthermore, in order to represent security constraints, authorization rules and audit rules in the metamodel we have added the AuditConstraint class, the ARConstraint class and the AURConstraint class, which inherit from SecurityConstraint. To specify constraints, depending on particular information of a user or a group of users, we have introduced the UserProfile metaclass. Observe in Fig. 6 the new classes that we have added to the relational package from CWM, as well as the new associations between classes. The new classes contain attributes of each of the types specified in Fig. 5. These attributes allow us to represent all the security information captured during the conceptual modeling of the DWs design. The objectCond attribute refers particularly to an additional condition imposed upon the STable or SColumn object. The subjectCond attribute allows us to specify a condition for the users of the system.

In the following section, we show how we use the extension in the representation at the logical level of a secure MD model related to the management of pharmacy consortium businesses.

6. A case study

In this section, we apply our extension of the CWM relational metamodel to the context of a pharmaceutical consortium. This

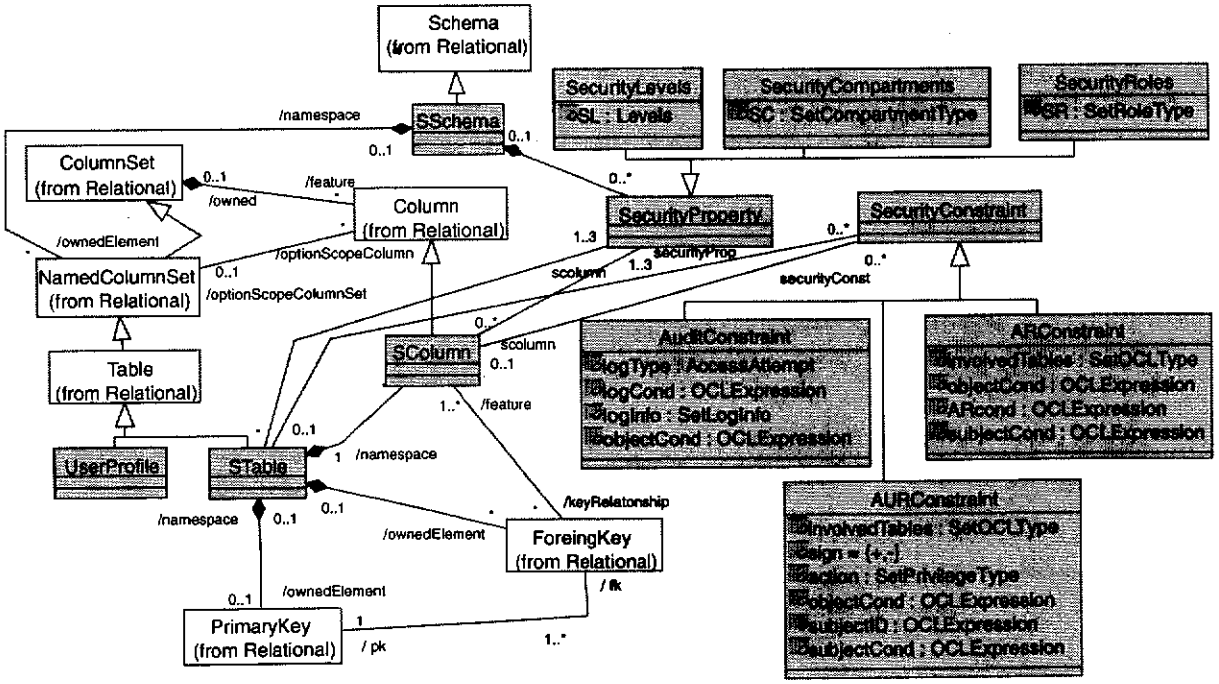


Fig. 6. New classes and associations.

consortium manages several pharmacies which offer various types of services to the community, and wishes to control all aspects relating to the sales of medicines through prescriptions. We have defined a classification of data and users that is typical for this type of business (the most general is Pharmacy Employee, which is then specialized into the Pharmacist and nonPharmacist roles, and which are in turn specialized into the assistant and technician roles in the former case, and into maintenance and administrative in the latter). At security levels, we have considered confidential, secret and topSecret. A pharmacovigilance group exists within the company, which is responsible for the security of the use of certain medicaments and a there is also committee which guards the health of the company's clients. We have defined four security compartments for this: pharmacovigilanceCenter, generalCenter, healthOversightCenter and commercialManagerCenter.

6.1. Defining the PIM

In Fig. 7 we show an instance of the Secure Multidimensional Model, i.e., our SMD PIM, which illustrates a part of the DWs that is required for the previous problem. The SFact Sales Prescription (stereotype SFact) contain all the sales information in one or more pharmacies, and can be accessed by users who have secret or topSecret security levels, play an Administrative or Pharmacist role and belong to pharmacovigilanceCenter, healthOversightCenter and commercialManagerCenter compartments. The sales attribute can only be accessed by users who perform the administrative role (tagged values SR of sales attribute) and belong to the commercialManagerCenter compartment, and therefore access to this attribute will be forbidden to other users who are (pharmacist and maintenance employees or belong to other different commercialManagerCenter compartments). The income attributes can be only accessed by users who perform the administrative role (tagged value SR of income attribute). Others static user classifications for the conceptual model classes defined in Fig. 7 are:

The SFact Sales Prescription contains four dimensions (Pharmacy, Patient, Medication and Time), which contain SBase hierarchies. Access to these SBase hierarchies is established in the same way as was done with the SFact. The UserProfile class contains the information about all users who will have access to this secure MD model. Each user has securityLevels (SL), securityRoles (SR) and securityCompartments (SC) associated with them.

Several security constraints have been specified by using the previously defined constraints, stereotypes and tagged values.

The following paragraphs correspond to notes 1, 2, 3, 4 and 5 in Fig. 7:

1. For each instance of the SFact class Sales Prescription, if the type of payment is through insurance then the security compartment will be commercialManagerCenter (commercialC, tagged value SC). This constraint is only applied if the user makes a query whose information comes from the DataPh.
2. We wish to record the subject, object and time for every frustrated access attempt to DataM (Data Medication) of the drug description.
3. Patient could be special users of the system. In this case, it might be possible for patients to access their own information as patient (for instance, to query their personal data). This situation can be specified as a constraint, composed of the except Sign and exceptCond tagged values in the Patient class.
4. We would like to record, for future audit, the subject, object, time and response for all access to Sales Prescription out of work time. The tagged values logType, logInfor and logCond have been defined for the Sales Prescription class.
5. For each instance of the SBase class DataM (Data Medication), if it is queried together with the SBase class Medication group, if the description of the Medication group is "Psychotropic" or "Drug", then the security compartment will be commercialC and pharmaC, otherwise it will be generalC (generalCenter).

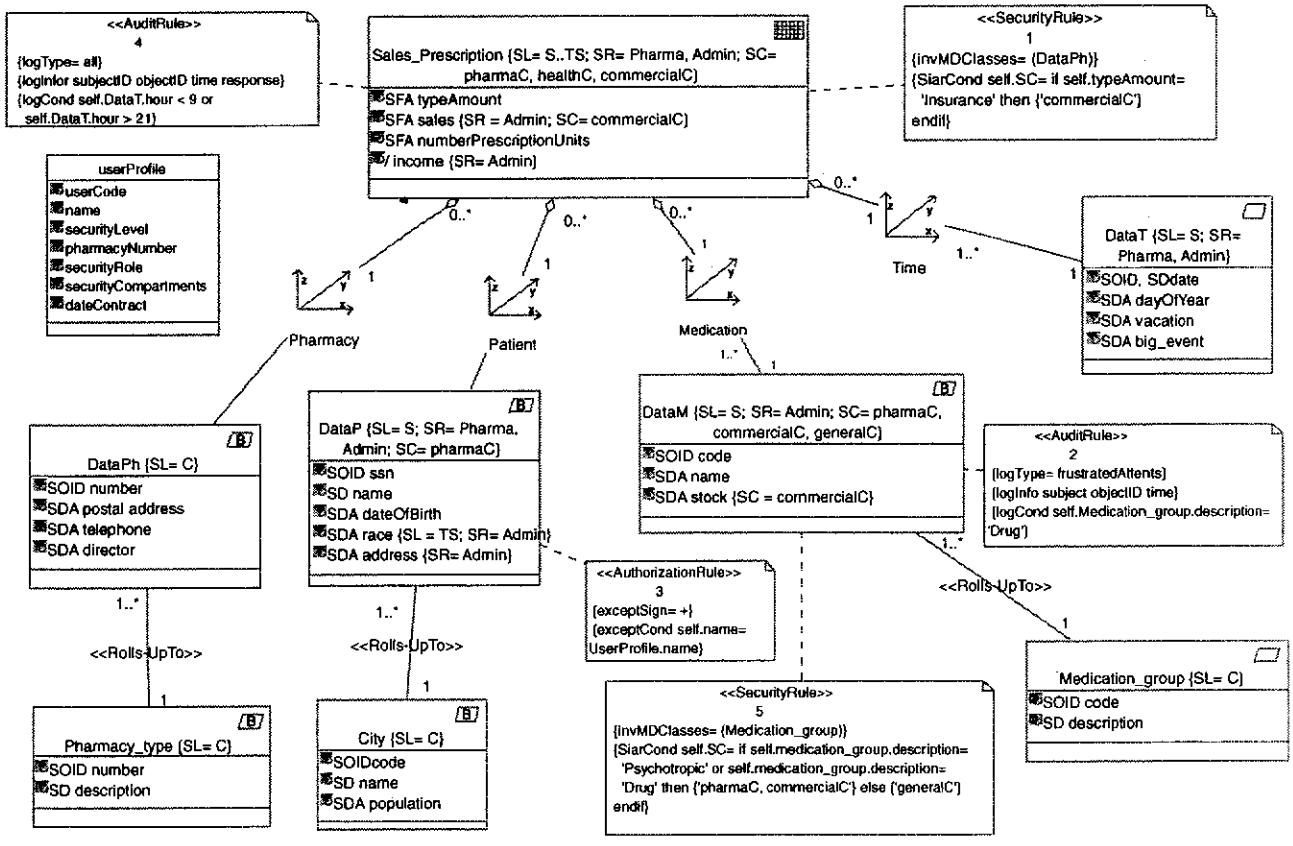


Fig. 7. Example of MD model with security information and constraints.

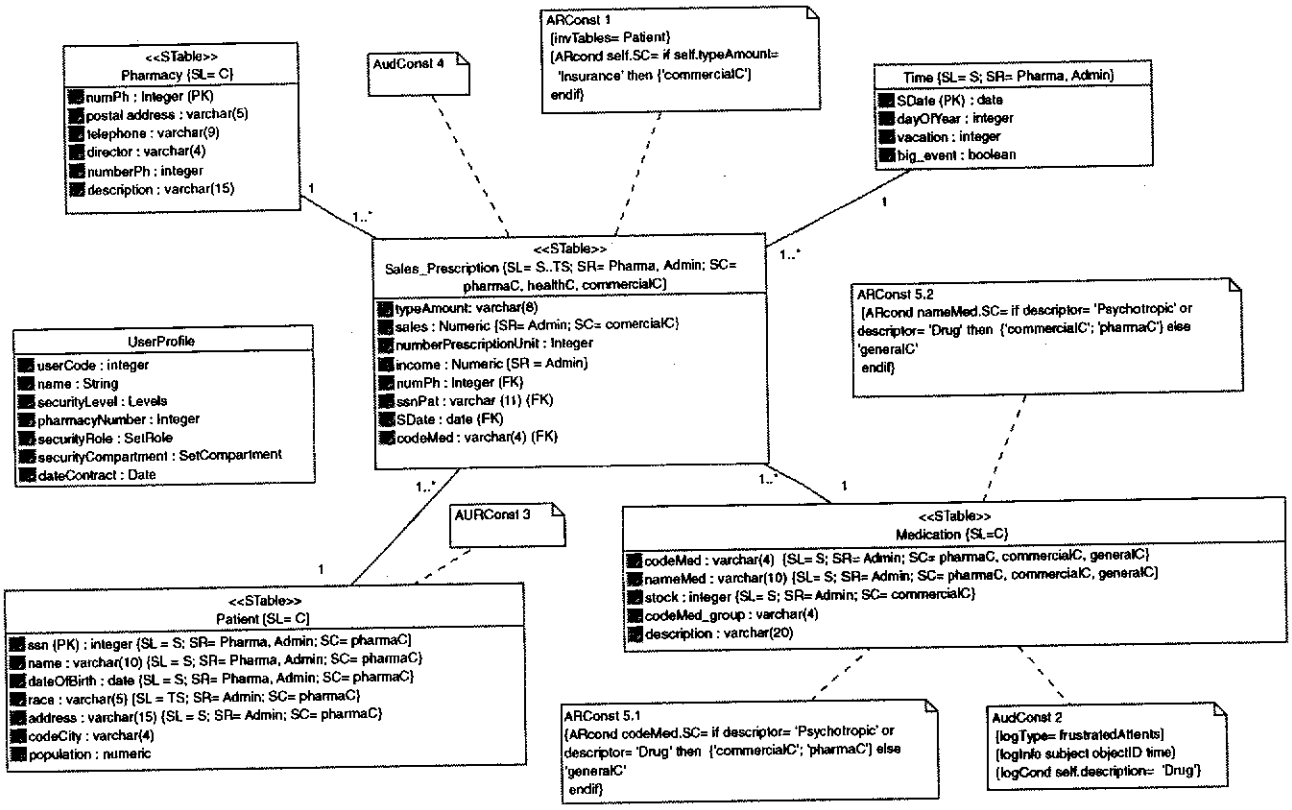


Fig. 8. A star scheme representing an instance of SECRDW metamodel at the logical level.

6.2. Defining the PSM

By using the PIM in Fig. 7 as a starting point, we apply a set of QVT relations [30] through which to achieve an instance of the SECRDW, i.e., our secure PSM. The transformation assures that SFact and SDimensions are transformed into STables with their associated security information. The UserProfile class is transformed into a classical Table from CWM. Fig. 8 represents a star schema at the logical level, which corresponds with an instance of the metamodel extended in subsection 5.3. With the extension of CWM we have formalized the concepts for a relational platform Although they are closest to the MD even when the logical paradigm used was not so similar to the relational model, the transformation is very interesting from the MD to the relational model with respect to security.

The SFact Sales Prescription is represented in Fig. 8 by means of the STable Sales Prescription. In this table we represent all its columns, as well as all the associated security information, that restricts access to the table itself and to its columns. All of the hierarchy that conform to a SDimension must be represented by means of a single STable. Observe in Fig. 8 that the STable Pharmacy contains as SColumn the attributes from the SBase DataPh and Pharmacy type classes from Fig. 7. This occurs analogously with the SBases Patient, Time and Medication classes. In order to build a star scheme the Sales Prescription table must contain columns such as Foreign Key(FK) which represent Primary Key (PK) in the tables that correspond with SDimensions at the PIM level. Hence, the STable Sales Prescription contain the columns typeAmount, sales, numberPrescriptionUnit, income, numPh (the PK in the STable Pharmacy), ssnPat (the PK in the STable Patient), SDate (the PK in the STable Time) and codeMed (the PK in the STable Medication).

The security information (SL, SR and SC) represented in the Sales Prescription class constitutes instances of the metaclass security property that appears in Fig. 6. This security information is modeled at the logical level in the title of the table itself (See Fig. 8). The security in the SBases DataPh and Pharmacy_type is the same. Observe in Fig. 8 that the STable Pharmacy contains the corresponding security information (i.e., SL= C) in its heading.

a)
```
SET_LEVELS ('SALAPolicy', 'User1', 'TS', 'S', 'S')
SET_GROUPS ('SALAPolicy', 'User1', 'Ph, Adm', 'Ph, Adm', 'Ph, Adm')
SET_COMPARTMENTS ('SALAPolicy', 'User1', 'pharmaC, healthC,
commercialC', 'pharmaC, healthC, commercialC', 'pharmaC, healthC,
commercialC',)
SET_USER_PRIVS ('SALAPolicy', 'User1', 'FULL, WRITEUP, WRITEDOWN,
  WRITEACROSS')
```

b)
```
CREATE FUNCTION Function1 () Return LBSCSYS.LABC_LABEL
As MyLabel varchar2(80);
Begin
  MyLabel:= 'S::Ph,Adm::pharmaC,healthC,commercialC';
  Return TO_LBAC_DATA_LABEL ('MyPolicy', 'MyLabel');
End;
APPLY_TABLE_POLICY ('MyPolicy', 'Sales_Prescription', 'Scheme', Function1')
```

c)
```
CREATE FUNCTION Function2 (typeAmount: Varchar2(20))
                    Return LBACSYS.LBAC_LABEL
As MyLabel varchar2(80);
Begin
  If typeAmount= 'Insurance' then MyLabel:= 'S::Ph,Adm::commercialC' else
       'S::Ph,Adm::pharmaC,healthC,commercialC'
  endif;
  Return TO_LBAC_DATA_LABEL ('MyPolicy', 'MyLabel');
End;
APPLY_TABLE_POLICY ('MyPolicy', 'Sales_Prescription', 'Scheme', 'Function2')
```

d)
```
Begin
  dbms_fga.add_policy(
       object_schema     => 'MyPolicy',
       object_name       => 'Medication',
       policy:name       => 'MyPolicy',
       audit_column      => 'code, name, stock',
       statement_types   => 'select',
       enable            => true
    );
End;
```

Fig. 9. Implementing our constraints in Oracle 10g.

In order to establish the security in the STable Patient we note that the attributes from the SBase City class has a security (SL= C, i.e., Confidential), whereas the attributes from the SBase DataP has more restricted security. Hence, the security (in its heading) for the STable Patient will be the least restricted (i.e., SL= C). The columns that correspond with attributes from DataP will have the security of the SBase DataP itself. Observe in Fig. 8 that the SColumns ssn, name, dateOfBirth have the security SL= S; SR= Pharma, Admin; SC= pharmaC. The attribute race has the security SL= TS; SR= Admin whereas the SBase DataP class has SL= S; SR= Pharma, Admin; SC= pharmaC so, the security for the SColumn race is SL= TS; SR= Admin; SC= pharmaC. The same reasoning is valid for the attribute address. In this way, in the STable Patient, a user with SL= S can only access the SColumns codeCity and population. The security for the STable Medication is established in the same way.

The security constraints SecurityRule 1, AuthorizationRule 3 and AuditRule 4 that appear in Fig. 7 are transformed into instances of the SecurityConstraint class which appears in Fig. 6. These instances are modeled in Fig. 8 by means of notes of UML with the names ARConst 1, AURConst 3 and AudConst 4 respectively. The AuditRule 2 includes a reference to the class SBase Medication group in the logCond attribute, so the logCond condition for the STable Medication is adapted, i.e., by giving a reference to the SColumn description. The SecurityRule 5 attempts to change the security for the SBase DataM class, thus establishing new values for securityCompartment (SC). We observed in Fig. 7 that the security of the SBase DataM class has been assigned to the SColumns codeMed, nameMed and stock. Hence, the constraint is transformed and applied to SColumns codeMed, nameMed and stock, but the SColumn stock has the SC= commercial, thus the constraint does not modify the security value for this attribute. Consequently, the SecurityRule 5 is transformed into two ARConstraints that appear in Fig. 8 with the names ARConst 5.1 and ARConst 5.2 which are associated with the SColumns nameMed and codeMed respectively.

6.3. Code Example in Oracle DBMS

To finish our case study we shall show some implementations of the security aspects modeled in the star scheme that appears in Fig. 8. The current standard from OMG used to apply the transformations model-code is MOF Model to Text Transformation Language MOF2-Text. However, we shall briefly show the possibilities that Oracle 10 g DBMS offers in order to implement security and audit measures by means of Oracle Label Security (OLS10g), Virtual Private Databases (VPD) and Oracle Fine-Grained Auditing (FGA). We shall only explain the security aspects that our extension contemplates, and to do this we first created a security policy named "MyPolicy" and valid levels, compartments and hierarchical groups.

In Fig. 9a) we show how the User1 satisfies the security properties for the Sales Prescription table. Fig. 9b) shows how we define and establish the security information for the Sales Prescription table by labeling functions from OLS, although it is not possible to consider security at the column level. The ARConst 1 is implemented by means of the labeling function represented in Fig. 9c). The FGA allows us to define and implement the AudConst 2 (see Fig. 9d)). In AudConst 2 we cannot implement the logType and logCond 2 because the FGA does not allow us to choose the audit type (logType).

7. Conclusions and future work

In this work, we have defined an extension of the relational package from CWM which has been applied to the construction of a star scheme for DWs. This star sheme permits the representation of all the security and audit measures captured during the conceptual modeling phase of the design of DWs. The proposal is aligned with MDA, and thanks to its kindnesses we can establish security aspects in all the design phases of the DWs, from the secure PIM, with the proposal of conceptual modeling based on UML, and its corresponding representation at the logical level based on the extension discussed in this paper. In order to show the validity of our extension we have developed a case study to illustrate how we modeled the security and audit requirements represented during the conceptual modeling stage at the logical level. The contribution of our proposal is: the use of an accepted standard for the interoperability and the metadata interchange between commercial tools and, the extended metamodel from CWM which permits a rigorous integration of MDA and security in the context of DWs design. Our immediate future work consists of implementing the extended relational to some commercial tools and of developing the corresponding transformations between the different metamodels involved. Moreover, we shall extend the i* framework [36] in order to elicit security requirement for DWs at the business level and we shall accomplish this with the MDA in order to cover the whole lifecycle of DWs.

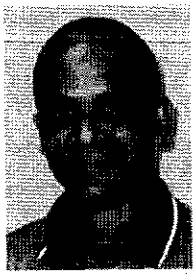
Acknowledgements

This work has been partially supported by the METASIGN project (TIN2004-00779) from the Spanish Ministry of Education and Science, and by the DIMENSIONS (PBC-05-012-1) and DADS projects (PBC-05-012-2) from the Regional Science and Technology Ministry of Castilla-La Mancha (Spain).

References

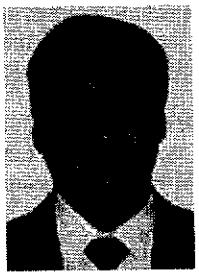
[1] G.C.M. Amaral, M.L.M. Campos, AQUAWARE: a data quality support environment for DataWarehousing, XIX Simpóosio Brasileiro de Banco de Dados (SBBD'04), Brasília, DF, Brasil, 2004, pp. 121–133.
[2] ANSI/SPARC Report, ACM SIGMOD Newsletter 7 (2) (1975).
[3] P. Devanbu, S. Stubblebine, Software engineering for security: a roadmap, presented at The Future of Software Engineering, Limerick, Ireland, 2000, pp. 227–239.
[4] G. Dhillon, J. Backhouse, Information systems security management in the new millenium, Communications of the ACM 43 (7) (2000) 125–128.
[5] W. Essmayr, E. Weippl, F. Lichtenberger, W. Winiwarter, O. Mangisengi, An authorization model for data warehouses and OLAP, Workshop On Security In Distributed Data Warehousing, in conjunction with 20th IEEE Symposium on Reliable Distributed Systems (SRDS'2001), USA, 2001, pp. 9–13.
[6] E. Fernández-Medina, J. Trujillo, R. Villarroel, M. Piattini, Access control and audit model for the multidimensional modeling of data warehouses, Decision Support Systems 42 (3) (2006) 1270–1289.
[7] E. Fernández-Medina, J. Trujillo, R. Villarroel, M. Piattini, Developing secure data warehouses with a UML extension, Information Systems 32 (6) (2007) 826–856.
[8] W.H. Inmon, Building the Data Warehouse, 3er EditionWiley & Sons, New York, 2002.
[9] N. Katic, G. Quirchmayr, J. Schiefer, M. Stolba, A.M. Tjoa, A prototype model for data warehouse security based on metadata, Proceedings of the 9th International Workshop on Database and Expert Systems Applications (DEXA'98), Vienna, Austria, 1998, pp. 300–309.
[10] R. KirkgÃoze, N. Katic, M. Stolda, A.M. Tjoa, A Security Concept for OLAP, 8th International Workshop on Database and Expert System Applications (DEXA'97), Toulouse, France, 1997, pp. 619–626.
[11] S. Luján-Mora, J. Trujillo, I.Y. Song, A UML profile for multidimensional modeling in data warehouses, Data & Knowledge Engineering (DKE) 59 (3) (2006) 725–769.
[12] Y. Liu, S.Y. Sung, H. Xiong, A cubic-wise balance approach for privacy preservation in data cubes, Information Sciences 176 (9) (2006) 1215–1240.
[13] T. Maier, A formal model of the ETL process for OLAP-based web usage analysis, KDD Workshop on Web Mining and Web Usage Analysis (WebKDD'04), Seatle, Washington, USA, 2004, pp. 23–34.
[14] J.-N. Mazón, J. Trujillo, M. Serrano, M. Piattini, A MDA approach for the development of data warehouses, Decision Support Systems 45 (1) (2008) 41–58.
[15] J.N. Mazón, J. Pardillo, J. Trujillo, A Model-Driven Goal-Oriented Engineering Approach for Data Warehouses. Workshop on Requirements, Intentions and Goals in Conceptual Modeling (RIGiM) in conjunction with the Twenty-Sixth International Conference on Conceptual Modeling (ER'07), Auckland, New Zealand, 2007, pp. 255–264.
[16] J. McDermott, Visual security protocol modeling, Proceedings of the 2005 workshop on New security paradigms NSPW'05, Lake Arrowhead, California, USA, 2005, pp. 97–109.
[17] E. Medina, J. Trujillo, A standard for representing multidimensional properties: the CommonWarehouse Metamodel (CWM), presented at 6th East-European Conference on Advances in Databases and Information Systems (ADBIS02), Bratislava, Slovakia, 2002.
[18] F. Melchert, A. Schwinn, C. Herrmann, R. Winter, Using reference models for data warehouse metadata management, 11th Americas Conference on Information Systems (AMCI'05), Omaha, NE, USA, 2005, pp. 1316–1326.
[19] OMG, Common Warehouse Metamodel Specification 1.1, 2003.

[20] OMG, Common Warehouse Metamodel (CWM) Specification 1.1, vol. 2, Extensions, 2002.
[21] OMG, in: J.M.a.J. Mukerji (Ed.), MDA Guide Version 1.0.1, OMG, 2003.
[22] OMG, MOF 2.0 QVT Final Adopted Specification, 2005.
[23] J. Poole, D. Chang, D. Tolbert, D. Mellor, Common Warehouse Metamodel, John Wiley & Sons, Inc., New York, 2002.
[24] T. Priebe, G. Pernul, A pragmatic approach to conceptual modeling of OLAP security, 20th International Conference on Conceptual Modeling (ER'01), Yokohama, Japan, 2001, pp. 311–324.
[25] T. Priebe, G. Pernul, Towards OLAP security design – survey and research issues, Proceedings of the 3rd ACM international workshop on Data Warehousing and OLAP (DOLAP'00), Virginia, USA, 2000, pp. 33–40.
[26] J. Poole, D. Chang, D. Tolbert, D. Mellor, Common Warehouse Metamodel Developers Guide, Wiley Publishing, Inc, Indianapolis, Indiana, 2003.
[27] A. Rosenthal, E. Sciore, View security as the basic for data warehouse security, Workshop on Design and Management of Data Warehouse (DMDW'00), Sweden, 2000.
[28] F. Saltor, M. Oliva, A. Abelló, J. Samos, Building secure DataWarehouse schemas from federated information systems, Heterogeneous Information Exchange and Organizational Hubs, 2002, pp. 123–134, KA.
[29] A.S. Santana, A.M.d.C. Moura, Metadata to support transformations and data & metadata lineage in a warehousing environment, Data Warehousing and Knowledge Discovery (DAWAK'04), Zaragoza, Spain, 2004, pp. 249–258.
[30] E. Soler, J. Trujillo, E. Fernández-Medina, M. Piattini, A set of QVT relations to transform PIM to PSM in the design of secure data warehouses, Second International Conference on Availability, Reliability and Security (ARES'07), Vienna, Austria, 2007, pp. 644–654.
[31] E. Soler, R. Villarroel, J. Trujillo, E. Fernández-Medina, M. Piattini, Representing security and audit rules for DW at the logical level by using the CWM, First International Conference on Availability, Reliability and Security (ARES'06), Vienna, Austria, 2006, pp. 914–921.
[32] S.Y. Sung, Y. Liu, H. Xiong, P.A. Ng, Privacy preservation for data cubes, Knowledge and Information Systems 9 (1) (2006) 38–61.
[33] M. Thess, M. Bolotnicov, XELOPES Library Documentation Version 1.2.3, Prudsys AG, 2004.
[34] R. Villarroel, E. Fernández-Medina, M. Piattini, J. Trujillo, A UML 2.0/OCL extension for designing secure DWs, Journal of Research and Practice in Information Technology 1 (38) (2006) 31–43.
[35] L. Wang, J. Sushil, W. Duminda, Securing OLAP data cubes against privacy breaches, presented at IEEE Symposium on Security and Privacy, Berkeley, California, USA, 2004.
[36] E. Yu, Modelling Strategic Relationships for Process Reengineering. PhD thesis, University of Toronto, Canada (1995).
[37] X. Zhao, Z. Huang, A formal framework for reasoning on metadata based on CWM, 25th International Conference on Conceptual Modeling (ER'06), Tucson, AZ, USA, 2006, pp. 371–384.

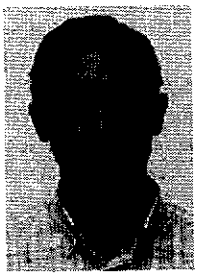


Emilio Soler is a graduate in mathematics from the Pedagogical University of Matanzas (Cuba) and is also an assistant professor at the Computer Science Department of the Matanzas University (Cuba). He is currently a Ph.D. student at the School of Computer Science at the University of Alicante (Spain), and his research activity is in the field of security in data warehouses, MDA and information systems.

Juan Trujillo received a Ph.D. in Computer Science from the University of Alicante (Spain) in 2001. His research interests include database modeling, the conceptual design of data warehouses, MD databases, OLAP, as well as object-oriented analysis and design with UML. With papers published in international conferences and journals such as ER, UML, AD-BIS, CAiSE, WAIM, Journal of Database Management (JDM)and IEEE Computer, Trujillo has served as a Program Committee member of several workshops and conferences such as ER, DOLAP, DSS, and SCI and has also spent some time as a reviewer for several journals such as JDM, KAIS, ISOFT and JODS.



Eduardo Fernández-Medina holds a Ph.D. in Computer Science from the University of Castilla-La Mancha. His research activity is in the field of security in databases, data warehouses, web services and information systems, and also in security metrics. Fernandez-Medina is co-editor of several books and chapter books on these subjects, and has presented several dozen papers at national and international conferences (DEXA, CAISE, UML, ER, etc.). He is the author of several manuscripts in national and international journals (Information Software Technology, Computers And Security, Information Systems Security, etc. and belongs to various professional and research associations (ATI, AEC, ISO, IFIP WG11.3 etc.).



Mario Piattini has an MSc and a Ph.D in Computer Science from the Politechnic University of Madrid. He is a Certified Information System Auditor from the ISACA (Information System Audit and Control Association). The author of several books and papers on databases, software engineering and information systems, Piattini leads the ALARCOS research group of the Department of Computer Science at the University of Castilla-La Mancha. His research interests are: advanced database design, database quality, software metrics, object-oriented metrics and software maintenance.

:OMPUTER STANDARDS & INTERFACES
'he International Journal on the Development and Application of Standards for Computers, Software)uality, Data Communications, E-topics, Interfaces and Measurement

'ublication information

:omputer Standards & Interfaces (ISSN 0920-5489). For 2008 volume 30 (6 issues) is scheduled for ublication. Subscription prices are available upon request from the Publisher or from the Regional ales Office nearest you or from this journal's website (http://www.elsevier.com/locate/csi). Further iformation is available on this journal and other Elsevier products through Elsevier's website: ittp://www.elsevier.com). Subscriptions are accepted on a prepaid basis only and are entered on a alendar year basis. Issues are sent by standard mail (surface within Europe, air delivery outside urope). Priority rates are available upon request. Claims for missing issues should be made within six onths of the date of dispatch.

rders, claims, and product enquiries

ease contact the Customer Service Department at the Regional Sales Office nearest you:
rlando: Elsevier, Customer Service Department, 6277 Sea Harbor Drive, Orlando, FL 32887-4800, SA; phone: (+1) (877) 8397126 [toll free number for US customers], or (+1) (407) 3454020 [customers itside US]; fax: (+1) (407) 3631354; or (+1) (407) 3639661; e-mail: usjcs@elsevier.com or spcs@elsevier.com
nsterdam: Elsevier, Customer Service Department, PO Box 211, 1000 AE Amsterdam, The etherlands; Tel.: +31-20- 4853757; Fax: +31 20 4853432; E-mail: jp.info@elsevier.com
kyo: Elsevier, Customer Service Department, 9-15 Higashi-Azabu 1-chome, Minato-ku, Tokyo 106-)44, Japan; Tel.: +81- 3-55615033; Fax: +81-3-55615047; E-mail: jp.info@elsevier.com
ngapore: Elsevier, Customer Service Department, 3 Killiney Road, #08-01 Winsland House I, ngapore 239519; Tel.: +65-6349 0222; Fax: +65-6733 1510; E-mail: asiainfo@elsevier.com.sg
o de Janeiro: Elsevier, Rua Sete de Setembro 111/16 Andar, 20050-002 Centro, Rio de Janeiro - I, Brazil; Tel.: +55-21-509-5340; Fax: +55-21-507-1991; E-mail: elsevier@campus.com.br [Note (Latin nerica): for orders, claims and help desk information, please contact the Regional Sales Office in New rk as listed above]

lvertising information

vertising orders and enquiries can be sent to: **USA, Canada and South America:** Mr Tino DeCarlo, e Advertising Department, Elsevier Inc., 360 Park Avenue South, New York, NY 10010-1710, USA; .: +1-212-6333815; Fax: +1-212-6333820; E-mail: t.decarlo@elsevier.com. **Europe and ROW:** mmercial Sales Department, Elsevier Ltd., The Boulevard, Langford Lane, Kidlington, Oxford OX5 B, UK; Tel.: +44-1865-843016; Fax: +44-1865-843976; E-mail: media@elsevier.com. **Japan:** The vertising Department, Elsevier K.K., 9-15 Higashi-Azabu 1-chome, Minato-ku, Tokyo 106-0044,)an; Tel.: +81-3-55615033; Fax: +81-3-55615047.

thor enquiries. For enquiries relating to the submission of articles (including electronic submission ere available) please visit this journals homepage at http://www.elsevier.com/locate.csi. You can track :epted articles at http://www.elsevier.com/trackarticle and setup e-mail alerts to inform you of when an cle's status has changed. Also accessible from here is information on copyright, frequently asked :stions and more.

glish language help service: Authors who require information about language editing and copy-ting services pre- and post-submission please visit http://www.elsevier.com/locate/languagepolishing :ontact authorsupport@elsevier.com for more information. Please note Elsevier neither endorses nor :s any responsibility for any products, goods or services offered by outside vendors through our service ı any advertising. For more information please refer to our Terms & Conditions http://www.elsevier.com/ nsandconditions.

A mailing notice: *Computer Standards and Interfaces* (ISSN 0920-5489) is published bi-monthly Elsevier (P.O. Box 211, 1000 AE Amsterdam, The Netherlands). Annual subscription price in the USA $1,108 (valid in North, Central and South America), including air speed delivery. Periodical postage d at Rahway NJ and additional mailing offices.
A POSTMASTER: Send change of address to: *Computer Standards and Interfaces*, Elsevier, 6277 ı Harbor Drive, Orlando, FL 32887-4800.
FREIGHT AND MAILING in USA by Mercury International Limited, 365, Blair Road, Avenel,)7001.

ELSEVIER

Volume 30, Issue 6, August 2008

COMPUTER STANDARDS & INTERFACES

www.elsevier.com/locate/csi

CONTENTS

Abstracted/indexed in: INSPEC, Pascal, Ei Compendex, UnCover, SCISEARCH, Social SciSearch, Inside Conferences, Information Science & Technology Abstracts. Also covered in the abstract and citation database SCOPUS®. Full text available on ScienceDirect®.

0920-5489(200808)30:6;1-F