LNCS 2736

14th International Conference, DEXA 2003
Prague, Czech Republic, September 2003
Proceedings

DEXA 2003

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Vladimír Mařík
Olga Štěpánková
Czech Technical University
Faculty of Electrical Engineering
Department of Cybernetics
Technicka 2, 16627 Prague 6, Czech Republic
E-mail: {marik/step}@labe.felk.cvut.cz

Werner Retschitzegger
University of Linz
Institute of Applied Computer Science
IFS - Department of Information Systems
Altenbergerstr. 69, 4040 Linz, Austria
E-mail: werner@ifs.uni-linz.ac.at

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

CR Subject Classification (1998): H.2, H.4, H.3, H.5, I.2, J.1

ISSN 0302-9743
ISBN 3-540-40806-1 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin GmbH
Printed on acid-free paper SPIN 10929148 06/3142 5 4 3 2 1 0

Preface

The 14th DEXA 2003 International Conference on Database and Expert Systems Applications was held during September 1–5, 2003 at the Czech Technical University in Prague, Czech Republic. The DEXA line of conferences has already gained its own reputation and respected position as a platform for the exchange of ideas among theoreticians and practitioners in the wider area of computer science, but mainly in the areas of database and knowledge-based technologies.

Since DEXA 1993, which was held in Prague, DEXA has grown into a multiconference consisting of four more focused and specialized conferences besides DEXA itself, namely the DaWak conference, EC-Web conference, eGOV conference, and this year happening for the first time, the HoloMAS conference. In addition, the DEXA workshop is a special event offering enough space for specialized discussion, and acting – in a certain sense – as an incubator for new conferences.

The DEXA conference itself is growing in volume and quality each year. This time there were 236 papers submitted and reviewed and the program committee selected 91 of the best papers to be included in this volume. Each of the submitted papers was carefully reviewed by at least three independent PC members or external reviewers.

The DEXA proceedings quite clearly reflect the current trends in the database area and we are happy with the balanced content of both the conference and the proceedings.

We would like to express our thanks at this point to all the institutions that actively supported this event, namely:

- Czech Technical University, Prague, Czech Republic
- DEXA Association, Linz, Austria
- FAW, Johannes Kepler University, Linz, Austria
- Austrian Computer Society
- Microsoft Research, Cambridge, UK
- The Gerstner Lab, as part of the EU Center of Excellence MIRACLE at the Czech Technical University, Prague, Czech Republic

We would also like to thank the whole DEXA implementation team, especially the PC members and the reviewers who did a wonderful job in preparing the technical content of the conference. Special thanks go to Prof. Roland R. Wagner and Prof. A Min Tjoa, who remain persistently the main driving forces behind the DEXA line of events, and also to Gabriela Wagner, who dedicated all her efforts to the success of the DEXA event.

Prag, Linz
June 2003

Vladimir Mařík
Olga Stepankova
Werner Retschitzegger

Program Committee

General Chairperson

Valdimir Mařík, Czech Technical University, Czech Republic

Conference Program Chairpersons

Olga Stepankova, Czech Technical University, Czech Republic
Werner Retschitzegger, University of Linz, Austria

Workshop Chairpersons

A Min Tjoa, Technical University of Vienna, Austria
Roland R. Wagner, FAW, University of Linz, Austria

Program Committee Members

Michel Adiba, IMAG, Laboratoire LSR, France
Hamideh Afsarmanesh, University of Amsterdam, The Netherlands
Ala Al-Zobaidie, University of Greenwich, UK
Bernd Amann, CNAM, France
Frederic Andres, NII, Japan
Kurt Bauknecht, University of Zurich, Switzerland
Trevor Bench-Capon, University of Liverpool, UK
Alfs Berztiss, University of Pittsburgh, USA
Sourav S. Bhowmick, Nanyang Technological Univ., Singapore
Jon Bing, University of Oslo, Norway
Christian Böhm, UMIT, Austria
Alex Borgida, Rutgers University, USA
Omran Bukhres, Purdue University, USA
Luis Camarinah-Matos, New University of Lisbon, Portugal
Antonio Cammelli, IDG-CNR, Italy
Fabio Casati, HP Laboratories, USA
Wojciech Cellary, University of Economics at Poznan, Poland
Elizabeth Chang, Curtin University, Australia
Stavros Christodoulakis, Technical University of Crete, Greece
Panos Chrysanthis, Univ. of Pittsburgh, and Carnegie Mellon Univ., USA
Paolo Ciaccia, University of Bologna, Italy
Rosine Cicchetti, IUT, University of Marseille, France
Carlo Combi, University of Udine, Italy

Don Cowell, University of Greenwich, UK
John Debenham, University of Technology, Sydney, Australia
Misbah Deen, University of Keele, UK
Elisabetta Di Nitto, Politecnico di Milano, Italy
Nina Edelweiss, University of Rio Grande do Sul, Brazil
Johann Eder, University of Klagenfurt, Austria
Thomas Eiter, Technical University of Vienna, Austria
Gregor Engels, University of Paderborn, Germany
Peter Fankhauser, GMD-IPSI, Germany
Ling Feng, University of Twente, The Netherlands
Eduardo Fernandez, Florida Atlantic University, USA
Simon Field, Matching Systems Ltd., Switzerland
Burkhard Freitag, University of Passau, Germany
Mariagrazia Fugini, Politecnico di Milano, Italy
Antonio L. Furtado, University of Rio de Janeiro, Brazil
Georges Gardarin, University of Versailles, France
Alexander Gelbukh, CIC, IPN, Mexico
Parke Godfrey, York University, Canada
Paul Grefen, Eindhoven University of Technology, The Netherlands
William Grosky, Wayne State University, USA
Le Gruenwald, University of Oklahoma, USA
Abdelkader Hameurlain, IRIT, University of Toulouse, France
Igor T. Hawryszkiewycz, University of Technology, Sydney, Australia
Mohamed Ibrahim, University of Greenwich, UK
Yahiko Kambayashi, Kyoto University, Japan
Magdi N. Kamel, Naval Postgraduate School, USA
Nabil Kamel, American University in Cairo, Egypt
Gerti Kappel, University of Technology, Vienna, Austria
Dimitris Karagiannis, University of Vienna, Austria
Randi Karlsen, University of Tromsö, Norway
Rudolf Keller, Zühlke Engineering AG, Switzerland
Latifur Khan, University of Texas at Dallas, USA
Myoung Ho Kim, KAIST, Korea
Masaru Kitsuregawa, Tokyo University, Japan
Gary J. Koehler, University of Florida, USA
Donald Kossmann, Technical University of Munich, Germany
Petr Kroha, Technical University Chemnitz-Zwickau, Germany
John Krogstie, SINTEF, Norway
Josef Küng, University of Linz, Austria
Lotfi Lakhal, University of Marseille, France
Jiri Lazansky, Czech Technical University, Czech Republic
Michel Leonard, University of Geneva, Switzerland
Tok Wang Ling, National University of Singapore, Singapore
Mengchi Liu, Carleton University, Canada

Peri Loucopoulos, UMIST, UK
Sanjai Kumar Madria, University of Missouri-Rolla, USA
Akifumi Makinouchi, Kyushu University, Japan
Simone Marinai, University of Florence, Italy
Heinrich C. Mayr, University of Klagenfurt, Austria
Subhasish Mazumdar, New Mexico Tech, USA
Dennis McLeod, University of Southern California, USA
Robert Meersman, Free University of Brussels, Belgium
Elisabeth Metais, CEDRIC/CNAM, Paris, France
Zoran Milosevic, University of Queensland, Australia
Mukesh Mohania, IBM-IRL, India
Tadeusz Morzy, Poznan University of Technology, Poland
Noureddine Mouaddib, University of Nantes, France
Günter Müller, University of Freiburg, Germany
Waseem Naqvi, Raytheon Inc., USA
Erich J. Neuhold, Fraunhofer-IPSI, Germany
Gultekin Ozsoyoglu, Case Western Reserve University, USA
Francois Pacull, Xerox Research Centre Europe, France
Georgios Pangalos, University of Thessaloniki, Greece
Stott Parker, University of Los Angeles (UCLA), USA
Oscar Pastor, Technical University of Valencia, Spain
Marco Patella, University of Bologna, Italy
Barbara Pernici, Politecnico di Milano, Italy
Günter Pernul, University of Regensburg, Germany
Gerald Quirchmayr, University of Vienna, Austria
Fausto Rabitti, CNUCE-CNR, Italy
Wenny Rahayu, La Trobe University, Australia
Isidro Ramos, Technical University of Valencia, Spain
P. Krishna Reddy, University of Science and Technology, Hong Kong
Harald Reiterer, University of Konstanz, Germany
Norman Revell, Middlesex University, UK
Sally Rice, University of South Australia, Australia
Jerome Robinson, University of Essex, UK
John Roddick, Flinders University of South Australia, Australia
Colette Rolland, University Paris I, Sorbonne, France
Elke Rundensteiner, Worcester Polytechnic Institute, USA
Domenico Sacca, University of Calabria, Italy
Simonas Saltenis, Aalborg University, Denmark
Marinette Savonnet, University of Bourgogne, France
Erich Schweighofer, University of Vienna, Austria
Ming-Chien Shan, HP Laboratories, USA
Keng Siau, University of Nebraska-Lincoln, USA
Michael H. Smith, University of California, USA
Giovanni Soda, University of Florence, Italy

Günther Specht, Technical University of Ilmenau, Germany
Uma Srinivasan, CSIRO, Australia
Bala Srinivasan, Monash University, Australia
Zbigniew Struzik, CWI, Amsterdam, The Netherlands
Makoto Takizawa, Tokyo Denki University, Japan
Katsumi Tanaka, Kyoto University, Japan
Zahir Tari, University of Melbourne, Australia
Stephanie Teufel, University of Fribourg, Germany
Jukka Teuhola, University of Turku, Finland
Bernd Thalheim, Technical University of Cottbus, Germany
Jean Marc Thevenin, University of Toulouse, France
Helmut Thoma, IBM Global Services, Basel, Switzerland
A Min Tjoa, Technical University of Vienna, Austria
Roland Traunmüller, University of Linz, Austria
Aphrodite Tsalgatidou, University of Athens, Greece
Susan Urban, Arizona State University, USA
Genovena Vargas-Solar, LSR-IMAG, France
Krishnamurthy Vidyasankar, Memorial Univ. of Newfoundland, Canada
Pavel Vogel, Technical University of Munich, Germany
Roland R. Wagner, University of Linz, Austria
Kyu-Young Whang, KAIST, Korea
Michael Wing, Middlesex University, UK
Werner Winiwarter, University of Vienna, Austria
Vilas Wuwongse, Asian Institute of Technology, Thailand
Gian Piero Zarri, CNRS, France
Arkady Zaslavsky, Monash University, Australia
Aidong Zhang, State Univ. of New York at Buffalo, USA

External Reviewers

Zaher Aghbari
Kunihiko Kaneko
Seok Il Song
Mohand Boughanem
Max Chevalier
Claude Chrisment
Franck Morvan
Josiane Mothe
Olivier Teste
Chun Tang
Yong Shi
Li Zhang
Daxin Jiang
Pengjun Pei
Daoying Ma
Dimitrios Theotokis
Anya Sotiropoulou
Pierluigi Plebani
Barbara Oliboni
Malu Castellanos
Christian Baumgartner
Angela Bonifati
Mario Cannataro
Gianluigi Greco
Antonella Guzzo
Giuseppe Manco
Riccardo Ortale
Cristina Sirangelo
Giorgio Terracina
Peter Fischer
Andreas Grünhagen
Steffen Rost
Luciano Garcia Bañuelos
Edgard Benitez Guerrero
Vu-Tuyet Trinh
Khalid Belhajjame
Tania Cerquitelli
Anibal Arias
Christian Koncilia
Marek Lehmann
Harald Kosch
Roberto Tedesco
Giuseppe Amato
Federica Mandreoli
Pavel Zezula
Franca Debole
Chiara Renso
Jutta Willamowski
Damian Arregui
Alessio Ceroni
Andrea Passerini
Sauro Menchetti
Samuil Angelov
Hajo Reijers
Alexander Hirnschall
Wijnand Derks
Ednan Masovic
Thosten Priebe
Björn Muschall
Christian Breu
Eduardo Mena
Isabel Diaz
Javier Jaen
Jennifer Pérez
Nieves R. Brisaboa
Patricio Letelier
Morad Benyoucef
Sarita Bassil
Ting Chen
Liang Liang Fang
Pierluigi Plebani
Chunsheng Liu
Shan Wei
Wanjun Sun
Qiong Ruan
Masashi Toyoda
Noriko Imafuji
Shingo Otsuka
Norio Katayama
Miyuki Nakano
Yitong Wang
Mirella Moura Moro
Renata de Matos Galante
Carina Friederich Dorneles
Vanessa de Paula Braganholo
Daniela Leal Musa
Jan Ma
Andreas Meissner
Thomas Risse
Juan Carlos Casamayor
Juan Sanchez
Vicente Pelechano
Patrick Lehti
Kaiyang Liu
Jiying Wang
Sven Van Acker
Jan De Bo
Majed AbuSafiya
Thomas Schlienger
Andreas Erat
Martin Steinert
Erich Gstrein
Surya Nepal
Wojciech Wiza
Jarogniew Rykowski

Table of Contents

Invited Talk

Spatial Database Systems I

XML III

Spatial Database Systems II

XML IV

Mobile Computing I

Transactions

Mobile Computing II

Bioinformatics

Mobile Computing III

Information Retrieval I

Information Retrieval II

Information Retrieval III

Multimedia Database Systems

Web Applications

Ontologies I

Object-Oriented Database Systems I

Ontologies II

Object-Oriented Database Systems II

Query Optimization I

Workflow I

Query Optimization II

Workflow II

Knowledge Engineering I

Policy F

1 Introd

For effective
sources to
information
and use diffe
intelligent a
adapt the ch
automaticall
correlating e
can be taken
This time
can be achi
defining the
business logi
the informat
systems and
caller makes
whether the
more, then c
placed". This
database syst
The integ
timely busin
that require
financial sec
front-end inf
applications
operational t
of transactio
information f
allow greater

Designing Secure Databases for OLS*

Eduardo Fernández-Medina and Mario Piattini

Escuela Superior de Informática.
University of Castilla-La Mancha.
Paseo de la Universidad 4,
13071, Ciudad Real. Spain
Tel: 34 926 29 53 00
{Eduardo.FdezMedina,Mario.Piattini}@uclm.es
http://www.inf-cr.uclm.es

Abstract. Some Database Management Systems (DBMS) allow to implement multilevel databases, but there are no methodologies for designing these databases. Security must be considered as a fundamental requirement in Information Systems (IS) development, and has to be taken into account at all stages of the development. We propose a methodology for designing secure databases, which allows to design and implement secure databases considering constraints regarding sensitive information from the requirements phase. The models and languages included in the methodology provide tools to specify constraints and to classify the information into different security levels and to specify which roles users need to play to access information. The methodology prescribes rules to specify the database and the security information with the Oracle*9i* Label Security (OLS) DBMS. It also has been applied in an actual case by the Data Processing Center of the Ciudad Real Provincial Government.

1 Introduction

The modern society forces companies and enterprises to evolve, and to manage information properly in order to achieve their objectives and survive in the digital era. Organizations depend increasingly on IS, which rely upon large databases, and these databases need increasingly more quality and security. Indeed the very survival of the organization depends on the correct management, security and confidentiality of this information [1].

Databases are present in many situations of our real life, managing and storing a huge amount of important information. So, it is important to protect databases and IS [2]. Sometimes, databases also store information regarding private or personal aspects of individuals, like identification data, medical data or even religious beliefs, ideologies, or sexual tendencies. Because of this, there are laws to protect the individual privacy (e.g., *Spanish Constitutional Law for the Personal Data Protection*

* This research is part of the DOLMEN project (TIC2000-1673-C06-06) and RETISSI project (TIC2001-5023-E) supported by the Research Projects Subdirection of the Ministry of Science and Technology.

V. Mařík et al. (Eds.): DEXA 2003, LNCS 2736, pp. 886–895, 2003.

(LOPD)[1] – [3]). Failure to comply with these laws used to be very strict, enforcing severe penalties. That information should then be equipped with mechanisms that prevent non-authorized access, fulfilling the existing Data Protection Laws.

As some authors remarked [5, 6], we think that database protection is a serious requirement which must be considered carefully, not as an isolated aspect, but as an element present in all stages of the database life cycle, from the requirement analysis to implementation and maintenance. For this purpose, different ideas for integrating security in the system development process are proposed [7], but they only considered database security from a cryptographic point of view. Chung et al. also insist on integrating security requirements in the design, by providing the designers with models specifying security aspects, but they do not deal with database specific issues [8].

There are a few proposals that try to integrate security into conceptual modeling such as the Semantic Data Model for Security [9] and the Multilevel Object Modeling Technique [10], but they have not been very spread. One more recent proposal is UMLSec [11] where UML is extended to develop secure systems. This approach is very interesting, but it -again- only deals with IS in general, whilst conceptual and logical database design, and secure database implementation are not considered. Moreover Castano et al. presents a very interesting methodological approach for designing security in databases, but it does not consider the integration with the database development process [12]. Also, traditional database methodologies, do not consider security in their proposals [13, 14].

To overcome this problem, we propose a methodological approach, which allows us to design databases taking into consideration security aspects from the earliest stages, until the end of the development. This approach could also be an extension of the existing methodologies and modeling standards, since the organizations who are really interested in database security would not have to make a great effort to adapt to a new methodology. The methodology we proposed extends different UML models and the Object Constraint Language (OCL). It allows us to create conceptual and logical model of multilevel databases, and to implement them by using Oracle 9i Label Security [15].

In order to develop the methodology, we have used the '*Action Research*' method [16], applying the methodology to the redesign of a database for the Ciudad Real Provincial Government (Spain). This database was managed by an application, called SALA (System for the Accounting of the Local Administration), that had different confidentiality problems, which we have solved through a new secure design. The general aim of this application is to control the budget and the accounting of the Provincial Government. This application manages not only economic information about companies and individuals, but also *personal information of individuals*. If minimal security measures are taken into account, someone could illegally explore economic and personal information, by collecting addresses, account numbers, telephone numbers, information about economic transactions, etc. It is possible to know the habits of companies and individuals, and therefore to get a profile of them. In this case the organization would have to face up to legal responsibilities.

[1] LOPD is an adaptation of the European Union Directive 95/46/CE of the European Parliament and Council about people protection regarding the personal data management and the free circulation of these data [4].

In the next section we present an overview of the secure database design methodology, including the models and languages that have been defined. Finally in section 3 we comment conclusions and future work.

2 Methodology Overview

This methodology allows us to classify the information according to its confidentiality properties and to which user roles will have access permissions. It is also possible to specify security constraints on that classification. The methodology ends defining rules to specify the database, the security information and the security constraints with OLS.

The methodology be iterative and incremental, driven by use cases, and centered on the architecture. The stages of the methodology are *Requirements Gathering*, *System Analysis*, *Multilevel Relational Logical Design*, and *Specific Logical Design*.

In order to give support to the methodology, we have extended Rational Rose, to include and manage the security information of the elements into the use case and class diagrams. It also permits definition of security constraints and their lexical and syntactical checking.

In the following sections, we present each stage in more detail, illustrating them with a portion of the case study.

2.1 Requirements Gathering

As in any other development methodology, the goal of this stage is to collect and represent requirements, with the particularity that we also have to consider security requirements. The most important artifact of this stage is the *extended use case model*, which allows us to indicate special security characteristics of actors and use case through stereotypes. The extended use case model introduces the concept of *secure use case* and *authorized actor*. A secure use case is a use case that should be deeply studied from the point of view of security. An authorized actor is an actor that must have special authorizations in order to execute a particular use case.

This stages consists of the following activities: Gathering initial requirements, creating the business model and the system glossary, looking for actors, looking for use cases, looking for persistent elements, describing use cases, analyzing security in actors and in use cases, defining priorities in use cases, structuring the use case model, looking for relationships between use cases, and reviewing use cases.

For space reasons it is not possible to develop in detail the extended use case model. More details can be found in [17].

2.2 System Analysis

The aim of this stage is to build the database conceptual model, considering all the requirements that have been collected in the previous activities. The conceptual model will be composed of the *extended class diagram*, and a set of *security constraints* that are expressed through the OSCL language [18].

The extended class diagram makes possible to specify security information in classes, attributes and associations, which indicates the conditions that the subjects have to fulfill to access them, regarding *security levels* and *roles of authorized users*. If one security level, for instance, is assigned to a class, it means that subjects have to be classified in at least the same level in order to access the information. If a set of roles is assigned to an element, it means that the subjects have to play at least one of those roles to access the element.

The OSCL language allows the specification of security constraints that define the information about security of classes, attributes or associations, depending on a particular condition. For instance, in the following example:

Context CreditorOfTheExpenseBudget **inv**:
self.SL=if Refunds <= 3000 then U else if Refunds <= 10000 then S else T

The constraint specifies that the security level of the objects belonging to the class *CreditorOfTheExpenseBudget* will be more restrictive if the value of the attribute *Refunds* have one particular value. As we can see the syntax of OSCL is easy to understand, because this language is based on the well-known OCL.

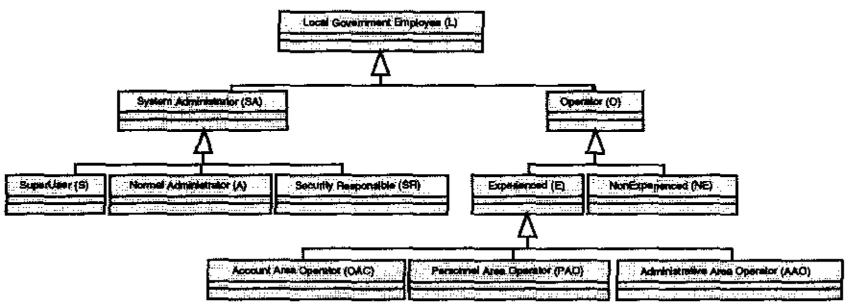

Fig. 1. Roles Hierarchy

The activities of this stage are architecture analysis, use case analysis, classes analysis, security analysis, and package analysis. All of these activities are composed of many more tasks. The components of the security analysis activity are as follows:

- Defining the valid security levels for the system.
- Assigning security levels to the classes, attributes and associations, taking into account the security properties of the information, and the *inherent constraints*[2] of the extended class model.
- Classifying classes, attributes and associations into different authorized user roles, if necessary.
- Specifying security constraints, which define the security information of different model elements.
- Analyzing other kinds of security constraints (not only about confidentiality).

---

[2] The extended class model has different inherent constraints that all instances must fulfill. For example, the security level of the attributes should be equal to or more restricted than the security level of the class to they belong.

- Defining the authorization information of the users, which is composed of the security level and the roles that users play.

Part of the hierarchy of roles that has been defined for the case study database is shown in Figure 1. Figure 2 illustrates an example of an extended class diagram. The security levels[3] that have been defined for this database are Unclassified (U), Confidential (C), Secret (S), and Top Secret (T). For each role, a short name is also defined, which is used in the diagrams. For instance, the class 'EconomicalData' has defined the security level 'T' and the role 'OAC' (Account Area Operator). This means that the information of the objects that belongs to that class will only be accessible to users who have security level 'Top Secret' and who play role 'Account Area Operator'. If there is no security information associated to a class, then all users can access it.

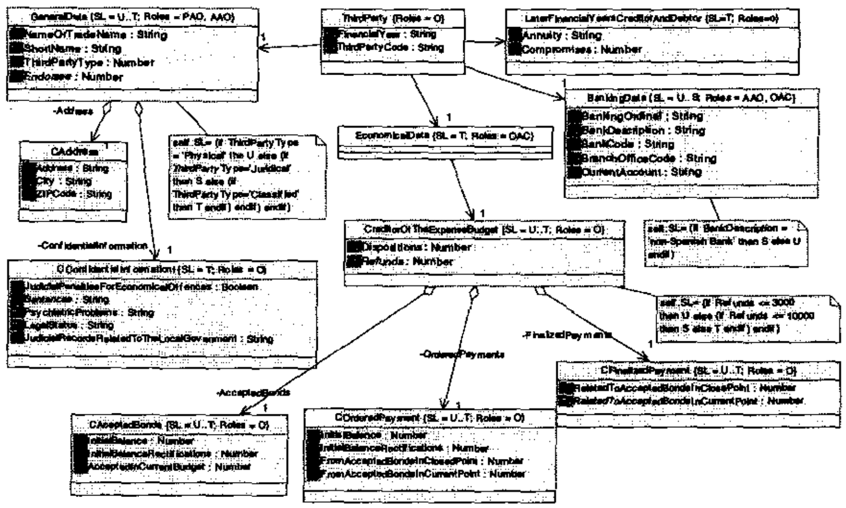

Fig. 2. Third Parties Class Diagram

We can also observe in Figure 2 three OSCL constraints, which define the security level of the objects, depending on the value of different attributes. For instance, the security constraint associated with class 'BankingData' indicates that the security level of its objects will be 'Secret' if the value of the attribute 'BankDescription' is equal to 'Non-Spanish Bank', and 'Unclassified', in any other case.

2.3 Multilevel Relational Logical Design

This stage is the bridge between the conceptual model and the implementation with a specific logical model. We think it is very important to keep the independence

[3] In this methodology it is possible to define a particular set of security levels, depending on the complexity of the database.

between a "general logical model" and the different specific logical models because multilevel and other authorization issues vary considerably from one product to another. For the moment we have considered only a general relational security database model because relational databases are the most used and widespread at present [19], but it could be possible to develop secure object-relational or object oriented databases.

The three components of the general multilevel relational model are:

- Database relational model: This component includes the definition of each relation of the database, considering the necessary attributes for representing the confidentiality information
- Meta-information of the model: Each relation has associated a meta-information tuple, which includes the data type of the attributes, and the valid values of the attributes related to security information of the tuple and attributes.
- Security Constraints: All the security constraints defined in the conceptual model are specified in this model without losing or modifying their semantics.

The activities of this stage deal with the transformation of all elements in the extended class diagram into the multilevel relational model.

Database Relational Model

BankingData(Id, BankOrdinal, BankDescription, BankCode, BranchOfficeCode, CurrentAccount, TFinancialYear, TThirdPartyCode, SecurityLevel)

→ ThirdParty(FinancialYear, ThirdPartyCode)

LaterFinancialYearsCreditorAndDefaulter (Annuity, Compromises)

CreditorOfTheExpenseBudget(Id, Dispositions, Refunds, Bon_InitialBalance, Bon_InitialBalanceRectifications, Bon_AcceptedInCurrentBudget, Ord_Pay_InitialBalance, Ord_Pay_InitialBalanceRectifications, Ord_Pay_BondsClosedPoints, Ord_Pay_BondsCurrentPoints, Fin_Pay_ClosedPoints, Fin_Pay_CurrentPoints, SecurityLevel)

Meta-information

<BankingData, U..S, AAO, OAC, Id: VarChar; BankOrdinal: VarChar; BankDescription: VarChar; BankCode : VarChar; BranchOfficeCode:VarChar; CurrentAccount: VarChar; TfinancialYear: VarChar; TThirdPartyCode : VarChar; SecurityLevel : SL>

< LaterFinancialYearsCreditorAndDefaulter, T, O, Annuity: VarChar; Compromises: Real>

< CreditorOfTheExpenseBudget,U..T, O, Id :VarChar; Dispositions: Real; Refunds :Real; Bon_InitialBalance: Real; Bon_InitialBalanceRectifications: Real; Bon_AcceptedInCurrentBudget : Real; Ord_Pay_InitialBalance :Real; Ord_Pay_InitialBalanceRectifications: Real; Ord_Pay_BondsClosedPoints : Real; Ord_Pay_BondsCurrentPoints :Real; Fin_Pay_ClosedPoints : Real; Fin_Pay_CurrentPoints : Real; SecurityLevel : LS>

Security Constraints

Context BankingData **inv:**
Self.SecurityLevel = (if self.BankDescription = "Non-Spanish bank" then S else U endif)
Context CreditorOfTheExpenseBudget **inv:**
Self.SecurityLevel = (if Refunds <= 3000 then U else (if refunds <= 10000 then S else T endif) endif)

Fig. 3. Multilevel Relational Model

A fragment of the multilevel relational model of our example can be seen in Figure 3. For space reasons, we have selected only a subset of the classes of the class diagram. We can observe that each class appears in the relational model and in the metainformation section, and the constraint section includes the security constraints related to the considered classes. Obviously, we have done a translation of the data types used in the conceptual model into logical data types.

2.4 Specific Logical Design

In this stage we specify the secure database in a particular logical model: Oracle Label Security (OLS). We have chosen this model because it is part of one of the most important database management systems, that allows the implementation of label-based databases; and because the organization wanted to support the new database in this DBMS.

In the context of OLS, a security policy is the most important element, and includes different parameters, such as valid security levels, groups and compartments, and different options that define the way of managing the security. Taking that into account, the activities of this stage are as follows: Defining the database model (all the tables), defining the security policy and their default options, defining the security information in the security policy, creating the authorized users and assigning their authorizations, defining security information for tables through labeling functions, implementing security constraints through labeling functions and access control predicates, and finally, if necessary, implementing operations and controlling their security.

```
CREATE_POLICY('SecurityPolicy','SecurityLabel', 'HIDE, CHECK_CONTROL,
      READ_CONTROL, WRITE_CONTROL')

CREATE_LEVEL('SecurityPolicy', 1000, 'U', 'Unclassify')
CREATE_LEVEL('SecurityPolicy', 2000, 'C', 'Confidential')
CREATE_LEVEL('SecurityPolicy', 3000,'S', 'Secret')
CREATE_LEVEL('SecurityPolicy', 4000, 'T', 'Top Secret')

CREATE_GROUP('SecurityPolicy', 1, 'L', 'LocalGovernmentEmployee')
CREATE_GROUP('SecurityPolicy', 2, 'O', 'Operator', 'L')
CREATE_GROUP('SecurityPolicy', 3, 'SY', 'SystemAdministrator', 'L')
CREATE_GROUP('SecurityPolicy', 4, 'S', 'SuperUser', 'SA')
CREATE_GROUP('SecurityPolicy', 5, 'A', 'NormalAdministrator', 'SA')
CREATE_GROUP('SecurityPolicy', 6, 'SR', 'SecurityResponsible', 'SA')
CREATE_GROUP('SecurityPolicy', 7, 'E', 'Experienced', 'O')
CREATE_GROUP('SecurityPolicy', 8, 'NE', 'Non-Experienced', 'O')
CREATE_GROUP('SecurityPolicy', 9, 'AAO', 'AccountAreaOperator', 'E')
CREATE_GROUP('SecurityPolicy', 10, 'PAO', 'PersonnelAreaOperator', 'E')
CREATE_GROUP('SecurityPolicy', 11, 'OAC', 'AdministrativeAreaOperator', 'E')
```

Fig. 4. Security Policy, Levels and Groups Definition

In Figure 4, we show the way of defining the security policy, the security levels and the user groups in OLS. 'SecurityLabel' is the name of the column that stores the sensitive information in each table, which is associated with the security policy. The option 'HIDE' indicates that the column 'SecurityLabel' will be hidden, so that users will not able to see it in the tables. The Option 'CHECK_CONTROL' forces the system to check that when a subject introduces or modifies a row, the user has reading access. The option 'READ_CONTROL' applies a policy read enforcement for select, update and delete operations. Finally, the option 'WRITE_CONTROL' applies policy write enforcement for insert, delete and update operations.

When a new security level is defined, we have to specify the name of the policy, a number -which indicates the order of the levels-, a short name, and the name of the security level. Also, when a new group is created, we have to specify the name of the policy, the number of the group, a short name, the name of the group, and the short name of its father in the hierarchy.

```
SET_LEVELS('SecurityPolicy', 'User1', 'T', 'S', 'S')
SET_GROUPS('SecurityPolicy', 'User1', 'O', 'O', 'O')
SET_USER_PRIVS('SecurityPolicy', 'User1', 'FULL, WRITEUP, WRITEDOWN, WRITEACROSS')
```

Fig. 5. User definition

Once the security policy, the levels and groups have been defined, we can identify the users in the system, and assign them privileges if necessary. In Figure 5 the user 'User 1' is defined with the following information: Max security level 'T', default security level 'S', minimum security level 'S', read access groups 'Operator', write access groups 'Operator', and default groups 'Operator'. Since it is not usual to assign special privileges to users, we show how this is possible. The description of all the possible options can be seen in [15].

```
CREATE FUNCTION Function1 (BankDescription: VarChar) Return LBACSYS.LBAC_LABEL
As MyLabel varchar2(80);
Begin
  If BankDescription='Non-Spanish bank' then MyLabel := 'S::AAO,OAC'; else MyLabel := 'U::OAA,OAC';
  end if;
  Return TO_LBAC_DATA_LABEL('SecurityPolicy', MyLabel);
End;
CREATE FUNCTION Function2( ) Return LBACSYS.LBAC_LABEL
As  MyLabel varchar2(80);
Begin
  MyLabel := 'T::O' ;
  Return TO_LBAC_DATA_LABEL('SecurePolicy', MyLabel);
End;
CREATE FUNCTION Function3(Refunds: Real) Return LBACSYS.LBAC_LABEL
As MyLabel varchar2(80);
Begin
  If Refunds <=3000 the MyLabel := 'U::O';
    else if Refunds <= 10000 then MyLabel := 'S::O'; else MyLabel := 'T::O';
        end if;
  end if;
  Return TO_LBAC_DATA_LABEL('SecurityPolicy', MyLabel);
End;

APPLY_TABLE_POLICY ('SecurityPolicy', 'BankingData', 'Scheme', , 'Function1')
APPLY_TABLE_POLICY ('SecurityPolicy', 'LaterFinancialYearsCreditorAndDefaulter', 'Scheme', ,
'Function2')
APPLY_TABLE_POLICY ('SecurityPolicy', 'CreditorOfTheExpenseBudget', 'Scheme', ,'Function3')
```

Fig. 6. Labeling Functions

The way of assigning security information to the row, once they are inserted, is through labeling functions. When there are no security constraints associated with a table, the labeling function always assigns the same security information to the row. The security constraints are also implemented by the labeling function. Figure 6 shows three labeling functions, and the command by which they are assigned to the tables, which are associated with the relations that have been defined in Figure 3. 'Function1' creates the security information, depending on the value of the column 'BankDescription'. 'Function2' always creates the same security information, and finally, 'Function3' creates the security information depending on the value of the column 'Refunds'. These functions are associated with tables; therefore it is possible to reuse the same labeling function for several tables.

3 Conclusions

The criticality of IS, and specially databases for modern business, together with new requirements of laws and governments, make necessary more sophisticated approaches to ensure database security.

Traditionally, information security deals with different research topics, like access control techniques, cryptographic methods, etc. Although all these topics are very important, we think that it is fundamental to use a methodological approach, where security-at different levels- is taken into consideration at all stages of the database development process. In this paper we have summarized a methodology, which extends the most accepted modeling languages, process models, constraint languages and security models in the industrial and research community. The methodology has been refined and proved in the design of a secure database in a Spanish local government, solving its confidentiality problems. We have also developed a CASE tool to automatically support the management of use case and class diagrams and OSCL security constraints.

There are several interesting directions in which we are extending the proposal presented in this paper: It could be interesting to improve and extend the languages and techniques involved in this methodology, for example, to consider new kinds of security constraints, such as temporal, integrity or availability constraints [20]. We are also improving the gathering requirements stage in order to reuse legal requirements [21].

References

1. Dhillon, G. & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM,. 43, 7,* 125–128.
2. Brinkley, D. & Schell, R. (1995). What is there to worry about? An introduction to the computer security problem. In Abrams, M., Jajodia, S. & Podell (Eds.), *Information security, an integrated collection of essays* (Chapter 1). California, IEEE Computer Society.
3. Spanish Constitutional Law (15/1999). *December 13th, on personal data protection.* BOE no. 298, 14/12/1999 (in Spanish).
4. Directive (95/46/CE). Directive 95/46/CE of the European Parliament and Council, dated October 24th, about People protection regarding the personal data management and the free circulation of these data. DOCE no. L281, 23/11/1995, P.0031–0050.
5. Devanbu, P. & Stubblebine, S. (2000). Software engineering for security: a roadmap. The future of software engineering. In proceedings of the Finkelstein, A. (ed.) 22nd International Conference on Software Engineering (pp. 227–239).
6. Ferrari, E. & Thuraisingham, B. (2000). Secure Database Systems. Advanced Databases: Technology Design. Eds.: Piattini, M. and Díaz, O. Artech House. London.
7. Hall, A. & Chapman, R. (2002). Correctness by construction developing a commercial secure system. IEEE Software, 19, 1, 18–25.
8. Chung, L., Nixon, B., Yu, E. & Mylopoulos, J. (2000). Non-functional requirements in software engineering. Boston/Dordrecht/London, Kluwer Academic Publishers.
9. Smith, G.W. (1991). Modeling security-relevant data semantics. In proceedings of the IEEE Trans. On Software Engineering, 17, 11, 1195–1203.

10. Marks, D., Sell, P. & Thuraisingham, B. (1996). MOMT: A multilevel object modeling technique for designing secure database applications. Journal of Object-Oriented Programming.9, 4, 22–29.
11. Jürjens, J. (2002). UMLsec: Extending UML for secure systems development. In Jézéquel, J., Hussmann, H. & Cook, S. (Eds.), UML 2002 – The Unified Modeling Language, Model engineering, concepts and tools (pp. 412–425). Germany, Springer.
12. Castano, S., Fugini, M., Martella, G. & Samarati, P. (1994). Database Security. Addison-Wesley
13. Batini, C., Ceri, S. & Navathe, S. (1991). Conceptual database design. An entity-relationship approach. New York, Addison-Wesley.
14. Connolly, T. & Begg, C. (2002). Database systems. A practical approach to design, implementation, and management. Addison Wesley.
15. Levinger, J. (2002). Oracle label security. Administrator's guide. Release 2 (9.2). Retrieved July 1, 2002, from http://www.csis.gvsu.edu/GeneralInfo/Oracle/network.920/a96578.pdf.
16. Avison, D., Lau, F., Myers, M. & Nielsen, A. (1999). Action research. Communications of the ACM, 42(1), 94–97.
17. Fernández-Medina, E., Martínez, A., Medina, C. and Piattini, M. (2002). Integrating Multilevel Security in the Database Design Process. In proceedings of the 6th International Conference on Integrated Design and Process Technology (IDPT'2002). June. Pasadena, California.
18. Piattini, M. & Fernández-Medina, E. (2001). Specification of security constraints in UML. In proceedings of the 35th Annual 2001 IEEE International Carnahan Conference on Security Technology (ICCST 2001), pp. 163–171. October, 2001. London (UK).
19. Leavitt, N. (2000). Whatever happened to Object-Oriented Databases?. Industry Trends, IEEE Computer Society, August, 16–19.
20. Conrad, C. & Turowski, K. (2001). Temporal OCL: Meeting specification demands for business components. In Siau, K. & Halpin, T. (Eds.), Unified modeling language: Systems analysis, design and development issues (Chapter 10). Hersey, PA., Idea Group Publishing.
21. Toval, A., Olmos, A & Piattini, M. (2002). Legal Requirements Reuse: A Critical Success Factor for Requirements Quality and Personal Data Protection. IEEE Joint International Requirements Engineering Conference (RE´02). IEEE Computer Society, 95–103.