World Multiconference on Systemics, Cybernetics and Informatics

July 22-25, 2001
Orlando, Florida, USA

PROCEEDINGS

Volume VII

Computer Science and Engineering: Part I

Organized by IIIS
International Institute of Informatics and Systemics

Member of the International Federation of Systems Research

IFSR

Co-organized by IEEE Computer Society
(Chapter: Venezuela)

EDITORS
Nagib Callaos
Belkis Sanchez
Luis Hernandez Encinas
Jerzy Grzymala Busse

ISBN 980-07-7547-1

PROGRAM COMMITTEE

Chairman: Prof. William Lesso (USA)

Abe, Akinori (Japan)
Abe, Jair Minoro (Brazil)
Abi-Raad, Maurice (Australia)
Acuña Castillo, Silvia Teresita (Argentina)
Ali, Zulfiqur (United-Kingdom)
Allegra, Mario (Italy)
AlMohammad Bader, AlBdaiwi (Kuwait)
Ammenwerth, Elske (Germany)
Amos, David (France)
Andrieux, Laurent (France)
Anzaloni, Alessandro (Brazil)
Audestad, Jan Arild (Norway)
Aveledo, Marianella (Venezuela)
Badawy, Wael (Canada)
Baïna, Jamal (France)
Banathy, Bela A. (USA)
Banathy, Bela H. (USA)
Beheshti, Mohsen (USA)
Bemley, Jesse L. (USA)
Bica, Marin (Romania)
Boiko, Igor (Canada)
Bozinovski, Stevo (Macedonia)
Brankovic, Ljiljana (Australia)
Bruzzone, Agostino G. (USA)
Burge, Jamika (USA)
Buzuloiu, Vasile (Romania)
Cano Escriba, Juan Carlos (Spain)
Carretero, Jesús (Spain)
Castillo, Oscar (Mexico)
Cernuzzi, L (Paraguay)
Champarnaud, Jean-Marc (France)
Chandra, Ramesh (India)
Chen, Chung-Ming (Taiwan)
Chen, Pei-Min (Taiwan)
Cheng-Li, Liu (Taiwan)
Chiu, Yi-Jen (USA)
Cohen, Eli (USA)
Curcio, Igor (Finland)
Da Silva, Ivan Nunes (Brazil)
David, Amos (France)
Duale, Ali (USA)
Dubois, Daniel (Belgium)
Dujet, Christiane (France)
Duong, Tuan (USA)
Eastabrook, Glenn (Canada)
Elizondo, César (Mexico)
Esquivel, Susana (Argentina)
Farooqui, Aamir (USA)
Fernandez, Jorge (USA)
Ferri, Fernando (Italy)
Fong, Anthony (Hong-Kong)
Fulantelli, Giovanni (Italy)
Gammoudi, Mohamed Mohsen (Tunisia)
Ganz, Aura (USA)
Garcia-Zambrana, Antonio (Spain)
Gendron, Michael (USA)
Goldman, C. (Israel)
Gou, Bei (USA)
Gou, Hongmei (China)
Granja-Alvarez, Juan Carlos (Spain)
Grout, Ian (Ireland)
Grzymala-Busse, Jerzy (USA)
Gunay, Kibarer (Turkey)
Guo, Qinglian (Japan)
Gutierrez, Rafael (USA)
Guu, Sy-Ming (Taiwan)
Ha, Quang (Australia)
Hamid, Issam A. (Japan)
Hanratty, Timothy (USA)
Hantos, Peter (USA)
Hernandez-Encinas, Luis (Spain)
Hideo, Fujimoto (Japan)
HongSheng, Li (China)
Horvath, L. (Hungary)
Hu, Yunfa (China)
Iliopoulos, Costas (United-Kingdom)
Izworski, Andrzej (Poland)
Jacob, Lillykutty (Singapore)
Jacomet, M. (Switzerland)
Jha, Manoj (USA)
Jordan, Andrzej (Poland)
Jozwiak, Lech (The Netherlands)
Juric, Matjaz B. (Slovenia)
Kamijo, Shunsuke (Japan)
Karlin, Jay (USA)
Karras, Dimitris A. (Greece)
Kasabov, N. (New Zealand)
Kaupp, Gerd (Germany)

Kawai, Shigeru (Japan)
Kim, Daeyoung (USA)
Klovsky, Daniel D. (Russian)
Koide, Seiji (Japan)
Kolodnytsky, Mykola (Ukraine)
Kraiem, Naoufel (Tunisia)
Krajcar, Slavko (Croatia)
Kvasnica, Milan (Czech-Republic)
Lastra, Jose (Finland)
Lau, Vincent (Hong-Kong)
Lebby, Gary (USA)
Lee, Hsuan-Shih (Taiwan)
Lee, Jong kun (Korea-(Republic-of))
Lefevre, T (Thailand)
Liang, Jie (USA)
Long, Steven (USA)
Loutfi, Mohamed (United-Kingdom)
Lu, Ning H. (USA)
Luo, Zhi-Wei (Japan)
Maciel, Paulo (Brazil)
Martin, Curtis (USA)
Masaki, Murakami (Japan)
Meijer, Bart R. (The Netherlands)
Motus, Leo (Estonia)
Mounir Alaoui, Salim (USA)
Mow, Wai Ho (Hong-Kong)
Muravyov, Sergey (Russian)
Najarian, Kayvan (USA)
Nakashima, Hideyuki (Japan)
Naranjo, Michel (France)
Naviner, Lirida (France)
Neagoe, Victor-Emil (Romania)
Neelov, Igor (Finland)
Ng, H.S. Raymond (Hong-Kong)
Nishio, Satoru (Japan)
Ohsawa, Yukio (Japan)
Ohta, Toshizumi (Japan)
Ohyama, Yasuhiro (Japan)
Oka, Ryuichi (Japan)
Okun, Oleg (Finland)
Palade, Vasile (Romania)
Patel, Ahmed (Ireland)
Patterson, Jr. F. G. (USA)
Pelaez, Javier R. (Brazil)
Perales, Francisco José (Spain)
Petrounias, Ilias (United-Kingdom)
Pham, Tuan (Canada)
Piattini, Velthuis Mario (Spain)
Pierre, Samuel (Canada)
Postigo, José (Aegentina)
Potaturkin, Oleg (Russian)
Power, Gregory (USA)
Power, James (Ireland)
Prokop, Roman (Czech-Republic)
Protheroe, Dave (United-Kingdom)
Ramesh, B. Inampudi (India)
Refice, Mario (Italy)
Remmel, Jeff (USA)
Rishe, Naphtali (USA)
Rodríguez, Manuel (Spain)
Rosario, Dalton (USA)
Sadka, Abdul H. (United-Kingdom)
Saglietti, Francesca (Germany)
Sancho, Gómez José Luis (Spain)
Saseetharran, M. (Sasheei) (USA)
Shinonaga, Hideyuki (Japan)
Sommerer, Christa (Japan)
Succi, Giancarlo (Canada)
Surdu, John (USA)
Suzuki, Naoki (Japan)
Szabo, Raisa (USA)
Takahashi, S. (Colombia)
Tamulis, Arvydas (Lithuania)
Teixeira, Antonio Luis Jesus (Portugal)
Testorf, Markus (USA)
Tinetti, Fernando G. (Argentina)
Torres, Michel (Venezuela)
Trofimov, Vyacheslav (Russian-Federation)
Tsai, Cheng-Fa (Taiwan)
Tseng, Shian-Shyong (Taiwan)
Uchôa, Elvira (Brazil)
Vacher, Jean-Philippe (France)
Vafaie, Haleh (USA)
Van der Schaar, Mihaela (The Netherlands)
Vanhala, Jukka (Finland)
Vergez, Christophe (France)
Verna, Didier (France)
Watanabe, Tomio (Japan)
Welzl, Michael (Austria)
Whymark, Greg (Australia)
Wieczorkowska, Alicja (Poland)
Wolfram, Klein (Germany)
Wong, Kin Yeung (Hong-Kong)
Wu, Xuezhong (China)
Xenos, Michalis (Greece)
Xia, F. (Macau)
Xiong, Yingen (China)
Yamaguchi, Yoko (Japan)
Yasser, E. (Egypt)
Yigang, He (China)
Yu, Guoyang (China)
Zboril, F. (Czech Republic)
Zeeuw, G. (Holland)
Zhang, Qingying (China)
Zhang, Yiying (Canada)
Zimmermann, Kerstin (Austria)
Zong, Xuli (USA)
Zubairi, Junaid (USA)

Additional Reviewers of Invited Sessions

Abe, Akinori (Japan)
Abe, Jair (Brazil)
Abi-Raad, Maurice (Australia)
Acuña, Silvia Teresita (Argentina)
AlMohammad, Bader (Kuwait)
Andina de la Fuente, Diego (Spain)
Andrieux, Laurent (France)
Augusto, Juan Carlos (Argentina)
Bala, Jerzy (USA)
Banachowski, Lech (Poland)
Bastos-Filho, Teodiano (Brazil)
Bemley, Jesse (USA)
Biajiz, Mauro (Brazil)
Bica, Marin (Romania)
Bikker, Henk (Netherlands)
Black, Paul (USA)
Boiko, Igor
Bose, Bella (USA)
Bouguettaya, Athman (USA)
Brown, Shiree (USA)
Bruzzone, Agostino (Italy)
Burge, Jamika (USA)
Butrylo, Boguslaw (Poland)
Cano, Juan-Carlos (Spain)
Cantu Ortiz, Francisco Javier (Mexico)
Carelli, Ricardo (Argentina)
Casanova, Marco (Brazil)
Castillo, Oscar (Mexico)
Chekmasov, Maxim (USA)
Chen, Chung-Ming (Taiwan)
Chen, Tai-Ann (USA)
Chen, Tsao (USA)
Cheng, L. L. (Hong-Kong)
Chiu, Yi-Jen (USA)
Chojnacki, Artur (Netherlands)
Ciarlini, Angelo (Brazil)
Cline, Harvey (USA)
Côrtes, Sérgio (Brazil)
Cull, Paul (USA)
Curcio, Igor (Finland)
Da Silva Araújo J., Joao B. (Portugal)
De Giusti, Armando (Argentina)
Doh, Yoonmee (USA)
Duale, Ali (USA)
Dumitrache, Ioan (Romania)
Elfrey, Priscilla (USA)
Elmasri, Ramez (USA)
Farah, Yusuf (USA)
Ferré, Xavier (Spain)
Flich, Jose (Spain)
Fung, W. K. (Hong-Kong)
Giambiasi, Norbert (France)
Giribone, Piero (Italy)
Gong, Yun (USA)
Gou, Bei (USA)
Gou, Hongmei (China)
Grzymala-Busse, Jerzy (USA)
Guo, Qinglian (Japan)
Gutierrez, Martha (USA)
Gutierrez, Rafael (USA)
Ng, H. S. (Hong-Kong)
Hadjarian, Ali (USA)
Hamid, Issam A. (Japan)
Hanratty, Timothy (USA)
Hasselbring, Wilhelm (Germany)
Hattori, Shimmi (Japan)
He, Yiwei (Japan)
Hernandez-Encinas, Luis (Spain)
Holmes, Donald (USA)
Hong, Tzung-Pei (Taiwan)
Hongsheng, Li (China)
Hu, Wen-Chen (USA)
Hu, Yunfa (China)
Huang, Biqing (China)
Hwang, Gwo-Jen (Taiwan)
Inmon, William (USA)
Ishida, Kazumari (Japan)
Izworski, Andrzej (Poland)
Jacob, Lillykutty (Singapore)
Jaseemuddin, Muhammad (Canada)
Jha, Manoj (USA)
Jordan, Andrzej (Poland)
Jozwiak, Lech (Netherlands)
Kamay, Vic (Australia)
Kamijo, Shunske (Japan)
Kawai, Shigeru (Japan)
Kibarer, Günay (Turkey)
Koide, Seiji (Japan)
Kolodnytsky, Mykola (Ukraine)
Kouba, Zdenek (Czech-Republic)
Krajcar, Slavko (Croatia)
Kuchcinski, Krzysztof (Sweden)
Kunii, Tosiyasu (Japan)
Lam, K. P. (Hong-Kong)
Lee, Hsuan-Shih (Taiwan)
Leguizamon, Guillermo (Argentina)
Leung, K. Y. (Hong-Kong)
Liao, Yuan (USA)
Lin, Miao-Tsong (Taiwan)
Liu, Ngai Hang (Hong-Kong)
Loumeau, Patrick (France)
Mahboob, Athar (Pakistan)
Maldonado, José Carlos (Brazil)
Manzoni, Pietro (Spain)
Matkovsky, Philip (USA)
Mccarthy, Richard (USA)
Medjahed, Brahim (USA)
Melin, Patricia (Mexico)
Michalewicz, Zbigniew (USA)
Moore, Dennis (Australia)
Morales-Porras, Andres (Venezuela)
Moreno Sánchez-C., Ana M. (Spain)
Mostafavi, Taghi (USA)
Mouchards, Laurent (France)
Mounir Alaoui, Salim (USA)
Moura, Ana Maria (Brazil)
Muravyov, S. (Russian-Federation)
Nagaoka, Takashi (Japan)
Nakazawa, Minoru (Japan)
Navathe, Sham (USA)
Naviner, Lirida (France)
Neagoe, Victor-Emil (Romania)
Neagu, Daniel-Ciprian (Romania)
Neuhold, Erich (Germany)
Nishio, Satoru (Japan)
Ohta, Toshizumi (Japan)
Ohyama, Yasuhiro (Japan)
Oka, Ryuichi (Japan)
Okada, Isamu (Japan)
Okuda, Takahiro (Japan)
Okun, Oleg (Finland)
Oliveira, José Palazzo
Palade, Vasile (Romania)
Patriciu, Victor (Romania)
Perkowski, Marek (USA)
Pillai, Radhakrishna (Singapore)
Polkowski, Lech (Poland)
Pozo-Coronado, Luis (Spain)
Radzik, Tomasz (UK)
Raman, Rajeev (UK)
Refice, Mario (Italy)
Remmel, Jeffrey (USA)
Ren, Shouju (China)
Robinson, Charles (USA)
Saake, Gunter (Germany)
Sadka, Abdul H. (UK)
Sagot, Marie France (France)
Sahuquillo, Julio (Spain)
Sancho-Gomez, Jose Luis (Spain)
Sarcinelli-Filho, Mário (Brazil)
Sattler, Kai-Uwe (Germany)
Savino, Michelina (Italy)
Schneebeli, Hansjorg (Brazil)
Scott, Martin (USA)
Seibel, Luiz (Brazil)
Selvakumar, S.
Sha, Lui (USA)
She, Jin-Hua (Japan)
Shinonaga, Hideyuki (Japan)
Shirani, Shahram (Canada)
Silva, Diva (Brazil)
Silva, Sidney (Brazil)
Simari, Guillermo (Argentina)
Siqueira, Sean (Brazil)
Slezak, Dominik (Poland)
Slusarczyk, Aleksander (Netherlands)
Smyth, Bill (Australia)
Srbljic, Sinisa (Croatia)
Stewart, Greg (Canada)
Sumiyama, Kazuki (Japan)
Sun, Yung-Nien (Taiwan)
Suzuki, Naoki (Japan)
Suzuki, Shigeyuki (Japan)
Synak, Piotr (Poland)
Tanaka, Asterio (Brazil)
Taniar, David (Australia)
Teixeira, Antonio (Portugal)
Teorey, Toby (USA)
Testorf, Markus (USA)
Tinetti, Fernando G. (Argentina)
Traina Junior, Caetano (Brazil)
Triñanes, Jorge (Uruguay)
Tseng, Shian-Shyong (Taiwan)
Tudruj, Marek (Poland)
Uyar, Umit (USA)
Vafaie, Haleh (USA)
Vanhala, Jukka (Finland)
Vidal, Vania (Brazil)
Vieira, Marina (Brazil)
Wang, J (Hong-Kong)
Wheeler, Patrick (USA)
Wolinski, Christophe (France)
Wong, Eric Wing-Ming (Hong-Kong)
Wong, Kin Yeung (Hong-Kong)
Yamaguchi, Yoko (Japan)
Yamamoto, Yoko (Japan)
Yeung, Alan Kai-Hau (Hong-Kong)
Zexiang, Li (Hong-Kong)
Zhao, Qing (USA)
Zhixiang, Wang (China)
Zhou, Shuigeng (China)
Zimmermann, Kerstin (Austria)
Zong, Xuli (USA)
Zude, Zhou (China)

ACADEMIC AND SCIENTIFIC SPONSORS

- WOSC: World Organization on Systemics and Cybernetics (France)
- The Centre for Systems Studies (UK)
- Systems Society of Poland
- Society Applied Systems Research (Canada)
- Slovenian Artificial Intelligence Society
- Simon Bolivar University (Venezuela)
- Polish System Society (Poland)
- Italian Society of Systemics
- ISSS: International Society for the Systems Sciences (USA)
- ISI: The International Systems Institute (USA)
- IEEE/Latin-America
- IFSR: International Federation of Systems Research (Austria/USA)
- IEEE Computer Society (Chapter: Venezuela)
- Cybernetics and Human Knowing: A Journal of Second Order Cybernetics and Cybersemiotics (Denmark)
- CUST, Engineer Science Institute of the Blaise Pascal University (France)
- Concurrency and Architecture Group, the Telematics Engineering Department of the University of Las Palmas of Gran Canaria (Spain)
- The Tunisian Scientific Society (Tunisia)

HONORARY PRESIDENTS
Bela Banathy
Stafford Beer
George Klir

PROGRAM COMMITTEE CHAIR
William Lesso

GENERAL CHAIR
Nagib Callaos

CHIEF ADVISER
Michel Torres

ORGANIZING COMMITTEE CHAIR
Belkis Sanchez

ORGANIZING COMMITTEE CO-CHAIR
Jorge Molero

HARDCOPY PROCEEDINGS PRODUCTION CHAIR
María Sanchez

CDs PROCEEDINGS PRODUCTION CHAIR
Juan Manuel Pineda

EXECUTIVE ASSISTANT
Jeannette Castellano

MANAGER OF PROGRAMMING
Floramely Arias

OPERATIONAL ASSISTANT
Marcela Briceño

CONTENTS

VOLUME VII

COMPUTER SCIENCE AND ENGINEERING: PART I

Document and Natural Language Processing

Intermediate Representation Engineering for the Java Virtual Machine – Invited Session
Organizer: James Power (Ireland)

Mathematical Methods and Optimization in Problem Solving Systems

Multimedia Data Retrieval and Human Interface – Invited Session Organizer: Ryuichi Oka (Japan)

Parallel and Distributed Systems

Robotics and Control Systems

Theoretical Methods in Cryptology – Invited Session
Organizer: Luis Hernandez-Encinas (Spain)

Rough Sets: Theory and Applications – Invited Session
Organizer: Jerzy Grzymala-Busse (USA)

Database Security (DS'2001) – Invited Session
Organizer: Mario Piattini Velthuis (Spain)

Parallel and Distributed Systems

Issues in Database and Data Warehouse Security

Manuel A. SERRANO
Computer Science Department, University of Castilla – La Mancha
Ciudad Real, Spain

and

Eduardo FERNANDEZ-MEDINA
Computer Science Department, University of Castilla – La Mancha
Ciudad Real, Spain

ABSTRACT

We live in a technical world, where information is a valuable asset. Companies must store and use a great amount of data in order to be competitive. Electronic crime is growing and this is forcing organizations to secure its information system.

Usually, information systems managed by organizations contain personal data, which must be secure to assure that individual rights are not violated.

Security must be considered from the early stages of the design of an information system, in order to avoid problems derived from the publish of sensitive data, break down of the system, incoherence of data, reveal of business rules and any other action that can be derived from the reveal, modify or delete of data of the information system.

Keywords: Database Security, Data Warehouse Security, Security Risk, Database Access Control, Database Security Design, Data Warehouse Security Design.

1. INTRODUCTION

Nowadays, we live in an information society. Technological advances in communications, transport, banking, manufacturing, medicine, and other fields are demanding more sophisticated information requirements in organizations worldwide. Companies must handle large quantities of data, while maintaining a high level of security in order to ensure that information needs are met.

The electronic crime is growing and this force organizations to take a look at how information systems can maintain security without disregarding the technological needs of real-time systems in a global market. It is important therefore, that in information systems analysis and design, security requirements are taken into account.

Security is an important quality characteristic as described in the ISO/IEC (International Organization for Standardization / International Electrotechnical Commission) [6]. According to this standard, the main components of internal and external quality are reliability, efficiency, usability, functionality, maintainability, and portability. All of these quality factors have several quality sub-factors, viewing security as a quality sub-factor of functionality. This standard defines security in the following way:

"Security is the capacity of the software product to protect data and information so that unauthorized persons or systems cannot read or modify them and so that access is not denied to authorized personnel."

Usually, information systems contain information that can be considered sensitive and to which access must be restricted. Often they contain personal information about individuals, which must be specially protected; such as social security numbers, addresses, phone numbers, religious affiliation, sexual preferences, and medical data, among others. If this information is used without certain security precautions, individual rights may be violated. The information systems that manage this type of information must be provided with security techniques in order to guarantee that personal rights are not infringed upon.

The use of information technologies is regulated by law, serving mainly to ensure that citizen's rights are upheld. Most countries have established data protection laws, especially when this data is of a personal nature. Information systems that do not guarantee data security will not only be facing fines and penal sanctions for violating law, but also the negative impact of security breaches [10].

As a consequence of the technological changes that are occurring at an ever increasing pace, there is a great need for security support. Technology has produced the evolution of several fields with special characteristics from a security point of view, requiring important changes in the traditional ways of handling security. Some of these fields are:

1) The progress that Internet has experienced, and especially the access to databases via the web requires secure communications. Information must be safely transmitted.
2) Electronic business, given its dynamic nature, demands the fulfillment of new data security requirements. It is of vital importance to guarantee the security of e-business in order to convert it into another secure and reliable way to do business.
3) The arrival of data warehousing has brought about the necessity to establish new security techniques owing to architectural problems, of inference, administration and auditing. Also, the use of data recuperation techniques like data mining can lead to privacy problems, provoking new security requirements. [16].

All of these factors, including legislative, regulative, and technological factors, justify the importance of security in information technologies. In addition, there is the economic perspective of ensuring long-term growth and stability in this technologically driven environment. For instance, Baskerville [1] confirms that a fifth of US organizations suffer one or more physical or logical information system disruptions within a three year time period. The study also concludes that 12% of the US companies were electronic fraud victims with the average fraud amounting to $75,000 per company.

Database security is concerned mainly with the following aspects: confidentiality, integrity, and availability. Respectively, these refer to problems associated with the discovery of confidential information by unauthorized persons, the alteration of information by unauthorized personnel, and unavailability of information when it is needed [3]. The range of possible threats that affect each one of the security factors is so broad that they cannot be attacked as a group, but each threat must be addressed individually. In this chapter, we present a state of the art of database security, focusing it on confidentiality.

In this paper we will make a brief travel around the techniques that exist for ensure the security of information system. First, we will analyze the ways to control the access to our system. Next we will see some design methodologies of secure databases and some problems that arise from the implantation of data warehouses. Finally we will see the future trends and some conclusions.

2. ACCESS CONTROL TECHNIQUES

In this section, we will look at an aspect of great importance to information system security: The access control to information system resources. In the following lines basic concepts relating to access control are described, and in the following sections a selection of the most important access control techniques are analyzed, such as discretionary, mandatory, task-based and role-based access control.

Access control is a mechanism through which we ensure or try to ensure that resources can only be accessed by authorized personnel, and that this personnel can only perform authorized activities.

Usually, access control to resources is done using authorization rules, which are signified by <s,o,a> which indicate that the subject s can access to an object o performing action a.

- *Subjects* are the entities to which access to the objects can be authorized. Although these are usually individual users, they can also be user groups, roles, or even processes that are performed in the name of users.
- *Objects* are elements whose access we want to control. In relational database systems, the objects can have different granularity, in other words, both complete relations, views and individual attributes can be accessed.
- *Actions* are the possible operations that can be performed, and that in relational databases are usually *select*, *insert*, *delete*, and *update*.

Discretionary Access Control.
This is the oldest strategy to manage the access control. This strategy relies on the fact that the subjects can access the objects according to their identity and some rules of authorization.

Authorization rules specify the actions that each subject can perform on each object of the system. When the user try to make an operation on an object, the system searches among the authorization rules for a rule that allow the user to do that action on that object. If no rule is found, the system denies the access.

Mandatory Access Control.
The mandatory access control is based on the model designed for operating systems by *Bell and La Padula*. This control policy classifies subjects and objects in different levels of security. These levels usually are "unclassified", "confidential", "secret" and "top secret".

There are two basic rules when accessing data:

- A subject can read an object if the subject security level dominates the object level.
- A subject has writing access to an object if the security level of the subject is the same of the object level (A subject can modify objects of its level).

In order to support this access control policy, it is necessary to use a database management system that allows us to classify the data by levels. These databases, which can classify the data by levels, are known as "multilevel databases".

Task-Based Access Control.
This is a paradigm for access control and management of authorizations that are different from usual, known as "*Task-based authorization control (TBAC)*", which is appropriate for distributed computation and for information processing activities with multiple access control points. An in-depth review of this technique is shown in [17].

This model deals with activities or tasks to represent authorizations modeling them as time periods during which an authorization remains valid. The main idea is to grant the correct amount of permission at the right time, and only those which are strictly necessary, as well as retract permission once unnecessary. Therefore, what is shown is a method where the access control permits are granted and revoked in line with a mechanism of control validity of the authorizations, also without the necessity of manual management.

In TBAC, access control is seen as a tuple with 5 elements: *"Subject* X *Object* X *Action* X *Usage and validity counts* X *Authorization-step"*, where each authorization-step represents an abstraction where permissions are grouped and trustees that are in charge of administrating these permissions, activating and deactivating them opportunely. Therefore, each authorization step maintains its proper state of protection. A usage counter is associated with a permit, and when this counter reaches its limit, the associated permit is deactivated and the corresponding action is no longer allowed.

Role-Based Access Control.
Role based access Control (RBAC) is an alternative to traditional, discretional and mandatory access control methods. Traditionally, security management requires low-level controls,

and normally some access control lists need a considerable maintenance effort.

In RBAC, permissions are associated with roles, and user are made members of the roles. This is the way that users obtain permissions, which greatly simplifies permit management. The roles represent each functional group of organizations, grouping in each one users with similar functions and responsibilities. Through this mechanism it is very easy to carry out certain actions such as change users from one role to another, as well as add or eliminate from the roles certain permissions as required. For instance, the roles in a bank could be clerk and accountant, where each one of these has a unit of privileges. Some of these, as in this case, are hierarchical and shared. This access control technique has been widely published. Updates and new utilities constantly come up, like [13] and in [5].

3. SECURE DATABASE DESIGN

Database design, due to its great complexity, is an activity that requires a methodological approach. Although most software development organizations have accepted this fact, it is not usual for the models and techniques to take security aspects into consideration.

Normal database development methodologies usually consist of the following three phases [4][2]:

- Conceptual modeling. In this stage an analysis of requirements is made and a good representation of the information that makes up the universe of discourse is obtained. Usually an entity-relationship scheme is obtained.
- Logical Design. The objective of this phase is to adapt the conceptual scheme obtained in the previous stage to the data model on which the desired database management system is based.
- Physical design. In this stage the objective is to install as efficiently as possible the logical scheme.

These methodologies should be complemented by adding various models or extending the existing ones. In the initial stages it would be necessary (if they exist) to identify and model the security requirements and determine the security policies and access control necessary for each particular case. In the more advanced stages it is necessary to design multilevel databases and access control policies respecting the requirement identified in the previous stages.

Secure Conceptual Database Models.
An important aspect of the design of secure databases is the modeling of security requirements. It is necessary to use a model which allows both designers and users to mould their security requirements in-depth, just as is done with other semantical aspects like integrity in the universe of discourse.

There is a few proposal for secure database modeling. One of these proposal was SDMS (Semantic Data Model for Security) [14][15], which consists of the extension of the conceptual models used in database design.

The use of a model like SDMS helps the designer in the identification of inference problems (the ability to use data from a certain level of sensitivity to deduce data from another superior level), aggregation problems (if the aggregation of some data with a security level must have a higher security level) and overclassification (if a higher than necessary level is assigned to the data).

In the SDMS, secret restrictions are identified, such as:

Semantic restrictions: these specify the level of classification that data and its associations receive.

Access control restrictions: These specify the authorized users to access groups or data elements.

Secret semantic restrictions are described in the model using objects, attributes, and associations, and they are represented using diagrams similar to entity-relationship, highlighting the figures corresponding to those that are attached to the classification level (Unclassified, Secret, Confidential, etc.).

A concept worth mentioning is the "identifier" which is an object attribute which from the perspective of security allows object identification. This concept does not completely coincide with the candidate key of the relational model, seeing as there are "almost unique" attributes that even though they can be repeated (thus voiding them as candidate keys), they must be considered identifiers. In this sense the identifiers are said to be "quasi-keys".

As far as classification level is concerned, it can be specified as one value (S, for example) a set of values (U,C) or a range (U-S).

Just as what happens with semantic models, in addition to these elements a unit of restrictions is described. These are:

- Inherent, which can be divided into:
  - Uniform classification, if all the objects instances that the restriction applies to are classified at the same level.
  - Value-dependent classification, if the objects, attributes, or associations are classified according to their values, for example with salary greater than $200,000 are classified as "S", while the others are "U".
  - Explicit, which are those that can not be directly represented in the data model, like associations among attributes of different objects.
- Implicit, with two important restrictions:
  - The result of associating any data with a classified attribute is classified with a level that is at least as much as the attribute.
  - If two classified attributes are associated, the resulting classification is the higher of the attribute classification and the direct association classification.

Associated with the graphic, the model includes a language to express security restrictions, based on an extension of the language ALICE (Assertion Language For Integrity Constraint Expression), which essentially results in the ability to represent explicit restrictions.

The language has an underlying logical representation, which facilitates the analysis of the application requirements in terms of security.

Secure Database Logical Models.
In the 80's and early 90's some prototypes of secure database logical models appeared, and some of the most important are the following:

- SeaView. It is based on a viewing concept, in such a way that a subject with security level L can only view relations that are classified at level L or below. It is comprised of two models, the MAC (mandatory access control) and the TBC (Trusted Computing Base). The first defines the mandatory security policy, and the second defines multilevel relations and formalizes the discretional security policy.
- LOCK Data Views. In this prototype the language for consultation SQL is improved with declarations that allow the management of the security levels of the elements classified in the databases. It is composed of both compulsory and discretional security policies.
- The Jadodia and Sandhu Model. This model extends the standard relational model to consider the classification levels. Therefore a multilevel relation consists of a scheme of a multilevel relation and a collection of requests of the relation. This model defines a series of properties so that the principles of the mandatory security policy are complied with.

Many models have appeared for modeling and implementing secure object oriented databases. These models differ in many aspects, above all because each one focuses on different aspects of the problem of security. In [8] a taxonomy of these models is presented in which the differences between these models are analyzed. The following are examples of these models:

- The SODA model. It is a very simple model for secure databases based on a general object-oriented model. The objects or instances are assigned an accreditation. According to these security levels and in accordance with the properties defined by Bell and Lapadula, a subject is allowed to carry out the method of an object or messages are sent between the objects.
- The SORION model. Each entity of the system, subjects, objects, variables, messages etc. is assigned a security level. A list of rules is proposed in order to ensure that none of the operations violate the security policies established.
- The Millen-Lunt model. It is based on an architecture by layers. The security kernel that provides the mandatory access control is found in the lowest level. In the next layer the object system that implements the object-oriented services is located. Rules for managing the layers adequately are defined in the model.

A Methodology For Security Databases Design.
In the following paragraphs a methodology based on OMT [12] is analyzed. This methodology is MOMT [7] formulated to design secure applications based on multilevel databases.

Multilevel Design. MOMT is an extension of OMT incorporating semantic characteristics in order to be able to design multilevel databases. Therefore each element of data will be assigned an appropriate and independent security level.

Stages of Methodology. Just like OMT, MOMT is made up of three principal stages:

- The analysis phase: It is the principal stage of methodology and consists of three models: the multilevel object model, the dynamic multilevel model and the functional multilevel model, each representing in turn the static, dynamic and transformational characteristics of the system.
- The system design phase: in this stage, the high level structure of the system is defined.
- The design object phase: where a detailed base is drawn up to implement the objects.

Models of the Methodology.
The most important phase in the development of databases is analysis because more effort should be made at this stage since diverse abstractions of the problem can be obtained from this, as well as help in understanding clearly, what exactly it is that the system should do. In this part we describe the most important aspects of the analysis stage in MOMT, focusing on the three models that the methodologies consider: the object model, the dynamic model and the functional model. A highly detailed study of this method can be found in [7].

Not all databases require the same level of security, it depends on the type of data they are going to deal with, the environment for which they are designed to be used in, etc. In this stage of methodology, the designer evaluates the required level of security for the design he is working on.

The Multilevel Object Model. The object model captures the static aspects of the applications, all the different parts of the system and all the associations between those parts are represented in this model, considering the desired level of security for each entity and association.

In the object model, each object will be associated with a level of security of such a form that it will be unseen in inferior levels of security. The different objects are grouped into classes through which the properties that they will subsequently inherit are defined. It seems logical that a group of objects should also be associated with a level of security. Just as in the case of each individual object, each class will be unseen in levels of security inferior to its own, and be visible in equal or superior levels. A relationship exists between a class and the instantiated objects relative to the particular security level of each one, and this is the following: if an object (OB1) belongs to a class (CL1) and the security level of the object is LevelOB1 and that of class LevelCL1, then LevelOB1 must be greater or equal to LevelCL1. In other words, a object with a security level lower than the level of the class to which it belongs cannot exist, since otherwise it could not inherit the class properties.

Each class can have a range of associated security levels. The lowest level in the range indicates the level of the class. The range of levels of a class specify the required levels of security in the class. In other words the level of an instance of a class has to be included in the range of levels of the class.

In terms of attributes, a class can have different levels, but the level of an attribute has to be greater than the level of the class. Furthermore, the security level of the attribute with the role of identifier has to be the same as that of its class. The value of an attribute can have a range of associated levels, since the values applied to attributes will have to have a security level within this range.

The methods, which are the medium through which the operations are implemented also, have to have an associated level of security and have to fulfil a specified relationship with that of their class. The security level of the methods has to be dominant over the level of the classes. In other words it has to be greater or equal to the level of the class.

The associations will also have a level of protection. The level of security demanded by each of the associations always has to be equal or superior to he classes to which it relates. In the same way, an instance of an association, in other words a link, will have a greater or equal level than that of the association, and that of the related object.

The mechanism of generalization permits us to refine the classes (superclasses) into more specific groups which inherit the properties of the first groups (subclasses). The considered rule for the relationships of generalization is that the security level of the subclasses has to be dominant or more restrictive than the security level of the superclass in such a way that makes it impossible for a 'person' class with a 'confidential' level to inherit properties from a 'countable' class with a 'non-classified' level. In this case security would be violated since a subclass would be able to access the properties of the superclass, that should effectively remain inaccessible.

The Dynamic Multilevel Model. The dynamic model represents aspects related to time and changes in the objects. An event is a stimulus provoked by an object that has a certain effect on another object, changing the value of its properties. In other words, changing its state. Since an interaction happens between objects, and given that these can have distinct security levels, it will be necessary to adapt the model so that no security violations of the system occur.

The key information used in this model will give rise to all the graphic representations used as diagrams of the plan of events, events diagrams, etc. These are the events produced and the order or sequence in which these are produced.

The aim of a dynamic multilevel model (in terms of security) is to analyze each stage and determine the security problems which can arise, resolve them if possible and if not, negotiate with the client to reach an agreement in terms of the modifications necessary to the security requisites and assume the detected security risks.

The objects can be classified as active or passive. The objects that cannot produce events (passive objects) will only have the security level which is assigned to them during the construction of the object model, whilst the objects that can generate events (active objects) will be assigned two security levels: one which is the inherent level of the object and another level (operational level) in which the object can operate and which will never be superior to the level of the object.

The security related actions that will have to be carried out will firstly determine which are the active objects and which are passive, and subsequently assign an operational level to each active object (the inherent level of the object both passive or active have now been assigned to construct a multilevel object model).

Once all the types of objects and events have been identified, it is then necessary to carry out an event analysis to check that no security problems have arisen.

Finally a diagram of states has to be drawn up for each one of the classes which show the possible states that the objects are able to carry, depending on the received events and showing as such, the behavior of the objects.

The Multilevel Functional Model. This model helps to construct the class methods determining not only their security levels but also the levels of execution for each method. For the construction of this model, when or how the functions will be executed is not taken into account. This will be supported by flow charts showing the data, and specification techniques or processes like pseudocode.

The level of execution of a method has dominance over the security level of the class with which it is associated. The level of execution of the functions will vary in each stage, depending on the level of the object which triggers the event and provokes the execution of the method, and taking into account that the level of execution has to be greater or the same as the object with which it is associated.

4. SECURE DATA WAREHOUSE DESIGN

Data warehouses are a especial type of information systems. A organization, usually have lots of transactional databases, which contain the data that each department need. So often information is duplicated in different applications of the company. These transactional databases are dedicated to the daily work.

In order to have an effective decision support system, we must recollect all the information stored in the transactional databases and merge it in a big database: a data warehouse. This data warehouse contains a resume of all the data of the company. The data is stored with a structure that optimizes the queries to the information system.

Usually, each transactional database has its own security system. But it is difficult to migrate each of the individual security systems to the global security system of the data warehouse. Indeed, some of the security rules of the transactional databases may have no sense in the data warehouse context.

Another problem a data warehouse must face is conceptual, a decision support system is oriented to provide a large quantity of information, structured in some way, to make decision, which is opposite to security restrictions that try to avoid the revealing of information. Indeed, the problem is worse than this, since a decision support system try to expose information to inference trends and patterns to make good decision, but this can be a security hole because we can inference data that is not in the data warehouse and that is private. Also we can inference business rules making queries to the data warehouse.

It is necessary to include security restrictions in the early stages of development of a data warehouse, in order to assure that the information, which will be stored in the data warehouse, will be secured.

When adding security restrictions to the data warehouse schema, we must not forget to specify a method to import, to the data warehouse, the security information that we have in the transactional databases, which are the data sources of our decision support system.

Due to the special security restrictions that a data warehouse has, it is advisable to perform a risk analysis as we can find in [11].

5. CONCLUSIONS

The field of security is an incredibly open concept which embraces everything from the organizational politics of security to the encryption of a piece of data being transmitted through a network and passing through an infinity of intermediate levels.

Security in databases is a subject which currently has many lines of investigation open, amongst which are those relating to new access control techniques, new models for the management of multilevel database systems, security in web-oriented databases, security in datawarehouses, etc. Our investigation is centered mainly on the following three fields:

a) The adaptation of the development methodology for MOMT secure multilevel databases to the unified modeling language (UML).
b) Create a methodology to add security issues to the data warehouse design
c) The amplification of the query language SQL:1999 so that it would be possible to consult multilevel databases.
d) Given the importance of establishing satisfactorily security requirements, we aim to design a formal language for the specification of security requirements.

In this paper we have justified the repercussions which a lack of security can have on society, and we have drawn up a synthesis of the principal aspects that affect confidentiality in the design of databases: the control of access, the modeling of security requirements.

Finally we have seen the principal security problems that can arise in the design of a decision support system based on a data warehouse.

6. ACKOWLEDGEMENTS

This research is part of the RETISBD project, supported by the Ministry of Culture and Education (TIC2000-1873-E), which is a special action into the National Program of the Information Technologies and Communications.

7. REFERENCES

[1] Baskerville, R., Information Systems Security Design Methods: Implications for Information Systems Development. *ACM Computing Surveys*. Vol. 25. Nº 4. December 1993, pp. 375-415.

[2] Batini, C., Ceri, S. and Navathe, S.. *Diseño conceptual de bases de datos*. Addison-Wesley / Diaz de Santos. 1992.

[3] Castano, S., Fugini, M., Martella, G. and Samarati, P. *Database Security*. Addison-Wesley, 1994

[4] Connolly, T., Begg, C. and Strachan, A.. *Database Systems*. Addison-Wesley., 1998.

[5] Ferraiolo, D., Barkley, J. and Kuhn, R. A role-based access control model and reference implementation within a corporate intranet. *ACM Transactions on Information and Systems Security*, Vol. 2, Nº 1, February 1999, pp. 34-64.

[6] ISO/IEC 9126-1. *Information technology- Software product quality - Part 1: Quality model.*, 1999.

[7] Marks, D., Sell, P. and Thuraisingham, B. MOMT: A multilevel object modeling technique for designing secure database applications. *Journal of Object-Oriented Programming*. Vol. 9. Nº 4, 1996, pp. 22-29.

[8] Oliver, M. and Von S. A taxonomy for Secure Object-Oriented Databases. *ACM Transactions on Database Systems*, Vol. 19, Nº 1, March 1994, pp. 3-46.

[9] Parker, D. *Computer Security Management*. Reston, Reston, Mass, 1981.

[10] Peso, E. and Ramos, M.A. *LORTAD, Análisis de la Ley*. Diaz de Santos. Madrid., 1998

[11] Rodero, J.A., Rodero, J.A., Piattini, M. Análisis de Riesgos y Seguridad en los Almacenes de Datos. *Actas de la VI Reunión Española sobre Criptología y Seguridad de la Información, Ra-Ma*, 2000, pp. 53-63.

[12] Rumbaugh, J., Blaha, M, Premerlani, W., Eddy, F. and Lorensen, W. *Object-Oriented Modeling and Design*. Prentice Hall, Englewood Cliffs, 1991.

[13] Sandhu, R. and Bhamidipati, V. The URA97 model for role-based user-role assignment, in *Database Security XI: Status and Prospects*. Eds.: T.Y. Lin and S. Qian. Chapman and Hall, London, pp. 262-275. 1997.

[14] Smith, G.W. The Semantic Data Model for Security: Representing the Security Semantics of an Application. *Proceedings of the Sixth International Conference Data Engineering, IEEE*, pp. 322-329., 1990.

[15] Smith, G.W. Modeling Security-Relevant Data Semantics. Proceedings of the *IEEE Trans. On Software Engineering, Vol. 17. Nº 11*, November, 1991. pp. 1195-1203.

[16] Thuraisingham, B., Schlipper, L., Samarati, P., Lin, Jajodia, S. and Clifton, C. Security issues in data warehousing and data mining: panel discussion, in *Database Security XI: Status and Prospects*. (eds. T.Y. Lin and S. Qian), Chapman and Hall, London, pp. 3-16. 1997.

[17] Tomas, R. and Sandhu, R. Task-based authorization controls (TBAC): a family of models for active and enterprise-oriented authorization management, in *Database Security XI: Status and Prospects*. (eds. T.Y. Lin and S. Qian), Chapman and Hall, London, pp. 166-181. 1997.