Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 1997 Proceedings

Americas Conference on Information Systems (AMCIS)

8-15-1997

Security in heterogeneous interoperable database environments

W. Eßmayr
Softwarepark Hagenberg, we@faw.uni-linz.ac.at

Security in heterogeneous interoperable database environments

W. Eßmayr
Research Institute for Applied Knowledge Processing
Softwarepark Hagenberg
Hauptstraße 99, A-4232 Hagenberg, Austria
e-mail: we@faw.uni-linz.ac.at
Pernul
Dep. of Information Systems
University of Essen
Altendorfer Straße 97, D-45143Essen
Germany
e-mail: pernul@wi-inf.uni-essen.de
A M. Tjoa
Institute of Software Technology
Technical University of Vienna
Resselgasse 3, A-1040 Vienna, Austria
e-mail: tjoa@ifs.tuwien.ac.

Abstract: The paper deals with the security of interoperable heterogeneous database environments. It contains a general discussion of the issues involved as well as a description of our experiences gained during the development and implementation of the security module of IRO-DB - an European ESPRIT III funded project with the goal to develop interoperable access between relational and object-oriented databases.

Key words: database federation, security, heterogeneity, authorization, access control

Security in homogeneous *database systems* has been an issue for several years now. Various techniques have been proposed addressing the general security requirements *confidentiality* (protecting information from unauthorized access), *integrity* (protecting information against malicious or accidental modification), and *availability* (to serve authorized users whenever requested).

To achieve interoperability between existing heterogeneous databases (component databases, CDBS) a database federation (federated database system, FDBS) may be built. In comparison to the centralized approach a FDBS provides two main advantages: First, it provides users with the capability to retrieve data located at different heterogeneous databases by using a single database interface and second it provides companies a means to integrate existing data from different sources within a global view. Interoperability is a significant advantage but it also increases the need for protecting the security of CDBSs and their local users dramatically. Most existing mechanisms ensuring security requirements have to provide new functionality when applied to FDBSs. In particular, we see the following requirements:

- *Identification* and *authentication*: The federation might wish to authenticate the local sites to which a connection for global users should be established. In turn, each local site might wish to authenticate the federation site to which it should offer its local data. Additionally, the various CDBSs might wish to identify and authenticate global users at their local sites, respectively. Mechanisms have to be provided to relieve the authentication process for global users in order to prevent them from multiply typing in authentication information (for example, passwords).

- *Authorization* and *access controls*: Security subjects (users, roles, etc.), access types (read, write, method calls, etc.), and security objects (classes, instances, etc.) may be heterogeneous in granularity among the CDBSs constituting a federation. A FDBS has to provide a level of granularity which allows to identify and integrate the various local concepts. Furthermore, authorization techniques as well as the administration of authorizations might differ significantly

in CDBSs. A powerful data model combined with a powerful security model has to be provided by the FDBS in order to specify a global security policy and to overcome the heterogeneity issues mentioned above.

- *Integrity* and *consistency* constraints: The data model of the FDBS has to provide means to specify multi-site integrity and consistency constraints since the data offered by the federation may be scattered over various local sites as well as copied from one site to another site.
- *Auditing*: Security auditing like identification and authentication has to be performed at the federation site as well as at the various local sites. Additional audit records have to be provided if control passes from the global layer of the federation to a particular CDBS at the local layer.

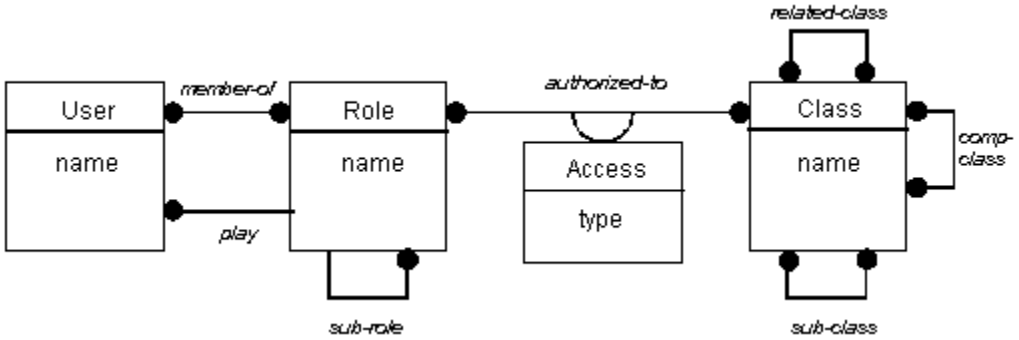

Figure 1: Elements of the FADAC security model (in OMT notation)

Within the ESPRIT III project IRO-DB (*interoperable relational and object-oriented databases*) we designed and implemented a security concept for IRO-DB. The system uses (see Gardarin et al., 1994) a three layered architecture having a *local*, a *communication*, and an *interoperable* layer. An object-oriented data model (ODMG) is used to provide interoperability among relational and object-oriented databases. All CDBSs at the local layer of IRO-DB have to implement a *local database adapter* (LDA) which makes the local system appear as if it was an ODMG compliant database. Local ODMG schemata are exported over the communication layer and imported at the interoperable layer where federated views on the exported data may be defined. In analogy to the extended ODMG data model, a powerful security model has been designed and is used throughout the layers of IRO-DB. The model characterized as *federated, administrative, discretionary access controls* (FADAC, see Eßmayr et al. 1995, 1996a, and 1996b) can be summarized as follows:

- *Discretionary access controls*: Each security object (i.e. a class) is owned by the creator of the object (i.e. a user or a role). The owners have unrestricted access to security objects but are not allowed to grant authorizations to other users because in database federations it seems to be dangerous to leave security administration in the hand of a possibly large number of users distributed over several CDBSs.

- *Administrative*: In IRO-DB delegation of authorizations is centralized to administrative authorities and not decentralized in the hand of distributed users. FADAC uses *role-based access controls* (RBAC, compare Sandhu and Coyne, 1996) requiring users to play different roles in order to access different data. Some of the roles could have administrative rights in order to administrate security. Following the administration paradigm intends to prevent the known problems of cascading and cyclic authorizations and addresses the need to administer security issues properly in a federation of many CDBSs. Combining the administration paradigm with discretionary access controls tries to preserve flexibility and prevents the case that security subjects initially have no access to security objects they just have created.

- *Federated*: Mapping between local and global security concepts is provided in a way that each LDA makes its local security information appear as if it was FADAC compliant. The local security information is exported over the communication layer and imported at the interoperable layer where global security subjects may be defined as mappings to various local subjects and

global authorization rules may be specified. In order to enforce elaborated security policies FADAC provides powerful access control concepts at the interoperable layer including positive, negative, as well as implied authorizations with the aim to ensure consistency between global and local authorization states.

FADAC consists of several elements which can be illustrated together with their relationships as shown in Figure 1.

Roles are regarded as obligations and duties describing what has to be done regardless of who does it. Each role should be *authorized* for exactly those accesses that are needed to fulfill the duties of the job (principle of least privilege). A role hierarchy can be designed using the *sub-role* relationship which may reflect the organizational and functional structure of a company. Users are the existing persons of the system and need to play a role in order to access data. They can choose among several roles they are a *member-of* but may only play one role at a time. This policy prevents authorization conflicts among the roles of a user and it seems to be no limitation to real-life situations as long as users can easily change the role they need to play. The security objects of IRO-DB are classes which may, according to ODMG, be structured with general relationships (*related-class*), within a class hierarchy (*sub-class*) and a class composition hierarchy (*comp-class*). Authorizations may also be granted to higher level security objects (i.e. schema, database or federation) which in fact represent authorizations for sets of classes. A role may be *authorized-to* access a class with either one of the elementary access types, i.e. *read*, *write*, *create* or *delete* (covering relational CDBSs), with executing a *method* (covering object-oriented CDBSs), or, finally, as the *owner* of a class which is the most powerful authorization type and implies all other possible accesses for that class. Content dependent authorizations are realized in making use of the concept of *mappings* at the interoperable layer, which are an IRO-DB extension to ODMG. Mappings are primarily used to integrate different local import schemata into an interoperable schema. Since a mapping is a class which determines its instances by executing a query, it can be used to provide view-based protection allowing for any predicate that can be expressed within a query. Furthermore, method authorizations can be used to realize specific kinds of predicates, if needed. Global subjects (users and roles) also have to be mapped to corresponding local subjects, one for each CDBSs, in order to be able to access local data. A global request must then suffice the global security policy, checked for the global subject at the interoperable layer, and must *not* violate any of the local security policies, checked for the corresponding local subjects at the local layer by each of the engaged LDAs. This architecture ensures the security needs of local sites since it enables them to specify the roles and users that should be exported to the federation. Furthermore, it guarantees the security policies of each local site participating in the federation and allows to specify additional restrictions at the federation site to govern unauthorized aggregation and inference of local data.

References

Eßmayr, W., Kastner, F., Pernul, G., Preishuber, S., and Tjoa, A M. (1995) Access Controls for Federated Database Environments. *Proc. Joint IFIP TC 6 and TC 11 Working Conf. on Communications and Multimedia Security*, Graz, Austria.

Eßmayr, W., Kastner, F., Pernul, G., Preishuber, S., and Tjoa, A M. (1996a) Authorization and Access Control in IRO-DB. *Proc. of the IEEE 12th Int. Conf. on Data Engineering*, New-Orleans, Louisiana, USA.

Eßmayr, W., Kastner, F., Pernul, G., Tjoa, A M. (1996b) The Security Architecture of IRO-DB, *Proc. 12th IFIP TC 11 Int. Conf. on Information Security*, Island of Samos, Greece.

Gardarin G., Gannouni S., Finance B., Fankhauser P., Klas W., Pastre D., Legoff R., Ramfos A. (1994) *IRO-DB: A Distributed System Federating Object and Relational Databases*. In: Bukhres O. and Elmargarmid A.K., Object-Oriented Multidatabase Systems, Prentice Hall.

Sandhu, R.S., Coyne, E.J. (1996) Role-Based Access Control Models, *IEEE Computer*, 2/96.