22

The security architecture of IRO-DB *)

W. Eßmayr, F. Kastner
Research Institute for Applied Knowledge Processing
Softwarepark Hagenberg
Hauptstraße 99, A-4232 Hagenberg, Austria
e-mail: {wolfgang, fritz}@faw.uni-linz.ac.at

G. Pernul
Information Systems Department
University of Essen
Altendorfer Straße 97, D-45143 Essen, 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.at

Abstract

This paper describes the security architecture of the IRO-DB database federation, a system supporting interoperable access between relational and object-oriented databases. The security policy developed is a federated, administrative, discretionary access control policy supporting positive, negative, as well as implied authorizations. It includes a procedure for conflict resolution within the set of specified authorization rules, and concentrates on role-based security. Additionally, the integration of heterogeneous, local security policies of database systems joining the federation is discussed.

Keywords

Database security, role-based security, discretionary access controls, interoperability, object-oriented database systems, relational database systems, federated database systems

---

*) This work is supported in part by the European ESPRIT III program under project Nr. 8629.

S. K. Katsikas et al. (eds.), *Information Systems Security*

1 INTRODUCTION

Many organizations maintain information spread over several independent, possibly heterogeneous databases. While the independent databases may have been working sufficiently during the last years, in many organizations the need to integrate existing databases into a database federation, i.e. building a *federated database system* (FDBS), becomes evident. This may be because certain applications require federated views on the information available, covering a more global aspect. Even database federations between different organizations or companies may often be desirable in order to enforce inter-company communication. It is important to note that in FDBSs the participating *component database systems* (CDBSs) must keep their autonomy and as a result, existing local applications are still supported.

In database federations security plays an augmented role. As the need to share information securely and the need to maintain the autonomy of local databases joining a federation often present conflicting requirements, some of the aspects of autonomy have to be sacrificed in order to achieve a powerful federation. However, local database administrators would only offer their local data to the federation, if secrecy and integrity were still warranted. So, the federated security system has to be at least as secure as each of the local systems and on the other hand as transparent as possible to interoperable users.

The work reported in this paper describes the security architecture of IRO-DB (interoperable relational and object-oriented databases), an European ESPRIT-III funded project. Based on the taxonomy of design choices proposed in our previous work Eßmayr et al. (1995) a *federated administrative discretionary access control* (FADAC) policy used in IRO-DB evolved. FADAC is role-based and uses discretionary access controls with a combination of ownership and administration paradigm. It integrates heterogeneous, local security policies and uses implied authorizations to encourage object-oriented and semantic modeling concepts.

The remainder of the paper is organized as follows: Section 2 provides an overview of database federations in general, the IRO-DB federation, security in IRO-DB and discusses related work. Section 3 concentrates on the design choices concerning *granularity* of authorization subjects, objects and types. Section 4 discusses the concepts of *authorization*, section 5 describes *access control* in IRO-DB and section 6 treats the integration of local security policies into the FADAC policy. Finally, section 7 gives some conclusions and outlines ideas for future research work.

2 GENERAL OVERVIEW

2.1 Database Federations, Interoperability

A federated database system (FDBS) consists of a uniform federated layer integrating an arbitrary number of component database systems (CDBSs) while giving the users the illusion of working with a homogeneous, central database system. FDBSs may be characterized as loosely coupled or tightly coupled (Sheth and Larson (1990)). This classification depends on the management of the federation. In a *loosely coupled* federation the user is responsible to create and maintain the federation and no control is enforced by the federated system and its administrator(s), whereas in a *tightly coupled* federation the administrator(s) are responsible

for creating and maintaining the federation and actively control the component databases (CDBSs). Furthermore, FDBSs may be categorized by three orthogonal dimensions, namely, *distribution*, *heterogeneity* and *autonomy* of the CDBSs.

2.2 The IRO-DB Federation

IRO-DB (Gardarin et al. (1994)) is a FDBS providing homogeneous access to several heterogeneous, relational, and object-oriented CDBSs in following a three-layered architecture.

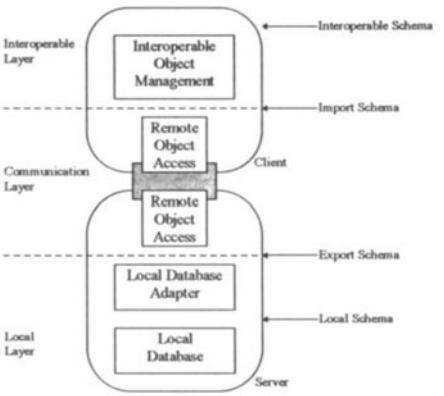

Figure 1 Schemata at the three levels of the IRO-DB architecture.

The *local layer* supports access to heterogeneous component database systems (CDBS) on the basis of a uniform data model (ODMG, compare Atwood et al. 1993). It consists of local database adapters (LDAs) which translate the local database schemata into ODMG compliant schemata. All queries pass these adapters before they are executed at the CDBS. The results of the queries take the same way back to the application on top of the interoperable layer. The *communication layer* provides services for remote database access. These services are mainly for exchange of local schemata with the interoperable layer and for query and result management. The task of the *interoperable layer* is to hide the CDBSs by means of interoperable schemata. The interoperable schemata are used to combine related data from the local databases and overcome inconsistencies in structure, naming, scaling behavior and semantics.

2.3 Security in IRO-DB

One of the most important issues in IRO-DB is security, i.e. the development and implementation of authorization and access control mechanisms in order to protect the information and to restrict user access according to the security policy of an organization.

In general, security models for databases may be discretionary or mandatory. Discretionary access controls (DAC) assume the ownership of information by users or a central authority

and access to information may be granted and revoked from users. Mandatory access controls address a higher degree of security as they additionally control the flow of information between users. They assume data at different classification levels and a level-based security policy. Within IRO-DB we deal with DAC-based protection only.

From the security point of view IRO-DB belongs to the class of tightly coupled federations because IRO-DB assumes the existence of a federation security system administrator who is responsible to administrate security issues and includes authorization and access control mechanisms at the interoperable level in order to control user access.

Distributed data being available from multiple sites cause the problems of inference and aggregation to exacerbate. The FDBS needs to be able to prevent users from obtaining an unauthorized collection of data, that contravenes a more global policy on the aggregation of information, even when the CDBSs are unaware of this global policy.

2.4 Related Work

Although considered as an important topic for general databases (for example, see Pernul 1994) providing security and access control in an interoperable heterogeneous database environment has not been studied frequently in literature so far. Wang and Spooner (1987) were the first who addressed discretionary access control in heterogeneous database management systems. They proposed a solution to the problems of content-dependent access control in a heterogeneous databases by introducing views and present a framework for investigation of further security issues. Jonscher and Dittrich (1993 and 1994) discussed confidentiality for database federations enforced by discretionary access control. They developed the access control policy *ARGOS* (Jonscher and Dittrich (1995)) within the *CHASSIS* project which aims at providing an integration framework to support the secure construction and operation of interoperable information systems. Morgenstern et al. (1992) summarized a panel contribution on security issues for federated database with the viewpoints of several authors. Pernul (1992) discussed integration of heterogeneous access control strategies, in particular discretionary and mandatory protected CDBSs, in a database federation. His work was within the AMAC access control technique.

Related to our work are also some approaches made for access control in homogeneous central database management systems. Fernandez et al. (1994a) developed an authorization model for object-oriented databases. This authorization model contained user access control and administration of authorization and consisted of a set of policies, a structure for authorization rules and algorithms to evaluate access requests against the authorization rules. Fernandez et al. (1994b) dealt with user group structures in object-oriented database systems. They presented a generalized approach to user group structures based on object-oriented concepts. Nyanchama and Osborn (1994) presented access rights administration in role-based security systems. They developed a model for role organization using graph theory. Bertino et al. (1991) presented an authorization model for database systems which support object-oriented concepts as well as semantic data modeling concepts. Special effort was given to the development of deducing implicit authorizations from an explicitly defined authorization.

3 GRANULARITY DESIGN CHOICES

3.1 Authorization Subjects

Authorization subjects are the active entities of a security system which are responsible for changes of a database state and cause information to flow among different authorization objects and subjects. In IRO-DB *users* are the existing persons working with the FDBS which have to play a *role* in order to access the database objects. Roles represent the functional position of users in a company and are organized in a hierarchy which reflects the organizational and functional structure of the company.

3.2 Authorization Objects

Authorization objects are the passive entities of a security system that contain and receive information and represent the asset to be protected. In IRO-DB these are *classes*, *databases*, *schemata* and the *federation*. IRO-DB does not allow for authorizations lower than the class-level since content and attribute dependent authorizations can be realized by the IRO-DB concept of *derived* classes which in fact are views as known in the relational world.

3.3 Authorization Types

An authorization type is the kind of action an authorization subject may execute over an authorization object. Table 1 shows the authorization types with respect to authorization objects in IRO-DB.

Table 1 Authorization types in IRO-DB

	Class	*Database*	*Schema*	*Federation*
read	read the attribute values of the class-instances	read the security information of a database	read the class-definitions of a schema	not applicable
write	write (modify) the attribute values of the class-instances	write (modify) the security information of a database	write (modify) the class-definitions of a schema	not applicable
create	create an instance of a class	create security information of a database	create a class in a schema	create (add) a database or schema to the federation
delete	delete an instance of a class	delete security information in a database	delete a class of a schema	delete (remove) a database or schema from the federation
method -access	access a class-instance with a method	not applicable	not applicable	not applicable
own	own a class	own a database	own a schema	own a federation

4 AUTHORIZATION

Authorization comprises all policies that determine how access is granted to and delegated among particular authorization subjects.

4.1 Closure Assumption

The closure assumption describes the basic attitude of a security system: an *open policy* allows everything unless explicitly forbidden whereas a *closed policy* represents the inverse situation. IRO-DB assumes the closed policy for security reasons since a large database federation has to integrate various CDBSs with many interoperable and local users.

4.2 Kinds of Authorization

Basically, authorizations may either be positive (permissions) or negative (prohibitions). IRO-DB allows for both in order to augment the flexibility of the security system. Negative authorizations allow to exclude authorization subjects from a particular type of access and can be used to stop the sequence of implications within the concept of implied authorization.

4.3 Authorization Paradigm

Authorizations may be granted and delegated either by one central authorization unit (administration paradigm) or decentralized by the owners of authorization objects (ownership paradigm). For IRO-DB we choose a combination of administration and ownership paradigm. Following the administration paradigm intends to prevent the problems of cascading and cyclic authorizations and addresses the need to administer security issues properly in a federation of many CDBSs. Integrating the ownership paradigm tries to preserve flexibility and prevents the case, that authorization subjects have no access to their authorization objects.

4.4 Implied Authorization

Most of the security models imply some sort of automatic authorization, meaning that not every kind of access needs to be explicitly specified or granted. If the number of authorization objects and/or subjects is large, the administrational expenditure may be significantly reduced, especially in the case of a centralized authorization paradigm. Implied authorization can also be used to encourage some object-oriented concepts like inheritance or access to complex objects. In IRO-DB, authorizations are propagated along any of the implication domains, namely, the authorization subject, type, object, and federation domain as can be seen in the following list of implication rules:

1. An authorization for a role r implies authorizations of the same type (positive or negative) for all of the sub-roles of r.
2. An ownership authorization on a particular authorization object implies all other positive types of authorizations applicable on that object (i.e. read, write, create, delete, and method-access in case of classes).
3. A method-authorization specifying the ability to execute a method m of a class C temporarily implies all authorizations necessary for the execution of m.

4. An authorization on a particular authorization object of a certain level of the granularity-hierarchy implies authorizations of the same type (positive or negative) on each of the lower level objects of the granularity-hierarchy.
5. An authorization on a class c implies authorizations of the same type (positive or negative) on each of the sub-classes of c.
6. A positive authorization on a composite (related) class c implies authorizations of the same type on those instances of the component/related classes that are *part-of* (*referenced-in*) c.
7. A negative authorization on a component (related) class c' implies a negative authorization of the same type on the composite (related) class which c' is *part-of* (*referenced-by*).
8. Interoperable roles that are authorized to access a derived class c may only be played by those local users that are authorized to access all of the import classes from which c is derived.

For a comprehensive discussion of the concept of implied authorization in IRO-DB see Eßmayr et al. (1996).

5 ACCESS CONTROL

Access control consists of all actions that are required to check, whether a request issued by a particular authorization subject is allowed or not, and if allowed include all mechanisms that are required to enforce that the authorization subject behaves within his/her authorizations.

5.1 Authorization Rules

Discretionary access controls (DAC) are based on a collection of concepts, including a set of authorization subjects *(S)*, a set of authorization types *(T)*, and a set of authorization objects *(O)*. In general, an authorization rule is a quadruple, (s, t, o, p), where subject s has the authorization of type t to access authorization object o within the range of predicate p.

In IRO-DB authorization rules are defined as triples (s, t, o), where $s \in S$, the set of authorization subjects (i.e. users and roles), $t \in T$, the set of positive or negative authorization types (i.e. ownership, read, write, create, delete, method-authorization) and $o \in O$, the set of authorization objects (i.e. class, database, schema, and federation). A positive authorization (s, t, o) means that subject s is *permitted* to access authorization object o with type t. A negative authorization $(s, \neg t, o)$ means that subject s is *prohibited* to access object o with type t. Note, that ownership can not be negative. An authorization base is a set of authorizations (s, t, o) with t positive or negative; that is, $AB \subseteq S \times T \times O$.

5.2 Predicates

Predicates are used to additionally restrict access to authorization objects dependent on several constraints. An IRO-DB authorization rule does not include a predicate because of the existence of derived classes at the interoperable layer which primarily are used to integrate import classes coming from local schemata. As derived classes determine their instances by executing a query, the security system can use them to provide view-based protection which allows for attribute and content dependent predicates. Furthermore, methods can be used to realize specific predicates, if needed.

5.3 Conflict Resolution

Conflicts occur if two authorization rules determining contradicting authorization types between a subject and an object exist. In IRO-DB the concepts of ownership, positive/negative, and implied authorizations may conflict since other possibilities are explicitly avoided. The conflicts are resolved in following three policies:

1. Ownership takes the highest priority.
2. Negative authorizations override positive authorizations (for security reasons).
3. Explicit authorizations override implicit authorizations (intent of the grantor).

6 THE INTEGRATION OF LOCAL SECURITY POLICIES

In IRO-DB, each *local database adapter* (LDA) on top of a CDBS as well as the IRO-DB system at the interoperable layer maintains a *security & data dictionary* (SDD) containing the descriptions of local respectively interoperable security policies and database objects in an IRO-DB uniform way. The description of database objects correspond to the ODMG standard, security policies are formulated according to the FADAC policy mentioned above.

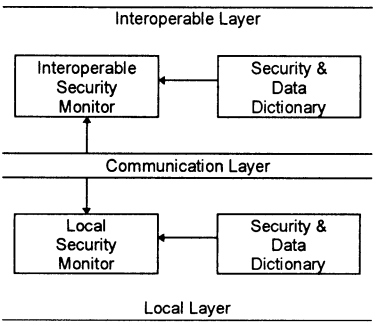

Figure 2 The integration of local security policies.

The information contained in the SDD is used by the IRO-DB security monitors to provide the required security mechanisms (identification, authentication, authorization, access control and auditing). If the *interoperable security monitor* notices a request referencing local database objects the request is delegated via the communication layer to the *local security monitor* of the particular LDA in order to decide locally if it should be allowed or not. As the security information of the local SDDs is not transferred to the interoperable layer because of security reasons, functions are provided at the local as well as at the communication layer for performing local security mechanisms remotely from the interoperable layer.

7 CONCLUSIONS

Database federations are still challenging since problems concerning distribution, heterogeneity and autonomy of component database systems joining a federation have not been fully solved yet. Many efforts have been performed on translating schemata of different data models, overcoming semantic heterogeneities or globalizing transaction management, but the interests in developing federated security systems have been very small so far.

It is important to note that the main motivation behind this work is not to build a secure system for very sensitive environments (i.e. trusted systems) but to include authorization and access control in a general purpose system representing state-of-the-art database technology. We provide a complete taxonomy of design choices made for security in IRO-DB, which is an ESPRIT-III project intending to develop a federated database system and to provide interoperability of relational and object-oriented databases. Additionally, a set of rules necessary for the concept of implied authorization is discussed. An important issue is the integration of heterogeneous component security policies which is addressed in providing a uniform and powerful security policy (FADAC) at each layer of the IRO-DB architecture.
Currently, the theoretical work has been finished and the implementation of the IRO-DB security system is about to start. Future work will concentrate on providing dynamic implication rules for implied authorization. This will mean a significant improvement of interoperability since CDBSs will independently specify the precise effects of the concept of implied authorization.

8 ACKNOWLEDGMENTS

The authors would like to thank all partners of IRO-DB ESPRIT-III, a joint project of GMD-IPSI (Germany), Ibermática (Spain), Intrasoft (Greece), Intellitic, Infosys, O2 (France), GOPAS (Germany), and FAW Linz (Austria), for many interesting discussions on technical meetings.

9 REFERENCES

Atwood, T., Duhl, J., Ferran, G., Loomis, M., and Wade, D. (1993) *The Object Database Standard: ODMG-93, Release 1.1.* Morgan Kaufmann Publishers, San Francisco, California, USA.

Bertino, E., Kim, W., Rabitti, F. and Woelk, D. (1991) A Model of Authorization for Next-Generation Database Systems. *ACM ToDS,* Vol. 16/1.

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. (1996) Authorization and Access Control in IRO-DB. *Proc. of the 12th Int. Conf. on Data Engineering*, New-Orleans, Louisiana, USA.

Fernandez, E.B., Gudes, E. and Song, H. (1994a) A Model for Evaluation and Administration of Security in Object-Oriented Databases. *IEEE Trans. on Knowl. & Data Eng.,* Vol. 6/2.

Fernandez, E.B., Wu, J., and Fernandez, M.H. (1994b) User Group Structures in Object-Oriented Database Authorization. *Proc. IFIP WG 11.3 Database Security*, 1994. In:

Database Security VIII, Status and Prospects (J. Biskup, M. Morgenstern, C. E. Landwehr, Eds). North Holland (Elsevier).

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.

Jonscher, D. and Dittrich, K.R. (1993) Access Control for Database Federations. *DBTA Workshop on Interoperablity of Database Systems and Database Applications*, Fribourg.

Jonscher, D. and Dittrich, K.R. (1994) An Approach for Building Secure Database Federations. *Proc. 20th Int. Conf. on Very Large Databases (VLDB)*, Santiago, Chile.

Jonscher, D. and Dittrich, K.R. (1995) Argos - A Configurable Access Control System for Interoperable Environments.

Morgenstern, M., Lunt, T.F., Thuraisingham, B. and Spooner, D.L. (1992) Security Issues in Federated DBSs: Panel Contributions. *Proc. of the Working Conf. of the IFIP WG 11.3 on Database Security.*

Nyanchama, M., Osborn, S. (1994) Access Rights Administration in Role-Based Security Systems. *Proc. IFIP WG 11.3 Database Security*, 1994. In: Database Security VIII, Status and Prospects (J. Biskup, M. Morgenstern, C. E. Landwehr, Eds). North Holland (Elsevier).

Pernul, G. (1992) Canonical Security Modeling for Federated Databases. *Proc. of IFIP TC2/WG 2.6 Conf. on Semantics of Interoperable Database Systems (DS'5)*, Lorne, Australia.

Pernul, G.(1994) Database Security. In: *Advances in Computers*, Vol.38, pp. 1-72. (M. C. Yovits, ed.). Academic Press.

Sheth, A.P. and Larson, J.A. (1990) Federated Database Systems for Managing Distributed, Heterogeneous, and Autonomous Databases. *ACM Computing Surveys*, Vol.22/3.

Wang, C.Y. and Spooner, D.L. (1987) Access Control in a Heterogeneous Distributed Database Management System. *Proc. Sixth Symp. on Reliability in Distributed Software and Database Systems,* IEEE Computer Society Press.

10 BIOGRAPHIES

A Min Tjoa is full professor at the Technical University of Vienna where he is the director of the Institute of Software Technology. His research interests include information modeling, database security, software reuse, and workflow management.

Günther Pernul is full professor of Information Systems at the University of Essen, Germany. His main research areas are authorization and access controls, database security, and information systems analysis and design.

Wolfgang Eßmayr is assistant of the Research Institute for Applied Knowledge Processing at the University of Linz. His research interests include database security in object-oriented and federated database systems and optical music recognition.

Friedrich Kastner is assistant of the Research Institute for Applied Knowledge Processing at the University of Linz. His main research areas are relational and object-oriented database technology, federated database systems and data modeling.