Mathematical Problems of Cmputer Sience 19, 1998, 98-102.

An Integrated Design and Testing Tool Set for Access Differentiation Systems in Distributed Applications Built on Databases

S. K. Shoukourian, A. M. Vasilyan, A. A. Avagyan, *A. K. Shukurian

Yerevan State University, *Yerevan State Medical University

Abstract

The paper suggests a detailed outline of a design and testing methodology for access differentiation systems (ADS) in distributed applications which use databases. The approach combines different protection mechanisms and tools in DBMS, OS and state of the art for application programming tools (object-oriented environments, system description and verification tools, SQL tools), that are usually used separately, in order to provide a practical integrated approach to the development of protection systems for specific applications with a particular emphasis on automation of design, implementation and verification. The appropriate model as well as tools for its mapping to a DMBS are suggested. Remote users connected via global computer networks are considered too.

1. Introduction

A formalized "top to bottom" design approach was described in [1] for distributed applications built on databases, which were considered as a medium between virtual and real user environments for a specific medical application.

Several initial design steps were adduced briefly. In particular, a choice of a DBMS was derived from real time processing restrictions, parallel execution of queries, users. authorization, description of the different users access to the resources of a database, database integrity, etc.

Due to limitations for the paper size, the step connected with the choice of a DBMS was described in a simplified form. The SQL server was chosen as a DBMS, which supports the requirements above, and the SQL as a corresponding interaction language.

At the same time SQL server does not provide some existing important requirements to user identification and user rights descriptions in such systems.

Merging different components within a unified distributed application posits new essential problems for software. Particularly protection tools, which are sufficient separately, become deficient during the integration due to specific additional links and relationships not considered formerly. E.g., it is impossible to protect a shared object in the virtual operating room using only DBMS protection tools, if the object is stored as a record in DB tables. The solution of the problem should be found only within the more general application framework. Appropriate tools are absent or unavailable.

The present paper suggests a detailed outline of a design and testing toolset for access differentiation systems (ADS) in distributed applications which use databases. The approach combines different protection mechanisms and tools in DBMS, OS and state of the art for application programming tools (object-oriented ¯environments, system description and verification tools, SQL tools), that are usually used separately, in order to provide a practical integrated approach to the development of protection systems for specific applications with a particular emphasis on automation of design, implementation and verification. The appropriate model as well as tools for its mapping to a DMBS are suggested. Remote users connected via global computer networks are considered too.

An application example of the suggested technique for a two-level client-server architecture is adduced. The server is implemented using the DBMS MS SQL Server 6.5 and tools for a local use by a client as well as for a connection to remote users through Internet are implemented using MS Visual Basic 5.0 environment.

2. A unified approach for ADS design and testing

An approach (**Figure 1**), suggested in the paper, is to be applied after first steps of the formalized design, including design of an object-oriented model of the system [2] is and a preliminary rough distribution of the system functions between a client and a server [1].

The approach allows apply the unified design technique of ADS to various classes of objects within the system. The matter of the technique is a combination of miscellaneous mechanisms and tools for access differentiation, which are usually used separately, within the framework of a unified shell.

It is supposed that as a result of previous steps a specification of an ADS, including a tabular description of objects and appropriate limitations for these objects, is already obtained (formulated). The first design stage of the protection system is to define basic data structures and basic algorithms for access differentiation, defined on these structures. Simultaneously a design of appropriate structures and algorithms for the ADS testing has to be carried out. This allows test, reveal and remove mismatches for a given set of limitations at each design stage during an ADS design.

At first design and testing of ADS for users within a local network will be considered. This part of the ADS will be named Internal Security System (ISS).

Taking into consideration the limitations considered in [1], it is expedient to choice as a shell of the realization an open environment, supporting client-server architecture, active protection handling, an open interface with databases, including definition of structured and distributed structured objects. The programming environment of MS Visual Basic 5.0 [3,4] satisfies to the listed requirements. Within this environment an outcome of the target ADS synthesis consists of two parts: a component of protection control (CPC) and a component of protection generation (CPG). CPP is implemented as an ActiveX component in MS Visual Basic, and CPG is generated on the server of the source database as a SQL script. The result of actuating this SQL script is creation of a specialized protection database and APIs for procedures, saved on the server.

The synthesis of the above-stated two components is based on the integration of already tested structures and algorithms from appropriate libraries.

The tools of on-line and off-line functional testing of the protection system also are represented as the SQL scripts.

A similar technique will be applied for design and testing of ADS for external users. The appropriate part of the ADS will be named External Security System (ESS).

3. Key objects of protection

The objects of protection are divided into three classes: functional resources, resources of the information field, time resources and workstations. A protection system is specified by the definition of:

- protection functions in general;
- common functions for all classes;
- protection functions for separate classes and objects;

- a set of limitations for the used functions.

For such a specification a synthesis of the system can be done simultaneously for separate classes, only a correlation between a given class and functions common for the all classes has to be considered.

For a given object of protection component parts of its general specification are as follows:

- a list of used classes;
- a way of a user authentication (for example, by a server of the database or by an authentication service of the network operating system);
- an additional support for the list of user operations;
- control of a total number for system users;
- control of a total capacity of disk memory required;
- control of a response time for a query which checks up on authorities built by the protection system.

Design and synthesis of a protection system for time resources and workstations can be reduced to the creation of interfaces to appropriate services of an operating system and, therefore, to the usage of standard or sufficiently known procedures [5], and these classes are not considered further.

An identical processing environment for functional and the information field resources, i.e. the server of the database, determines similar mechanisms of their design and testing. However, if protection of functional resources is set by a multilevel hierarchy of relatively static resources, the resources of the information field are described by a three-level hierarchy, but at the same time they need more dynamic control for access differentiation.

4. Extension of ISS for external users

A direct addition of the external users to the Internal Security System (ISS) described above, by increasing parameters of protection, does not seem expedient due to the following basic restriction.

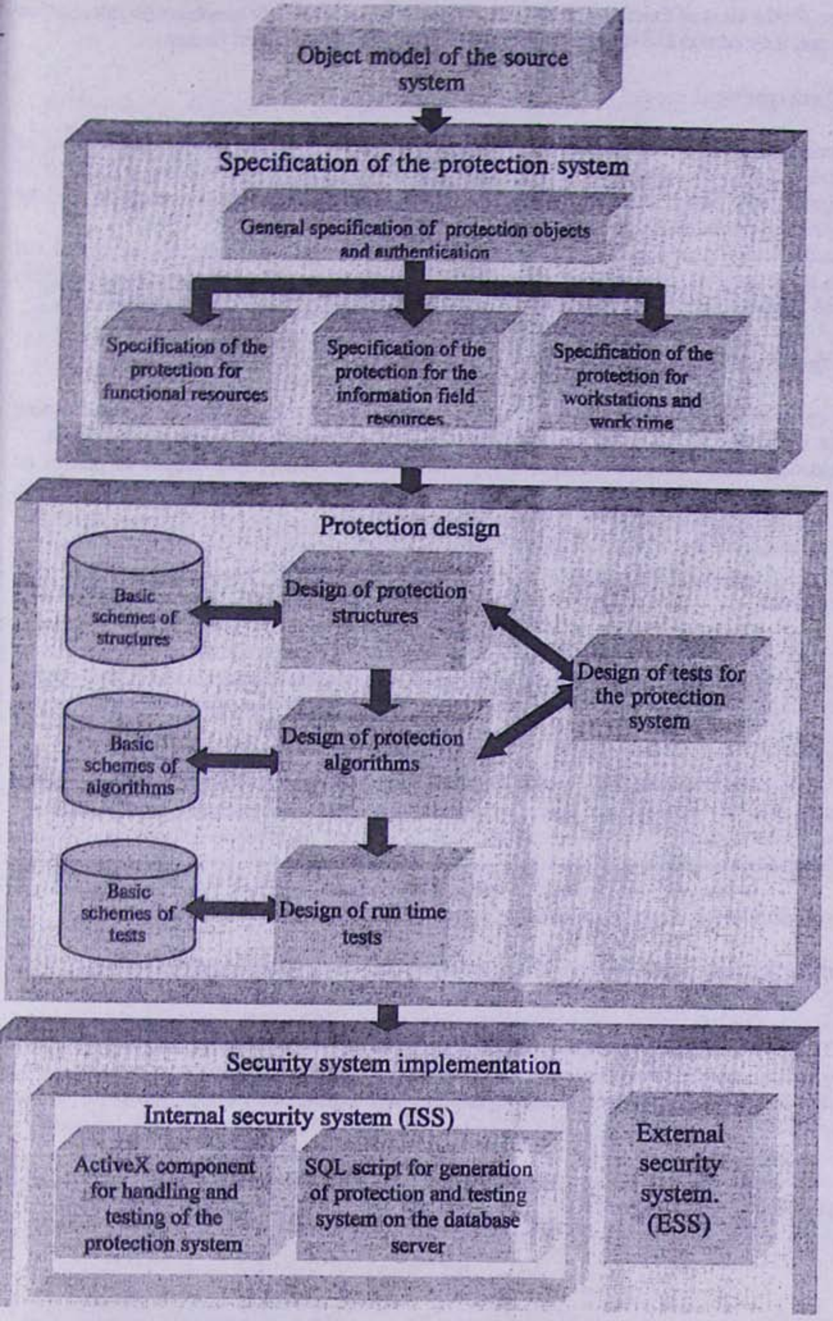
The external connections are performed through existing global computer networks and, in particular, through the highly prevalent Internet network. Difficulties of effective protection methods construction for these networks lead to a significant deterioration of the ISS characteristics and numerous opportunities of the ISS break by the Internet users [6].

Therefore we choose a limited way of access to resources of the system for external users, based on the following rules:

- an external user has access rights only to information, which is exposed in a form of a request for the manipulation from the outside;
- any application to the system is considered only, if it is a response to the previously sent request;
- the exposed information is isolated from the database of local users.
- responses of external users are registered in the appropriate request forms and are brought into the database only as additions, after preliminary testing and checking.

This way of access is realised as a separate subsystem of ADS named External Security System (ESS). It is based on main structural units of request and response schemes or templates.

A specific form is obtained from the appropriate template by performing operations of forms edition considered below. A new template design is also available. A variety of templates and relationships between them define a natural hierarchy. Design and testing of ADS for the mentioned hierarchy of templates could be done similarly to the design and testing of the protection


Object model of the source system
Specification of the protection system
General specification of protection objects and authentication
Specification of the protection for functional resources
Specification of the protection for the information field resources
Specification of the protection for workstations and work time
Protection design
Basic schemes of structures
Design of protection structures
Design of tests for the protection system
Basic schemes of algorithms
Design of protection algorithms
Basic schemes of tests
Design of run time tests
Security system implementation
Internal security system (ISS)
ActiveX component for handling and testing of the protection system
SQL script for generation of protection and testing system on the database server
External security system. (ESS)

system for the class of functional resources, adduced above. Thus only templates for information exchange, their edition and the design of new templates will be examined further.

5. Mathematical model

The constructed model of protection is naturally connected with the appropriate algebra of descriptor chains. The problems of a complete set of equivalent transformations for chains of descriptors, their optimisation on criteria of a chain length and time of interpretation will be considered in our further publications.

The mathematical justification for tests of checking the protection system can be carried out within the framework of a model considered in [6]. An example of online tests design for ESS, derived from results obtained for this model, will be also examined in our further publication.

6. Conclusion

The approach proposed here can serve as the foundation of an integrated design and testing tool set supporting access differentiation design for distributed applications built on databases.

The existing CASE tools for distributed applications design can be redeveloped as part of an integrated design and testing tool for distributed applications-supporting formal definition, implementation, and testing of the ADS for a given application.

Such an integrated tool will reduce the risk and cost of development and maintenance.

References

1. S. K. Shoukourian, A. M. Vasilyan, A. K .Shukurian, Draft on a virtual operating room for prediction of bearing function changes and operative interventions under some pathologies of middle ear, Proceedings of the International Conference on Critical Technologies, Yerevan, 1995.

2. S. K. Shoukourian, A. K. Shukurian, A. A. Avagyan, A. M. Vasilyan, Designing a virtual operating room for prediction of operative interventions under some pathologies of middle ear. A case of the database, Proceedings of 9th World Congress on Medical Informatics, Medinfo '98, Seoul, Korea, August 1998.

3. Visual Basic® 5.0 Programmer's Guide. Microsoft® Press 1997.

4. William R. Vaughn, Hitchhiker's Guide to Visual Basic® & SQL Server™, Microsoft® Press 1997.

5. P. Dusserre, F.-A. Allaert, L .Dusserre, Basic rules for the security of frosen section diagnosis through image transmission between anatomo-pathologists, Proceedings of Medical Informatics Europe' 97 MIE'97, "Studies in Health technology and Informatics", vol.43, pp. 171-175, IOS Press, 1997.

6. S. K. Shoukourian, A Unified Design Methodology for Off-line and On-line testing, IEEE Design and Test of Computers, April-June, 1998, pp. 73-79.