Proceedings of the International Multiconference on Computer Science and Information Technology pp. 821–826
ISBN 978-83-60810-14-9
ISSN 1896-7094

Access Control Models in Heterogeneous Information Systems: from Conception to Exploitation

Aneta Poniszewska-Maranda
Institute of Computer Science,
Technical University of Lodz, Poland
anetap@ics.p.lodz.pl

***Abstract*—The development of the information systems should answer more and more to the problems of federated data sources and the problems with the heterogeneous distributed information systems. The assurance of data access security realized in the cooperative information systems with loose connection among local data sources is hard to achieve mainly for two reasons: the local data sources are heterogeneous (i.e. data, models, access security models, semantics, etc.) and the local autonomy of systems does not allow to create a global integrated security schema.**

The paper proposes to use one common set of access control concepts to support the access control management in security of heterogeneous information systems. The UML (Unified Modelling Language) concepts can be used to define and implement the most popular access control models, such as DAC, MAC or RBAC. Next, the concepts derived from different models can be joined to use one common approach comprehensible for each administrator of each cooperative information system in the federation.

I. Introduction

THE development of the information systems should answer more and more the problems of federated data sources and the problems with the heterogeneous distributed information systems. It is necessary to solve the problems with structured or semantic conflicts on the level of information stored in the systems, to assure the acknowledgment of security constraints defined for the local information sources and to create the control process on the global level of cooperative information systems. We do not solve all these problems in this paper. We only propose to use one common set of access control concepts to support the access control management in the security of heterogeneous information systems. The UML (Unified Modelling Language) [1], [2] concepts can be used to define and implement the most popular access control models, such as DAC (Discretionary Access Control), MAC (Mandatory Access Control) or RBAC (Role-based Access Control) [3], [4], [5], [6]. Next, the concepts derived from different models can be joined to use in the security management one common approach comprehensible for each administrator of each cooperative information system in the federation.

The assurance of the data access security realized in the federated information systems with loose connection among local data sources is hard to achieve mainly for two reasons: the local data sources are heterogeneous (i.e. data, models, access security models, semantics, etc.) and the local autonomy of systems does not allow to create a global integrated security schema. Each of systems, subsystems or applications of the federated information system can be secured by a different security policy, and one common approach joining the concepts from different policies can help in the process of security policy integration on the global level.

The paper is structured as follows: the first part presents the access control in heterogeneous information systems and the creation process of security scheme. The second part deals with the connection of UML concepts with the concepts derived from three types of access control models, i.e. DAC, MAC and the extended RBAC. The third part describes the creation of user profiles based on presented access control models. Finally, the fourth part presents the common access control approach comprehensible for security administrators of each information system in the federation.

II. Access control in heterogeneous information systems

The security policies of a system generally express the basic choices made by an institution for its own data security. They define the principles on which access is granted or denied. The access control imposes constraints on what a user can do directly, and what the programs executed on behalf of the user are allowed to do. A security access system can be defined by using two parts that cooperate with each other: the security access strategy, which describes all the environments and the specifications of the entire organization on the security level (i.e. organizational and technical aspects), and the access model with:

- a set of concepts to describe objects (data access) and subjects (users),
- a definition of the users' access rights to data,
- an access control policy which describes how users can manipulate data, defines data structure and administers the user' access rights to data.

Two categories of security policies of the information systems can be distinguished: discretionary security policy or

mandatory (non-discretionary) security policy. It is possible to find access control models based on these policies:

- *Discretionary Access Control (DAC)* model [3] manages the users' access to the information based on the user' identification and on the rules defined for every user (subject) and object in the system using the access control matrix. For each subject and object in a system there are authorization rules that define the access modes of the subject on the object.
- *Mandatory Access Control (MAC)* model [3] is based on the classification of subjects and objects in the system. Each subject and each object is attached to a security level, which is composed of a classification level and a category. The classification levels are arranged by their sensibility degree: Top Secret, Secret, Confidential and Unclassified. In this model each subject has his own authorization level that allows him the access to the objects starting from the classification level, which has lower or equal range.
- *Role-Based Access Control model (RBAC)* model [4], [5], [6] requires the identification of roles in a system. The role is properly viewed as a semantic structure around which the access control policy is formulated. The role can represent the competency to do a specific task and it can embody the authority and responsibility of the system users. The permissions are associated with roles and the users are assigned to appropriate roles. The roles are created for various job functions in an organization and the users are assigned to roles based on their responsibilities and qualifications. The user playing a role is allowed to execute all access modes to which the role is authorized. The user can take different roles on different occasions.
- *Extended RBAC (eRBAC)* model [7]—each role realizes a specific task in the enterprise process and it contains many functions that the user can take. For each role it is possible to choose the necessary system functions. Thus, a role can be presented as a set of functions that this role can take and apply. Each function can have one or more permissions, and consequently a function can be defined as a set or a sequence of permissions. If an access to an object is required, then the necessary permissions can be assigned to the function to complete the desired job. Specific access rights are necessary to realize a role or a particular function of this role. These rights determine the possibility to execute an application or to access necessary data, and moreover they correspond with these functions. Thus, the specific permissions have to be defined for each function (Fig. 1).

The objectives of the security policy in cooperative information systems are to respect the local security model of each system (each model specifies the security principles of a local system) and to control the indirect security that comes from global cooperation level: a member of a local system may in another local system access only the equivalent

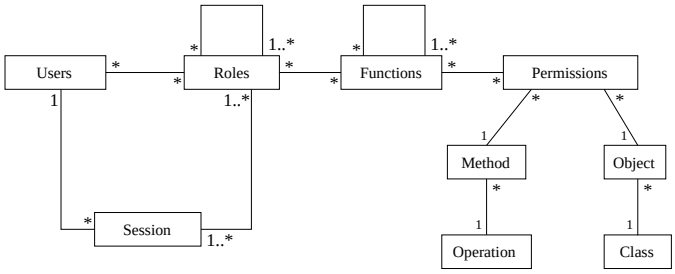

Fig. 1. Extension of the RBAC model

information according to his local profile. It is possible to find the situations in which some information systems have to cooperate with each other creating the set of cooperative information systems. Each system can have another security policy for describing the access control rules to access its data. This situation can involve some difficulties and heterogeneities in definition of the global security model. The following types of global security heterogeneities were found [8]:

- heterogeneity of the information system security strategies (centralized vs. decentralized authorization, ownership vs. administration paradigm, etc.),
- heterogeneity of security policies between MAC models, DAC models, RBAC models and their extensions,
- different kinds of access rights (positive, negative or mixed), different authorization units (subjects, users, group, roles), different access administration concepts (Grant, Revoke, etc.),
- heterogeneity of security entities: elements of security concept model (databases, domain, types/classes/relations or object, etc.) between local schemes.

This paper deals with the second point—the problem of heterogeneity of security policies. Each system in the federation can use another security policy and in consequence another access control model. The possible solution is to find the common concepts in order to connect all security concepts from different models. It should be possible to present different elements from different access control models using one common approach—the ideas that are universal for all the models. This way, the access control in the heterogeneous information systems can be presented using one common set of concepts in order to manage such system in a common and simpler way.

Two types of actors cooperate in the creation stage of an information system and the security scheme associated with it [9]: the information system developer who knows specifications of an information system that need to be realized and the security administrator who has the knowledge of the general security policy that should be respected on the enterprise level.

The creation process of the security scheme in heterogeneous information systems is proposed as follows (Fig. 2):

- Application developer creates the system application or a set of system applications using the UML concepts. UML is used to define the application Model containing all elements that express the needs of the users.

- Application developer initiates the process of user profile creation (e.g. role engineering for eRBAC model) [10], [9] based on the security rules concerning this application.
- The application Model created by the developer is translated to the concepts of access control models (e.g. DAC, MAC or eRBAC) based on the connection of UML concepts with the concepts of DAC/MAC/eRBAC model (Section 3). Also the process of user profile creation is finished on the developer level (Section 4).
- Security administrator receives the Model containing the lists of access control elements which are presented in a special form, e.g. in the XML files. The administrator finishes the process of user profile creation using the rules of the global security policy (Section 4).
- The application Model together with its associated access control rules (defined by the developer and by the administrator) are transformed to the common access control Model using the common concepts for the heterogeneous security systems (Section 5). The results of this transformation are given in the XML files with its associated DTD files which are legible and comprehensible for each security administrator of each information system in the federation.
- Security administrator(s) can manage the federation of the heterogeneous information systems on the access control level using the common set of concepts.

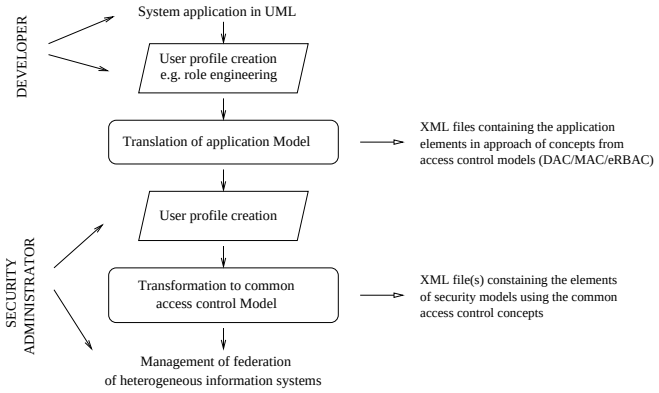

Fig. 2. Creation process of security scheme in heterogeneous systems

The next sections presents the theoretical groundwork for the main stages of this process.

III. Connection of UML concepts with concepts of access control models

The methods of the object-oriented analysis and conception can be considered an evolution of the systemic approach towards greater coherence among the information system objects and their dynamics. The Unified Modelling Language can be mentioned in this category as a standard for the object-oriented modelling in the field of software engineering [1], [2]. It contains a suite of diagrams for requirements, analysis design and implementation phases of the development of systems. Due to the diagrams, it is possible to visualize and manipulate the modelling elements. Out of different types of diagrams defined by the UML and representing different viewpoints of the modelling, three types, i.e. class diagram, use case diagram and interaction diagram, are in the focus of attention of the presented study. The UML has been chosen for the representation of security models because nowadays it is a standard tool, properly reflecting the description of the information system and its needs. UML gives the possibility to present the system using different models. The purpose is to define and implement the access control models, such as DAC, MAC and extended RBAC with the use of UML. To achieve this, the UML concepts and concepts from three models should be joined.

A. Concepts of DAC model associated with UML concepts

The elements of the UML class diagram and interaction diagram, e.g. sequence diagram, can be used to define the concepts of the DAC model (Fig. 3):

- *DAC subject* (user) is found in the instance of actor class from UML class diagram supported eventually by UML constraints,
- *DAC object* defined by UML object,
- *DAC operation* defined by UML operation and furthermore
- user identification can be described by UML constraints.

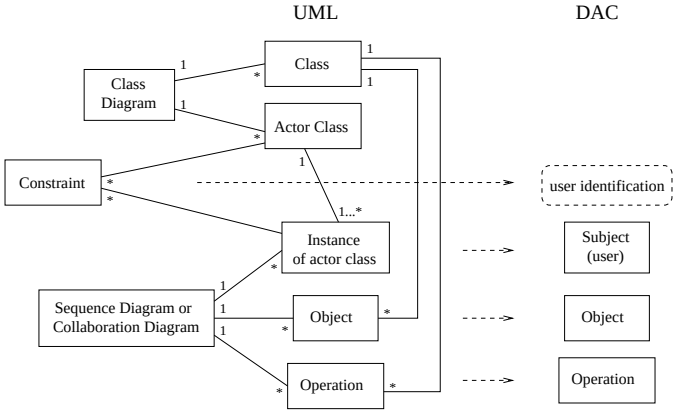

Fig. 3. UML concepts and their relationships with DAC model

B. Concepts of MAC model associated with UML concepts

Similarly, the elements of the UML class diagram and interaction diagram, e.g. sequence diagram, can be used to find the elements of the MAC model (Fig. 4):

- *MAC subject* is defined by the instance of actor class from UML class diagram supported eventually by UML constraints,
- *MAC object* defined by UML object,
- *MAC operation* defined by UML operation and furthermore
- authorization level can be represented by UML stereotypes or element properties,

- security level, i.e. classification level and category, presented by UML element properties or by UML constraints.

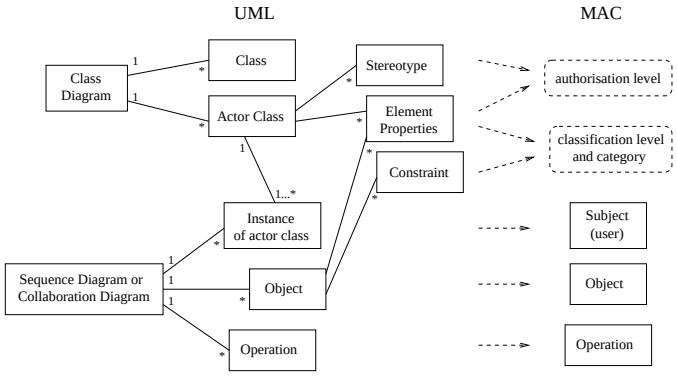

Fig. 4. UML concepts and their relationships with MAC model

C. Concepts of extended RBAC model associated with UML concepts

Two types of the UML diagrams have been chosen to present and implement the elements of the extended RBAC model: use case diagram and sequence diagram (Fig. 5). The presentation of connections between the UML and the extended RBAC concepts is described widely in [7]:

- *RBAC role* is joined with UML actor,
- *RBAC function* joined with UML use case,
- *RBAC methods* and objects with methods and objects of UML,
- *RBAC permissions* can be found in the interaction diagrams,
- *RBAC constraints* are joined with constraint concept existing in UML [10],
- relations of different types that occur between the elements of the extended RBAC model can be found in the use case diagrams and in the interaction diagrams.

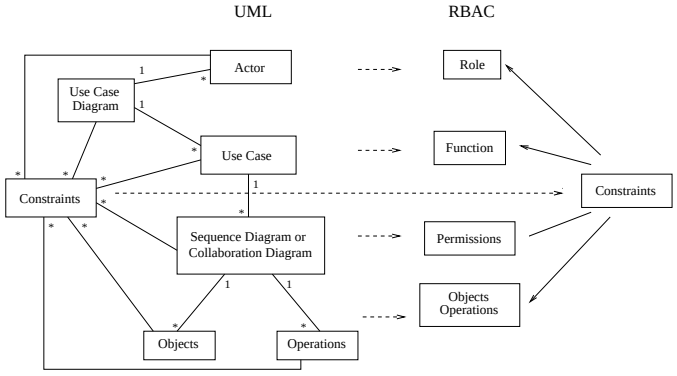

Fig. 5. UML concepts and their relationships with extended RBAC model

IV. Creation of User Profiles Based on Access Control Models

System security policies demand that for each user a set of operations that he will be allowed to execute should be clearly defined. Consequently, for each user a set of permissions should be defined. It suffices to specify the permissions for the execution of certain methods on each object accessible for that user. According to the connections between UML and three access control models given above, a definition of user profiles on the developer and administrator levels can be proposed.

A. DAC model

The authorization rules for the subjects and objects in the DAC model using the UML concepts are defined with the use of class diagram, from which it is possible to obtain the list of system subjects, i.e. system users. The users have the authorizations to realize different operations (i.e. read, write, execute, own) on different objects depending on the definitions of elements situated in the class diagram or in the interaction diagrams in which these subjects participate. These types of UML diagrams allow obtaining the list of objects and the list of operations realized on these objects for each subject in an information system. The user identification is realized by the UML constraints attached to the classes in a class diagram, or to the actors or objects in the interaction diagrams. The notion of ownership policy, characteristic for the DAC model, can be determined with the use of direct or indirect relations between objects in the interaction diagrams or between their classes in the class diagram.

B. MAC model

The implementation of the MAC model using the UML concepts is realized also with the use of the class diagram and the interaction diagrams, which allow to obtain the list of the system users (i.e. system subjects) and the lists of the system objects on which these users can perform different operations. The characteristic notions for the MAC model, such as authorization level and security level (i.e. classification level and category) can be obtained using the UML extension mechanisms, such as stereotypes, element properties or constraints, defined for the model elements in the class diagram or in the interaction diagram.

Both in the DAC model as well as in the MAC model, the definition of the user's authorizations to execute some operations on different objects (i.e. the definition of the user's permissions) with all the model characteristic notions can be realized by the system developer. The security administrator is responsible for any changes in these definitions that can be made by the new assignments of the information system elements or addition of the new constraints defined for the system elements.

C. Extended RBAC model

The implementation of the extended RBAC model using the UML concepts is realized with the use of the sequence diagrams, where permissions are assigned to the rights of execution of the methods realized in each use case [7]. The UML meta-model is applied to define the roles of the RBAC model, the functions that are used by these roles to co-operate with the information system and the permissions needed to

realize these functions. Owing to the use case diagrams a list of actors co-operating with the information system is obtained. An analysis of these diagrams allows the automatic specification of relations of the following types: R-R (role-role) relation (with the use of the generalization relation between the actors), R-F (role-function) relation (with the use of the association relation between the actors and the use cases) and F-F (function-function) relation (the generalization relation between the use cases). The description of a use case using the interaction diagrams (e.g. sequence diagrams) presents activities needed to realize the functions of a system. Each activity is a definition of execution of a method on an object. Therefore the F-P relations can also be automatically managed. Our definition of a set of roles in an information system with the use of the UML diagrams contains two stages: assignment of a set of privileges (permissions) to the use case in order to define the function and assignment of a set of use cases (functions) to the actor in order to define the role.

In order to create a set of roles assigned to a user profile, users should be assigned to roles. This stage is realized by the security administrator.

V. Common concepts for heterogeneous information systems

In an information system the access control is responsible for granting direct access to system objects in accordance with the modes and principles defined by protection policies. An access control system defines: the *subjects* (active entities of a system) that access the *information* (passive entities) executing different *actions*, which respect the access rules. The subjects can describe the *users* or the processes that have access to the data stored in a system. The information, i.e. the data, determines the system *objects* on which the actions represented by the most popular *operations*, i.e. read, write, delete, execute, can be performed. Therefore, it is possible to distinguish three main sets of elements describing the access control rules: **subjects**, **objects** and **operations**.

We propose to represent the elements of access control models, i.e. DAC, MAC and eRBAC, using these three sets and additionally the concept of constraints (Fig. 6). A security constraint is an information assigned to the system elements that specifies the conditions to be satisfied so that the security rules and global coherence of a system can be guaranteed [10].

This connection is possible with regards to the features of access control concepts [3] and the concepts of access control models (Section 2). It can be realized by the automatic transformation of XML files, containing the application elements in approach of concepts of access control models (DAC/MAC/eRBAC), to the XML file(s) containing these elements using the common concepts. It is necessary to create the DTD (Data Type Definition) files for these XML files to define their structures. The root elements of DTD files for each access control model are given as follows:

- DTD file for DAC model:
  $< !ELEMENT\ DAC(user+, object+, operation+, userIdentification*) >$

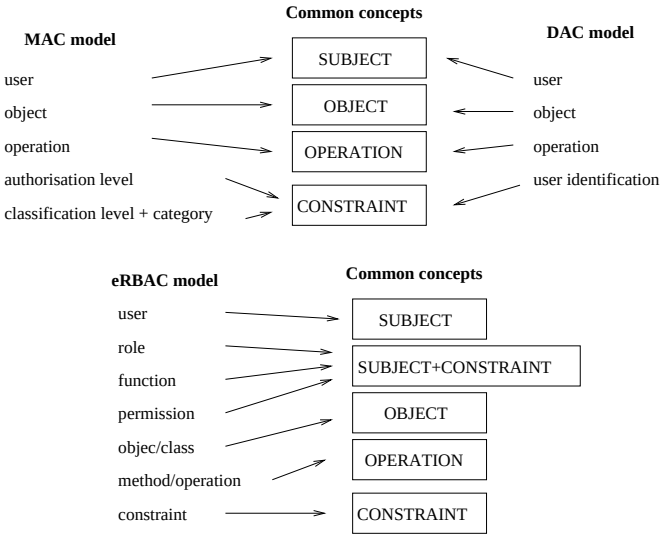

Fig. 6. Common concepts for access control models

- DTD file for MAC model:
  $< !ELEMENT\ MAC(user+, object+, operation+, authorizationLevel*, classificationLevel*, category*) >$
- DTD file for eRBAC model:
  $< !ELEMENT\ eRBAC(user+, role+, function+, permission+, method+, object+, operation+, class+, constraint*) >$

The root element of DTD file containing the common concepts for describing the security elements of each access control model is as follows:

$< !ELEMENT\ commonModel(subject+, object+, operation+, constraint*) >$

It describes the common concepts of heterogeneous security systems. The XML files based on such DTD file are intended for security administrator(s) to manage the federation of heterogeneous security systems.

VI. Conclusions

The paper describes the creation and management of security scheme in heterogeneous information systems on the access control level. We propose to use one common set of access control concepts to support the access control management in heterogeneous security systems.

The UML concepts are proposed to support the access control management in the information system security. UML can be used to realize the access control models as DAC, MAC or the extension of the classic RBAC model and next to help in the creation of user profiles based on these access control models. UML, a standard language for object analysis and design nowadays, has been chosen in view of the fact that it enables the complex presentation of the information system and different aspects of information system security. The implementation of access control models is realized using the UML concepts connected earlier with the concepts of these models.

The complexity of the information systems generates the need for new more effective techniques and tools. The object approach and modelling using UML gives the possibility to create the security scheme for the heterogeneous information systems that accepts different access control models, such as DAC, MAC or extended RBAC model.

REFERENCES

[1] G. Booch, J. Rumbaugh, and I. Jacobson, "The unified modeling language user guide," *Addison Wesley*, 1998.
[2] O. M. Group, "Omg unified modeling language specification," *Reference Manual*, 2005.
[3] S. Castaro, M. Fugini, G. Martella, and P. Samarati, "Database security," *Addison-Wesley*, 1994.
[4] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996.
[5] R. S. Sandhu and P. Samarati, "Access control: Principles and practice," *IEEE Communication*, vol. 32, no. 9, pp. 40–48, 1994.
[6] D. Ferraiolo, R. S. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed nist role-based access control," *ACM Transactions on Information and Systems Security*, 2001.
[7] A. Poniszewska-Maranda, G. Goncalves, and F. Hemery, "Representation of extended rbac model using uml language," *Proc. of SOFSEM 2005, LNCS 3381, Springer-Verlag*, 2005.
[8] E. Disson, D. Boulanger, and G. Dubois, "A role-based model for access control in database federations," *Information and Communications Security, Proc. of 3th ICICS, China*, 2001.
[9] A. Poniszewska-Maranda, "Access control coherence of information systems based on security constraints," *Proc. of 25th International Conference on Computer Safety, Security and Reliability, LNCS, Springer-Verlag*, 2006.
[10] ——, "Security constraints in access control of information system using uml language," *Proc. of 15th IEEE WETICE, England*, 2006.