A Research on the Authorization Model Based on Organizational Management in E-Gov

Jiangnan Qiu, Jiang Tian and Yanzhang Wang

School of Management, Dalian University of Technology, Dalian 116024, P.R.China
qiu_jn@tom.com tian_jiang@126.com yzwang@dlut.edu.cn

Abstract. Firstly considering the problems in e-government authorization model, we analyze the features of government business process. Then an inner-organization authorization model based on organization is proposed. Then based on the proposed model, an authorization model for inter-organizational business process collaboration is designed. This model can resolve the problem of separating organization and authorization, reduce the difficulty of authorization management to make it more suitable for government management mechanism, and be of great application values.

Keywords: *Authorization model, Organization management, Inter-organizational systems*

1. INTRODUCTION

In the trend of network, informatization, economic globalization, government information system as a basis of national information technology infrastructure, has a direct impact on the country's competitiveness and socio-economic development process. Along with the continuous deepening building of e-government, the government system complexity is growing. As for orienting different service client, government has different application system, such as OA, DSS and Administrative License Procedure System, etc. In the procedure of these systems integration, organization and authorization management has become a crucial problem needed to be resolved.

Modern computer systems become more and more complex, and security management has become increasingly difficult. With the business complexity increasing, organizations need to collaborate with each other to form virtual organizations to share resources. Virtual organization is a combination of heterogeneous and independent organizations. When a new virtual organization establishes its security policy, each participant's identity and roles need to be identified. Therefore, security models like RBAC provided such useful concept in this area.

RBAC (Role-based Access Control) realized the separation of user and access permissions, and has been widely used in the procedure of system construction. But when facing to complex government information system composed of multi-systems, if we still use RBAC model to realize authorization management, there will be some

Please use the following format when citing this chapter:

Qui, J., Tian, J., Wang, Y., 2007, in IFIP International Federation for Information Processing, Volume 254, Research and Practical Issues of Enterprise Information Systems II Volume 1, eds. L. Xu, Tjoa A., Chaudhry S. (Boston: Springer), pp. 415-424.

problems[1]. RBAC model only consider user, role and operation authorization management in a single system, furthermore, from the perspective of management, it did not resolve the problem of authorization problems in complex systems, and emerging a lot of duplicate work. When a user belongs to different roles in multi systems, it requires repetitious assignment. If the responsibility of the user changed, it need to repetitious modify the relationship between user and roles, thus, making heavy permission management work. Additionally, from the perspective of management mechanism, the changing situation of positions is only known by human resource department, in particular, the internal functions of adjustment is generally not informed to outsiders. At this time as a system administrator (generally some staff working in information department) will not be able to make timely adjustment of the corresponding relationships between users and roles, leading to the competence of permission management accuracy, or even the turmoil of the entire system empowering management.

However, the security policy must adapt to the new requirements: according to the environment, not static but dynamic [2]. They must be self-adaptable based on temporary conditions, user location, and prior actions. Organizations participated in virtual organizations must express its own policies. Therefore, appropriate security policies should be able to demonstrate their own rules in a single framework. Classical access control model is not flexible enough to meet this demand for independent context.

To solve these problems above, on the basis of large number of exploration and practice, this paper firstly designed a meta-organization model, and then analyzes the process features of government systems which solved the problems of the separation of organization management and permission assignment in complex government information systems, significantly reduces management complexity overhead. At last, based on this model, we further showed an inner and inter organizational authorization architecture. The proposed authorization model based on organization management is very useful to deal with these new requirements. In this model, access control will not be applied directly to the subject, action and object. Instead, within organization roles execute activities on views. This is used to make static permission assignment, and this model also allows administrators assign more complex and dynamic authorization.

2. GOVERNMENT ORGANIZATION META-MODEL

Organization is an organic system composed of elements according to certain structures and relationships, in order to accomplish certain objectives, and advancing to an orderly state in space, time and functions. Traditional organization models played an important role in the history of organization development, but for their stiff structures, they are not suitable for the requirement of inter-organizational business process integration technology which need to be based on a flexible organization model supporting authority, resources and activity assigning with high efficiency.

Nowadays, the society environment is continuously changing, which requires the organization structures should be more agile and flexible to make information interchanging expedite and active agilely, as well as be adaptable to environment.

This kind of flexible organization is called Flexible Organizations. E-government business integration has a close relationship with organization structures. Organization meta-model is basis for flexible organization modeling and collaboration between distributed organizations. The under using organization models are the instances of meta-model classes which are also the interchanging standards in collaboration models.

According to the analysis above and related works, this paper design an organization meta-model oriented to business processes, as shown in Figure 1. This meta-model constitutes 4 parts: static organization model (SOM), authority and access control model (ACM), process model (PM) and resource model (RM). The SOM is the basis of the entire framework; ACM provides authority and authentication mechanism for task assignment and using resources; PM is responsible for executing tasks and relies on RM to assist it to finish the processes.

Essentially, organization meta-model is the way the organization elements affected and contacted each other. The different property elements are the basis of organization building, and the number and the combination manner affect the complexity and the degree of order. Formally, according to the model in Figure 1, organization meta-model and its related definition in government organization information system are defined as following:

Organization meta-model is defined as a duple having five basic elements: OMM= {Resource, OP, OU, Role, Task}, and there into:

1) Resource includes Human Resource (HR) i.e. personnel and Non-Human Resource (NHR), Resource= {HR, NHR}. Personnel is the subject of organization behaviors, diversified decision making and concrete work are done by them. In other words, organization behaviors are the personnel's actually. Personnel is the crucial element, as well as the most important and active one. Besides, HR has ability property. Non-human resource includes Info Resource and Application Service. Info resource is aggregated with Info Object which serves as digital resources and assists Activity executing; Application service is aggregated with Business Process and serves as encapsulated service package to be registered outside and used by other organizations in collaboration work [3].

2) OP (Organization Position) is a component in static organization model. It is aggregated with personnel according to their ability, and can recur into more complex ones through OP structure. For the state of government organization structure is relatively steady, an authority framework based on positions is built, instead of traditional based on the changeful authority mapping between personnel and roles. Organization meta-model just need to configure the mapping relationship between personnel and position only once, but not need to configure mapping relationship between personnel and all application roles. This method not only resolve the problem in government authority management, but also suitable for government interior management mechanism.

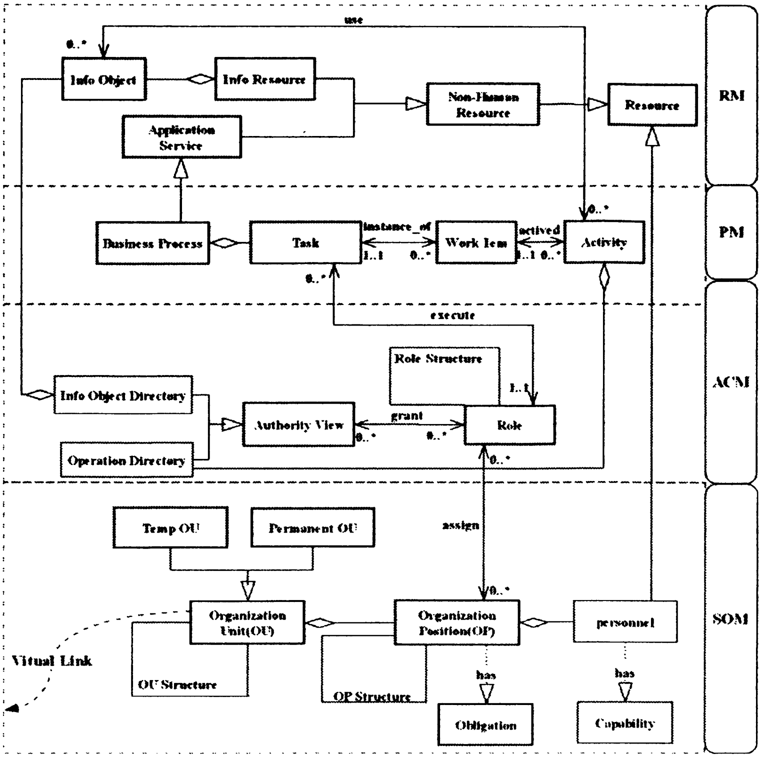

Figure 1. Organization Meta-model [4]

3) OU (Organization Unit) is composed of positions. OU is the parent class of Permanent OU and Temp OU. The former generally indicates the departments with relatively steady functions, and that the latter will be dynamically formed according to the requirement of projects with dynamic, effectiveness and flexibility features. Meanwhile, Temp OU is also an important component when conducting business integration process through Virtual Link.

4) Role is an information system component describing the status and responsibility of personnel in workflow systems, and it is the subject executing business activities. There is an aggregation relationship between roles, and can compose into more complex ones with more authority view which is an abstraction of resources. The authority view includes Info Object Directory composed by Info Object and Operation Directory. Operation Directory stores operation which is lowest activity granularity unit (such as add, delete, update, etc).

5) Task is the basic unit of business process having multi tasks in a certain sequence to achieve defined goals of organizations. Work item is the instance of a task in a defined process. If a work item is executed, it is called activity which is composed of operations.

3. INNER ORGANIZATION AUTHORIZATION MODEL

In government information systems, organization structure is set up based on positions and mapping relationship between positions and roles is relatively steady. Therefore, we set positions as the entire system roles. We construct an integrated role model through mapping between user and position, as well as position and roles in every application systems, instead of original relatively volatile mapping between user and roles.

Before designing the authorization, we would like to explain some related concepts and definition for establishing a good foundation for authorization model in theory. This paper defines the concepts as follows:

1) User: Any person who interacts directly with a computer system.

2) Subject: An active entity, generally in the form of a person, process, or device, that causes information to flow among objects or changes the system states[1]. In our model subject is user.

3) Object: A passive entity that contains or receives information.

4) Access: A specific type of interaction between a subject and an object that results in the flow of information from one to the other.

5) Access control: The process of limiting access to the resources of a system only to authorized programs, processes, or other systems (in a network) [5].

6) Role: A job function within the organization that describes the authority and responsibility conferred on a position assigned to the role. In our model role is actually a set of permissions.

7) System Administrator: The individual who establishes the system security policies, performs the administrative roles, and reviews the system audit trail.

8) Permission: A description of the type of authorized interactions a subject can have with an object .

9) Hierarchy: A partial order relationship established among entities, such as roles, positions, system admin.

According to the analysis above all, an inner organization authorization model (as show in Figure 2) is designed.

This authorization model is designed based on the organization meta-model above, and divided into three parts according to government business system: 1) Business layer; 2) System Management layer; 3) Business Management layer;

As shown in Figure2, business layer is the set of resource, activity and context. System administrator is responsible for abstract entities in concrete layer and assigns permissions to roles. Positions in business management layer do the activities according the permission assigned [6].

Business layer is the basis of entire framework. In our model, the entity Object will mainly cover inactive entities such as data files, emails, printed forms, etc. Seeing that we will also have to structure the objects and to add new objects to the system, we believe that an entity regarding objects is needed: the entity View. That is View is a set of objects having the same properties. And this job is done by system administrator through USE relationship. Entity Activity is the abstraction of actions having the same security policies also done by system administrator through Consider relationship [7]. Context environment impact authorization policies, and is a crucial factors set to be evaluated before permitting a subject access an object in the procedure of authorization using the rules. Context can exam the existing constraints, whether the authorization is validate, and which constraints need to be updated, etc.

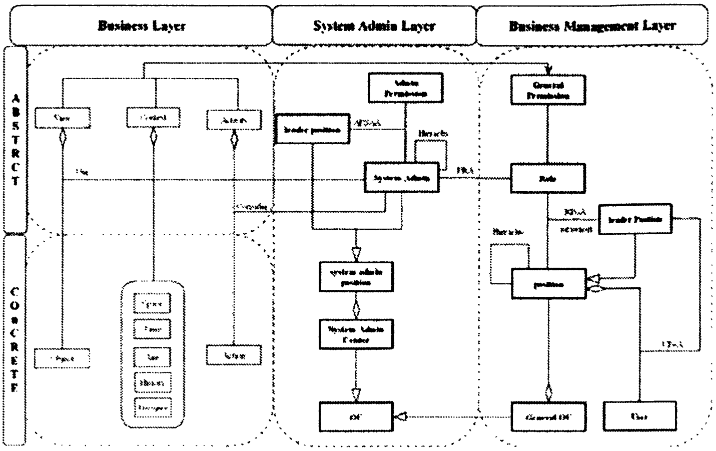

Figure 2. Inner Organization Authorization Model

There are five types of context: The Time context depends on the time at which the subject is requesting for an access to the system, and the Space context depends on the subject location, and the Aim context depends on the subject objective (or purpose), and the Prerequisite context depends on characteristics that join the subject, the action and the object, and the History context depends on previous actions the subject has performed in the system. View, Context and Activity compose the general permission to be assigned to role.

System admin layer include two kinds of positions: system administrators and their leader. Leader position is responsible to set up system administer positions and assign admin permission to them. System administrators assign general permissions to roles which actually are sets of general permission according their given admin permissions.

In general OU, leader position sets up positions according their own business process within OU. Then leader position assigns users to positions and roles to positions. Thus there is a mapping relationship between users and roles which make users get corresponding general permissions.

Through the abstraction of the entities in concrete layer and definition of permission assignment, this model provided a very efficient way to structure organization with authorization, and structured security policies rules which are very suitable for the security requirement in government information systems.

4. INTER-ORGANIZATION AUTHORIZATION MODEL

With the government business complexity growing, the collaboration opportunity between organizations is more and more. Hence, there is need to consider about the security issues across organizations, and construct inter-organizational authorization model.

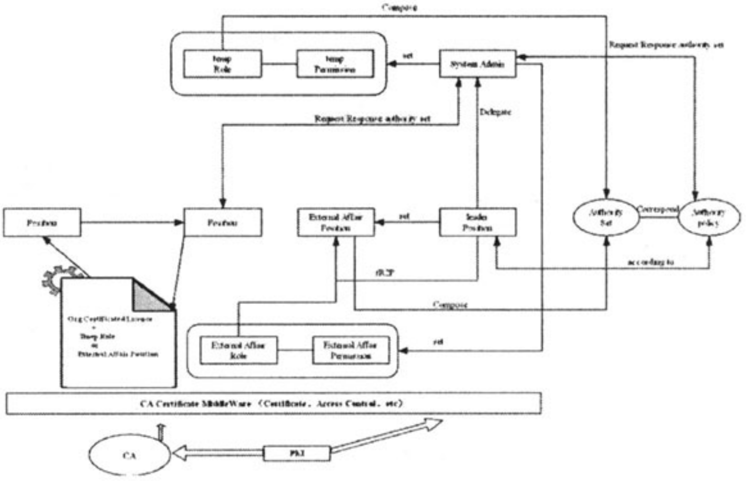

Figure 3. Inter-Organization Authorization Model

From the perspective of management, we designed the inter-organizational authorization model as shown in Figure 3. Leader position in OU B firstly defines the authority policies with its OU and delegate system administrator to set up two entities: external positions or temp roles. External position is a kind of special position which is responsible to deal with external affairs, just like a service window within an organization; Temp roles is a set of temp permissions to be granted to positions from other OU for them to directly participate in OU B's business processes and use resources under the authorized permission . When system administrators receive the delegation request from leader position, they start to assign temp permissions to temp roles and setup external roles according to defined security policies. Then leader position assigns the external affair roles to external positions.

If a position in OU A (called PA) send collaboration request to a position in OU B (called PB), PB firstly identify the PA's identity. If passed, PB transfers this request to system administrator, the latter queries the authority policy database to get corresponding authority set, and then send back to PB with organization certificated license and session time. PB again sends these results to PA. Thus PA can do the collaboration work with temp role or with the staff occupy the external affair positions.

The advantages of this inter-organizational authorization model are as following: 1) It supports the normal collaboration process between government organizations from management perspectives. 2) It realizes the minimal permission principle which means just giving the proper permissions to requesters. 3) Session time guarantee the requester can only hold the permissions in a certain time period, which make prohibit the requesters do illegal actions out of security time.

5. SECURITY PRINCIPLES AND CONSTRAINT

In this paper, the basic idea of authorization model is that the role is a set of permissions; positions can get general permission by mapping them to roles. Through many to many mapping relationship among positions, roles and permissions, we can realize or modify access control polices. This model supports the security principles as following:

1) Minimal permission principle. When assigning permissions to roles, we only give the permissions needed to execute tasks, and only give proper roles to positions. Thus when users are executing the tasks, the permissions they hold will not more than the tasks needed.

2) Responsibility separation principle. To make constraint on conflict roles, there are two ways: One is static separation, in position to role assignment, assign conflict roles to different positions; The other is dynamic separation, that is, decide to activate which roles when positions executing the sessions [8].

3) Entity abstraction principle. When defining permissions, we do not directly define the concrete layer into permissions; instead, from the perspective of application layer, we abstract them [9].

The context we defined in this paper can realize the dynamic constraint mechanism. Dynamic constraint mechanism can make business process be more suitable to actual application rules. Our model can realize the following constraints:

1) Time constraint. Some tasks need to be finished in specified time period, or can only be executed in specified time point.

2) Executing order constraint. The possible executing order can the following sequence: a. Serial order that is the next task must be executed until the former one is finished; b. parallel order that is two tasks can be executed at the same time; c. select order that is only one task can be executed, the other should be cancelled.

3) Delegation constraint. That is a user in a position can define who will do the next step of the tasks by getting the permission from leader positions and system administrator. As shown in Figure 4.

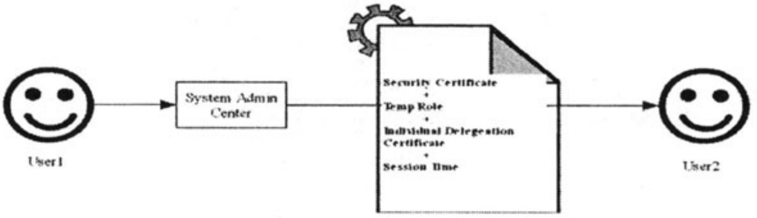

Figure 4. Inter-Organization Authorization Model

6. IMPLEMENTATION STEPS

Suppose that an organization plans to develop an access control system. To this purpose, the security administrator (hereafter denoted by SA) must identify which data have to be protected, how data can be accessed, and who can access those data under which privileges. These activities can be performed in three main steps, described in the following.

1) During the first step, the SA must choose an access control policy. For example, the SA may decide to adopt a discretionary policy because of its flexibility.

2) During the second step, the SA must specify an access control model compliant with the chosen discretionary policy. To this purpose, the SA must specify: a. relevant domain components (for example, groups and/or roles); b. a set of rules specifying how domain components are hierarchically organized (for example, role inheritance hierarchies [10]); c. a set of rules specifying how conditional authorizations are automatically derived by the system, starting from the authorizations explicitly specified; d. a set of rules specifying the integrity constraints the generated authorizations must satisfy. If the chosen model supports both positive and negative authorizations, the SA must also specify a mechanism to deal with conflicts that can possibly arise in the set of entailed authorizations.

3) Once the model has been specified, the SA can start the analysis of the specified model, to identify possible weaknesses and interesting properties. For example, he/she can check whether constraints are well defined, that is, they admit the existence of at least one model instance, or examine the dependencies existing among authorizations. Based on the analysis results, the model can be refined, for example adding or deleting some integrity constraints.

7. CONCLUSIONS

This paper has presented a new security policy model that aims to solve several limits of previous models. This model is centered on the concept Organization. The work we do is as following:

1) We define and clarify the basic government organization meta-model which is the basis of the entire framework.

2) In inner organization authorization model section we define the access control related concepts, abstract entities and give an inner organization authorization model which is very suitable for the actual government need.

3) According to the actual collaboration method, we designed an inter-organizational authorization model for better sharing resources and do collaboration work in virtual organizations.

4) At last, we give the security principles, constraints and implementation steps to give readers a guide to make a new security system.

The work above has made a good foundation of the entire government information system construction. In the future, we will base on them to do research on the business process model of E-Government form a systematic in fracture to give some reference guide for E-Government construction in theory.

REFERENCES

1. E. Bertino, P.A. Bonatti, and E. Ferrari, TBAC: A Temporal Role-Based Access Control for the World Wide Web, in *Proc. of Fifth ACM Workshop on Role-Based Access Control* (Berlin, Germany, July, 2000).
2. R. Viviani, A Type/Domain Security Policy for Internet Transmission Sharing and Archiving of Medical and Biological Data, *International Workshop, Policies for Distributed Systems and Networks (Policy 01)* (Bristol, January, 2001).
3. E. Kohen, R.K. Thomas, W. Winsborough, and D. Shands, Models for Coalition-Based Access Control (CBAC), *Seventh ACM Symposium on Access Control Models and Technologies (SACMAT' 02)* (Monterey, California, June, 2002).
4. Q. Jiang and T. Jiang, A Distributed and Hierarchical Government Organization Model, *Inter-organizational Business Integration. ICICIC2007* (2007).
5. E. Bertino, S. Jajodia, and P. Samarati, Supporting Multiple Access Control Policies in Database Systems, in *Proc. of IEEE Symposium on Security and Privacy* (Oakland, USA, 1996).
6. S. Oh and R. Sandhu, A Model for Role Administration Using Organization Structure, *Seventh ACM Symposium on Access Control Models and Technologies (SACMAT)* (Monterey, California, June 3-4, 2002), pp.155-162.
7. G. Dinolt, L. Benzinger, and M. Yatabe, Combining Components and Policies, *Proc. of the Computer Security Foundations Workshop VII* (Franconia, 1994).
8. G.-J. Ahn and R. Sandhu, Role-Based Authorization Constraints Specification, *ACM Transactions on Information and System Security.* Volume 3, Number 4, (2000).
9. F. Cuppens, L. Cholvy, C. Saurel, and J. Carr`ere, Merging Regulations: analysis of a practical example, *International Journal of Intelligent Systems.* Volume 16, Number 11, (2001).
10. J.B.D. Joshi, E. Bertino, and A. Ghafoor, Temporal Hierarchies and Inheritance Semantics for GTRBAC, *Seventh ACM Symposium on Access Control Models and Technologies* (Monterey, California, June, 2002).