An Access Control Model of Workflow System Integrating RBAC and TBAC

Xiangning Zhou [1] and Zhaolong Wang [2]
1 School of Information and Electronic Engineering
ShanDong Institute of Business and Technology, Yantai 264005, China
E-mail: dulier@tom.com
2 Network Center YanTai University, Yantai 264005, China

Abstract. Basing on the integration of two models, RBAC and TBAC, an access control model called Role-Task Based Access Control (R&TBAC) is given, which takes two parts as combining sites, one is the role and trustee, the other is the role permission assignment and trustee permissions. A set of fundamental conceptions, a series of authorization processes, a formalized description and some modeling tools about this model are given. This model has both intuitionistic and dynamic characteristics. It also has some other advantages, such as economical for memory space, convenient to maintain and control etc.

1 Introduction

Adding some dynamic characteristics for RBAC96 model [1], such as task state [2], recycle time [3], or using TBAC model [4-6] directly can achieve the access control in the workflow system. But in some systems including the workflow technology, some abstracting ways of RBAC are needed to divide and describe some activities connected with access control in the system. At the same time, some descriptive ways of TBAC are also needed to describe the dynamic characteristics in the system.

In order to meet the above needs, a new model called R&TBAC is given, which based on roles and tasks. The descriptive capability and security of the model has also been analysed.

2 The necessity of using RBAC and TBAC integrated

First of all, the station is corresponding to the role in the RBAC. So using the PA matrix in the RBAC to control access is benefited to understand. But in the workflow

system, taking tasks into the PA matrix directly will lead the rows of the matrix increasing sharply. In the mean time, the dynamic permission about authorize/revoke is needed in the RBAC model.

Secondly, the schedule and constraints in the workflow can be well described by the concept "depending" in the TBAC model. For that matter, TBAC is better than RBAC. But during the application of the TBAC model, for the trustee who wants to execute some public processing flow is crowded, the more popular the public process is, the more resource kinds the processing flow needs to access. So if every trustee has the permission of each kind of the resource, the number of records in the permission of the public processing flow will increase sharply. Of course, dividing the public processing flow into some different processing flows can solve this problem, but it needs a great deal of reduplicate codes, which induce the descend of maintainability.

So basing on the experience in real OA system development, a new access control model R&TBAC is proposed, which integrates the RBAC and TBAC and adopts static and dynamic permission altogether.

3 R&TBAC access control model

3.1 Basic definitions

Some definitions about the R&TBAC are as follows:

Definition 1 The basic definitions set in the R&TBAC ={User (U), Role(R), Authorization step (As), Permission (P)}.

Hereinto:

(1) User (U) is the user set, which includes all the users in the system.
(2) Role (R) is the roles set, which includes all the roles abstracted from departments and duties.
(3) Authorization step (As) is authorization step, which means one process in a workflow. It is the minimum process unit that can be controlled in the access control.
(4) Permission (P) includes all the access permissions that can be authorized to users. Resource (res) and operation (op) to this resource can be called access permission.

The definitions derived from the basic definitions are as follows:

Definition 2 The derived definitions set in the R&TBAC ={Trustee (T), Authorization unit (Au), unit Permission (uP), trustee Permission (tP), Session (S)}.

Hereinto:

(1) Trustee (T) includes all roles that have been authorized the authorization step.
(2) Authorization unit (Au) is an authorization step organization, which may include one or many authorization steps logically connected. Au is corresponding to the real tasks. Normally Au has two kinds, one is general Au and the other is atomic Au. In the former, authorization steps will be executed orderly, while in the latter, every As connects with each other closely, which results in the whole failure if one fails.

(3) unit Permission (uP) is a subset of Permission, which includes all access permissions that can be authorized to trustee by As or Au.
(4) trustee Permission (tP) includes all access permissions that have been authorized to trustee by As or Au. tP is a subset belong to uP.
(5) Session (S) includes all sessions. By session, users can be or not be a role.

Based on **definition 1** and **definition 2**, there are some relations and constraints among the definitions.

Definition 3 The relations and constraints set among the definitions in the R&TBAC ={Role Hierarchy (RH), Dependency (D), User Role Assignment (URA), Role Permission Assignment (RPA), Constraint}.

Hereinto:

(1) Role Hierarchy (RH) is partial order relation in the Role(R). It is called role hierarchy relation.
(2) Dependency (D) is the relations between As or Au. It includes sequence dependency, failure dependency, divided permission dependency and agency dependency.
(3) User Role Assignment (URA) assigns relations for users and roles. The relations mean a many to many mapping, from user (U) to role (R), which show the user is assigned to be a role.
(4) Role Permission Assignment (RPA) assigns relations for roles and permissions. The relations mean a many to many mapping, from permission (P) to role (R), which show the role is assigned permission.
(5) Constraint means all criteria on the mapping.

3.2 Authorization processing in R&TBAC model

The authorization can be expressed by five-parameter set (S, O, op, L, As). S means the main body, corresponding to the role in the model. O means object, corresponding to the resource in the model. Op is operation. L is the abbreviation of lifecycle. As is authorization step. The above five-parameter set means the subject (S) has the access permission to operate op on object (O) during the lifecycle (L) activated by As. The detailed processing is as follows:

1. Initialization

Initialize all roles (R) and RH. URA and RPA should be assigned. Initialize all As and Au. The relations between As and As, Au and Au should be assigned. T and uP should be assigned to every As.

2. The dynamic authorization should be finished in the workflow.

A. Using the following way, the trustee's tP can be gotten.
(1) According to URA and T, the role (r) connected to As is confirmed.
(2) According to r and RPA, all r' authorizations can be confirmed. It is called rPA.
(3) The joinset of rPA and uP is the tP.

B. Using the following way, authorize, revoke and period of validity can be gotten.
(1) Before the As is activated, five-parameter set is void and all permissions in tP can not be used.
(2) As soon as the As is activated, the lifecycle (L) of every five-parameter set begin to count down. At the same time, trustee (t) owns his permissions in the tP.

(3) In the life cycle, five-parameter set is available.
(4) When the As stops, five-parameter set is invalid. And all permissions in the tP are revoked.
(5) When As is not activated again, all five-parameter sets that describe tP are all invalid. And all permissions in the As are revoked.

3.3 The formalized description of R&TBAC

The brief model of R&TBAC is shown as **fig.1**. The figure only shows the referred and modified parts. The other parts of model RBAC and model TBAC can be found in references [1,5,6]). The formalized description is as follows:

(1) URA $\subseteq$ U$\times$R;
(2) RPA $\subseteq$ R$\times$P;
(3) RH $\subseteq$ R$\times$R;
(4) Wf is made of a series of Au, the relations between the Au is Au $\times$Au $\subseteq 2^D$ D={sequence dependency, failure dependency, divided permission dependency, agency dependency};
(5) The mapping between Au and T is 1:n; $\boldsymbol{H}$(Au) $\rightarrow r$,$\boldsymbol{H}$ is a function selecting a role (r) from T, hereinto: $r \in$T, T=$\{r_1, r_2, ..., r_n\}$.
(6) The relationship between Au and uP is 1:1. The formula $\boldsymbol{I}$ (Au) $\rightarrow$ uP means $\boldsymbol{I}$ is a function used to initialize uP as soon as Au is initialized.
(7) The relationship between Au and tP is 1:n. The formula $\boldsymbol{F}$ (Au, RPA, r) $\rightarrow$ tP, $r \in$ T, $\boldsymbol{F}$ is a function used to initialize tP. It can get a sub set tP from uP according to RPA and r, hereinto, tP=$\{p_1, p_2 ... p_n\}$.
(8) $\boldsymbol{G}$ (Au, P_1) $\rightarrow$ P_2, $P_1 \subseteq$ tP, P_2 = tP – P_1, $\boldsymbol{G}$ is a function used to revoke the authorization.

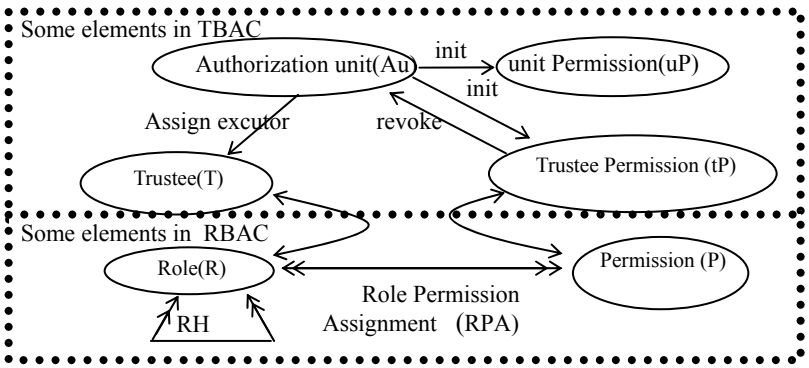

Fig.1. The brief model of R&TBAC

3.4 The descriptive tools of R&TBAC

In the R&TBAC model, the signs in TBAC model are continued to use. The set operators shown in Tab.1 and the authorization matrix shown in Tab.2 are the descriptive tools of R&TBAC.

Table 1. The set operators used in R&TBAC

Sign	Examples	Description
=	Set1={ role1,role2,…}	The set1 includes role1, role2…
	Set1=Set2⋂Set3	The Set1 is endued with the joinset of Set2 and Set3.
∈	User1 ∈{role1,role2,…}	User1 can acts as role1 or role2 …
∪∩⊃⊂⊇⊆		Same meaning to set operations.

Table 2. The authorization matrix used in R&TBAC

Role	Resource	Operation (op)	Lifecycle (L)	Authorization step (As)

The authorization matrix can select one or many columns according to the situation. The wildcard character can be used in the selected columns, such as, in the RPA, only three columns are selected, role, resource, operation, shown in Tab.3

Table 3. The authorization matrix example used by RPA

Role	Resource	Operation (op)	Description
*	A	R	All roles can execute the operation (R) to A.
Role1	B	W	The role1 can execute the operation (W) to B.
Role2	C	*	The role2 can execute all operation to C.

4 The descriptive capability and security analyze of R&TBAC model

R&TBAC model has strong descriptive capability. It inherits the intuitionistic characteristic of RBAC model and the dynamic characteristic of TBAC model. The concept R and uP are encapsulated by As and Au, which makes the concept As and Au accords with the true working better. The united static authorization matrix (RPA) has global restriction and control, while the dynamic authorization matrix uP can change and control according to the needs flexibly. The two matrix have complementary advantages. In practical development, it can save the memory and improve the work efficiency and maintainability.

R&TBAC model fits two famous principles about security. One is the least privilege principle. The combined usage of trustee (T), lifecycle (L), unit permission (uP) and role permission assignment (RPA) makes every trustee (t) only get its sufficient and necessary permission in every As. The other principle is separation of duty. R&TBAC model adopts divided permission dependency and the constraints among roles to control the responsibilities among users and operations, which makes it easy and efficient.

5 Conclusion

Every element in the RBAC and TBAC model has been abstracted and defined in R&TBAC. And the needed relationships in the workflow have been combined in R&TBAC model, which can express the workflow's control mechanism clearly. The R&TBAC model has been used in the OA project of Yantai University. It has been validated that the model has excellent descriptive capability, high security and easy to implement.

References

1. R.S. Sandhu, E.J. Coyne and H.L. Feinstein, et al. Role Based Access Control Models. *IEEE Computer*, 29(2), 38-47(1996),

2. S. Kandala and R. Sandhu,*Secure Role-based workflow Models.* Proc of the 15th IFIP WG 11.3 Working Comference on Database Security. Niagara, Ontario, Canda, Kluwer Academic Publishers(2002).

3. X.M. Wang, Z.T. Zhao and K.G. Hao, "A Weighted Role and Periodic Time Access Control Model of WorkFlow System". *Journal of Software,* 14(11), 1841-1848 (2003).

4. R.K. Thomas and R.S. Sandhu, *Towards a task-based paradigm for flexible and adaptable access control in distributed applications.* Proc of the 1992-1993 CM SIGSAC New security Paradigms Workshops. Little Compton,Rhode Island, US:ACM Press (1993).

5. R.K. Thomas and R.S. Sandhu, *Conceptual Foundations for a Model of Task-based Authorizations*,Proc of the 7th IEEE Computer Security Foundations Workshop. Franconia NH:IEEE Com , 66-79(1994).

6. J.B. Deng and F. Hong, "Task-Based Access Control Model", Journal of Software, 14(01), 0076-0082(2003).