Task-Role Based Dual System Access Control Model

Cui-xiao ZHANG, Ying-xin HU, Guo-bing ZHANG

Computer Department, Shijiazhuang Railway Institute, Shijiazhuang 050043, P.R.China

Summary

Combining role-based access control model and task based access control model, this paper puts forward a new task-role based access control model. Task is core in this model, task associates role and permission. It realizes permission dynamic management. This paper also gives the formal description of this model, and gives application example.

Key words: *Access Control; Task; WorkFlow; TRBAC*

1. Introduction

Along with popularization of computer applications, more and more enterprises sets up own information system. More important information need be transmitted through network. So, how to insure the information not be filched and not be juggled become hot research point of the current computer technique and network safe technique. International Standard Organization ISO defines five level safety services: identity authentication service, access control service, data secrecy service, data integrality service and undeniable service. Access control is an important component. Access Control is to allow or limit the ability and range of main body to access object by some means. By limiting the interview to the key resources, prevent the illegal customer from intruding or resulting in of break because the immodesty of the legal customer operation, thus guaranteeing that the system resources is subjected to control and use legally. The aim of access control is to limit the behavior and operation of system user.

The current research heat of access control is mainly concentrated to Role-Based Access Control (RBAC) and Task-Based Access Control(TBAC). These two methods have the characteristics and limit singly. This paper analyzes the characteristics of these two methods first, then puts forward a new kind of dual system access control mechanism that combines the task and role, and gives application example.

2. Role-Based Access Control & Task-Based Access Control

2.1 Role-Based Access Control (RBAC) Model

The main idea of RBAC is role, the safe manager defines various roles according to the demand, and assign appropriate permission to roles, user is assigned role of its responsibility according to different post. Thus,access control is divided into two parts, that is access permission is associated to role, role is associated to user, realize logical separation of user and access permission. The policy based role brings convenience to permission management.

For example if position of a user changes, We just take off its current role, join new role which stands for its new position. Study show, the variety between role/perimission is more slower than variety between the role/user, and appoint the user to role doesn’t need a lot of techniques, which administration manager can complete, but appoint permission to role is more complicated, need the certain technique, can be undertake by the specialized technical personnel, but don't appoint the permission of the user for them, this is in accordance with the circumstance in the actuality. Except convenient to permission management, Role-based access control can describe the role hierarchy primely, realize the principle of least permission and principle of separation of responsibility.

2.2 Task-Based Access Control model (TBAC)

TBAC resolves the safe problem from the application and the business enterprise position. Task is its core, the access permission control is not static and invariable, it can change along with context of task, it provides dynamic, real-time safe management during task processing.

TBAC model can be expressed by five tuple (S,O,P, L,AS) generally, among them, S means the body, O means object, P means permission, L means the life period, AS means that the authorization step. Because task has time limitation, so in task-based access control model user uses their permission has time limitation too. Therefore, if P is the permission which the AS activate, then L is the survival term of AS. Before AS is activated, its permission can not be used. When AS is triggered, its user starts own its permission, its life expects to start pour to account the hour at the same time.

TBAC access strategy and its internal module relations generally is installed by system manager directly. By dynamic management of authorization step, TBAC supports least privilege policy and least reveal policy. When running task, user just be assigned permission needed, when task is not running or ended, user don’t own assigned permission.

In actual application, we usually need RBAC and TBAC at the same time. For example, position (role)of somebody maybe change, its function(permission) changed too, this is the characteristic of RBAC. But when this person carries out a certain concrete task, the programming and sub-task of the workflow involves carry out the demarcation of the order of task sequence match TBAC.RBAC lack the concept of workflow, just combining TBAC, it can solve the problem of sequence and relationship of sub-tasks during task running.

The TRBAC(Task-Role-Based Access Control) model that puts forward below combine RBAC and TBAC , authorization is divided into the static authorization and the dynamic authorization, the static authorization connects role, the dynamic authorization connects task. It carrys out two organic combine, include both advantages, raised the vivid consumedly.

3 Task Role Based Access Control model (TRBAC)

The main idea of TRBAC is to withdraw the task and role to be two basic characteristics. It appoints task to role, then appoints permission to task. The purpose of connection of permission and task is to realize permission dynamic management , but the purpose of role and task connection is to carry out of related information between task and object. When the permission of role updates, using task as resonance is convenient for role management.

3.1 Basic Concepts

(1) Task: Task is logic unit of workflow. It can have correlation to many users,can include many sub-tasks.

(2) Task instance: Task instance is a dynamic concept.It is the solid example of running task.

(3) Authorization Step: It Means an original authorization processing step, meaning a process procedure to object in work flow.

(4) Dependence: Dependence means correlation between tasks. It includes sequence dependence, failure dependence, agent dependence and so on.The dependence is a dynamic leash. Dependence reflect the principle to take task as the access control center.

(5) Role: Role means the performance some one qualifications of the task, body now a certain right and responsibility.

In a word, the business process of a workflow is made up of some tasks which have dependence to each other, each task is carry out by some roles, only When the dependence between task satisfy, the role of the task then can acquire the homologous permission to carry out the task.

3.2 TRBAC Formal Description

3.2.1 TRBAC Model

Figure 1 describes the component and relationship of component of TRBAC model. In TRBAC model, role is appointed to user, user acquire task to carry out by role, and own its permission when execute task.

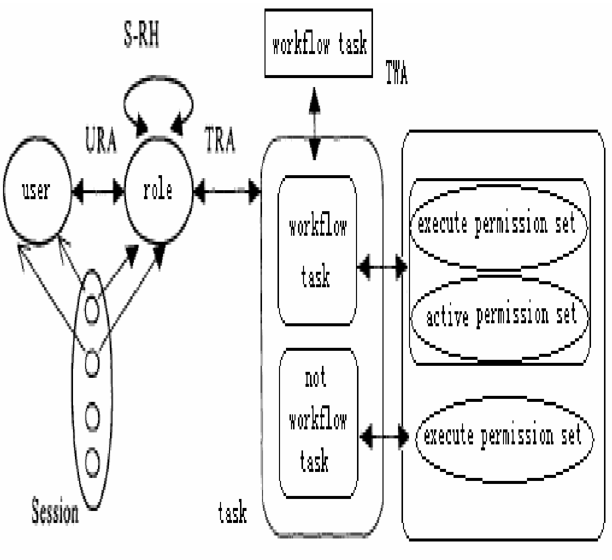

Figure 1 TRBAC model

(Define 1) User(U):The user usually means employee gather.U={u_1,u_2,u_3,…,u_n}.

(Define 2) Role(R):The role is to link user and task, the role is different from employee position in the company organization or responsibilities. R={r_1,r_2,r_3,…r_n}.

(Define 3) Task(T):The task is an indivisible minimum performance unit.

(Define 4) Permission(P):The permission is an abstraction set that has some operations to the some object . The permission of Not WorkFlow(NWF) task is the set of executive permission task need; the permission of WorkFlow(WF) task is set of active permission which trigged by task needed. The active permission set of current task is the executive permission set of next task.P={p_1,p_2,p_3,…p_n}.

(Define 5) Session(S):The Session is mapping of user to role. When user activate role, user set up a session,user can activate multi-roles.A session can map to a user, a Session can map to multi-role.expressed as U:S → U,R:S → 2^R.

(Define 6) a task is made up of three parts,that is beginning condition, performance information and end condition .

(1) Beginning condition: Before the activity start , beginning condition must be checked, only the beginning condition is all satisfied, then that activity can start.

(2 Performance information:It is the core of the activity, explaining the mission to complete by whom, time limit and handle way of timeout.

(3) End condition:After activity start , the system starts to search the end condition of that activity every some minute, to make sure whether it complete or not.

3.2.2 Formal description

(Attribute 1): User-Role Assignment(URA):The URA is duality relationship of U and R. A user can have multi-roles, a role can be assigned to multi-users.The relationship between user and role is many-many. expressed as URA $\subseteq U \times T$.

(Attribute 2): Task-Role Assignment(TRA):The TRA is duality relationship of T and R..A task can be assigned to multi-roles,a role can carry out multi-tasks.The relationship between task and role is many-many. expressed as TRA $\subseteq$ $T \times R$..

(Attribute 3): Permission-Task Assignmeng (PTA):Carrying out the task demands permission, the PTA is duality relationship of P and T. expressed as PTA $\subseteq P \times T$.

Attribute 4:Business Procedure(BP):It Can be seen as running task set.BP={T_1,T_2,T_3,…T_n}

(Attribute 5) Role Hierarchylayer(RH): The RH$\subseteq$ R×R, is an partial ordering relation, expressed as "$\leq$", it means grade relation between roles within organizes.

4. Application example

We will explains the operation appearance of that model with the following order processing flow. Figure 2 is the processing flow of order。

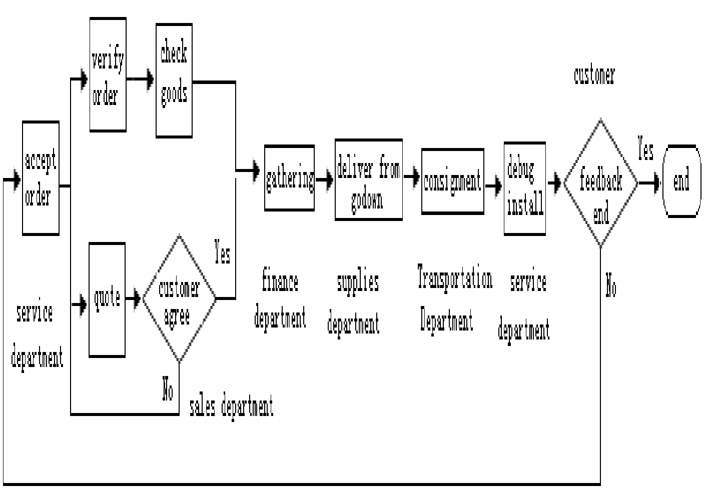

Figure 2 processing flow of order

4.1 The flow element description

U={ user 1, user 2, user 3, user 4, user 5, user 6, user 7, user 8}

R={order member, sales department employee,

Transportation Department employee, service department employee, service department engineer, general manager, area manager, finance department, supplies department}

T={ accept order, verify order, merchandise quote, deliver goods, adjust and install, all information search, area information search , accept the payment, deliver from godown}

P={ write customer's need, fill in the order, countersign the quotation, fill in to deliver the invoice, fill in the work daily record, search all informations, search the area information , fill in to accept the payment list, fill in form of deliver from godown}

4.2 The flow element relationship

URA={(u1,r1),(u2,r2),(u3,r3),(u4,r4),(u5,r5), (u6,r6),(u7,r7),(u8,r8)}

TRA={(t1,r1), (t2,r2), (t3,r2), (t4,r3), (t5,r4), (t6,r5), (t7,r6), (t8,r7), (t9,r8)}

PTA={(p1,t1), (p2,t2), (p3,t3), (p4,t4), (p5,t5), (p6,t6), (p7,t7), (p8,t8), (p9,t9)}

4.3 Application example

4.3.1 The active access control application

The task t1, t2, t3, t4, t5, t8, t9 constitutes the workflow. The processing flow is following:

（1） User 1 served as the order member accept customer's order, write customer's need, the task's processing complete, then activate the next task to fill in the order or quote, that task is completed by user 2, if customer doesn't agree the quote , quote task need be executed repeatedly until customer's satisfied or the work flows the be over.

（2） If the payment exceed the time limit non-arrival, that the work flows to carry out the failure dependence, changing direction that customer workflow be over. If the payment arrive, carrying out the in proper sequence dependence, user 8 is responsible to register information of delivering from godown, then transportation Department user 3 performances deliver the goods task, filling in to deliver the invoice.

（3） Only task of delivering the goods is over, activate the "install" task, engineer's user 4 then can adjust to try to install the merchandise and fill in the work daily record, otherwise engineer's user 4 although have the permission of the performance" install", before task is activated, that permission is invalid.

The characteristics of permission is valid along with the task activate, invalid along with the end of task is suited for each task of the active access control.

4.3.2 The Passive Access Control Application

The information search task is belongs to NWF, practicing the passive access control. Area manager user 6 own the permission of ”area information search”, He can search area information at any time. Same, general manager user 5 can at any time search all information, including the area information.

5. Conclusion

Safe access control is very important for the large and complicated workflow application. This paper introduces a new kind of access control method, that is Task Role-Based Access Control model(TRBAC).The TRBAC can integrate the actual work flow and relation which access control needed together, combine advantage of RBAC and TBAC. It can express control mechanism of complicated workflow clearly.

References:

[1] Deng-shi LI.Access Control Policy in Workflow[J]. Journal JIANGHAN Unversity. 005:(3) 45-48

[2] Ji-bo DENG,Fan HONG.Task-Based Access Control Model[J].Journal of software,2003,14:(1)76-82

[3] Ting-ting LIU,Hui-fen WANG,You-liang ZHAN G. Authorization Support Role-Based Access Control Model and Its Implementation[J],Journal of Computer-Aided Design &Computer Grapgics.2004，16(4):414-419

[4] Ferraiolo D,Sandhu R.Proposed NIST standard for role-based access control[J].ACM Transactions on Information and System Security,2001,4(3):224-274

[5] Han Weili.Role-based constrained access control model and implement supported by constraints among permissions[J].Journal of Compuer-Aided Design & Computer Graphics,2002,14(4):334-338

[6] R Sandhu,E J Conyne,H Lfeinstein,et al.Role-Based Access Control Models[J]. IEEE Computer, 1996,29(2): 38-47

Cui-xiao ZHANG received the M.E. degrees, from Northeast Univ. in 1994. After working as a research assistant (from 1994), an instructor(from 1996),an assistant professor (since 2001) in the Dept. of Computer,Shijiazhuang Railway Institute. Her research interest includes computer network, information system, and their application. She is master tutor since 2004.

Ying-xin HU received the B.E. degrees, from Shijiazhuang Railway Institute in 2001.

Her research interest includes computer network, information system and their application.

Guo-bing ZHANG Received the B.E. degrees, from Northeast Univ. in 1993.In 1993 he begins to woek. Since 2005 He works as senior engineer. His research interest includes computer network and computer maintenance.