A TEMPORARILY-SPATIALLY CONSTRAINED MODEL BASED ON TRBAC IN WORKFLOW SYSTEM

Limin Ao*, Wei Zhou, Xiaodong Zhu
College of Information Engineering, Northeast Dianli University, Jilin, Jilin 132012, China
** Corresponding author, Address: College of Information Engineering, Northeast Dianli University, Jilin, Jilin 132012, China, Tel: +86-432-4807268, Email: aolm@163.com*

Abstract: A temporarily-spatially constrained model based on TRBAC (Task-Role Based Access Control) is proposed in workflow system. Temporary and spatial Constraint is that user is not only constrained by temporality, but also constrained by spatiality when user executes the task. The model suggests that a property of security level should be increased in task. The newly increased property can make the workflow more safety and flexibility.

Keywords: TRBAC, Workflow, Constraint, Security.

1. INTRODUCTION

Workflow is a kind of business flow entirely or partly disposed by computer (WFMC, 1995). The task can only be executed by user who was authorized. For the sake of the task can not be executed by non-authorized users and make task completed favorably, a safer access control model suitable for workflow management system is needed.

Traditional access control model consist of DAC (Discretionary Access Control) and MAC (Mandatory Access Control) (Shen, et al., 2005). DAC and MAC are not suitable for workflow management system. So Ferraiolo and Kuhn proposed the model of RBAC (Role-Based Access Control) in 1992. Then R.Sandhu in University of George Mason described the model of RBAC in 1996(Sandhu, et al., 1996) that is called the model of RBAC96. It has some disadvantages when make it combined with workflow

technologies. The model of TRBAC can deal with the problem effectively. This paper adds space-time constraints on TRBAC and proposed authorized model TSC-TRBAC with space-time constraints. The model indicates that execution of workflow is not only constrained by time, but also by spatial, and increases the property of security for task. Therefore, it can keep synchronization between workflow and authorization.

2. TASK-ROLE BASED ACCESS CONTROL (TRBAC)

Task as an individual conception in TRBAC was proposed (Xing, et al. 2005). A conceptual model of TRBAC is relevant to this paper in Fig.1.

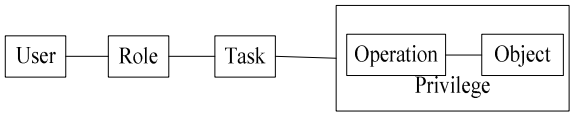

Fig.1: A conceptual model of TRBAC

User will obtain the corresponding privilege through task that executed by himself. Once task has been executed completely, privilege will be disposed automatically. Privilege will be assigned until user will get another task in the next time. It really achieves assignment according to requirement of user and makes the operation of administrator more convenient. To assure task will be completed on time, temporal constraint is needed in the workflow management system. Particular narration about this point in literature (Xing, et al., 2005). Temporal constraint has been recognized by the people who is doing the research in the area of workflow and obtains great success in practical work. To keep the safety of task in the workflow, constraints about physical space to executer of task is proposed in this paper. Although literature [6] (Xu, et al., 2006) put forward the conception of spatial constraints, it only talked about logical space to executer of task. However, the problem also exists in the system relatively.

2.1 Definitions

Definition 1. The binary group (TS; $\leq$) is a region of tense, TS=$\{t\in R|t\geq 0\}$ is a set of time, $\leq$ denotes total order in TS.

Definition 2. $[t_s,t_e]$ denotes a temporal interval, $t_s,t_e\in$ TS, and $t_s < t_e$. The temporal interval is bounded by a lower bound t_s and a upper bound t_e. If

interval $[t_1,t_2]$ in the interval $[t_3,t_4]$, iff $t_3 \leq t_1$ and $t_4 \geq t_2$. If a temporal point t_1 in the interval $[t_3,t_4]$, iff $t_3 \leq t_1 \leq t_4$.

Definition 3. $IP=\{IP_i|i=1,2,\ldots,n\}$ is a set of IP address.

Definition 4. $MAC=\{C_i|i=1,2,\ldots,n\}$ is a set of MAC address.

Definition 5. $WT=\{wt_i|i=1,2,\ldots,n\}$ is a set of workflow task, task is a static conception in workflow. It is a set of operation, defined by user to complete some function.

Definition 6. $TI=\{ti_i|i=1,2,\ldots,m\}$ is a set of task instance. A task instance is an instance of task. It is a pentad group consist of role, privilege, state of task, temporal and spatial constraints.

Definition 7. $M: WI \rightarrow TI$ is a mapping of instance. It makes each task mapped to the corresponding task instance. To the task instance ti_i, if $M(ti_i)=wt_i$, then ti_i is a instance of wt_i.

To essence of model, task can be operated by users from different department. TRBAC can control operation of task-execution in any department through add the property of IP address in it. If we don not use spatial constraints, users would have the privilege of inter-departmental operation. Administrator of task should consider whether the constraints of IP and MAC address are needed according to practical situation.

2.2 Description of basic elements in TRBAC

$U=\{u_i|i=1,2,\ldots,m\}$ states a set of users,

$R=\{r_i|i=1,2,\ldots,n\}$ states a set of role,

$IP=\{IP_i|i=1,2,\ldots,o\}$ states a set of IP address,

$MAC=\{C_i|i=1,2,\ldots,p\}$ states a set of MAC address,

$S=\{$sleep, activity, terminate, hang, abortion$\}$ states the state of task. It is a set include five element,

$WT=\{wt_i|i=1,2,\ldots,j\}$ states task in workflow. Task have upper security should be restricted by physical space,

$OP=\{op_i|i=1,2,\ldots,l\}$ states set of operation,

$OBJ=\{obj_i|i=1,2,\ldots,q\}$ states set of object,

$P=\{P_i|i=1,2,\ldots,x\}$ states set of privilege, and $P_i=(op_i, obj_i, [t_{si},t_{ei}], IP_i, C_i)$. IP_i,C_i are selective option,

$TI=\{ti_i|i=1,2,\ldots,k\}$ states set of task instance, and $ti_i=(r_i, P_i, S, [t_{si},t_{ei}], IP_i, C_i)$.

URA (User Role Assignment) indicates that relationship between user and role, $URA \subseteq U \times R$.

RTA (Role Task Assignment) indicates that relationship between role and task, $RTA \subseteq R \times T$.

TPA (Task Privilege Assignment) indicates that relationship between task and privilege, TPA$\subseteq$T×P.

2.3 Delegation

Delegation is denoted by septenary group in TSC-TRBAC. Like (U, R, T, P, [t_s, t_e], IP, C). IP and C are separated into options and will be option. As an option when security level is higher or otherwise. User u is assigned right of task execution when time in t_s point and revoked in t_e point.

Task T has many states. The state of task can be expressed with a figure of state transition (Song, et al., 2005).

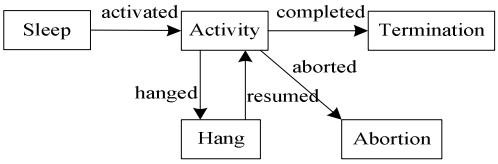

Fig.2: State transition of task

Signification of every state:

(1) Sleep: It states that there is not have task instance in workflow.

(2) Activity: It states that task instance is created.

(3) Termination: It states that task is completed.

(4) Hang: It states that task is suspended by administrator because of certain reason in the process of task execution.

(5) Abortion: It states that task what could not be executed is terminated forcibly by administrator in the process of task execution.

3. APPLICATION OF TSC-TRBAC

There is very important part about managing the people and controlling the resource in workflow management system. To assure the task can be completed successfully in workflow and enhance the security of workflow management system more, it is necessary of restricting the user and object in system. This paper will apply model of TSC-TRBAC to organization modeling tools in workflow.

3.1 Framework of modeling tool

This modeling tool is based on framework of .NET. It adopts traditional three-layer system framework, namely, expression layer, business logic layer

and data layer. The expression layer is regarded as an interface between users and system. This part is carried out by technology of ASP.NET. The business logic layer is a bridge that connects users and database. It is core of system and achieved by language C#. The main function of data layer is to store some relevant model data with database. System adopts Microsoft SQL Server 2000 as a database to store data about organizational model. The framework of system is shown in Fig. 3.

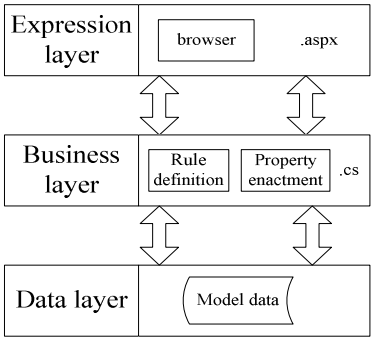

Fig.3: Framework of system

3.2 Elements of model in organization modeling

According to the main idea of TSC-TRBAC, each element has relationship with others in model. Relationship between them is very tight, so it is very important to design a reasonable database. Based on description on elements in model, the table of department, users, role, task (operation), privilege, relation between users and role(play), relation between role and task(hold), relation between task and privilege(authorize) and so on.

3.3 Process model of Petri Net

Organizational model should be applied by process model. The system adopts Petri Net for process modeling. Van der Alast in university of Holland Eindhoven introduced technology of Petri Net in process of workflow modeling. According to extending Petri Net, he proposed workflow net. The essence of modeling with workflow net is a method that applies Petri Net to process definition in workflow.

Definition 8(Petri Net): triple group N=(S, T ; F) is called Directed Net, for short Net. Sufficient and necessary condition is (Yuan 2005):

(1) $S \cap T = \Phi$;

(2) $S \cup T \neq \Phi$;

(3) $F \subseteq S \times T \cup T \times S$ ("×" is Cartesian product);

(4) dom(F)□cod(F)= S□T, and, dom(F)={x| ∃ y : (x,y)□F}, cod(F)={y|∃x : (x,y)□F}, they are domain and range.

Definition 9 (Workflow Net) (Yuan 2005): Directed Net is Sufficient and necessary condition of WF_net:

(1) PN has a source place i□P, and ·i=Φ.

(2) PN has a sink place o□p, and i·=Φ.

(3) Each node x□P□T belong to a path from i to o.

Model of Petri Net has many elements, such as place, transition, arc and token. Place is mapped to condition or state and transition is mapped to task in workflow net. Token denotes a specific operation object in process flow. We can check the required condition about task by selecting relational table between place and transition. If you want to know the next task, it is necessary of selecting relational table between transition and place. Owing to place is mapped to condition in workflow net, so this paper will put constraint condition into relational table called place. To maintain security of system, constraint condition must be checked when task is executed by users.

3.4 Example

If we have a workflow that students submit thesis. The task consists of four parts in workflow, such as thesis-written, thesis-examined, thesis-revised and thesis-submitted. Two tasks of thesis-written and thesis-revised is completed by the role of student and thesis-examined and thesis-submitted is achieved by the role of mentor. The mentors in college of computer can examine thesis written by students in the same college. Mentors in other college have no privilege to do this job. Although we have achieved the least granularity of privilege through adopting TRBAC to access control safely, TRBAC can not control inter-departmental operation by the same role itself. In this example, in another word, mentors in college of management or others also have right to examine thesis written by students in college of computer. It is fall short of practical situation. The measure we have introduced into this paper is that role which executes task should be restricted by spatial constraints, such as IP address or Mac address according to segment of IP address in different departments. This method can dominate inter-departmental operation of role effectively when keep synchronization between delegation flow and workflow.

4. CONCLUSION

The thought of model is that users who have the same role can carry out inter-departmental operation. It improves fatalness of system in the process of task execution in this way. This paper has an idea to deal with the above problem. Through executer of task implementing the physical space constraints to control inter-departmental operation of role and better guarantee security for the implementation of the tasks.

ACKNOWLEDGEMENTS

This work was supported by Doctoral Startup Foundation of Northeast Dianli University (BSJXM-200601).

REFERENCES

WFMC. The Workflow Reference Model, Doc. No. TC00-1003.http://www.wfmc.org/

Hai-bo SHEN,Fan HONG. Survey of Research on Access Control Model[J]. Application Research of computers,2005,6:9-11(in Chinese).

Ravi S.Sandhu,Edward J.Coyne,Hal L Feinstein,Charles E.Youmar. Role-Based Access Control Models[J]. IEEE Computer. 1996,29(2):38.

Guang-lin XING,Fan HONG. A Workflow Access Control Model Based on Role and Task[J]. Engineering and Application of computers,2005(2):210-213(in Chinese).

Guang-lin XING,Fan HONG. Workflow Authorization Model Based on RBAC[J]. System of Microcomputer,2005,26(3):544-547(in Chinese).

Hong-xue XU,Xiu-ying GUO,Yong-xian LIU. Temporarily-Spatially Constrained Workflow Authorization Model Based on RBAC[J]. Transaction of Northeastern University(Edition of Natural Science),2006,27(2):217-220(in Chinese).

Shan-de SONG,Wei LIU. Task-Role-Based Access Control Model[J].Computer Engineering and Science,2005,27(6):4-6(in Chinese).

Chong-yi YUAN. Principle and Application of Petri Net[M].Beijing: Publishing House of Electronics Industry,2005.3(in Chinese).