An Improved Access Control Model for the CSCD Environment

Ai Fei(✉) and Zhang Ping

School of Computer Science & Engineering, South China University of Technology,
Guangzhou, China
{aifei,pzhang}@scut.edu.cn

Abstract. For the Computer Supported Collaborative Design (CSCD) environment's groups, dynamics and distribution characteristics, the paper proposes a Task & Role-Based access control model (T & RBAC) and makes the informal definition of the model. The T & RBAC model is based on the T-RBAC model, and extends the definition of the Users, Roles, Tasks, Permissions and the other factors. In the T&RBAC model, Roles are classified into two classes: job position and business role. As a passive role, permissions are preasigned to the job function Role. By the other way, the business role is assigned to the task in the business process, and the permissions are actived by the context of the task's excuted status, so that the paper realizes the active and passive access control. Finally, we applied the T&RBAC model in the CSCD system and validated the model.

Keywords: CSCD · Access control · T-RBAC · Task · Role

1 Introduction

The Computer Supported Collaborative Design (CSCD) is based on the computer technology, multimedia technology and network communication technology, it supports the members of team to work together in order to accomplish a mutual design project in a shared environment by the interactive consultations, division of the works and the mutual collaboration [1] [2]. In the collaborative environment, the members of the team share the design resources through internal and external networks, but the shared resources are all the business securities of the enterprise. How to ensure these resources' availability, accuracy, and how to avoid hacking have been the critical problems in collaborative work environment [3] [4].

From the system's point of view, the CSCD system is passive and provides the functional HCI. But by the perspective of the collaboration work, the collaborative design is the business process and is active. The collaborative environment changes in the context of the design tasks' executed. The purpose of this paper is to propose a proper model of the access control for the CSCD's environment. The improved access control model named the Task and Role-based access control model (T & RBAC) is founded on the two core concepts of the Task and the Role, which reflect the characteristics of CSCD environment.

V.C.M. Leung et al. (Eds.): TridentCom 2014, LNICST 137, pp. 472–479, 2014.
DOI: 10.1007/978-3-319-13326-3_46

The remainder of this paper is organized as follows: Section 2 reviews the previous research related to the access control, including the weaknesses of their applications in the CSCD environment. Section 3 describes the work modes in the CSCD environment, and those modes induce the different access modes of the information objects for the user. Section 4 proposes the T&RBAC model and makes formal definitions of the model. Section 5 depicts the T & RBAC model's implement in a CSCD system which supports the collaborative industrial design work among the team members who distribute in the different regions. Section 6 presents the conclusion of this paper.

2 Related Work

International Organization for Standardization (ISO) divided the security service into five levels: authentication, access control, data security, data integrity, and denying. The access control is one of the important security parts. Access control [5] is the means to make a proper access to the protected resources, it's final objective is to ensure the authenticated users to access the authorized resources availably, in order to avoid damaging fault to make the resources to be outflowed.

So far, many traditional access control models have been developed. The main ones include the Discretionary access control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), and Task-Role-based access control (T-RBAC). DAC [6,7] depends on the object's owner, who can not only access the own object but also pass the access rights of the object to the others. DAC is very flexible to the owner, but it is too weak in the access control area, for it cannot guarantee the "need-to-do" and separation of duty(SOD) principles. On the contrary, MAC [8] is too strong. It sets the security levels on the objects and users mandatorily. Only those users whose security level is higher than the object's can access the object.

In the early 1990s, National Institute of Standards and Technology(NIST)[9] proposed a role-based access control model (RBAC). The core concept of the RBAC [10] is Role. From an enterprise perspective, the notion of the role is a job position or an organization, the role collects the access privileges. As shown in fig. 1, the users get the object's access rights through the role.

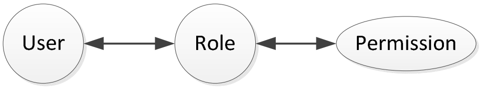

Fig. 1. RBAC Approach. This shows the approach how the user to get the permissions of the object in the RBAC model.

Although RBAC is policy neutral and can perfectly reflect organization of the enterprise environment, but the access control strategy is based on passive access control and cannot fit the active access control. T-RBAC [11] is based on the RBAC. It not only contains the concepts of the RBAC, but also imports an other core concept of the Task. Task is the foundational unit of the business work, the model classifies the task into four classes and deals with each task differently according to it's class. The users obtain the permissions through the role assigned to the task. As shown in fig. 2, the permissions are granted to the task, and the task is some like the sub-role of the role.

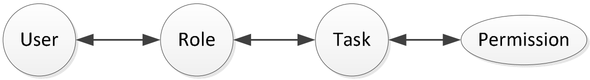

Fig. 2. T-RBAC Approach. This shows the approach how the user to get the permissions of the object in the T-RBAC model.

In conclusion, DAC is very flexible for the object owner, but it is too weak in access control. By the way, it is based on the control list . As the amount of the objects and users increases, the control list size will become larger and be more complicated to be managed; DAC is more used in the Operation System. MAC is too strong. It is based on the security levels attached to the users and objects, and guarantees the confidentiality and integrity of the information. However, it is difficult for "information shared" in the enterprise environment and inconvenient to the business process; RBAC is based on the organizational structure or group of users. The relationships between the role and permission are predefined, and the administrator only allocates the user to the role. RBAC decreases the complexity of the permission management, but it is not suitable for the workflow environment. Le Yang, Xiao Daoju, LI Cheng-kai, [12] [13] [14] have done a lots of works in the RBAC. They applied the RBAC in the CSCW environment by extending the RBAC model. T-RBAC is based on the role and the task. In the session, the user activates the access privileges by his business work. Currently, most of the collaborative work environments adopt T-RBAC model as their access control policy [15][16][17][18].

3 Requirements of Access Control in CSCD Environments

CSCD is one of the concurrent engineering[19] methodology ,it's objectives are better product quality, shorter lead-time, more competitive cost and higher customer satisfaction [20]. With the advancement of the computer and information technology, CSCD has been wildly applied in the product design field. CSCD not only supports the multidisciplinary design teams, but also crosses the boundaries of the area and time zones.

As an engineering process, CSCD is mainly based on the project. As shown in fig. 3, CSCD is structured on the organizations and projects. The users access the information by their business actives and job functions. The one type of the tasks are related to the job position in the organization. In general, such tasks are management actives which are assigned to the users according to their job positions, and they are passive; the others are related to the business role in the project. These tasks compose the business process, and on the IT's view, they are actives of the workflow. In the project, the users are allocated to the tasks by their business role, and such tasks own the special properties, such as task status, start time, end time, mutual relationship (serial, parallel, and feedback), input and output data. As a logical unit of the workflow, the active task can be completed by a person or by more people. Additionally, the task of the workflow is not insulated to each other, but depends on the other task. For example: task B is activated only after the Task A has been finished ; the output data of the task A is the Task B's input data; while the failure of the Task B occurs , the workflow would return back to the task A, etc.

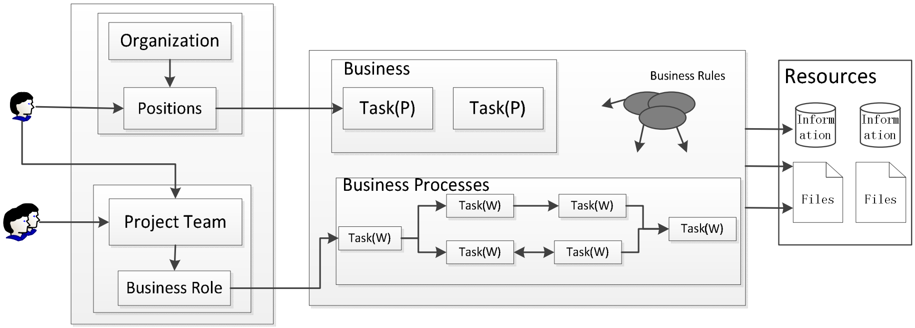

Fig. 3. CSCD's Features. This shows the features that the user gets the resources in the enterprise.

4 T & RBAC Access Control Model

As shown above, the previous works on access control do not fully meet the requirements in the CSCD environment. We presented a proved access control model T&RBAC based on the T-RBAC. T&RBAC contains the concepts of the T-RBAC, but it considers the factors in the CSCD environment more. In T-RBAC, the access rights only are assigned to the task. However in the T&RBAC, the users get the access right through the roles and the assigned tasks. The role is mapped to the job position in the organization, and the task is the active of the product design workflow. Table 1 shows Relationship between factors of CSCD and components of T&RBAC.

Table 1. Relationship between factors of CSCD and components of T&RBAC

The factors in the CSCD environment	The base components in T&RBAC
Information	Object
User, Agent	User
job position, business role	Role
Task	Task
Business process	Workflow

4.1 Formal Description of T & RBAC

Fig. 4 shows the brief overviews of T&RBAC. In the T&RBAC model, the permissions are assigned to the job position roles and the tasks. During a session, the user accesses the HCI of the CSCD system by the role according to his job position. What informations can user access by the HCI is bounded to the task that is allocated to the role of the user.

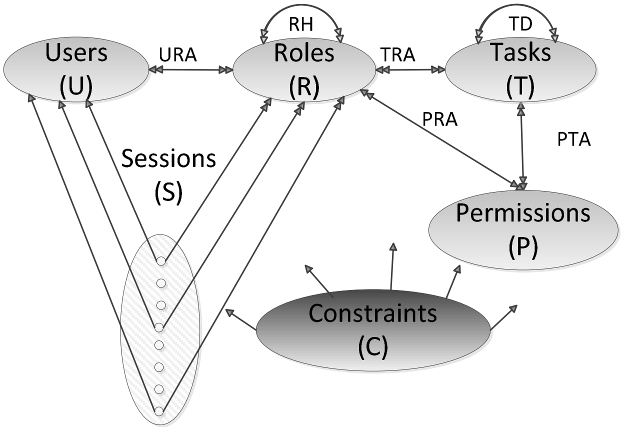

Fig. 4. T & RBAC Model. This shows the components in the T&RBAC model.

The base components in the T&RBAC are defined as follows:

Users (U): Users is a set of users and agents in the CSCD environment.

Roles (R): Roles contain two aspects. One is the position in the organization, and the other one is the business role in the business process.

Tasks (T):Task is an active of the co-design business process , it is atomic and finishes a unit of job.

Sessions (S): A session is the life time while the user is bounded to the active roles and the tasks in the workflow. When the tasks are finished or suspended, or when the user logouts from the CSCD system, the session will end.

Permissions (P): Permissions is an access policy that the authorized subject can interact on the object, including the set of the access objects and the set of operations which affect on the objects;

Constraints (C): Constraints is the abstraction of the business rules in collaborative design process, including role inheritance constraints, permissions conflict constraints, the task dependency constraints, the access scope of the Object, permissions' being activated constraints, etc.

Properties 1 (role inheritance RH). $RH \subseteq 2^R$, means that there is a hierarchy in the roles. We take senior role as the ancestor role and the junior role as the descendant role. Such hierarchy relationship can also be described as a partial order relation (≥).

1) While the ancestor role is active in a session, the permissions assigned to the descendant role are inherited to the ancestor role;

$$P_i, P_j \in P, P_i \in PRA(R_i), P_j \in PRA(R_j), R_i \geq R_j \Longrightarrow \{P_i, P_j\} \subseteq PRA(R_i)$$

2) While the ancestor role's permissions exclude from the permissions of the descendant role, the resolution is remaining the prior permissions. For instance, descendant role R_i is not permitted to read the object Ob_j , while the ancestor role R_j can write object Ob_j , then the ancestor role remains the write operation to the Ob_j;

$$P_i, P_j \in P, P_i \in PRA(R_i), P_j \in PRA(R_j), R_i \leq R_j, P_i \leq P_j \Longrightarrow \{P_j\} \subseteq PRA(R_j)$$

Properties 3 (Users-Roles assign URA). $URA \subseteq R \times U$, a many-many relationship between the Users and Roles.

1) While a ancestor role and its descendant role are assigned to a user together, the user activates the permissions assigned to the ancestor role in a session.

$$\mathrm{R_i, R_j \in URA(\,U), R_i \leq R_j \Longrightarrow Activated(R_j)}$$

Properties 4 (Tasks-Roles assign TRA). TRA ⊆ R × T, a many-many relationship between the Tasks and Roles.

1) If R_i excludes from R_j, the two roles could not be assigned to the tasks together. For example, the designer role and the auditor role cannot be assigned to a task .

$$\mathrm{R_i, R_j \in TRA(\,T) \Longrightarrow R_i \notin Excluding(R_j)}$$

Properties 5 (Tasks-Tasks dependence TD). $T \times T \subseteq 2^{TD}$, TD = { serial, parallel, feedback }.

Properties 6 (Roles-Permissions assign PRA). PRA ⊆ P×R, a role has a set of Permissions to execute the job. The mutual-exclusive Permissions cannot be assigned to one role.

Properties 7 (Tasks-Permissions assign PTA). PTA ⊆ P×T, a task has a set of permissions, and the permissions' being activated bases on the task status(TS).

Properties 8(Task Status TS). The task in the business process has executing status, including static, active, executive, suspending, and end status. When the status is static, suspending, or end state, task-related privileges will be revoked. While the task status is active or executive state, the task will activate all permissions assigned to itself till the status changes into other state.

4.2 Access Control Policy

In the section 3, we have described the features of the CSCD environment and the requirements of the access control. From the perspective of the CSCD environment, T & RBAC model supports the active and passive access control policy. Fig. 5 shows the approach of the T&RBAC model, the user accesses the CSCD system to complete the management jobs assigned to his job position in the organization. The permissions are pre-assigned to the role which reflects the structure of the organization, such role is a passive access control policy. On the collaborative design process, the project team members are the executor of the tasks. The task's status decides the user's permissions.

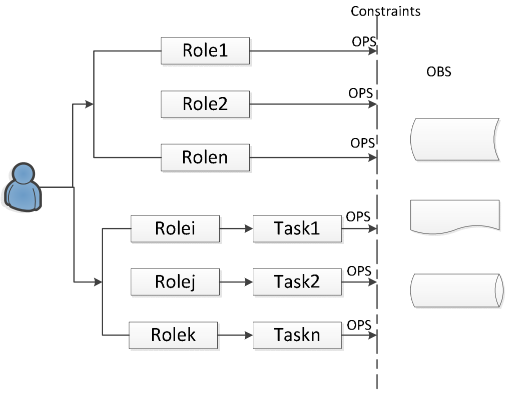

Fig. 5. T & RBAC Approach. This shows the approach that user accesses the object in the T & RBAC model.

5 T & RBAC Model's Implement in CSCD System

In this paper, we applied the T&RBAC model in the industrial product collaborative design platform. The platform supports the collaborative design between the multi-users who come from different departments, companies, or regions. These users compose of the project team. The market department submits the requirements of the new product to the product design department. The product manager makes a development plan of the new product according to the demand. The top leader of the enterprise audits the plan and decides to whether to start the product develop plan or not. Then the product design department appoints a project leader and allocates the mission book to the project leader. the project leader will establish a project team, and the members of the team come from multi-department or even multi-company . Then the leader decomposes the tasks, allocates the resources to the tasks. A new product development project management processes are shown in figure 6.

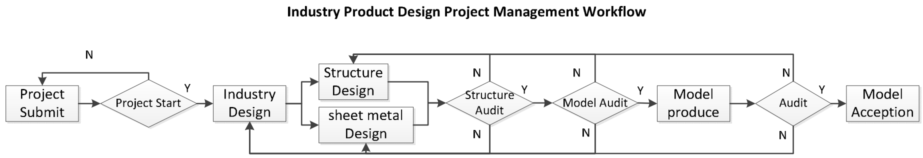

Fig. 6. Industry product design workflow

In the collaborative design process, according to the different types of the tasks, we defined the following roles in our collaborative design platform, such as shown in Table 2. Based on the management jobs in the organization and the tasks in the design process, the roles in the CSCD environment are granted the appropriate permissions to access the resources flexibly and safely.

Table 2. List of roles

Roles	Technical director, design manager, project leader, designer, reviewer, marketer, customer

6 Conclusion

The increasingly complex product development and high expectation of the customers drive the industry to apply new technologies to develop the new products. The CSCD is emerged in the requirement of the industry. This paper analyzes the characteristics of the CSCD environment and the resources access control requirements, and proposes the T&RBAC model based on the T-RBAC model. The main contributions of the T&RBAC are as follows:

1) Classify the Roles of CSCD in two classes: Job position Role and Business Role. Job position Role is a passive role and maps the function of the position in the organization; Business Role is assigned in the task of the design workflow, it is an active role.

2) Define the new attribute of the task which is the dependent relationship between the tasks. By this attribute, the model properly reflects the access control of the information in the business process.

3) Supports the active and passive access control. According to the management job in the organization structure, the permissions are pre-assigned to the roles. In the business process, the permissions can also be assigned to the tasks and be activated by the task status.

Lastly, we developed an industrial product collaborative design platform, and applied the T&RBAC to the platform to effectively control the access of the shared information between the multi-users.

References

1. Haibin, Y., Yun, Z.: Collaborative manufacturing. Tsinghua University Press, Beijing (2004)
2. Shen, W., Hao, Q., Li, W.: Computer Supported Collaborative Design: Retrospective and perspective. Computers in Industry **59**(9), 855–862 (2008)
3. Patel, A.: Security management for OSI networks. Computer Communications **17**(7), 544–553 (1994)
4. Stergiou, T., Leeson, M.S., Green, R.J.: An alternative architectural framework to the OSI security model. Computers and Security **23**(23), 137–153 (2004)
5. Defense, AD0.TnlstedComPuterSystemEvaluationCriteria (August 15, 1983)
6. Pfleger, C.P.: Security in Computing, 2nd edn. Prentice-Hall International Inc., Englewood Cliffs (1997)
7. Joshi, J., Aref, W., Ghafoor, A., Spafford, E.: Security model for web-based applications. Communications ACM **44** (2) (2001)
8. Amoroso, E.G.: Fundamental of Computer Security Technology. PTR, Prentice-Hall, Englewoods Cliffs (1994)
9. Ferraiolo, D.F., Gilbert, D.M., Lynch, N.: An Examination of Federal and Commercial Access Control Policy Needs. In: Proc. NIST-NCSC National Computer Security Conf., Nat'l Inst. Standards and Technology, Gaithersburg, Md., pp. 107–116 (1993)
10. Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role-based access control models. Computer (1996)
11. Sejong, O.: Seog Park. Task-role-based access control model, Information Systems **28**, 533–562 (2003)
12. Yang, L., Choi, Y., Choi, M., Zhao, X.: FWAM: A Flexible Workflow Authorization Model using Extended RBAC
13. Daoju, X., Chao, L., Xiaosu, C.: The Security model of CSCW system based on RBAC. J. Huazhong Univ. of Sci. & Tech. (Nature Science Edition) **32**(5) (May 2004)
14. Cheng-kai, L.I., Yong-zhao, Z.H.A.N., Bing, M.A.O., Li, X.I.E.: A Role-Based Access Control Model for CSCW Systems. Journal of Software **11**(7), 931–937 (2000)
15. Jun, Z., Yong, T.: Study of the Role and Task-based Access Control Technology for CSCW System. Computer Science **37**(7) (2010)
16. Ji-Bo, D., Fan, H.: Task-Based Access Control Model. Journal of Software **14**(1) (2003)
17. Fan, H., Xiaofei, Z.: Task-based access control model and its implemention, Huazhong. J. Univ. of Sci. & Tech. (Nature Science Edition) **30**(1) (January 2002)
18. Quan-bing, C., Hui-jin, W.: An improved access control model based on Task-Role. Journal of Jinan University (Natural Science) **31**(1) (2010)
19. Hartley, J.: Concurrent Engineering, Cambridge. Productivity Press, Mass. (1992)
20. Zongkai, L.: Collaborative design will design and CAD technology-induced changes. Journal of Software, Supplement **9**, 126–130 (1998)
21. Myers, B.A.: A brief history of human-computer interaction technology interactions. **5**(2), 44–54 (1998)