Front. Electr. Electron. Eng. China (2006) 4: 465–469
DOI 10.1007/s11460-006-0089-x

RESEARCH ARTICLE

ZHENG Xiao-lin, LEI Yu, CHEN De-ren

Research of user access control for networked manufacturing system

Abstract An integrated user access control method was proposed to address the issues of security and management in networked manufacturing systems (NMS). Based on the analysis of the security issues in networked manufacturing system, an integrated user access control method composed of role-based access control (RBAC), task-based access control (TBAC), relationship-driven access control (RDAC) and coalition-based access control (CBAC) was proposed, including the hierarchical user relationship model, the reference model and the process model. The elements and their relationships were defined, and the expressions of constraints authorization were given. The extensible access control markup language (XACML) was used to implement this method. This method was used in the networked manufacturing system in the Shaoxing spinning region of China. The results show that the integrated user access control method can reduce the costs of system security maintenance and management.

Keywords NMS, access control, authorization, XACML

1 Introduction

Networked manufacturing is a new manufacturing mode developed to cope with the challenges of economic globalization, and driven also by the development of information technologies [1]. Currently, the modes of networked manufacturing implemented include mainly self construction, IT outsourcing, application service provider (ASP) [2] and so on.

The problems of security in ASP based NMS is mainly about protecting valuable information in the system, and preventing unauthorized users from accessing private information either to seek profit from it or to destroy it. From the point of view of a user, valuable information in the ASP based system mainly includes data in the ASP server, and data transferred within the network. The security problems include privacy, integrity, availability and authenticity [3].

NMS integrates a mass of all-purpose services and special services, and it is open to all internet users. Therefore, it is significant to construct a hierarchical access control model to alleviate the cost of maintenance and management of security. To address the issues of security and management in networked manufacturing system, an integrated user access control method was proposed, in this paper.

2 Overview of access control

Access control is a strategy proposed to permit authorized subjects access to some objects, while blocking the access to the services for non-authorized subjects [4]. From the 1970's, many strategies of access control were proposed. They include autonomous access control, compulsive access control, role-based access control [5, 6], task-based access control [7], organization-based access control [8], coalition-based access control, relationship-driven access control, and so on.

The disadvantages of autonomous access control and compulsive access control are the binding of subject and object, and it is necessary to assign access permission for each pair of subject and object. When the number of subjects and objects arrive at a certain order of magnitude, the authorization task will become very difficult. In the model of role-based access control [5, 6], the administrator may create roles according to the functions or the requirements of the organization, and then assign the roles to users and assign the right to the roles. The key idea of role-based access control is to associate the right with the roles, and realize the authorization of users through role assignment. When the rights are changed, we can flexibly change the user's rights by changing the user's roles; thereby reducing the complexity of the management [4].

All the models of autonomous access control, compulsive

Translated from *Journal of Zhejiang University* (*Engineering Science*), 2005, 39(11): 1735–1739 (in Chinese)

ZHENG Xiao-lin(✉), LEI Yu, CHEN De-ren
College of Computer Science and Technology,
Zhejiang University, Hangzhou 310027, China
E-mail: xlzheng@cs.zju.edu.cn

access control and role-based access control protect the resources systemically. The principle of these access control models can be simply described as: if the subject requires accessing certain objects, and the subject has the permission, then the system will permit its access. We call these access control modes the passive security model. These models do not consider the environment of operation, and it may result in some loopholes in security. TBAC [7] will solve the security problem in the view of application and enterprise. It adopts the task-oriented concept, and constructs the security model and realizes the security mechanism in the view of task. In TBAC, the strategy of access control to object is not static, but changing with the context of the task's execution. We can call the task-based model as active security model.

In addition, there are many other access control models, such as the workflow based access control (WFBAC), CBAC RDAC, organization based access control and so on. These models expand the DAC, MAC, RBAC, and TBAC in specific environment. Wang et al. proposed an e-market access control (EMAC) [8] to satisfy the security requirements of e-market by integrating several access control models in one.

3 Hierarchical user relationship models of NMS

In the ASP based networked manufacturing system, we classify the user into four classes, namely, the free user, private user, enterprise user and virtual organization (enterprise coalition) user. Each kind of user has different rights to access resources in system. Therefore, we can divide resources in the system into different levels, as shown in Fig. 1.

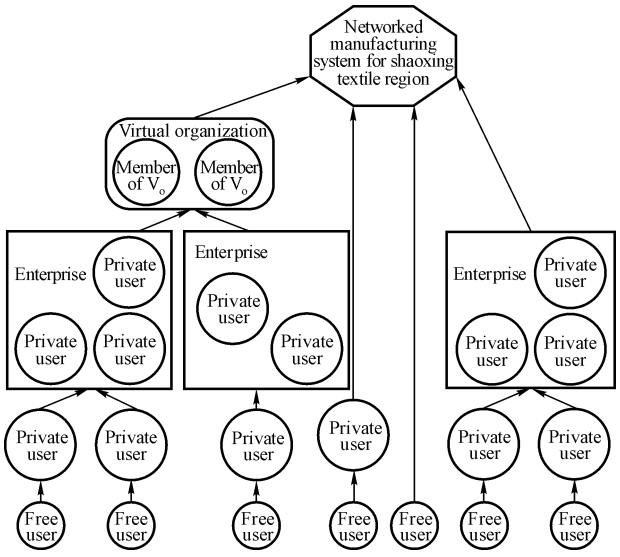

Fig. 1 Hierarchical user relationship model

We can see in Fig. 1 that, free users can access the free resources and services in the networked system. Free users can register to be private users, who can use some ordinary resources and application services. Private users can join certain enterprises (or can be authorized by an enterprise administrator) to become enterprise users. They can then make use of the special resources and services that belong to the enterprise. Sometimes, some enterprises will be grouped into a virtual organization or an enterprise coalition to accomplish a task. For example, the coalition can be composed of supplier, manufacturer and distributor. The administrator of the virtual organization or the enterprise coalition can authorize some enterprises to be the member of the coalition, so that these enterprises can access the resources and services in the possession of the coalition.

4 User access control model for networked manufacturing system

4.1 Reference model for user access control

Based on the user and resource relationship model, and benefit from EMAC [8], we proposed the user access control model for networked manufacturing system, as shown in Fig. 2.

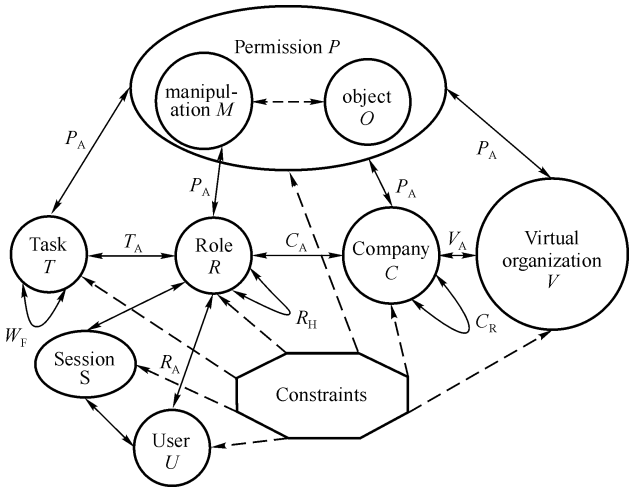

Fig. 2 Reference model of user access control

We can see in the Fig. 2 that this model is composed of sets, authorization, and constraints.

4.1.1 Sets

1) $U=\{u_1,u_2,\cdots,u_l\}$, a set of users. It is the data in networked manufacturing system, or the resource entities shown as data, which represent the users in the system, including free users, private users, enterprise users, and virtual organization users or coalition users.

2) $R=\{r_1,r_2,\cdots,r_m\}$, a set of roles. It is the post in the organization, and it stands for the qualification, right and

responsibility. Role is a semantic synthesis, which can be an abstract conception, or correspond to the job in real-life, such as designer, technologist, manufacturer, quality engineer, manager and so on.

3) $S=\{s_1,s_2,\cdots,s_n\}$, a set of sessions. Corresponding to a user or a group of active roles, it stands for the role-enabled process of user. A user can have several sessions, and activate different roles in different sessions, so the users can have different access permissions. The user should activate roles through sessions.

4) $T=\{t_1,t_2,\cdots,t_o\}$, a set of tasks. Task is a logic unit in work flow, and it is a distinguishable action. Task may be related with many users, and it also may contain several subtasks.

5) $C=\{c_1,c_2,\cdots,c_p\}$, a set of companies.

6) $V=\{v_1,v_2,\cdots,v_q\}$, a set of virtual organizations.

7) $O=\{o_1,o_2,\cdots,o_i\}$, a set of objects, which is the object accessed by the subject.

8) $M=\{m_1,m_2,\cdots,m_j\}$, a set of manipulations that were permitted;

9) $P=\{p_1,p_2,\cdots,p_k\}$, a set of permissions, $P=M\times O$. It is the right to access the data or the resources represented by data in the networked manufacturing system. Permission is an abstract concept in general, and it can be represented as two-tuple of (operations, objects). Here the operation is a manner of access to object.

4.1.2 Relationship between sets

The relationship between each set in the reference mode includes role authorization, task authorization, company authorization, virtual organization authorization, work flow, role's hierarchy and company relationships.

1) Role authorization (R_A), $R_A\in U\times R$, it is a many-to-many relationship between the user set U and the roles set R. Here $(u,r)\in R_A$ means that the user u has the right of role r.

2) Task authorization (T_A), $T_A\subseteq R\times T$, it is a one-to-many relationship between the set R and the set T. Here $(r,t)\in T_A$ means that the role r can perform the task t.

3) Company authorization (C_A), $C_A\subseteq R\times C$, it is a many-to-many relationship between the roles set R and the companies set C. Here $(r,c)\in C_A$, means that the role r can be a member of company c, so as to get the permission from administrator of company c, and access the resources and services of company c.

4) Virtual organization authorization (V_A), it is a many-to-many relationship between the companies set C and the set V of virtual organization. $V_A\subseteq C\times V$ which means that the company c can join the virtual organization v, thereby the members of company c can access the resources and services of virtual organization v.

5) Permission assignment (P_A), it is a many-to-many relationship between the set P and other sets such as R, T, C, V and so on. These relationships can be represented as $P_A\subseteq(P\times R)\bigcup(P\times T)\bigcup(P\times C)\bigcup(P\times V)$, which means that the permission P is assigned to roles r or task t, company c or virtual organization v.

6) Workflow (W_F), which is composed of many tasks.

7) Role's Hierarchy (R_H), $R_H\subseteq R\times R$, which represents the hierarchical relationship between the roles.

8) Company Relationships (C_R), $C_R\subseteq C\times C$, which represents the relationship between the companies.

4.1.3 Constraints of authorization between sets

Each of the authorization between sets should be enforced under some constraints, and we can classify these into different authorization levels (A_L). The constraints include restriction in all the processes of authorization, such as R_A, T_A, C_A, and V_A and so on.

4.2 Process model of user access control

The process of access control is showed in Fig. 3. It can be divided into the following five steps.

1) Role's authorization (R_A). In this step the main task is to validate the constraints of the roles of the users who access the system. Assuming the user u_l wants to access the resources or services possessed by a certain company in the networked manufacturing system, the company only permits the role r_m to access their resources or services. Then the administrator should validate constraints, and subsequently decide whether to authorize u_l or not. We can describe these steps as follows:

$$\left|\text{Role}(R,u_l)\cap A_L(\text{“}u_l\text{”},O,\text{“}r\text{”})\right|=r_m \tag{1}$$

Here the user u_l should be authorized with role r_m only after the role's constraints are validated.

2) Task authorization (T_A). T_A prescribes that a user should firstly take part in certain tasks, and only then can he be permitted access. For example, sometimes the quote of a certain product in collaborative commerce system can be accessed only when the user participates in the bid in auction. When the auction is finished, the permission will be canceled. This step can be represented as:

$$\left|\text{Task}(r_m,T)\cap A_L(\text{“}u_l\text{”},O,\text{“}t\text{”})\right|\geqslant 1 \tag{2}$$

which means that after the user u_l with role r_m passes the validation of constraints in task authorization, the user u_l can access the resources and services that can be accessed in executing tasks such as t_0.

3) Company authorization (C_A). When a certain user u_l wants to access the resources or services O belonging to the

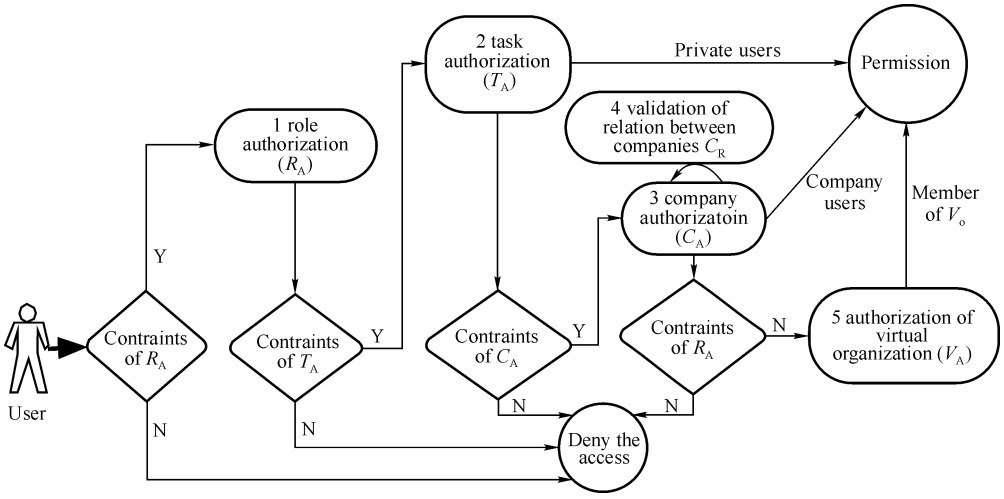

Fig. 3 Process model of user access control for networked manufacturing system

company c_p, he should be a member of the company c_p. This constraint in authorization can be described as:

$$\left|\text{Company}(u_l, C) \cap A_{\text{L}}(\text{“}u_l\text{”}, O, \text{“}c\text{”})\right| \geqslant 1 \tag{3}$$

4) Validation of the companies' relationship (C_{R}). When the user u_l of company c_1 wants to access resources or services belonging to company c_2, the relationship between the two companies should be validated at the user level. If these two companies are partners, administrator of c_2 can assign the user u_l in c_1 the right to access O. It can be expressed as:

$$\left|C_{\text{R}}(c_1, c_2, C_{\text{R}}) \cap A_{\text{L}}(\text{“}u_l\text{”}, O, \text{“}cr\text{”})\right| \geqslant 1 \tag{4}$$

5) Authorization of virtual organization (V_{A}). If an enterprise gains an order that exceeds its capability, it will seek some suppliers and partners to fulfill this order collectively. Here the company can register a virtual organization in networked manufacturing system, and invite these partners to join in the virtual organization. In such a case, if the user u_l of a company wants to access the services O in the virtual organization V, he should go through the validation of constraints in the virtual organization level, and it can be expressed as:

$$\left|\text{V}(u_m, V) \cap A_{\text{L}}(\text{“}u_l\text{”}, O, \text{“}t\text{”})\right| \geqslant 1 \tag{5}$$

5 Policy description based on XACML

The reference model and process model are proposed in the above sections, and in the next step we will describe the access control model in programming. We will introduce the XACML [9] into the networked manufacturing system, and describe our policies of access control.

Program 1 shows the policy set of role authorization for the manager of an enterprise to access the resources in system. This policy set of the role "manager" prescribed the rights hold by manager, such as signing a purchase order.

Similarly, we can use XACML to describe the policy set of task authorization, company authorization and authorization of virtual organization and so on, and finally to construct the entire policy set for access control in networked manufacturing system.

Program 1 Policy set of role "manager" described in XACML

```
<PolicySet xmlns="urn:oasis:names:tc:xacml:1.0:policy"
    PolicySetId="PPS:manager:role"
   PolicyCombiningAl-
   gId="&policy-combine;permit-overrides">
    <Target>
        <Subjects><AnySubject/></Subjects>
      <Resources><AnyResource/></Resources>
      <Actions><AnyAction/></Actions>
    </Target>
    <!-- Permissions for the manager role -->
    <Policy PolicyId="Permissions:for:the:manager:role"
          RuleCombiningAlgId=
                "&rule-combine;permit-overrides">
      <Target>
        <Subjects><AnySubject/></Subjects>
        <Resources><AnyResource/></Resources>
        <Actions><AnyAction/></Actions>
      </Target>
      <!-- Permission to sign a purchase order -->
        <Rule RuleId="Permission:to:sign:a:purchase:order"
                Effect="Permit">
       <Target>
        <Subjects><AnySubject/></Subjects>
        <Resources>
         <Resource>
                <ResourceMatch
        MatchId="&function;string-match">
```

```
    <AttributeValue DataType="&xml;string">
                    purchase order</AttributeValue>
      <ResourceAttributeDesignator
              AttributeId="&resource;resource-id"
              DataType="&xml;string"/>
     </ResourceMatch>
    </Resource>
   </Resources>
   <Actions>
    <Action>
     <ActionMatch
              MatchId="&function;string-match">
  <AttributeValue dataType="&xml;string">
                  sign</AttributeValue>
       <ActionAttributeDesignator
              AttributeId="&action;action-id"
                  DataType="&xml;string"/>
       </ActionMatch>
      </Action>
   </Actions>
    </Target>
  </Rule>
 </Policy>
</PolicySet>
```

6 Conclusions

The ASP-based implementing model for networked manufacturing system proposes greater stipulations towards security and user access control. In this paper, we proposed an integrated user access control method composed of RBAC, TBAC, RDAC and CBAC. And the XACML was used to implement this method. The results show that the integrated user access control method can reduce the costs of system security maintenance and management. Further research will focus on the resolution of conflicts between authorizations at different levels.

Acknowledgements This paper is supported by the National High-Tech. R&D Programs for CIMS, China (No. 2003AA414043, 2004AA414034).

References

1. Zheng Xiao-lin, Research of key techniques in application service provider (ASP) based networked manufacturing system, Ph. D. Thesis, Hangzhou: Zhejiang University, 2004: 1–72 (in Chinese)
2. Cherry T. C., Application service providers (ASP), http://www.cherrytreeco.com/current/reports/asp.pdf, Oct.1999
3. GROVES J., Security for application service providers, network security, 2001(1): 6–9
4. YU Shi-peng, Research on theory and application of role-based access control, Master Thesis, Peking: Peking University, 2003: 1–5
5. Sandhu R. S., Edward J. C., Hallf et al., Role-based access control models, IEEE Computer, 1996, 29(2): 38–47
6. Huang Yi-min, Yang Zi-jiang, Ping Lin-di et al., Practical way to implement role-based access control in security administration system, Journal of Zhejiang University (Engineering Science), 2004, 38(4): 408–413 (in chinese)
7. Thoms R. K., Sandhu R. S., Task-based authorization controls (TBAC): a family of models for active and enterprise-oriented authorization management, Proceedings of the IFIP WG11.3 Workshop on Database Security, California: Chapman & Hall, 1997: 166–181
8. Wang H. J., Cheng H. K., Zhao J. L. et al., Web services enabled E-market access control model, International Journal of Web Services Research, 2004, 1(1): 21–40
9. Anderson A., XACML profile for role based access control (RBAC), http://docs.oasis-open.org/xacml, 2004