# ACCESS CONTROL MODEL OF MANUFACTURING GRID

Hongxia Cai, Tao Yu, Minglun Fang
*CIMS&Robot Center, College of Mechatronics Engineering and Automation, Shanghai University, Shanghai, China; Email: hxcai@mail.shu.edu.cn.*

Abstract: The overall motivation for Manufacturing Grid is to realize resource sharing and collaboration in the field of Manufacturing. In order to protect the shared resources and services, the access control guarantees in the MG is necessary and important. Due to inherent heterogeneity, multi-domain characteristic and highly dynamic nature of Manufacturing Grid, we propose a new Manufacturing Grid Access Control Model to support the dynamic restricted rights management based on the current Role-based Access Control Model. We employ a distributed access control mechanism to realize the authorization from the local service nodes according to the global and local authorization policy. The implementation within the project of the Shanghai High Institutions Grid proves the authorization architecture and model are workable and our work is valuable.

Key words: Manufacturing Grid, security, Role-based Access Control Model

## 1. INTRODUCTION

Based on the technology of Grid, we developed a Manufacturing Grid system to realize resource sharing and collaboration in the field of Manufacturing. However, in the Grid environment, the access control challenges are not fully addressed by existing approaches. It is still one of the major remaining obstacles to the wide-spread adoption of the Manufacturing Grid. Due to inherent heterogeneity, multi-domain characteristic and highly dynamic nature of Manufacturing Grid, we propose a new Manufacturing Grid Access Control (MGAC) Model which complements the classic Role-based access control (RBAC) [1], while

*Please use the following format when citing this chapter:*
Cai, Hongxia, Yu, Tao, Fang, Minglun, 2006, in International Federation for Information Processing (IFIP), Volume 207, Knowledge Enterprise: Intelligent Strategies In Product Design, Manufacturing, and Management, eds. K. Wang, Kovacs G., Wozny M., Fang M., (Boston: Springer), pp. 938-943.

retaining its advantages (i.e. ability to define and manage complex security policies). The model dynamically adjusts Permission Assignments based on global project state. The MGAC model is scalable to combine the coarse-grain authorization policy at local service node with the global fine-grain authorization policy.

The rest of this paper is organized as follows. In section 2, we present the MGAC model. In section 3, we introduce its implementation within the project of the Manufacturing Grid, which is the part of Shanghai High Institutions Grid. A brief summary is given in section 4 along with concluding remarks.

## 2. ACCESS CONTROL MODEL OF MG

We will present an access control approach to the Manufacturing Grid which allows for the unified and centralized management of authorization. The MGAC model complements the current Role-based Access Control Model to support the dynamic authorization.

In RBAC model, the user has the privilege when he is assigned the role. In the MGAC, the privilege of the user is not only related with static role, but also subjected to the project state. The traditional RBAC model could not satisfy the distributed Manufacturing Grid architecture. In the MGAC, the user accesses the local service node by mapping the global role and to the local role.

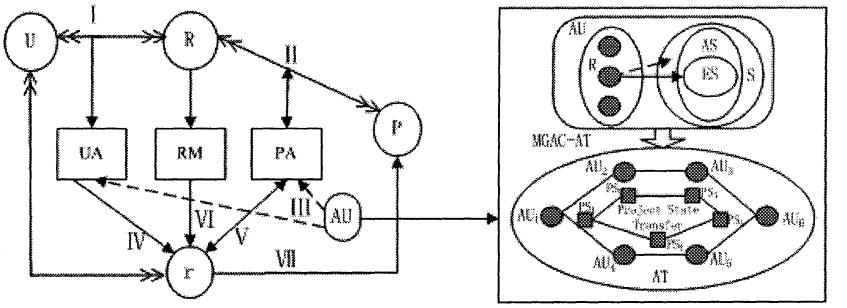


*Figure 1.* MG Access Control Model

Figure 1 is the Manufacturing Grid access control model. In the MGAC model, Ⅰ, Ⅱ shows the principle of the traditional RBAC which illustrates the relationship of the user-to-role-to-privilege assignment. Ⅳ, Ⅴ, Ⅵ, reflects the consistency between the local and global access control management.Ⅲ shows the dynamic authorization mechanism which is introduced in the

MGAC-AT. In the MGAC-AT, AU is the basic Authorization Unit which comprises the enabled-permissions set to the dynamic role. The AU is transited to confine the enabled permissions of the role according to the project state. We define the transition of the AU as AT. AT is the sequence of the AU: AT= {AU1, AU2 ..... AUn }

We formally define the MGAC model as follows:

$$MGAC=(U,R,r,P,AT) \quad (1)$$

U is the user, R is the global role, r is the local role, P is the privilege, AT is the authorization transition.

We define the following relationship: User assignment (UA), Permission Assignment (PA), Role Mapping (RM), Authorization Unit(AU):

- User assignment(UA), $UA \subset U \times R$, a many-to-many mapping user-to-role assignment relation;
- Permission Assignment(PA),$PA \subset P \times R$ , a many-to-many mapping, permission-to-role assignment relation.
- Role Mapping (RM), $RM \subset R \times r$, Global Role-to-Local role assignment relation.
- Authorization Unit (AU), $AU \subset r \times AS$, Local Role-to-Authorized Service assignment relation.

We assign the user the global role to have static privilege:

$$UA(R)=\{ua(u_i, R)|ua(u_i,R) \in UA,i=1,2,.....n\}; \quad (2)$$

$$PA(R)=\{pa(R, p_i)|pa(R, p_i) \in PA,i=1,2,.....n\}; \quad (3)$$

The authorization of the dynamic role can be transmitted according to the project state:

$$AU(R)=\{au(R, as_i)|au(R, as_i) \in AU,i=1,2,.....n\}; \quad (4)$$

We map the global role to local role:

$$RM(r)=\{rm(r, R_i)|rm(r, R_i) \in RM,i=1,2,.....n\}; \quad (5)$$

Whether the user can access the local service, it depends on:

$$Authorize(u,s) \rightarrow \exists R(u \in UA(R) \cap p \in PA(R) \cap AS \in AU(R) \cap R \in RM(r)) \quad (6)$$

So in the MGAC model, the authorization is dynamic convergence and consistency.

## 3. IMPLEMENTATION

The project of Shanghai High Institutions Grid sponsored by the Shanghai Technical Committee, has goals similar to those of the Grid, focusing on establishing a platform for resource sharing and collaboration in the field of rapid manufacturing and so on.

We have tested the scenario on our platform. In our platform, it allows for the unified and centralized management of access control rules to a set of services and resources that may be widely distributed and highly heterogeneous. The global policy repositories determine the global access rules in which the fine-grain policy is defined by the community about the role and privilege assignment, while the dynamic policy is related with the project state. The local policy repositories grant coarse-grain access to the virtual organization of MG. The distributed services are managed locally, while the privileges of the user are authorized at local service node.

Figure 2 is Access Control Working Flow in the MG. The MGAC Global Broker is responsible for authenticating the requesting Grid user, authorizing their request and determining whether the user has the global right to access the services or not. The authorization depends on the fine-grain policy from the global policy repositories and dynamic policy related with the condition of the project. We use the SAML [6] (Security Assertion Markup Language) for exchanging authentication and authorization information. The MGAC Local Broker checks if the global policy statement authorizes the request and the privilege is authorized to the community. The MGAC Local Broker maps the Global Role to Local Role according to the role mapping list. Policy enforcement is carried out by local operating enforcement mechanisms.

In our scenarios, according to the central fine-grain access control policy, the roles of rapid designer and project manager in the project group can access the task file and its attachment. The dynamic policy only allows the role of the rapid designer and so on to update the drawing when the project is in the state of design. According to the local course-grained polices, for example, at the one of the rapid design service node, the drawings are open to the community of MG. Of course, the local access control policy could forbid the blacklist accessing the design drawings. When the provider of the rapid prototyping began to machine, the rapid designer could not access files any more. As soon as the project finished, the global roles assigned to the users are withdrawn, and the users could not access resources any more.

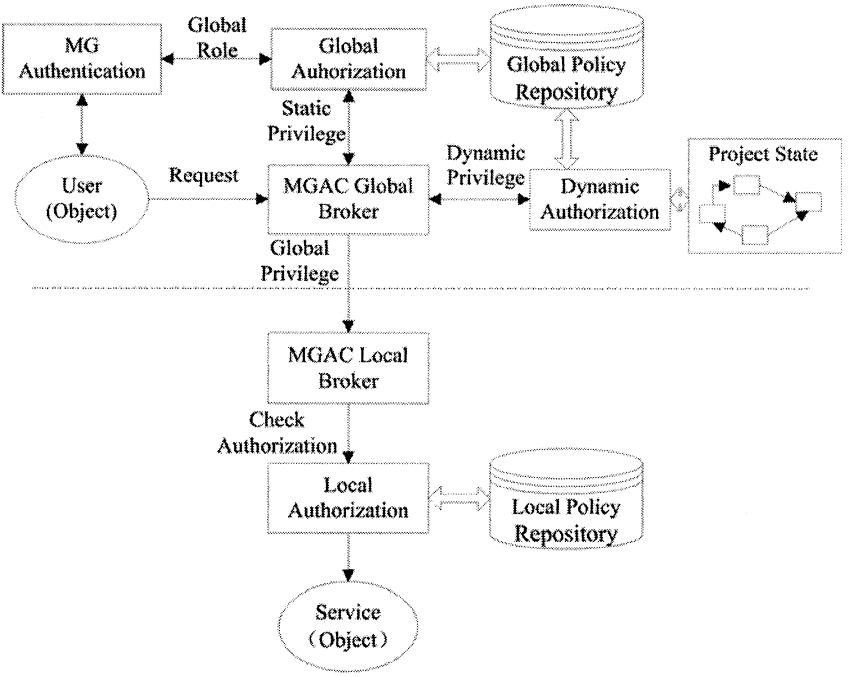


*Figure 2.* Access Control Working Flow in the MG

## 4. CONCLUSION

In this paper, we present a new access control model for the Manufacturing Grid. Compared with the traditional Role-based access control model, the Manufacturing Grid Access Control model is more scalable, more applicable to the distributed and dynamic Manufacturing Grid environment. The MGAC model solves the access control issues and satisfies the access control requirement in Manufacturing Grid. The implementation in the project shows that the research is valuable and the MGAC model is workable.

## 5. REFERENCES

1. R. Sandhu, E. Coyne, H. Feinstein, and C. Youman. "Role-based Access Control Models," *Proceedings of the 5th ACM Workshop on Role-Based Access Control,* 2000, pp. 38- 47.

2. Liu Lilan, Yu Tao, Shi Zhanbei, "Research on Rapid Manufacturing Grid and Its Service Nodes", *Machine Design and Research*, 2003, pp.57-59.
3. I. Foster, C. Kesselman, J. Nick, and S. Tuecke, "The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration," *Open Grid Service Infrastructure WG (GGF)*, June 2002.
4. L. Pearlman, V. Welch, I. Foster, and C. Kesselman, "A Community Authorization Service for Group Collaboration," *Proceedings of the IEEE 3rd International Workshop on Policies for Distributed Systems and Networks*, 2002.
5. P. Hallam-Baker et al, "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)", *Oasis Standard*, November 5th, 2002.
6. S. Godik et al, "eXtensible Access Control Markup Language (XACML) Vers. 1.1", *OASIS Standard*, July,2003