# A Multi-Level Cross-Domain Access Control Model Based On Role Mapping

Bin Lv, Di Zhang, Rui Mao & Haitian Yang
*Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China*
*University of Chinese Academy of Sciences, Beijing, China*

ABSTRACT: Inter-domain access control can guarantee the safety of resources sharing among different domains, role mapping is one of the key technologies which realizing access control. Traditional mapping mechanism, which involves congested traffic, has massive computational complexity and has a big traffic. In this paper, we proposed a cross-domain role mapping model under the circumstance of multi security level, which makes the resources and roles divided into different security levels, and establishes a hierarchy tree according to the different department that containing different roles and resources. With the help of inter-domain level service, we achieve the goal of cross-domain access control. Compared with the existing researches, the model in this paper is more practical and secure.
KEYWORD: Multi-level; Multi-domain; Access control; Interoperation

## 1 INTRODUCTION

Computer network can realize resources sharing effectively, with the rapid development of the network techniques, the interaction between different networks become more frequent, resources sharing get further improved (Al-Muhtadi, J. et al. 2001). Consequently, the information security issues become more server and complex (Chun-Xiao, Y.E. et al, 2012) (Crampton, J. et al, 2003). The safety of information system is the key problem to be solved in practical application. Access control technology, one of the five security service function (Geethakumari, G. et al. 2009), can limit the subject's access action in the system, guarantee the subject can access the object directly only in the case of authorized. Meanwhile, it prevents the exceeding authorized access of valid subject, ensure the confidentiality and integrity of data effectively (Jin, L. et al. 2009).

The early access control model, including discretionary access control (DAC) and mandatory access control (MAC), meet the needs of relatively safety of sharing data between different computers (Rajpoot, Q.M. et al. 2015) (Ren, H.P. 2013) (Roy, K. et al, 2012), solve the problem of basic access control management. While the DAC and MAC cannot meet the complex requirements in practical application, the role-based access control (RBAC) arises at the right moment. RBAC (Wang, J. et al. 2014) encapsulates privileges into roles, and users are assigned to roles to acquire privileges. This kind of interaction makes it simple and facilitates reviewing permissions assigned to a user. It also makes the task of privilege administration less cumbersome, overcome the shortcomings in policy management of DAC and MAC (Xia, L.N. et al, 2007) (Xie, L.X. et al. 2014).

Nowadays, information systems have certain changes in terms of level and scope, and it pays more attention to the breadth and depth in practical use, this makes the multi-level and multi-domain information system (Xiong, H. et al. 2015), a kind of complex information system which contains security level and trust domain, becomes more and more popular.

The commonly used access control model mostly evolved from the traditional DAC, MAC and RBAC, it concerns to the information system with point-shaped, linear-shaped and star-shaped structure, which is relatively simple (Xiong, X. et al. 2011) (Yang, Z. et al. 2013). For these classical models, the change of object's privilege in the system has little constraint in general. But in multi-level and multi-domain system, the object's privilege is constrained by multi-aspects, the common used access control model cannot meet the requirement of the system directly. The research on this aspect is one of the scientific highlights in recent years.

## 2 RELATED WORK

### 2.1 *Multi-level & multi-domain environment*

Compared with the previous distributed information system, the system which is in the multi-level & multi-domain environment has the concept of level and domain. The concept of level makes it more practical in line with reality application for the system, the concept of domain makes it more convenient for the interoperation between different systems. The multi-level & multi-domain system is wildly used in the area of finance and nation defense. Figure 1 gives a brief model.

As for these domain, each of them has the pyramid shaping. The user or resource in the upper layer has a higher level than the lower layer. The user can only access the resource which is in the same layer or lower layer with permission.

There are many security domains in multi-level & multi-domain system, each domain is relatively independent, and their functions are different, the object whose access authority needs to be controlled is also different. After an object is mapped from one domain to another domain, the privileges that it possesses are not applicable in new domain, hence, we need to adjust the privileges to adapt to the new environment after the mapping operation.

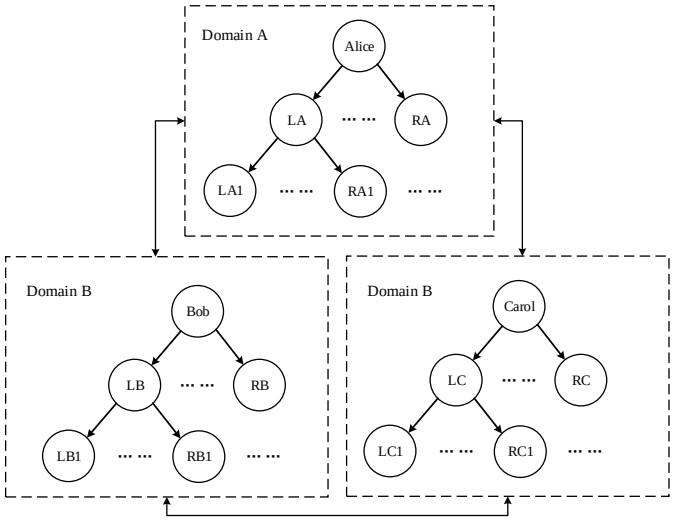


Figure 1. Brief model of multi-level & multi-domain system

### 2.2 *Basic access control model*

There are some commonly used access control models, contains the model based on object, task and role.

Object based access control model contains DAC and MAC. DAC connect the subject with object directly, restrict the subject's access privilege according to the association relationship. MAC is based on DAC. MAC implement access control according to the security attribute of subject and object. The attribute of subject and object is assigned by manager, and cannot be changed casually.

Task based access control model solve the problem from the view of application, implement security access control dynamically in the process of processing tasks.

Role based access control model add the concept of role between subject and object, which makes the privilege mapping between subject and object is divided into subject to role and role to object.

These kinds of models are most commonly used access control models, but all of these models are designed for ordinary information systems. For the multi-level and multi-domain information systems, it cannot establish the hierarchical relationship, and cannot satisfy the user roaming between different domains.

Crampto proposed SARBAC (scope administrative role based access control) based on RBAC, this model change the role range to administrative scope, simplify the role hierarchy management, but it does not distinguish the management role from regular role, and also does not improve the detail implement of the manager's management. Jalal proposed AIRBAC2000 (administrative interoperable role based access control), it introduce the inter-domain operation management role to manage the role mapping, providing a good method for interoperability, but the different privileges possessed by manager will lead to chaos in the management. Luning Xia proposed an administrative model for role based access control model, which use hierarchical namespace to manage the roles and resources, the resources of different namespace are not visible to each other, this simplify the integrated structure of roles, makes it easier to manage local autonomous RBAC systems.

These models have the corresponding improvements to the basic models, but still have the redundant assigned permissions, and also cannot solve the problem of cross-domain interoperability properly. As the size of system increases, the management of model is more difficult.

Aiming at the above problems, this paper analysis the character of multi-level security and cross-domain security, combing with the existing research of interoperability security. Ultimately we design the multi-level & cross-domain interoperability access control model to solve the above problems.

## 3 BASIC CONCEPT

### 3.1 *Resource security level*

We use hierarchical security level to identify the resources. Before the system is used, the manager classifies the resources with different levels according to different apartment or type, these levels information can be expressed as different tree structure, the node represents level mark of resources.

Resource security level is defined as: Re (resource, $hierarchy_1$, $hierarchy_2$ ……, $hierarchy_n$), Figure 2 gives a brief explanation.

### 3.2 *Subject security level*

Subject is the user that access the resources, its security level is acquired by the role that it possesses. The definition of role security level is familiar with the resource: Ro (role, $hierarchy_1$, $hierarchy_2$ ……, $hierarchy_n$), every role will have an identity on behalf of its duties. Figure 3 gives a brief explanation.

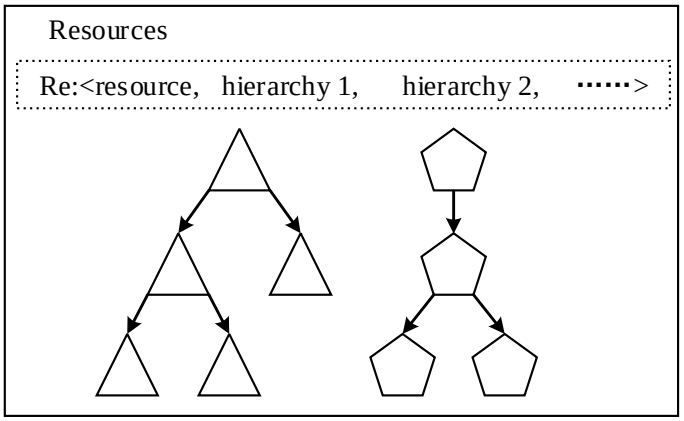


Figure 2. Security level trees of resources

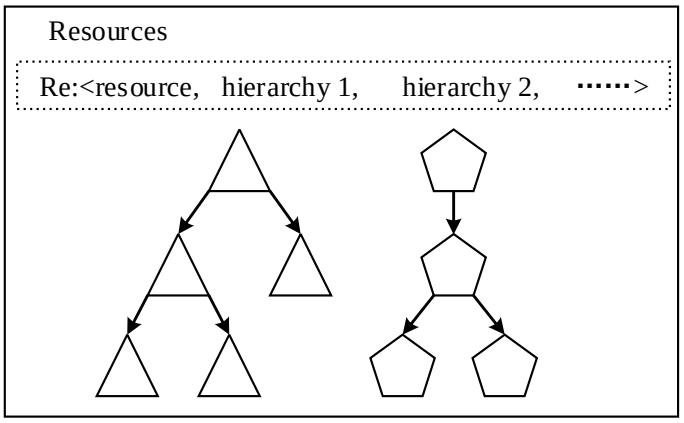


Figure 3. Security level trees of resources

According to the practical requirement, the manager formulate the original role level tree and resource level tree, distributing the corresponding security level. While the users access the resources, compare the security level of users and resources to make sure if the users have the privilege to complete this access procedure, in this way, we achieve the effect of the mandatory access, implement security access of resources.

## 4 THE DEFINITION OF ACCESS CONTROL RULES

### 4.1 *Formal description*

In order to describe the access control strategies formally, we define $R_A$ as the security level tree of domain A, $R_B$ as the security level tree of domain B. M>N represents the level of M is higher than N. $M_A \rightarrow N_B$ represents the mapping mechanism among different domains, that is to say M (domain A) is mapped to N (domain B), we define two kinds of mapping mechanisms: transfer mapping mechanism and non-transfer mapping mechanism.

#### 4.1.1 *Transfer mapping mechanism*

We suppose that there is a mapping $N_B \rightarrow M_A$, for any K belonging to A, if $K_A > M_A$, then we have $K_A > N_B$ . We can see it from Figure 4, $Guest_B \rightarrow Guest_A$, hence, the roles whose access level is equal or greater than the Guest in domain A can access the resources of Guest level in domain B.

#### 4.1.2 *Non-transfer mapping mechanism*

If the manager just wants to link the security level in his domain with the other domain, but the users with higher level in other domain cannot own this privilege. For instance, in Figure 5, Mana in domain B is mapped into Prof in domain A, without the inheritance relationship such as Prof to Stu. In this paper, we define this non-transfer mapping mechanism as $N_B \rightarrow (NT) \rightarrow M_A$.

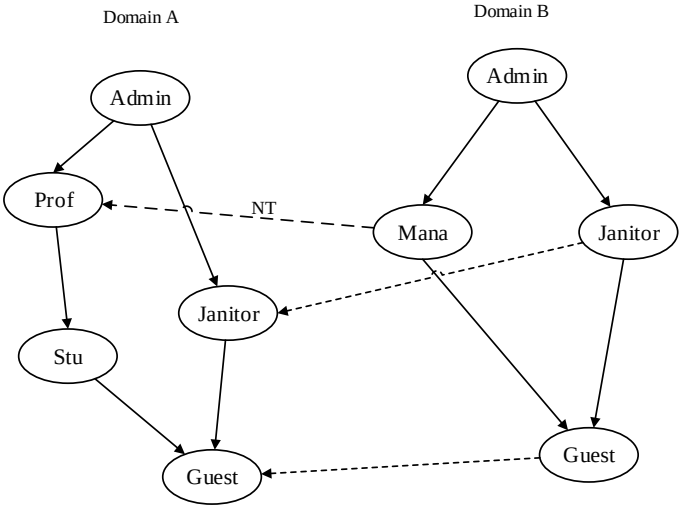


Figure 4. Example of intra-domain role mapping

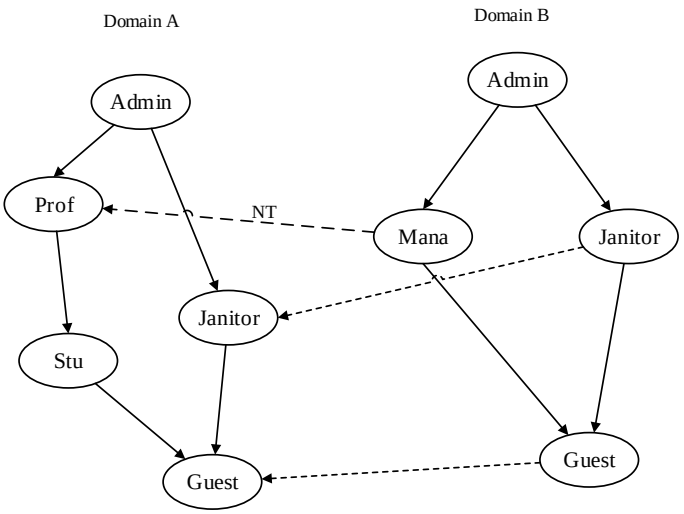


Figure 5. Example of intra-domain role mapping

### 4.2 *Mapping policies*

For the above two kinds of mapping mechanism, the following several policies are presented:

#### 4.2.1 *Default policy*

When a subject of domain B access domain A, domain A provide a default security level, any subject that can be mapped over can access the object, this makes it more convenient for cross domain access control.

#### 4.2.2 *Direct policy*

The access privileges between domain B and domain A are bound one by one, this makes it complete secure for cross domain access control.

#### 4.2.3 *Partial policy*

The role mapping mechanism need to be set by manager, in this case, we should use non-transfer mechanism. In the other cases, roles with inherit relationship can be mapped to role set with same level, we use transfer mechanism. This makes it easier to manage, and the mapping relationship of the system is leaner.

### 4.3 *Integrity and consistency*

In order to ensure the integrity and consistency of access control policy, we set out the following rules:

Integrity is the prevention of unauthorized modification of information from the same domain or the other domain. The model of this paper stipulate that the manager set a minimum security level, if a new subject has not been set as a security level then it possesses that minimum security level. In this way, we can control the minimum access privilege of all the mapping relationship. In general, the minimum security level can access non-sensitive data in public.

Consistency refers to that there is only one corresponding level to a security level in the domain, otherwise, there will be ambiguity of access control policy. The model stipulates that for any mapping relationship, any security level belong to different security level tree.

## 5 MULTI-LEVEL CROSS-DOMAIN INTEROPERABILITY ACCESS CONTROL MODEL

### 5.1 *Model architecture*

On the basis of Cross Domain Role Mapping Architecture, which is proposed by Geethakumari, based on the level of roles, we proposed multi-level cross-domain interoperation access control model, the architecture is shown in Figure 6.

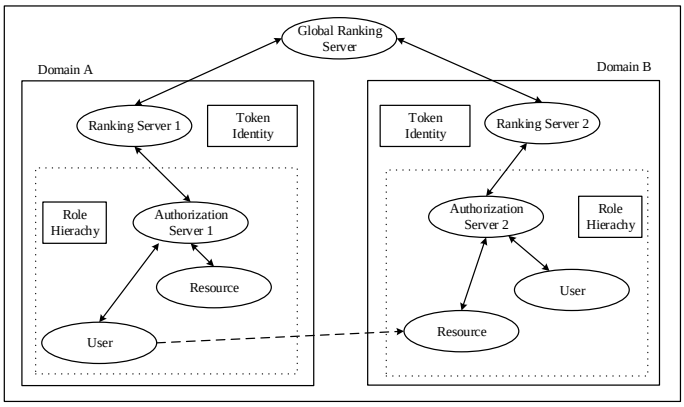


Figure 6. Multi-level cross-domain interoperation access control model

### 5.2 *Access control procedure*

As shown in Fig.5, domain A and domain B contain different users or resources node, there is an authorization server and a ranking server both in domain A and domain B. the ranking server saves the level information of sub-domain, global ranking server is used for redirection across different domain.

User-a in domain A request for the Resource-b in domain B, the whole procedure is as follows:

- User-a seek Resource-b, sending his identity and request operation.
- Resource-b asks the authorization server 2 for its decision.
- Authorization server 2 check the information of User-a, verify if he has the access privilege and what kind of operation privilege does he has.
- As the requests are from the different domain, authorization server 2 take the help of ranking server 2, checking all the role information that can access the resource. Global ranking server redirect the request to ranking server 1.

– There is information about roles and levels of User-a in ranking server 1, they are stored in a token. Then the token return, following the same path in reverse direction.
– According to the information in the token which is received by authorization server 2, comparing it with the role set that have the access privilege to Resource-b, such as the apartment or role level of this role, to ensure if there is a role that can be mapped.
– This algorithm is being executed to take final call whenever the mapping is success or denied.

## 6 PROBLEMS OF MAPPING POLICY

The existing research results shows that there will be conflict of security in cross-domain mapping mechanism, inherit ring is the most common problem. In the view of this conflict, there are so many solutions, but these methods are designed for their respective application framework and scenario, for the framework represented in this paper, we give our solution.

The role mapping relationship among different domains can be simplified to a mapping procedure of tree structure, just make sure the mapping tree do not violate their rule in the domain in the process of interoperability, and also should be consisted with the inter-domain access process which is described in this paper, so that we can achieve legitimate access. The implementation of the algorithm is given below.

Algorithm 1: determine whether the node in mapping tree is violated with the mapping conditions. The input parameter are mapping tree O and N. At first we judge that if O and N are violated with mapping condition, if there is violation, return false. Or we judge the parent node of O recursively until the parent node is empty. Consistency of style is very important. Note the spacing, punctuation and caps in all the examples below.

```
boolean MapTreeViolation (Tree O, Tree N) {
   if ( O.isDynamicMapping ( N ))
      return false;
   else if ( O.father != null ){
      if ( !MapTreeViolation ( Tree O.father, Tree N ))
         return false;
   }
   return true;
}
```

Figure 7. MapTree-Violation algorithm

Algorithm 2: determine whether there are roles belonging to the same domain in a mapping tree. The input parameter are root node M and role N. At first we judge that if M and N are roles in the same domain, if the answer is yes, return false. Or we judge the son node recursively until the son node is empty.

```
boolean MapTreeDomain (Tree M, Tree N) {
   if ( M.isSameDomain ( N ))
      return false;
   for ( int i = 0; i < count -1; i++ ){
      if ( !MapTreeDomain ( M.domain[i], N ))
         return false;
   }
   return true;
}
```

Figure 8. MapTree-SameDomain algorithm

## 7 MODEL ANALYSIS

Comparing the access control model which is proposed in this paper with the existing referenced access control models, the model has the following advantages:

– This model describes the subject, object, mapping relationship and the constraint conditions in detail, which makes the system easier for the administrator to manage with fine grain.
– In the aspect of level protection, this model establishes different level trees for the user of different organization or department, which improving the security and scalability of the model.
– There will be policy conflicts in the process of implementing multi-level cross-domain access control mechanism, it is very important to the system security. This model takes the inheritance ring into account, designing conflict detection and resolution algorithm to ensure consistency of policy, which improve the security of the system to a great extent.

## 8 SUMMARY

In the process of role mapping interoperability, we set a minimum security level which solve the safety of cross domain access to a certain extent, the role mapping access control mechanism in this paper is more realistic for multi-domain mapping operation, grouping the role into different tree structure. For the roles with same security level but different operating privilege, we limit its mapping operation. In allusion to the inherit ring problem in the role mapping process, we proposed our solution, enhance the security of the model. For the future, more works will be done to solve the other type of role conflict, to meet the actual demand.

## REFERENCES


Al-Muhtadi, J. et al. 2001. The AIRBAC 2000 Model: Administrative Interoperable Role Based Access Control. *ACM Transactions on Information and System Security* 3(2): 173-182.

Chun-Xiao, Y.E. & Guo, D.H. 2012. Research on secure interoperation in multi-domain environment. *Journal of Computer Applications* 32(12): 3422-3425.

Crampton, J. & Loizou, G. 2003. Administrative scope: A foundation for the role-based administration of roles. *ACM Transactions on Information and System Security* 6(2): 201-231.

Geethakumari, G. et al. 2009. A Cross-Domain Role Mapping and Authorization Framework for RBAC in Grid Systems. *International Journal of Computer Science & Applications* 6(1): 1-12.

Jin, L. et al. 2009. Research Development on Secure Interoperation in Multi-Domain Environment. *Computer Science* 36(2): 47-54.

Rajpoot, Q.M. et al. 2015. Attributes Enhanced Role-Based Access Control Model. *Proceedings of the 12th International Conference on Trust, Privacy and Security in Digital Business* 9264: 3-17.

Ren, H.P. 2013. Status and Developments of Access Control Model. *Computer & Digital Engineering* 41(3): 452-456.

Roy, K. & Bhowmick, A. 2012. A Proposed Mechanism for Cross-Domain Authorization in Grid Computing Environment. *International Journal of Emerging Technology and Advanced Engineering* 2(4): 163-166.

Wang, J. et al. 2014. Research on multilevel security access control policy processing method. *Information and Network Security*, *International Conference on IET* 2014: 180-184.

Xia, L.N. & Jing, J.W. 2007. An Administrative Model for Role-Based Access Control Using Hierarchical Namespace. *Journal of Computer Research and Development* 44(12): 2020-2027.

Xie, L.X. et al. 2014. Multi-Domain Role Trust Access Control Model. *Journal of Beijing University of Posts and Telecommunications* 37(3): 83-88.

Xiong, H. et al. 2015. Survey of security analysis for role-based access control. *Application Research of Computers* 32(11): 3201-3208.

Xiong, X. et al. 2011. Research of access control method on multi-level & multi-domain information system. *Computer Engineering & Design* 32(11): 3613-3617.

Yang, Z. et al. 2013. Model of domain based RBAC and supporting technologies. *Journal of Computers* 8(5): 1220-1229.