Dynamic Access Control Research for Inter-operation in Multi-domain Environment Based on Risk[⋆]

Zhuo Tang, Ruixuan Li, Zhengding Lu, and Zhumu Wen

School of Computer Science and Technology,
Huazhong University of Science and Technology, Wuhan 430074, Hubei, China
hust_tz@126.com, {rxli,zdlu}@hust.edu.cn, zoomer@thinkbank.com.cn

Abstract. For the complexity of the multi-domain environment and the ceaseless evolvement of the information secure sharing, the traditional access control method can not ensure the absolute security for the exchange of data resources. Through introducing the concept of risk, this paper proposes a dynamic access control model for multi-domain environment based on risk of inter-operations. The risk rank of an access policy can be calculated by the history of the inter-operations among domains, the security degree of the objects and the safety factor of the access events. Through adjusting the access policies which be considered the high risk, the risk in the system can be controlled in real time. The security analysis shows that this method can reinforce the facility of the access control and the security of the multi-domain environment.

1 Introduction

With the increase in information and data accessibility, there is a growing concern for security and privacy of data. The realization of the connections and the inter-operations among the different data sources under the distributed heterogeneous environment is becoming the practical problem. There is a growing concern for the security problem for the inter-operations between multi-domains. More and more researches try to resolve the defense for the vicious behaviors through the economic methods. In fact, recent research in these directions has suggested some economical models for a wide range of secure distributed systems, including a payment based security system for mobile agents [1] and game based model for secured grid computing [2]. However, risk remains un-quantified in these proposals. In fact, there exists an emerging consensus that every security question is indeed an economical question concerning the utility of the underlying system [3]. For example, it is easy to show that in a mobile agent based e-commerce system, both the protection of agents and hosts have a direct impact

[⋆] This work is partially supported by National Natural Science Foundation of China under Grant 60403027, Natural Science Foundation of Hubei Province under Grant 2005ABA258, Open Foundation of State Key Laboratory of Software Engineering under Grant SKLSE05-07.

S. Kim, M. Yung, and H.-W. Lee (Eds.): WISA 2007, LNCS 4867, pp. 277–290, 2007.

on the utility: attacks on a host by malicious agents will cause loss of commercial secrets such as customers private information, downtime to the system, loss of customers, which will eventually be counted as utility loss. Attacks on agents will result in similar consequences that will also lead to the lost of utility. Thus utility maximization and risk minimization are important issues in the design of a secure distributed system if we seek to gain maximum economical benefits from the underlying system. This is also an important target of the distributed system security. But at present, there are little literatures to demonstrate the actual signification of the risk of distributed system [4].

In the economic area, there exist the consanguineous relations between the risk and trust. Mayer and Rousseau [5] discussed the difference and the relationship between the risk and trust. Jarvenpaa [6] proposed definitely: trust can influence the risk in a certain extent. Further more, it can influence the subjects' behaviors. For example, there is the lower risk when you loan money to the familiar than stranger. Moreover, this literature considers that the extent of trust can influence the cognitive extent of the risk.

The objective of the inter-operations is to offer the rational distributing and effective share of the resource, and the cooperation of the distributed systems. It means the ability of the two software components to communicate and co-operate to complete a common task. It contains two meanings: the basic and the application. The basic inter-operations mean the communications and cooperation among the different platforms. And the applied inter-operations mean the cooperation among the distributed application components which above the computational platforms. This paper mainly discusses the later.

The multi-domain environment has the characteristic of dynamic and indetermination. As the frequent changes of the security policies in individual autonomy, the changes of the relationship among the domains, even the birth and the death of the individual domains, the any security polices can not insure the absolute security of the data resource in the process of inter-operations. For the access control method of the traditional model, the subject sometimes can use its permissions constantly once been authorized. It hardly satisfies the dynamic changes of the multi-domain environment. And it will bring many security risks and hidden trouble to the inter-operations among multi-domain environment.

In order to decrease the risk of inter-operations, for the problems of trust and risk of the security inter-operations under the application tier, which base the mappings between the users and roles in the different domains, this paper proposes a risk based dynamic access control model for multi-domain environment. In this model, through calculating the trust degree between the subjects firstly, we can ascertain the risk extent when a subject in one domain has an operation to the objects in the other domains. Therefore, we can receive the risk degree of the inter-operations. Using this risk degree, we can adjust the subjects' access privilege dynamically. The risky permissions will be revoked, and the utility of the system will be maximized.

The rest of the paper is organized as follows. Section 2 describes the related works. Section 3 presents algorithms for the calculating the risk of the inter-operations. Section 4 describes the dynamic access control model for multi-domain environment, followed by the conclusion in Section 5.

2 Related Works

In the recently 20 years, people have acquired the plentiful achievement for the research of the access control. Many access control models have been proposed. The most popular models include discretionary access control (DAC), mandatory access controls (MAC) and role based access control (RBAC). In the RBAC family which be proposed by Sandhu in 1996[7], the users' privilege is related with their roles, and the users acquire their privilege through roles. A role is a permission set for a special work station. When the users' privilege needs to be changed, we can do it by revoking the roles or re-distributing the user's roles.

Michael J. Covington et al [8] have proposed the Generalized Role Based Access Control (GRBAC) model. In this model, they extend the traditional RBAC by applying the roles to all the entities in a system. (In RBAC, the role concept is only used for subjects). By defining three types of roles, i.e., Subject roles, Environment roles, and Object roles, GRBAC uses context information as a factor to make access decisions. Guangsen Zhang et al. [9] also uses context parameters in their dynamic role-based access control model under the two key ideas: (1) A user‘s access privileges should be changed when the user's context changes. (2) A resource must adjust its access policy when the environment context information (e.g., network bandwidth, CPU usage, memory usage) changes. These above two papers make the access control dynamic and flexible but the decision-making process is not as powerful and precise as that in our model. They did not consider the aspect of security in making-decision process and the impact of security problems on the system.

The Nathan Dimmock's paper [10] uses the concept of outcome to calculate cost for each outcome and risk value. Comparing to this paper, they do not consider the context for risk assessment. So it loses the flexibility characteristic in evaluating risk. They did not consider risk as an important factor in their access control mechanism and they did not use risk directly in making decision.

There is little attention to the trust and risk in the access control research [11]. The term trust management system was introduced by Blaze et al. in [12], but the solution it proposes involves an unduly static notion of trust application programmers choose where to insert code to evaluate their notion of trust, for example at the starting point of a given execution session. Most of the past research combining access control with trust concepts focuses on a trust-management approach in which trust values flow in a manually defined way through access control policy. For example, in literature [13] and [14], the mutual trust relationship is founded by the continuously negotiation. Literature [15] illuminates the relationship between the trust management and distributed access control, and it extends the access control system of OASIS and the access control language. So, the access policy can be decided base on the trust and risk. But the trust mentioned in this paper is defined by the special operation, and the relationship between risk and trust is faint in this paper.

The above access control methods mostly base the traditional model. They are all short of the dynamic description for the subjects. With the complexity of the system and the dynamics of the applications, the changes of the access control objects are very large. Hence, these methods may increase the difficulty of the authorization. These access control models all try to protect the resource from the perspective of system. The weakness of these passive security models is that they cannot manage the privilege according to the environment dynamically. Once the subject acquire the privilege, it can use this privilege until it be revoked. It can bring the risk easily.

Compared with the traditional RBAC model, the paper's main contributions are as follows:

1. Introducing of a concept of risk into access control area. This method can ascertain the risk of inter-operations between the different domains in real time through the histories of the interactive events. It is better able to adapt to the distributed, complex, and diverse multi-domain environment.
2. Through adjusting the privilege of the subjects dynamically according to the risk levels of the access events, the functions of the access control system can be changed from the static protect for the resources to the dynamic authorization. The system can detect the environment and the security venture in real time, and the permissions of the subjects are not unchangeable anymore since be authorized. The system can identify the risky permissions automatically and revoke them duly.
3. This method can bring the convenience to the security management. The difference between this dynamic model and the traditional access control models is as follows: The management for the user's permission settings is according to the actual events and historical records. In this way, the permission management is more convenient, and the control to the authorization is more convincing.

3 The Risk of the Inter-operation in Multi-domains

In the traditional model of the trust relationship, trust was usually defined as a Boolean variable, that is to say, in the session of both trust entities, one trust another entirely, or absolutely not, there would never be middle status. For instance, the entity A trusts entity B, but it is hard to tell how much they trust each other. For this reason, we have to quantify their trust. In this section, firstly, we formalize the definitions of the permissions and the operations between the permissions in the multi-domain environment. On this basis, we introduce the description of the trust in multi-domains.

3.1 The Formalization of the Permissions

Definition 1. *Authorization Term. Authorization terms are 2-tuple of the form:* $< object, accessmode >$*, which is denoted as* $< O, A >$ *for short. It is the basic form of the permission. The set of authorization terms is denoted as* P*. We have* $P = \{< O, A >\}$*.*

Definition 2. *Permission Set. Permission set represents all permissions of some subject, which is the set of the authorization terms. We can formulize it as PS.*

For example, we can describe a role r_1's all permission as: $PS(r_1) = \{< file1, +read >, < file2, -write >\}$. That is to say the users, which are assigned to r_1, can read file1 and write file2. The denotation PS_u can also express the permission set of the user u. obviously, if a role r is assigned to a user u, then $PS(u) \supseteq PS(r)$.

In this paper, the denotation $role(u)$ represents the role set, which is assigned to user u. We can define the basic operators of the *PS*. The BNF definition for permission set as follows:

$$PS = PS|PS \cup PS|PS \cap PS|PS - PS|SoD(PS, PS)$$

Where the ∪,∩ and − are the basic operation in set theory, $SoD(PS_1(r), PS_2(r))$ denotes the separation of duties, it returns $PS_1(r)$ or $PS_2(r)$, but it can return the $PS_1(r)$ and $PS_2(r)$ concurrently.

$OS = \{O/D\}$ returns the controlled objects set for a subject. D denotes the object's domain. For instance $OS(r_1) = \{file1/A, file2/A\}$.

3.2 The Role-Mappings Based Trust Degree Between Domains

In a typical multi-domain environment, we partition the domains into external and local domains. The role mapping can be formalized as a 4-tuple: $< r_1, d_1, r_2, d_2 >$, r_1 is a role in domain d_1, $r_2$is a role in domain d_2 respectively, in general, d_1 is the local domain, and d_2 is the external domain. A subject in the local domain can access the objects in the external through the inter-domain mappings. As the mapping exhibits, the permissions of the role r_1 in the domain d_1 is $PS(r_1) = PS(r_1) \cup PS(r_2)$ and $OS(r_1) = OS(r_1) \cup OS(r_2)$.

Trust is one entity assessing to behavior credibility, reliability, integrity and performance of other entity. Trust relationship is such a case: if the subject meets the object's expectation, then the subject is trustable to the object.

Definition 3. *The trust degree denotes the trust extent between the different domains which be formed by the role-mappings. Which is formalized: C (d_1, d_2), depict the trust relationship between the domain d_1 and d_2. As its value range*

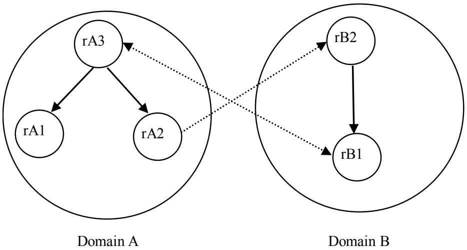

Fig. 1. The role-mappings between two domains

is [0, 1], supposing a role-mapping $< r_1, d_1, r_2, d_1, false >$, $C(d_1, d_2) = 1$ *means the complete trust, that is to say the all permissions of the role* r_2 *in the domain* d_2 *can be inherited by the role* r_1 *in the domain* d_1*; by contraries,* $C(d_1, d_2) = 0$ *means the complete distrust, that is to say the all permissions of the role* r_2 *in the domain* d_2 *are forbidden to be inherited by the role* r_1 *in the domain* d_1*.*

The trust degree between domains is changed according to the inter-operation events. This is denoted by the function as follows:

$$\delta : C \times E \to C \tag{1}$$

Where, E denotes the set of the inter-operation events. In general, if there are role-mappings exist between two domains, for each inter-operation, if the result is successful, the trust degree will be strengthened; by contraries, if the result is failed, it will be weakened.

The following subsection discusses how to found the trust relationship between two domains. In this paper, we consider the trust in the multi-domain environment through their past transaction experiences. Considering the inter-operations between the domain i and j, if the subject in domain i request to access the resources in domain j, according the estimate of each event, if the request is be satisfied, then the estimate from i to j is positive, that is denoted as $tr_k(i, j) = 1$, by contraries, if the estimate is passive, then $tr_k(i, j) = -1$. This paper defines the denotation s_{ij} as the appraisement for the all transactions between the domain i and j: $s_{ij} = \sum(tr_(ij)$. Let's use $sat(i, j)$ to denote the total of the positive appraisement, while the denotation $unsat(i, j)$ is used to denote the total of the passive appraisement. Then,

$$s_{ij} = sat(i, j) - unsat(i, j) \tag{2}$$

For the convenience of the denotation, we mapping the value of the trust value to [0, 1]:

$$C(i, j) = \begin{cases} \frac{s_{ij}}{sat(i,j)+unsat(i,j)} & s_{ij} \geq 0 \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

In this way, every domain maintains local trust degrees of the other domains which the local ever affiliates with. We can use a vector to describe the trust of a local domain to the externals: $T = \{C(i, 1), c(i, 2), \ldots, C(i, n)\}$, n is the number of the external domains.

3.3 The Risk of the Inter-operations in Multi-domain Environment

In general, a domain can maintain the trust vector for the externals domains which it interact with. As mentioned above, in the multi-domain environment, the risk of the inter-operations is up to the trust value of the domains $C(i, j)$, the security level of the operation object O_s, and the safety factor of the access action A_s. The following function defines the risk of the interoperation between the different domains:

Definition 4. $R_i = F(C(i,j), O_s, A_s)$. *The parameter* O_s*denotes the security level of the operation object, the more high level the role, the more security level the objects can be accessed. The* A_s*denotes the security extent of the access operation. In general, the risk of the inter-operations will be increased with the heightener of the security level of the objects. Reversely, it will be decreased with the heightener of the trust between the interrelated domains and the safety factor of the access action.*

The function of the risk for the inter-operations is defined as follows:

$$F(C(i,j), O_s, A_s) = O_s \times (1 - C(i,j)) \times (1 - A_s) \tag{4}$$

By (1), we can see the value of R_i is in the range of [0, 1]. Where, the value 0 denotes no risk, and the value 1 denotes the maximal risk. The following is the algorithm for the security level of all operation objects in the special domain. The basic idea is that the leaf nodes in a role hierarchy only access the objects with the lowest security level in a special domain. That is to say, if the objects can be only accessed by the senior role, their security level is higher in the domain. The detailed algorithm is as follows. The parameter k is the basic security parameter in a special domain. k is an integers. $k \geq 1$.

Algorithm 1. The calculation for the security level of the access control objects.

```
program Obj_Security_level()
begin
1. Searching the role hierarchy, find the deepest leaf nodes.
2. Setting the value of the security level of the objects which can be controlled by the leaf node as k. While, the "visited" flags of the nodes are modified as "already visited".
3. Finding the directly senior up from the leaf node, the security level of the objects which directly under the next senior node is on the basis of an increase for the objects controlled by the directly junior nodes.
4. Searching the all unvisited nodes down from the root node, the security level of the objects which directly under the next junior node is on the basis of a decrease for the objects controlled by the directly senior nodes.
5. Adjusting the security level of all nodes in the role hierarchy. The value of security level of all nodes is divided by the value of the root to be mapped to the range [0, 1]
end.
```

There is a role-mapping $< A_4, A, B_2, B, false >$ exist between the domains in the figure 2. In a moment, a user in the domain A requests the operation "write" to the object O_5 which is in the domain B: $< O_5, write >$. We set the basic security parameter k in this example as 1. Firstly, according to algorithm 1, We set security level of the directly controlled objects of the deepest leaf nodes B_4 , O_7 and O_8, as 1. Followed up, we can get that the security level of the directly controlled objects of B_2 is 2, and the security level of the directly controlled objects of B_1 is 3. By the step 5, we can get the security level of O_5: $\frac{(k+1)}{(k+2)} = \frac{2}{3} = 0.67$.

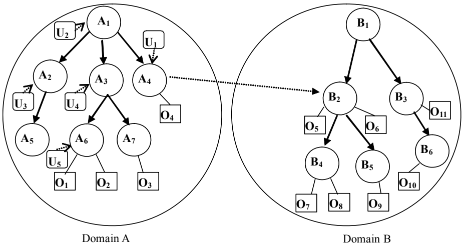

Fig. 2. The inter-operations between domain A and domain B

Table 1. The historical inter-operations between domain A and domain B

Sequence	Subject	Object	Operation	Status
1	U_1	O_5	read	successful
2	U_2	O_6	write	successful
3	U_3	O_7	read	failed
4	U_4	O_5	execute	successful
5	U_5	O_8	copy	failed
6	U_1	O_9	write	successful
7	U_1	O_{10}	read	successful

The safety factor for all access events in this example, which are denoted as *read*, *copy*, *write*, *execute*, is set as $(0.8, 0.6, 0.4, 0.2)$ respectively. We suppose that the inter-operation history between domain A and B is as the table 1 shows. There are seven access events which the subject is in domain A and the object is in domain B. And five of them are successful and two failed. By the above method to compute the trust degree between domain A and B, we have:$\frac{(5-2)}{7} = 0.43$. So, According to (4), we can get the risk of the above 2-tuple $< O_5, write >$ as:

$$R_i(O_s, C(i,j), A) = O_s \times (1 - C(i,j)) \times (1 - A_s) = 0.67 \times (1 - 0.43) \times (1 - 0.4) = 0.23$$

Thus, we can educe the risk rank in the multi-domain environment. In this instance, the risk is divided as 5 levels, which are as $\{potty, little, general, grave, verygrave\}$. The mapping from risk values to the risk ranks is as table 2 shows. This table can be configured by the administrators according to the special context.

Table 2. The mapping from risk values to the risk ranks

Sequence	ranks	values	description
1	I	$0 \leq R_i < 0.2$	potty
2	II	$0.2 \leq R_i < 0.4$	little
3	III	$0.4 \leq R_i < 0.6$	general
4	IV	$0.6 \leq R_i < 0.8$	grave
5	V	$0.8 \leq R_i < 1.0$	very grave

We can conclude from the table 2 that the above operation $< O_5, write >$, a user in the domain A requests the operation "write" to the object O_5 which is in the domain B, it's risk rank is II. This means that the operation $< O_5, write >$ has little risk. It may bring the failure for the operation. In the following sections, we will discuss how to avoid the risk through adjusting the privileges of the subjects.

4 The Risk-Based Dynamic Access-Control Model for Multi-domain

4.1 The Model of MD-R^{2}BAC

The traditional security mechanism is generally designed for static network and closed system. In these systems, the authorizations of the users are determinate, and the relationship between user's privileges and resources are found early. Based this, the protected resource are only be accessed by the authorized users. As these security models are simpler, we can call them traditional security model. But in the multi-domain environment, as the requestor and the provider of the resource can be in the different domains, because there is no absolute trust between these domains, it can not satisfy the all requests of the requestors through the traditional access control mechanism. Further more, the multi-domain environment changes frequently, and the real-time update is also unpredictable, so, the requestor and the provider of the resource may do not know each other. Therefore, the traditional models do not match the multi-domain environment well. This paper proposes a risk-based dynamic access-control model through importing the risk of the event context to the policies of RBAC.

The authorization of the traditional is general denoted as 3-tuple: $< S, O, A >$, where S represents the subject, O represents the object, and A is the set of the actions. If a 3-tuple $< s, o, a >$ exist, that is to say, the subject S can do the operation A on the object O. These 3-tuples are all predefined in the security system, and they are effective of all times. For the privilege constrain to the users, this access control method is passive and negative.

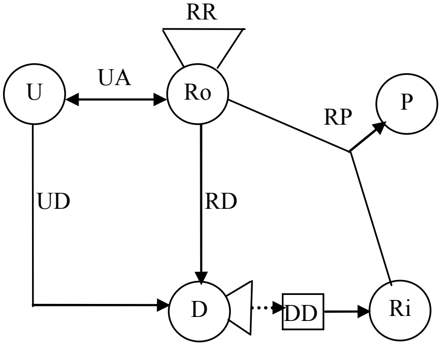

Fig. 3. The model of MD-R^{2}BAC

The following definitions contain some elements in the literature. The relationship between these definitions is as the figure 3.

Definition 5. *The variables and the relationships in this model.*

1. $MD-R^2BAC = (U, Ro, P, D, Ri)$, *where* U *is the set of the users,* Ro *is the set of the roles,* P *is the set of the permissions,* D *is the set of the domains, and* Ri *denotes the set of the risk banks.*
2. *User Assignment. This is a many-to-many relationship between users and roles. It is denoted as* UA, $UA \subseteq U \times Ro$. *This function can be expressed as* $assigned - user(ro) = \{u \in U|(u, ro) \in UA\}$.
3. *Permission Assignment. This is a one-to-many relationship from roles to permissions. And it is a function which from the roles and risk ranks to the permissions. It is denoted as* RP, $Ro \times Ri \rightarrow P$. *The function can be expressed as:* $assigned - permission(ro : Ro, ri : Ri) \rightarrow 2^P$.
4. *Role Relation. This relationship contains the hierarchy and inheriting between the roles. We denote the set of the relationship of roles as* RR, $RR \subseteq R \times R$.
5. *Risk between Domains. This is a mapping from the inter-operation between the domains to the risk rank. It is a function from a special inter-operation event to a certain risk rank. We can denote as* $DR : D \times D \times P' \rightarrow Ri, P' \subseteq P$.
6. *User Hypotaxis. This is a one-to-many relationship from roles to domains. It is denoted as* $RD : R \rightarrow D$.

Each user and role in the model must belong to a special domain, and a user or role can not be subject to two or more domains synchronously. This constrain is defined as follows:

- Constrain 1. Each user in the model must only subordinate to only domain.

$$< u, d_1 >\in UD \cap < u, d_2 >\in UD \rightarrow d_1 = d_2$$

- Constrain 2. Each role in the model must only subordinate to only domain.

$$< r, d_1 >\in RD \cap < r, d_2 >\in RD \rightarrow d_1 = d_2$$

The dynamic distribution of permission in the MD-R^{2}BAC is mainly embodied in relation of *DR*, *RP*. The ration *DR* can acquire the trust degree of two domains through the inter-operation history. All the more, it can acquire the risk rank of an access event according to the security extent of the access operation and the security level of the operation object. Where, the access event between different domains can also be denoted as 6-tuple: ¡S, O, A, D_1, D_2, ri¿. The meaning of the elements is the same as the authorization item. Hence, in the relation *DR*, we have $P' \subseteq P$.

RP is a real-time implementation of the dynamic function. It can adjust the authorization to a subject in a domain duly according to the risk rank of the inter-operation. This paper will detail the authorization and the adjustment in the following sections.

4.2 The Policy and Mechanism of the Access Control in MD-R^{2}BAC Model

MD-R^{2}BAC is an access control model which can be changed with the inter-operation history between different domains. It is a dynamic process that the users acquire the permissions through the roles. In this process, system can adjust the subject's permissions according to the risk rank of its operation. In this way, the access control implementation process can be divided into three steps: privilege distribution, ascertaining the risk rank, and dynamic adjustment of the privilege.

Privilege distribution. The privilege distribution includes that the administrator assigns the roles to user and predefine the permissions of the roles. Referred to above, the users' permissions can be denoted as a 2-tuple :¡ *u, ro¿*, the set is formalized as *ua*(*u*,*ro*). We use *UA(ro)* to denote that assigning the role *ro* to a set of users

$$UA(ro) = \{ua(ui, ro)|ua(ui, ro) \in UA(i = 1, 2, \ldots, n)\}$$

In the multi-domain environment, the privilege usually performs as the power of the subject to access the objects which in the different domain. The basic authorization item can be formalized as the 6-tuple $< s, o, a, d_1, d_2, ri >$,which is denoted as $atomp(s, o, a, d_1, d_2, ri)$. It means that a subject s in the domain d_1 can do the operation a to the object o which is in the domain d_2, and the risk rank of this operation is ri in the current context.

$$RP(ro) = \{atomp(s, o, a, d_1, d_2, ri)|atomp(s, o, a, d_1, d_2, ri) \in P\}$$

Ascertaining the risk rank. The risk rank ri in authorization item is a function of the access history events in the multi-domain environment. We have detail the process of calculation for the risk rank in the third part of this paper. The function which acquires the risk rank of an inter-operation is recorded as *risk_count(s,o,a,*d_1, d_2). It returns the risk rank of a subject s in the domain d_1 do the operation a to the object o which is in the domain d_2

$$Ri = \{ri|ri = risk\_count(s, o, a, d_1, d_2)\}$$

Dynamic adjustment of the privilege. The prominent character of MD-R^{2}BAC is that it can adjust the subject's privilege according to the risk rank of its operation to the objects. We can set a risk threshold RV between two different domains. For the subject which acquire the access permissions to the objects in the other domains through the role-mappings, we can check each authorization items, and revoke the items whose risk rank over the predefined threshold *RV*.

The dynamic adjustment of the privilege mainly reflected in the relation of privilege distribution *RP*. It is a function which from the roles and risk ranks to the permissions.

$$F(Ro, Ri) \rightarrow P, P = \{atomp_1, atomp_2, \ldots, atomp_n\},$$

this is the initial permission set.

$$G(Ro, Ri, P_1) \rightarrow P_2, P_1 \subseteq P, P_2 \subseteq P, P_2 = P - P_1,$$

G is the revoke function.

Return to the example in the third section, suppose that the initial permission set of the role A_4 in the domain A to the objects in the domain B is $PS(A_4) = \{< O_5, write >, < O_6, read >, < O_7, read >, < O_8, write >, < O_9, read >$, we can acquire the risk value of these five authorization items:

risk_count(A_4, O_5*,write,A,B) = Ri(*$O_s(O_5)$*),C(A,B),*A_s*(write)) = 0.23,*the risk rank is II;

risk_count(A_4, O_6*,read,A,B)= Ri(*$O_s(O_6)$*),C(A,B),*A_s*(read))=0.08,* the risk rank is I;

risk_count(A_4, O_7*,read,A,B)= Ri(*$O_s(O_7)$*),C(A,B),*A_s*(read))=0.04,* the risk rank is I;

risk_count(A_4, O_8*,write,A,B)= Ri(*$O_s(O_8)$*),C(A,B),*A_s*(write))=0.11,* the risk rank is I;

risk_count(A_4, O_9*,read,A,B)= Ri(*$O_s(O_9)$*),C(A,B),*A_s*(read))=0.04,* the risk rank is I;

If the predefined threshold RV is set as 0.2, base the policy of dynamic adjustment of the privilege, we will revoke the write permission of the subject $A_4$to the object O_5between domains A and B:

$$PS(A_4) = \{< O_6, read >, < O_7, read >, < O_8, write >, < O_9, read >\}$$

Through the privilege's dynamic adjustment, whether the subject can acquire some privilege lie on the risk rank of the relevant authorization items. The course which the subjects acquire the privilege is a dynamic and frequent process. We can decide on that whether the operation is can be executed base the operations history, the security level of the operation object, and the security extent of the access operation. Hence, the authorization is dynamic which will be adjusted with the time and the hierarchy of the subjects and objects.

4.3 The Security Analyses for the MD-R^{2}BAC

Comparing with the traditional security model, the contribution of the MD-R^{2}BAC is as follows:

1. It is adapted well to the dynamic change in the multi-domain environment. In the MD-R^{2}BAC, the change of operations and objects can bring the change of the authorization. Through the risk rank, this model can reflect the change of the operations and the hierarchy of the access objects. Further more, these changes in this model will not affect the special authorizations. Hence, it can be adapted well to the frequently change of the multi-domain environment.
2. The more security
   MD-R^{2}BAC first imports the concept of risk to access control model, and the ultimately minimal of a subject is up to the conclusion of the access history. The risky permissions will be revoked in the dynamic adjustment

for the authorizations. It will restrict the risky event from the source and advance the success probability of the inter-operations. Through the dynamic adjustment, this model supports these two famous security principles:

- The least of privilege. Through the risk control, the privilege with high risk rank will be revoked in time. When the subject accesses the other domain's objects, it only holds on the relative security privilege.
- The separation of duty. Sometimes, there are some sensitive objects can not be accessed by one subjects at the same time, and two different subjects also do not hope access one object simultaneity. These above can be regarded as the high risky events. These events can be identified by the estimate of the risk rank. And the system can revoke some part of the privileges to implement this security principle.

5 Conclusion and Future Work

In the multi-domain environment, the randomicity exist in the share of the information, the validity of the security mechanism, and the demand of the information exchange between users. For the complexity of the multi-domain environment and the ceaseless evolvement of the information secure share, the traditional access control method can not ensure the absolute security for the exchange of data resource. The traditional security mechanism is always designed for static network or closed system. As lacking the dynamic description of the subjects and objects, the traditional security mechanism hardly to adjust the subjects' privilege base the security status of the system.

Through introducing the concept of risk, this paper proposes a dynamic access control model MD-R^{2}BAC for multi-domain environment based the risk of inter-operations. This model can acquire the risk of the authorization items of the subject's privilege base the operations history, the security level of the operation object, and the security extent of the access operation. And the risky permissions will be revoked in the dynamic adjustment for the authorizations. The security analyses for the MD-R^{2}BAC indicate that this model can reduce the risk and hidden trouble for the information exchange in the multi-domain environment, and advance the security of the system obviously.

In this paper, we only discuss the risk for a single access operation in the multi-domain environment. When an attacker who combines multiple low risk operations into a new operation, how to assess the risk for the new multiple operation is a problem being worth paying close attention to. It will be our future works.

References

1. Sonntag, M., Hrmanseder, R.: Mobile agent security based on payment. Operating Systems Review 34(4), 48–55 (2000)
2. Kwok, Y.K., Song, S., Hwang, K.: Selfish grid computing: Game-theoretic modeling and nas performance results cardiff. In: CCGrid-2005. Proceedings of the International Symposium on Cluster Computing and the Grid, Cardiff, UK, May, pp. 9–12 (2005)

3. IEEE (ed.): IEEE Security and Privacy. Economics of Information Security, vol. 3. IEEE Computer Society, Los Alamitos (2005)
4. Grandison, T., Sloman, M.: A Survey of Trust in Internet Applications. IEEE Communications Surveys 3(4), 2–16 (2000)
5. Mayer, R.C., Davis, J.H., Schoorman, F.D.: An Integrative Model of Organizational Trust. Academy of Management Review (20), 75–91 (1995)
6. Jarvenpaa, S.L., Leidner, D.E.: Communication and trust in global virtual teams. Organization Science 10(6), 791–815 (1999)
7. Sandhu, R., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role Based Access Control Models. Computer 29(2) (1996)
8. Moyer, M.J., Covington, M.J., Ahamad, M.: Generalized role-based access control for securing future applications. In: NISSC 2000. 23rd National Information Systems Security Conference, Baltimore, Md, USA (October 2000)
9. Zhang, G., Parashar, M.: Context-Aware Dynamic Access Control for Pervasive Applications. In: Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2004), Western MultiConference (WMC), San Diego, CA, USA (January 2004)
10. Dimmock, N., Belokosztolszki, A., Eyers, D., Bacon, J., Moody, K.: Using Trust and Risk in Role-Based Access Control Policies. In: Proceedings of Symposium on Access Control Models and Technologies (2004)
11. Grandison, T., Sloman, M.: A Survey of Trust in Internet Applications. IEEE Communications Surveys 3(4), 2–16 (2000)
12. Blaze, M., Feigenbaum, J., Lacy, J.: Decentralized trust management. In: Proc. IEEE Conference on Security and Privacy. AT&T (May 1996)
13. Li, N., Mitchell, J.C., Winsborough, W.H.: Design of a role-based trust management framework. In: 2002 IEEE Symposium on Security and Privacy, pp. 114–131. IEEE, Los Alamitos (2002)
14. Teh-Ming, W., Fidelis, Y.: A policy-driven trust management framework. In: Nixon, P., Terzis, S. (eds.) iTrust 2003. LNCS, vol. 2692, Springer, Heidelberg (2003)
15. Dimmock, N., Belokosztolszki, A., Eyers, D., et al.: Using Trust and Risk in Role based Access Control Policies. In: SACMAT 2004, New York, USA, June 2-4, 2004 (2004)