WUJNS
Wuhan University Journal of Natural Sciences

Vol. 11 No. 6 2006 1688-1692

Article ID:1007-1202(2006)06-1688-05

Centralized Role-Based Access Control for Federated Multi-Domain Environments

□ YU Guangcan[1], LU Zhengding[1†], LI Ruixuan[1], MUDAR Sarem[2]

1. College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, Hubei, China;

2. School of Software Engineering, Huazhong University of Science and Technology, Wuhan 430074, Hubei, China

Abstract: The secure interaction among multiple security domains is a major concern. In this paper, we highlight the issues of secure interoperability among multiple security domains operating under the widely accepted Role Based Access Control (RBAC) model. We propose a model called CRBAC that easily establishes a global policy for roles mapping among multiple security domains. Our model is based on an extension of the RBAC model. Also, multiple security domains were composed to one abstract security domain. Also roles in the multiple domains are translated to permissions of roles in the abstract security domain. These permissions keep theirs hierarchies. The roles in the abstract security domain implement roles mapping among the multiple security domains. Then, authorized users of any security domain can transparently access resources in the multiple domains.

Key words: RBAC(role based access control); federated; multi-domain

CLC number: TP 305

0 Introduction

Our model, which called Centralized role-based access control (CRBAC) model, was motivated by the problem of controlling access to resources in federation environments. In a federation environment, multiple organizations or entities rely on a third party to administer trust relationships and work together to achieve a common goal. Security problem is magnified in the federation environment where distributed multiple organizations, each employing its own security policy, interoperate with each other [1,2]. We use the term security domain to refer to the organization employing its own security policy, and assume that the security policy is role-Based access control (RBAC) model[3,4].

Let's consider the scenario when three security domains A, B and C in the federation environment desire to interoperate securely. The three security domains respectively manage and control specific resources. If a user wants to achieve a task which needs to access resources distributed in the three security domains, he (she) must be authenticated three times in the three security domains, and in each security domain he(she) should be assigned to some roles respectively in order to obtain the permissions of accessing particular resources. Let the number of security domains is n, the similar operations must be done n times. This makes it very difficult also for users to achieve their tasks and for resources in security domains to be properly controlled.

In order to solve the problem, we propose a centralized role-based access control model which is based on an extension

Received date: 2006-05-15

Foundation item: Supported by the National Natural Science Foundation of China(60403027), the Natural Science Foundation of Hubei Province(2005ABA258) and the Open Foundation of State Key Laboratory of Software Engineering(SKLSE05-07)

Biography: YU Guangcan(1974-), male, Ph.D. candidate, research direction: distributed system security. E-mail:xgygcan@tom.com

† To whom correspondence should be addressed. E-mail: zdlu@hust.edu.cn

of the RBAC model. In our models, multiple security domains were composed to one abstract security domain which implements roles mapping among different security domains. Then, users can transparently access resources distributed in different security domains. We name the abstract security domain as the composite domain, and we also name the multiple security domains as the basic domain.

1 Basic Concepts and Principle of CRBAC Model

In practice, if a basic domain wants to share its own resources and attains the capability of accessing resources of other basic domains, it provides its own roles to the composite domain. Of course, basic domains can provide part or all of their roles to the composite domain, according to security policies of different basic domains. According to the demands of all basic domains, a global mapping policy is needed. The global mapping policy sets up relations among roles of different basic domains. Users can access resources distributed in multiple basic domains to achieve special tasks. The global mapping policy is used to build a composite domain. In the composite domain, elements in permissions set are made up of roles provided by different basic domains. In other words, permissions assigned to roles of the composite domain are roles coming from different basic domains.

In the paper, we call the roles, coming from basic domains and treated as permissions which assigned to a role *r* of the composite domain, as sub-roles of role *r*. So, roles of the composite domain implement the function of roles mapping among multiple basic domains. For example, Figure 1 gives the role hierarchy relations of three basic domains *A*, *B* and *C*. The three basic domains make up the composite domain *M*. Suppose that the three basic domains provide all of their roles to the composite domain in order to implement the maximal interoperability, so the permissions set of the composite domain *M* is $\{A_1, A_2, A_3, A_4, B_1, B_2, B_3, B_4, C_1, C_2, C_3\}$. If permissions A_1, B_2 and C_1 are assigned to role *r* of *M*, then among roles A_1, B_2 and C_1 coming from basic domains *A*, *B* and *C* respectively exist mapping relation. The mapping relation is inheritable. Because *r* of *M* has defined mapping relation among roles A_1, B_2 and C_1, then roles A_2, A_3 and A_4 which dominate role A_1 in the basic domain *A* can be mapped to roles B_2 and C_1. Similarly, roles B_3 and B_4 of *B* can be mapped to roles A_1 and C_1. Also, and role C_3 of *C* can be mapped to roles A_1 and B_2. But these mapping relations aren't transitive. If permissions A_1 and B_2 are assigned to role r_1 of *M*, thus r_1 defines a mapping relation between Roles A_1 and B_2. If permissions A_1 and C_1 are assigned to role r_2 of *M*, then r_2 defines a mapping relation between A_1 and C_1. Because mapping relations aren't transitive, there is not any mapping relation between roles C_1 and B_2.

Permissions set of the composite domain is made up of roles of basic domains, and there are hierarchy relations among roles of basic domains, so there also is a hierarchy relation among permissions of the composite domain. This hierarchy relation is defined as PH. Permissions hierarchy relation of the composite domain is decided by roles hierarchy relations of basic domains. Figure 1 also shows permissions hierarchy relation of the composite domain *M*. Let's suppose that permissions A_1, B_2 and C_1 are assigned to role *r* of *M*. Figure 2 illustrates the relation between the composite domain and basic domains.

The new characteristic of permissions in the composite domain brings forward new demands on permission-role assigning. In the following, we present some of rules in our CRBAC model.

Rule 1 The amount of permissions assigned to a role must be two or more. The role which only has one permis-

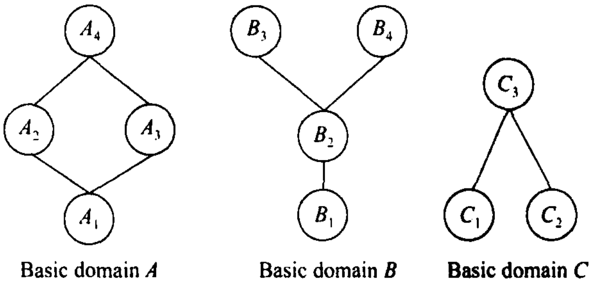

Fig. 1 Role hierarchies of basic domains

Note: Permission hierarchies of the composite domain

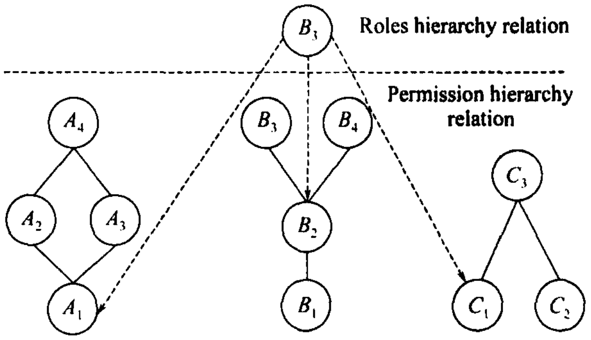

Fig. 2 The composite domain M

sion is meaningless because it can not implement the function of mapping among roles of different basic domains.

Rule 2 The sub-roles of any role of the composite domain must come from different basic domains. In other words, no more than two sub-roles come from the same basic domain. This rule is easily understood because there is no mapping relation among roles of the same basic domain. For example, the sub-roles of role r can be $\{A_1, B_2, C_1\}$, and can also be $\{A_1, B_2\}$, but $\{A_1, A_2, B_2\}$ is not allowed. The mapping relation between roles A_1 and A_2 is meaningless.

Rule 3 If sub-roles of multiple roles of the composite domain contain two or more roles which come from the same basic domains, the roles of different basic domains have the similar hierarchy relation. For example, the sub-roles of two roles r_1 and r_2 of the composite domain are $\{A_m, B_p\}$ and $\{A_n, B_q\}$ respectively, A_m and A_n come from the basic domain A, B_p and B_q come from B, roles A_m and A_n of the basic domain A have the similar hierarchy relation as roles B_p and B_q of the basic domain B. The rule prevents the following situation from happening: Sub-roles of r_1 is $\{A_2, B_3\}$, and sub-roles of r_2 is $\{A_4, B_4\}$. Role A_4 of the basic domain A is explicitly mapped to role B_4 of the basic domain B by role r_2 of the composite domain, and A_4 is implicitly mapped to B_3 inherent from A_2. So role A_4 can be mapped to both B_3 and B_4, thus may break the security policy of the basic domain B and is not allowed. This rule also prevents the following situation: Sub-roles of r_1 is $\{A_2, B_1\}$, and sub-role of r_2 is $\{A_1, B_2\}$. This is obviously illogical.

Rule 4: The sub-roles of roles in the composite domain can not contain each other. This means the following situation can not happen, sub-roles of r_1 and r_2 are $\{A_1, B_2\}$ and $\{A_1, B_2, C_1\}$ respectively, $\{A_1, B_2\} \subseteq \{A_1, B_2, C_1\}$. Because mapping relation among A_1, B_2 and C_1 have been set up by role r_2 already, the mapping relation between A_1 and B_2 set up by role r_1 is repeatedly built.

Users of the composite domain are made up of users of basic domains. The composite domain is an abstract security domain. It has no users, and doesn't have the responsibility of authenticating users' identity. Basic domains authenticate their own users' identity and maintain their users' information. In the composite domain, where sub-roles are assigned to roles as permissions, uses assigned to roles are made up of the users assigned to the sub-roles come from different basic domains. Let us suppose that the sub-roles of role r_1 of the composite domain are $\{B_1, A_2\}$, and users sets{Rose, Tom}and{Jerry, Marry}are assigned to roles B_1 and A_2 of basic domains B and A respectively. Then users set{Rose, Tom, Jerry, Marry}are implicitly assigned to role r_1.

The hierarchy relation among roles of the composite domain is determined by the hierarchy relation among permissions. In other words, when permissions are assigned to roles, the hierarchy relation among roles is determined following two rules.

Rule 5: If every sub-role of one role is dominated by a sub-role of another role, we think that there exists a hierarchy relation between the two roles, and the latter dominates the former. Suppose that sub-roles of r_1 are $\{A_1, B_2\}$, sub-roles of r_2 are $\{A_2, B_2, C_1\}$, according to Fig. 1, $A_2 \geq A_1$ and $B_3 \geq B_2$, so $r_2 > r_1$.

Rule 6: If the relation rule 5 defined don't exist between two roles, and then the two roles are not comparable. And there isn't any role hierarchy relation between them. Suppose that sub-roles of r_1 are $\{A_1, B_2\}$, sub-roles of r_2 are $\{A_1, C_1\}$, so r_1 and r_2 are not comparable.

2 The CRBAC Model Definition

The CRBAC model is based on an extension of the RBAC model. And the RBAC model is a family of reference models, composed of base model RBAC_0, role hierarchies model RBAC_1, constraints model RBAC_2 and consolidate model RBAC_3, and RBAC_0, RBAC_1 and RBAC_2 can be treated as specializations of RBAC_3. In fact, we extend RBAC_3 to the CRBAC model.

Hypothesis: There are n basic domains D_i $(i \in [1, n])$, all basic domains adopt RBAC model as their access control policy, corresponding role sets are DR_i $(i \in [1, n])$.

Definition 1 CRBAC model is made up of the following components:

U(Users), R(Roles), S(Sessions).

P(Permissions), $P \subseteq \bigcup_{i=1}^{n} \mathrm{DR}_i$, DR_i is a role set of the basic domain D_i.

PH(permission hierarchy), $\mathrm{PH} \subseteq \bigcup_{i=1}^{n} \mathrm{DR}_i H$, $\mathrm{DR}_i H \subseteq \mathrm{DR}_i \times \mathrm{DR}_i$, is a partial order on DR_i, corresponding to role hierarchy RH of RBAC_1, so PH is also a partial order on P, written as $\geq$.

$\mathrm{PA} \subseteq P \times R$, a many to many permission to role assignment relation, the assignment relation must satisfy the following conditions:

$\forall r \in R$, # $P_r > 1$, P_r is permission set of role r,

$\forall p_i \in P$ and $p_i \in \mathrm{DR}_m$, DR_m is the role set of the basic domain which p_i comes from, $\forall r \in R$, if $p_i \in P_r$, P_r is the permission set of role r, there does not exist a permission $p_j \in P_r$ and $p_j \in \mathrm{DR}_m$, $i \neq j$.

$\forall r_m, r_n \in R$, P_{r_m}, P_{r_n} are permission sets of r_m, r_n respectively. if $\exists\, p_{mx} \in P_{r_m}$, $p_{nx} \in P_{r_n}$, p_{mx}, $p_{nx} \in \mathrm{DR}_x$, and $\exists\, p_{my} \in P_{r_m}$, $p_{ny} \in P_{r_n}$, p_{my}, $p_{ny} \in \mathrm{DR}_y$, DR_x and DR_y are any two role sets of basic domains, then partial order between p_{mx} and p_{nx} is the same as partial order between p_{my} and p_{ny}.

$\forall r_m, r_n \in R$, $P_{r_m} \not\subset P_{r_n}$, P_{r_m} and P_{r_n} are permission sets of role r_m and r_n respectively.

$\mathrm{UA} \subseteq U \times R$, a many to many user to role assignment relation.

$\mathrm{RH} \subseteq R \times R$, is a partial order on R called role hierarchy, written as $\geq$, the partial order is defined by the following conditions:

$\forall p_i \in P_{r_m}$, $\exists\, p_j \in P_{r_n}$, P_{r_m} and P_{r_n} are permission sets of role r_m and r_n respectively, $p_j \geq p_i$, then $r_n \geq r_m$.

User: $S \rightarrow U$, a function mapping each session s_i to the single user user(s_i).

Roles: $S \rightarrow 2^R$, a function mapping each session s_i to a set of roles roles(s_i), and roles$(s_i) \subseteq \{\exists\, r' \geq r) \mid [((\text{user}(s_i), r') \in \text{UA}]\}$, and session s_i possess the permissions $\bigcup_{r \in \text{roles}(s_i)} \{p \mid \exists\, r'' < r)[(p, r'') \in \text{PA}]\}$.

Constraints: Our CRBAC model inherits all constraints of RBAC model[3,4]. Constraints of basic domains are prerequisite constraints of the composite domain. That means constraints of the composite domain can not break constraints of basic domains, this requires that roles of basic domains together with corresponding constraints are submitted to the composite domain. So, CRBAC model contains two portions of constrains: one portion corresponds constraints of basic domains, the other defines new global constrains. The definition of the latter is the same as RBAC.

3 Analysis and Comparison with Related Models

In this section, CRBAC model will be analyzed in detail and compared with related models.

Some researches have been done with respect to secure interoperability between different security domains. In Ref. [5] and Ref. [6], a multi-domain interoperable access control model called IRBAC2000 has been proposed. The role translation policies which transfer roles of foreign domains to roles of the local domain include default policy, explicit policy and partially explicit policy. Multi-domain interoperability was achieved through role mapping. When a user of one security domain tries to access resources of other security domains, one domain boundary must be crossed. This was called domain crossing. Multiple domain crossings can be a security hazard because it may allow infiltration and covert promotion. In IRBAC2000 model, these problems are not properly solved.

XML-based access-control policy specification language (X-RBAC)[7-9] extends RBAC model and provides access control at the element-level granularity of XML sources. A framework is proposed which describes security policy mapping among multiple security domains. But it does not propose a concrete method to map one security policy to another. In other words, X-RBAC model only provides a container which contains security policy mapping among multiple security domains, but how security policy of one security domain is mapped to another is not provided.

Like IRBAC2000, the distributed role-based access control for dynamic coalition environments (DRBAC)[10], is also a multi-domain interoperable access control model. The difference is that a credible center is available in CRBAC, IRBAC2000 and X-RBAC, but the credible center isn't available in DRBAC. The characteristic in dynamic coalition environments is that multiple organizations want to implement interoperability, but the credible authorization center is not acquirable. The roles defined in one security domain can be transitively assigned to roles of other domains. DRBAC model mainly solves complicated credible and monitor problem.

X-RBAC model proposes a framework to describe security policy mapping among multiple domains. The framework can be applied to both loosely coupled and federated multi-domain environments. In fact, the CRBAC model is proposed for federated multi-domain environments, and the IRBAC2000 and DRBAC models are suitable for loosely coupled multi-domain environments. If the four models are assimilated to UML element, the relation of the four models can be expressed by Fig. 3. We may pay special attention that X-RBAC proposes a descriptive framework but if does not propose a concrete method to map one security policy to another.

After the composite model is built according to CR-

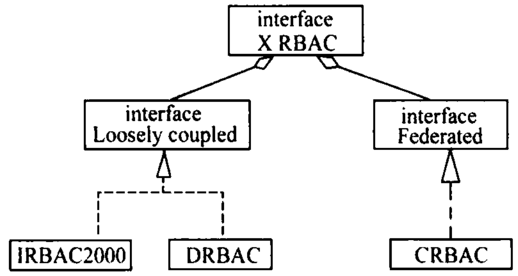

Fig. 3 Relation among X-RBAC IRBAC DRBAC CRBAC model

BAC model, when users of basic domains want to access resources distributed in other domains, what they need to do is to active proper roles of the composite domain. All interoperable operations are accomplished through roles of the composite domain. Possible fraudulent operations of basic domains are prevented. The infiltration and covert promotion mentioned above are also prevented. And most importantly, interoperability of any number of basic domains is possible.

4 Conclusion

In this paper, we proposed a new model in order to achieve interoperability among multiple basic domains. The model provides a mechanism which lead users transparently access resources that are distributed in different basic domains. The most importantly, the model itself is compatible with RBAC model and can be instantiated based on the existing security system which has already implemented RBAC model. The CRBAC model is suitable to be applied to federated multi-domain environments.

As a future work, we've planed to continue our researches on security context between basic domains and the composite domain. The CRBAC model is highly centralized. And the composite domain apparently becomes the bottleneck of the integration system, dispersing the functions of the composite domain remains to be researched.

References

[1] Joshi J, Ghafoor A, Aref W, *et al*. Digital Government Security Infrastructure Design Challenges[J]. *IEEE Computer*, 2001, **34**(2): 66-72.

[2] Gong L, Qian X. Computational Issues in Secure Interoperation[J]. *IEEE Transaction on Software and Engineering*, 1996, **22**(1):43-52.

[3] Sandhu R, Coyne E, Feinstein H, *et al*. Role Based Access Control Models[J]. *IEEE Computer*,1996, **29**(2):870-881.

[4] Ferraiolo D, Sandhu R, Gavrila S, *et al*. The NIST Model for Role-Based Access Control: Towards a Unified Standard [J]. *ACM Transactions on Information and System Security*, 2001, **4**(3):224-274.

[5] Kapadia A, Al-Muhtadi J, Campbell R, *et al*. *IRBAC2000: Secure Interoperability Using Dynamic Role Translation*, *Technical Report UIUCDCS-R*-200-2162 [R]. Urbana-Champaign:University of Illinois, 2000.

[6] Al-Muhtadi J, Kapadia A, Campbell R, *et al*. *A-IRBAC* 2000 *Model: Administrative Interoperable Role-Based Access Control, Technical Report UIUCDCS* [R]. Urbana-Champaign:University of Illinois, 2000.

[7] James B, Rafae B, Elisa B, *et al*. Access Control Language for Multi-Domain Environments[J]. *IEEE Internet Computing*, 2004, **8**(6):40-50.

[8] Bhatti R, Joshi J, Bertino E, *et al*. Access Control in Dynamic XML-Based Web-Services with XRBAC[C]// *Proceedings of the First International Conference on Web Services(ICWS)*. Las Vegas:IEEE Press, 2003:194-201.

[9] Vuong N N, Smith G S, Deng Y. Managing Security Policies in a Distributed Environment Using eXtensible Markup Language (XML) [C]// *Symposium on Applied Computing*, Las Vegas, March 7-9, 2001:405-411.

[10] Freudenthal E, Pesin T, Port L, *et al*. *dRBAC: Distributed Role-based Access Control for Dynamic Coalition Environments*, *Technical Report TR*2001-819[R]. New York: New York University, 2001.

□