Administrative Usage Control Model for Secure Interoperability*

HONG Fan, CUI Yongquan
College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, 430074, hubei, China
Yqcui1977@sohu.com

Abstract

The secure interaction between two or more administrative domains is a major concern. IRBAC2000 is a model that quickly establishes a flexible policy for dynamic role translation from foreign domains to local. A-IRBAC2000 mode utilizes RBAC to manage dynamic role translation between foreign and local domains. We will see that these mechanisms have significant shortcomings. We propose an improved Administrative Usage Control model named AUCON to overcome the weakness of previous models. AUCON provides administrates user-role assignment for local and foreign domain with unified method. It provides flexible enough mechanism to distinguish users of foreign and local domain and can enforce more strict control for foreign user. While retaining the advantage of traditional RBAC model, AUCON model is being implemented in experiment system.

1. Introduction

With today's revolutionary innovations in information technology and their impact on our society we are encountering a series of new problems on security and privacy issues. Secure interoperability between two or more domains is one of these areas and has been considered as a major issue. Kapidia etal proposed a model named IRBAC2000 that quickly establishes a security context for dynamic role translation. This mode can set up associations between the role hierarchies of the local and foreign domains [1-2].A-IRBAC2000 model utilizes Role-Based Access Control (RBAC) to management dynamic role translation between the local role hierarchies and foreign hierarchies [3].Distributed Role-Based Access Control (dRBAC) is a scalable decentralized trust-management and access-control mechanism for systems that span multiple administrative domains [4].However these models have significant shortcomings. Trust users from foreign domain can bring security risk to local domain. These models are lack of flexible mechanism to enforce more strict control for foreign users and roles.

We propose an improved Administrative Usage Control model named AUCON to overcome the weakness of previous models. This model provides administrates user-role assignment for local and foreign domain with unified formulation method. It provides flexible enough mechanism to enforce more strict control for foreign users, while retaining the advantage of traditional RBAC model.

The rest of this paper is organized as follows. Section 2 presents our motivation; we briefly review previous models and describe its weakness. Section 3 presents the AUCON model. We describe the AUCON model in formulation method and show the advantages of this model. Section 4 presents our experiment system to implement the AUCON model. Finally we get our conclusions.

2. Motivation and Review

2.1. IRBAC2000 model and A-IRBAC2000 model

For domains that utilize RBAC, kapadia etal proposed the IRBAC2000 model, which can be used to set up associations between the role hierarchies of the local and foreign domains. These associations result in

* Supported by the National Natural Science Foundation under Grant No. 60403027

HONG Fan was born in 1942. She is a professor and doctoral supervisor at the Information Security Lab. Her researches areas are access control theory and application. **CUI Yongquan** was born in 1977. He is a Ph.D. candidate at the Information Security Lab, the Huazhong University of Science and Technology. His current research interests include access control and network security.

Proceedings of the Seventh International Conference on
Parallel and Distributed Computing,Applications and Technologies (PDCAT'06)
0-7695-2736-1/06 $20.00 © 2006 IEEE

a combined partial ordering of the role hierarchies, which can be used to make meaningful access control decisions for secure interoperability.

Inspired by ARBAC model, A-IRBAC2000 model utilizes RBAC to manage dynamic role translation between the local hierarchies and foreign hierarchies, by means of defining prerequisite and role range, such as can_assignT(PSO1,In_domain(R1) ∧ ¬ mapped_to(QE1),[PE1,PE1]) [5-6].

There are some security risks in these models. If the foreign role is mapped into some one ocal role, this model provides few mechanisms to restrict the foreign user. In A-IRBAC2000 model the prerequisite condition has significant weakness. For example, GuestR1 is in domain R1 and is not mapped into QE1. Which means GuestR1 is satisfied with prerequisite. However, it's well known that the guest role has least privilege and to translate GuestR1 into the local role PE1 is prohibited.

2.2. UCON Model

UCON model encompasses traditional access control, trust management and digital rights management and goes beyond them in its scope. By unifying these areas, which offers a promising approach for the next generation of access control. A usage decision in UCON is made by polices of authorizations, obligations, and conditions. Authorizations are predicates based on subject and/or object attributes, such as role name, identity, security classification or clearance, etc. Obligations are preformed by subjects or by the system. Conditions are system and environment restrictions such as system load, network bandwidth, subject location, access time, etc [7-10].

3. Administrative Usage Control Model

3.1. Central conception of AUCON

In order to access object, user has to become a member of relevant role by the user-role assignment. The Authorization rules are a set of decision factors used to check whether a secure administrator is satisfied to execute user-role assignment. Whereas the obligations are mandatory requirements that a obligation subject has to perform before the user-role assignment is promised.

After one user is assigned to be a regular role, he can propose request to access certain rights on object. As figure 1 show, the Authorization component will evaluate subject attributes, object attributes and requested rights and decide the access request are promised not only by the authorization rules, but also by the Conditions component.

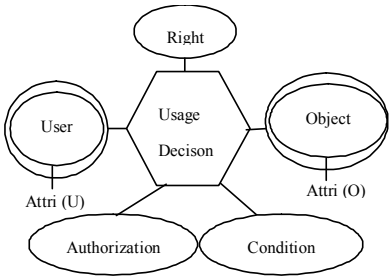

Figure 1. Access control of AUCON

3.2. AUCON Model Component

Administrative Usage Control Model has a set of component and is defined as follows.

Define1: the set of AUCON model is defined as follows.

AR is a partially ordered set of administrative roles with dominance relation ≥.

G is a set of actions to grant a role to a user.

U is a set of users.

R is a partially ordered set of regular roles with dominance relation ≥.

P is a set of collection of objects and rights and denote (o, r).

D is a set of administrative domain.

O is a set of objects.

Define 2:the functional mapping of AUCON model is defined as follows:

sAR:S->2AR, a functional mapping of subject to a set of AR.

actAR:S->2AR ,a functional mapping of subject to an active set of AR in a session.

sRan:S->2R, a functional mapping of subject to a set of regular role range.

gU:G->U, a functional mapping of grant to a user who is going to be a member of regular role.

gR:G->R, a functional mapping of grant to a role.

uDom:U->D, a functional mapping of user to an administrative domain.

uR:U->2R, a functional mapping of user to a set of regular role.

actR：U->2R , a functional mapping of user to an active set of role in a session.

pR:P->2R, a functional mapping of permission to a set of regular role.

Define 3: the attributes of subject and object are defined as follows.

Atrr（S）={sAR，actAR, sRan}

Attr（G）={gU，gR}

Attr（V）={vU，vR}

Attr（U）={uDom，actR, uR}

Attr（O）={pR}

Define 4：the authorization rules and obligations of AUCON model is defined as follows.

allowed（s,e,g）=>actAR(s) ≠ ϕ ∧ actAR(s) ∈ sAR(s)∧gR(g) ∈sRan(s)

The authorization rules means that the actively role set of subject is can ‘t be empty and the subject must active at least one administrative role and the role of grant must belongs to the administrative role range of the subject.

getPreOBL(s,e,g)= {(u,agree,x ∧ ¬ y)} u=gU(g),r=gR(g).

allowed(s,e,g)=》preFulfilled(getPreOBL(s,e,g))

postUpdate(uRA（u）): uRA（u）= uRA（u）∪ {r}

In the obligation component, the obligation subject is the user that is relevant to the user-role assignment. The user must be satisfied with the prediction condition, such as “$x \wedge \neg y$”. The prediction condition is the same as ARBAC model. For example, the prediction condition “$x \wedge \neg y$” means that the user must belongs to the role x explicitly or implicitly and the user can’t be any member of the role y. If the user-role assignment is succeeded, the role r will be joined into the role set of the user u.

Define5: the authorization process of access control to user is defined as follow.

P={(o,r)}

uR(u)={role| x,xR1|—> role }, if uDom(u)=’R1’

Role’ = {role| r1 ∈uR(u), r2 ∈pR((o,r)),r1 ≥role ≥r2 }

Role’’ = {role| r1 ∈actR(u), r2 ∈pR((o,r)),r1 ≥ role ≥r2 }

Allowed(u,r,o)=>Role’ ≠ ϕ

PreUpdate(actR(u)):

$$actR(u) = \begin{cases} actR(u) & \text{if } Role'' \neq \phi \\ actR(u) \cup \lambda\,(Role') & \text{if } Role'' = \phi \end{cases}$$

Where λis a none-deterministic selection function of an element from a set.

In this model, role can be assigned to the attributes of subjects and attributes of objects with rights. If the subject s is permitted to access the object, the subject has at least one role that can dominate some one role in the role set of the object o with the right r. If the role set Role’’ is empty, system will chose a role which is in the role set of user so as to dominate some one role in the role set of the object o with right r.

Condition（u,r,o）= CN1∩CN2 …∩CNn

CNi = <CT><OP><Value>

Where CNi denotes some one factor to be checked. CT means some constraint condition to be controlled by system. OP might be a logical operator which is in the set {≠,>,<,≥,≤,=} or is defined by user. <Value> is the fixed value, which is beforehand set by system administrator according to the security policy.

For example, we can define a condition as follow.

Conditions（u,r,o）=(Time>8:00 ∩Time<18:00) ∩(Security Level≥High) if uDom(u)=’R1’

This condition means that the user r that comes from the domain R1 can access the object o when time is between 8:00 and 18:00 and where the security level is not less than ‘high’. Because the condition component encompasses multiple factors and any factor can be added or deleted freely according to the system need. The model can provide flexible enough method to enforce more strict constraint to the foreign users than the local ones.

4. Framework of prototype system to implement AUCON model

We have already carried AUCON model into execution. The framework of prototype system is described in figure 2.

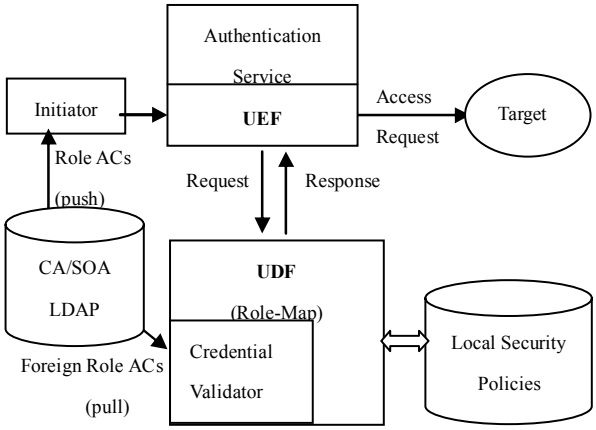

Figure 2. Framework of experiment system to implement AUCON

As shown in Figure 2, once the foreign user has obtained the Role Attribute Certification (AC), the user can contact the desired local security domain, which includes the desire the resource. The local Reference Monitor will check the access request(s, r, o, ac) and make access decision for the access request according to the local security policies database and dynamic contextual information.

In architecture point of view, the critical issue in enforcing AUCON model is the local reference monitor. The reference monitor associates usage control rules and detail contextual information for control of access to digital objects. ISO has published a standard for access control framework that defines reference monitor and trusted computing base. According to the standard, reference monitor consists

of two facilities Usage control Decision Facility (UDF) and Usage control Enforcement Facility (UEF).
UEF receives the access request from subject and sends appropriate answer information to subject. UEF sends the access request to UDF and asks UDF whether the request is allowed or not.

Credential Validation Module in UDF will check the validation of the relative role ACs through communication with the LDAP and translate the foreign role into the local role set. UDF includes authorization module and condition decision module. Authorization module will perform the check function just like traditional authorization process. It utilizes the role set of subject and object's attributes and local security rules and decides whether the request is permitted or not. Condition module checks whether condition factors are satisfied before and on going the request usage has been performed and the check result will influence whether the request is accepted or not.

5. Conclusion

In this paper we have introduced an improved model called administrative usage control for controlling security interoperability between two or multiple domains. AUCON model can overcome the weakness of prerequisite condition In A-IRBAC2000 model and provide unified user-role assignment for local and foreign user in formal method, which provides more convenience for system management. This model introduces obligations component that can enrich and refine the access control discipline in its definition and scope. Condition factors in AUCON model can be updated flexibly according to the security policy by administrator. We have already carried AUCON model into execution in an experiment system and achieved well purpose.

6. References

[1] Apu Kapadia, Jalal Al-Muhtadi, R.Campbell, D. Mickunas, "IRBAC2000: Secure Interoperability Using Dynamic Role Translation", *The 1st International Conference on Internet Computing*, June 26th - 29th, 2000,Monte Carlo Resort, Las Vegas,Nevada, USA.

[2] R. Campbell, Z. Liu, D. Mickunas, P. Naldurg, and S. Yi. "Seraphism:Dynamic interoperable security architecture for active networks", *IEEE OPENARCH 2000*, Tel-Aviv, March 2000.

[3] Jalal Al-Muhtadi, Apu Kapadia, Roy H. Campbell, and M. Dennis Mickunas. "A-IRBAC 2000 Model: Administrative Interoperable Role-Based Access Control". *Technical Report UIUC-DCS-R-2000-2163*.http://choices.cs.uiuc.edu/~almuhtad/

[4] Eric Freudenthal,et al. "dRBAC:Distributed Role-based Access Control for Dynamic Coalition Environments[EB/OL]". http://www.cs.nyu.edu/vijayk/papers/drbac-icdcs02.pdf,2002-06

[5] R. Sandhu, Edward J Coyne, Hal L. Feinstein, et al. "Role-Based Access Control Models". *IEEE Computer*, 1996,29(11), pp 38-47.

[6] Ravi Sandhu, Venkata Bhamidipati, and Qamar Munawer. "The ARBAC Model for Role-Based Administration of Roles", *ACM Transactions on Information and System Security*, 1999.2(1):105-135.

[7] Jaehong Park and Ravi Sandhu. "Towards usage control models: beyond traditional access control". *In Proceedings of the seventh ACM symposium on Access control models and technologies*, ACM Press. pp 57–64.

[8] R. Sandhu and J. Park, "Usage control: A vision for next generation access control". *In Proceedings of The 2nd International Workshop on Mathematical Methods*, Models and Architectures for Computer Networks Security, pp 17–31.

[9] J. Park and R. Sandhu. "The $UCON_{ABC}$ Usage Control Model", *ACM Transactions on Information and Systems Security*, Feb, 2004. 7(1): 128–174.

[10] XinWen Zhang, R.Sandhu. "Safety Analysis of Usage Control Authorization Models".*ASIACCS'06* March 21-24, 2006, Taipei,Taiwan.

7. Copyright forms and reprint orders

I will fill out and submit the Copyright Release Form to access the Electronic Copyright Form (ECF) system.