A New Research of Delegation Agent Model Based On RBAC

Ping Zhang
School of Mathematics and Statistics in Henan University of Science and Technology & Wisdom Tourism Collaborative Innovation Center of Central Plains Economic Zone in Henan Province, Luoyang China,471023
E-mail: zhangping76@126.com

Nian-Feng Shi
School of Computer and Information Engineering in Luoyang Institute Of Science And Technology & Wisdom Tourism Collaborative Innovation Center of Central Plains Economic Zone in Henan Province, Luoyang China,471023
E-mail: 13937953674@163.com

Hong Jiang
School of Mathematics and Statistics in Henan University of Science and Technology, Luoyang China, 471023
E-mail: 513811066@qq.com

***Abstract*-This paper proposed a advanced delegation agent model based on roles, which was QRBAC(Quick Role-Based Access Control) based on the model of RBAC(Role-Based Access Control). By means of introducing the model's system architecture and defining element of QRBAC, the model has a great application values in field of access control.**

Keywords-access control; role; RBAC; delegation agent

I. INTRODUCTION

Along with the develop of information technology, access control as a information security technology received great attention. Compared with traditional discretionary access control (DAC) and mandatory access control(MAC)[1], the access control based on role has the characteristics of authorization management complexity is low and flexible. But now the RBAC in practical application is still not very wide, many problems without the corresponding solutions, so people improve the model of RBAC constantly. While the delegation agent model based on RBAC realized the role of temporary delegation agent in real world, it can disperse principal's authorization management to general agent to carry out, and suitable for job placement, separation of power, and cooperative work. Existing delegation agent model based on RBAC include: RBDM1, RBDM, RDM2000, but they are discretionary realize delegation, the process of delegation depend on the agent's subjective opinion and lack of supervision and control. For example, at school the archives management and the record of student result can't complete by a man. When the filing clerk have something to go out, his authority can't delegated to the person that record of student results[2].

This paper based on the model of RBAC96 and RBDM, proposing a delegation agent model based on RBAC, named QRBAC. The delegation agent simply put is allow principal choose a suitable agent to carry out delegation, it has the characteristics of temporality, monotonicity, revocability.

II. RBAC BRIEF INTRODUCTION

The model of RBAC has basic parts； user, role, permission and session. The most basic model is RBAC96, it contains four basic model. The figure 1 shows the relationship between them.

RBAC0 is called the basic model, it only contains the most basic element of RBAC: user, role, permission and session. RBAC0 is the minimum requirements to meet for any support RBAC system. RBAC1 contains RBAC0 and adds the concept of role hierarchy, in this station, roles could inherit permission from other roles. RBAC2 also contains RBAC0 and adds constraint. Such as mutual exclusion of roles, role cardinality constraints, role of least privilege. RBAC3 is the complete model that contains RBAC0, RBAC1 and RBAC2.

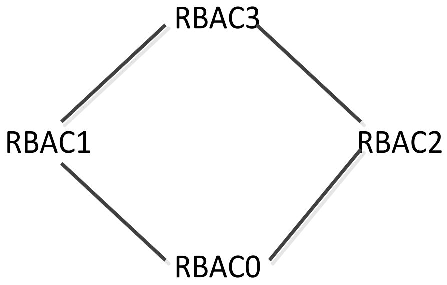

Figure 1. The relationship between the model of RBAC.

The core idea of RBAC is interrelation of security authorization and role, the users must first be corresponding role to further activate the role permissions, this greatly simplifies the process of authorization management. Roles can be created according to different work in the system, then according to the responsibility and qualification assign roles. Along with the increase of new system and new application, roles could be assigned more permission, also could be revoked corresponding permission. Practical application shows: compared with administrator alter role's permission, administrator alter user's role is more security, but the model of RBAC is defective in the aspect of job placement and cooperative work[3].

III. THE MODEL OF QRBAC

The agent element of QRBAC concludes delegating users, agent delegating user, agent delegating user, delegated role and delegated user. The user that initiate agent is called delegating user, written Uing; the user that agent principal's role is called agent delegating user, written Ua; the role was agent by principle users is called delegated role, written Red; the user that receive the delegated role is called delegated user, written Ued. In QRBAC, delegation roles to users is the delegation role that temporary generated and granted to determine user. Delegation roles to roles is the delegation roles that temporary generated and granted to temporary agent role in the process of agent between role to role. Regular roles is the role is not permitted to agent. Fixed delegation roles is the role can be agent. Temporal delegation roles is the role can accept the role in DTRR in the process of agent between role to role.

In the model of QRBAC, delegation roles to users (DTUR) is the agent of user to user. As the existence of role inheritance in QRBAC, the users assignment can be divided into direct assignment and indirect assignment. And in the process of assignment,there have initial assignment, delegation agent assignment,and delegated assignment. So QRBAC have five classes users including initial direct assignment(OS), initial indirect assignment(ID), agency direct assignment(AD), agency indirect assignment(AI), delegated direct assignment(D). Because of the model's characteristic of one step, the delegated role not exist indirect assignment.

The user of QRBAC can be divided into three classes. The initial user(Users_I(r)) is that the user's role was assigned initially by administrator; delegation agent user(Users_A(r)) is that the user was accredited by other initial user; the delegated user(Users_D(r)) is that the user's role was assigned by principal-agent user.

In QRBAC, the delegation process of user-user-user is restricted, principal can only agent the permission in FDR .In the delegation agent of role-role-role, total permission agent has carry out by the special delegating user(system administrator), this is largely improved the security of the system.

The QRBAC's basic process of the role agent is that in the agent of user to user, delegating user authorized the permission in FDR of R to temporary generated DTUR, then DTUR will be authorized to certain agent user, agent user can use permission directly also can through the same steps authorize permission to delegated user, in the agent of role to role, the special delegating user(system administrator) authorized the permission in FDR of R to temporary generated DTKR, then DTKR will be given to other role's TDR, so TDR's total user can enjoy the permission in DT. So alter the agent relationship as can-delegate $\subseteq \{Uing, \mathrm{Re}\,d, Ued, Ua, t\}$.

The model of QRBAC is shown in Figure 2.

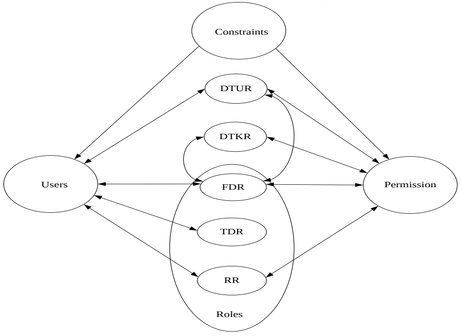

Figure 2. The structure of QRBAC.

IV. MODEL ANALYSIS

The model of QRBAC is based on the model of RBAC96 and RBDM, and making various improvement and perfection of the existing model. Firstly, QRBAC expanded the role limit of the delegating user, in the past RBDM, the agency relation is $\text{Can-delegation} \in R \rightarrow R$, user can only have one role[4]. This qualification is not rationality obviously, because agent user maybe assigned one or more role, even user possible not have any initial role. So the limiting condition can be a subset of role. If a user u1 have role r1,the u1 can delegates role r1 to the user that have role r2 and r3. Secondly, QRBAC0 support :agent-delegating, in RBAC0 the role agent limiting condition is $\text{Candeleget e} \subseteq R \rightarrow R$ that only support the agent between role. This process of delegating completely depend on principal's mind and ability, lacking the necessary supervision and control, exiting the risk of right abuse. QRBAC supports report authorization, in RBDM0 the role agency limiting condition is $\text{Candeleget e} \subseteq R \times R$ that can't support repeat authorization. But this is unreasonable in the real system ,this paper consider should abolish the limiting that RBDM0's agency relation don't support repeat authorization[5].

V. MODEL APPLICATION

A. *Authentication Process*

Identity authentication is the process of the system to examine the user's identity certification, essentially to find out whether a user has the right to the use and storage the resources he requested. PKI authentication service using a digital signature to confirm the identity, the basic process is to show a random inquiry data to the entity which need to be certified. The server contains certificate server, CA (Certificate Authority) and RNG (Random Number Generator); the client contains agent and USB Key in which the private key and the identifier of the USB Key stores. Each

USB Key's corresponding digital certificates, which contains corresponding the USB Key's public Key information, is stored in certificate server [6].

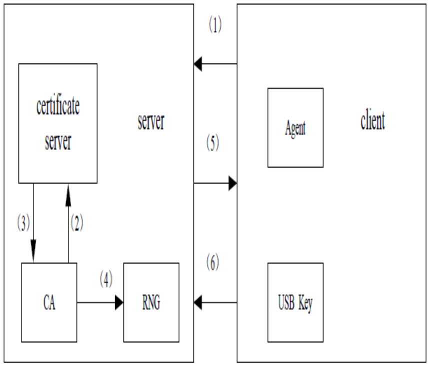

Figure 3. Schematic diagram of authentication process

As shown in Figure 3, the specific certification process is as follows:

- The client using USB Key identifier (each USB Key identifier is unique) starts certification request to the server;
- According to the user list, the CA server queries to the certificate server whether there is a USB Key identifier of the user;
- The certificate server process local query and return the result to CA;
- If the user's USB Key identifier does not exist, then close the client's network connection; otherwise, the CA sends control information to RNG, which will generate a random number i;
- The server sends the random number i to the client using TLS protocol and the client encrypts the random number i using the private key stored in USB Key, at is E(i) = I;
- The client sends I back to the server, ter the server decrypts the identifier, meaning D(I) = h, then judges Whether i is equal to h. If i=h, the certification succeeds; Otherwise, the authentication fails.

B. *Encryption Principle*

When illegal behaviors occur on the client side, the encryption module will be invoked. The core technology is to use transparent encryption kernel and to implement driver in the operating system kernel layer[7].

Transparent encryption has the following features:

- Forced encryption: after installation, all specified types of files are forced encrypted;
- Easy to use: no effects on the original operating habits, no needs to limit the port;
- No internal obstacle: internal communication does not need to make any processing can exchange;
- External blocked: once it leaves using environment, the file will become invalid automatically, so as to protect intellectual property rights.

Transparent encryption technology principle works as follows:

Transparent encryption technology is a technology closely integrated with windows, which works in underlying windows. By monitoring applications for file operations, it decrypts the cipher text automatically when opening files, and write plaintext in memory to storage medium automatically when writing files, so as to ensure the files in storage media are always encrypted. Common applications are running in user mode, and user level programs have no rights to directly access the kernel-level objects. To operate files stored in a variety of media needs API functions to access kernel-level codes . The file store process as shown in Figure 4.

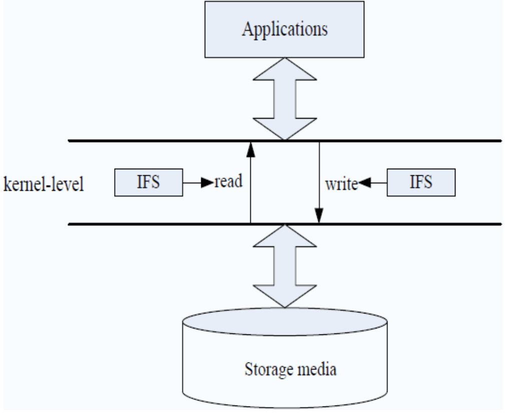

Figure 4. Schematic diagram of file store process

C. *Security Analysis*

As shown in Figure 3, Identity authentication process is implemented using asymmetric cryptography, whose security fundamentally depends on the security of private key used. Server CA's private key is secure guaranteed by security mechanism provided by host's encryption algorithm. The client's USB Key stores the identifier and the private key which is unreadable to prevent attackers from stealing[8]. So, the certification of the whole system is secure in the case of the private key on server side is secure. Meanwhile, the system's files protected by the high strength encryption algorithm can be encrypted automatically without user's operations, to be ensure encrypted files can only be normally used on the internal authorized computers while the files took out without authorization cannot be opened normally and appear garbled.

D. *Management Framework*

In the security module, all agents using or providing services must registered to administrative system server. The server trusted maintains all registered agents’ identity. The server takes charge of all agents' life cycle management, which must report all import switches and allows the server to control the life cycle.

The security module adopts hierarchical management to manage all Agents in the internal network. The advantage of hierarchical management is hierarchical authorization, to some extent, which can simply works and prevents illegal users exceeding access, and with a clear division of power and responsibility, improves the security of the system [9].

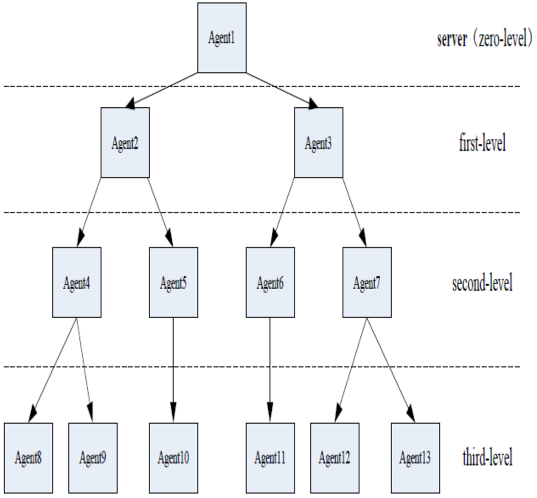

Figure 5. Schematic diagram of management framework

As seen in Figure 5, privileges in sequence from high to low are: zero-level, first-level, second-level and etc.... Agent1 which has zero-level privilege can view files in all other proxy hosts and generally speaking, system administrators and the unit's leader have this privilege. The zero-level privilege is unique, that means, for the whole system, only one host's proxy can have this privilege. Agent2 and Agent3 with first-level can manage 5 proxies belong to them. By analogy, according to the direction of the arrow, the high-level Agent can manage all low-level agents belong to it while the low-level Agent has no privilege to manage the high-level Agent.

VI. SUMMARY

From the role of agent, prerequisites, agent range, maximum depth and the largest agency of width these five aspect making constraint. Make a more comprehensive restriction conditions, increase the safety of the model. The advantage of this model is support principal-agent between user-user and role-role, and also support multi-step agent between user-user, single step agent between role-role, and a variety agent revocation strategy. The disadvantage of the model is not support part of the role agency, it remains, it remains to be imported in this respect.

ACKNOWLEDGEMENT

This research was financially supported by Henan University of Science and Technology Foundation for SRTP (No: 2014128), Scientific and technological research projects of the Henan Provincial Department of Education (No: 14A510021, 14B890004, 16A520009, 17A520006) , Science and Technology Projects of Henan Science and Technology Department (No: 122102210136, 142300410014, 152107000098, 162102210047), and Central Plains Economic Zone in Henan Province Tourism Wisdom Collaborative Innovation Center Open Project (No: 2015-ZHLV-007, 2015-ZHLV-014).

REFERENCES

[1] Linlin Wang, Xiaoming Guo, Shiping Yang. Research and Construction of the Role-based Delegation Model in RBAC[J]. MICROPROCESSORS 2007, 28(2):76-79.

[2] Wei Sun, Shuli Wang. Flexible Agent delegation model based on RBAC[J].

[3] JOURNAL OF COMPUTER APPLICATIONS 2010, 30(7):1797-1801.

[4] Ye Huang, Hanhu Wang. Research on a RBAC-based User-to-user Delegation Model[J]. COMPUTER AND MODERNIZATION modernization 2010(11) :127-131.

[5] Yali mou, Hao Zeng, Hong Yao. Role-tank based controlled delegation model[J]. COMPUTER ENGINEERING AND APPLICATIONS 2010,46(3): 87-90.

[6] Zhang Yu-qing. Public Key Infrastructure (PKI) implementation and management of electronic security[M]. Beijing: Tsinghua University Press, 2002.

[7] [4] CHEN Shang-yi. Transparent File Encryption Technology and its Application. Information Security and Communications Privacy[J]. 2007.11:75-77.

[8] [5] Ye S, Makedon F, Ford J. Collaborative in Peer-to-peer System[C].Proc. of the on Peer-to-peer computing. 2004 Automated Trust Negotiation 4th International Conference.

[9] [6] ZHU Sheng-lin, YANG Bo, ZHANG Ming-wu. Research on a Comprehensive Trust Management Model in Distributed Systems. Journal of South China Agricultural University[J]. 2007, 28(2):113-115.