Dynamic Role-Based Access Control Model

Jun Zheng
Key Laboratory of Intelligent Information Technology
School of Computer Science and Technology, Beijing Institute of Technology ,Beijing, China
Email:zhengjun@bit.edu.cn

Qikun Zhang ,Shangwen Zheng and Yuan Tan
School of Computer Science and Technology, Beijing Institute of Technology ,Beijing, China
Email:zhangqikun04@163.com

***Abstract*—With the rapid development of network and the coming of information age, access control is particularly important, role-based access control (RBAC) is an access control which is popular. RBAC authorizes and controls the roles corresponding to the users to operate the object. It solves problems of least privilege, separation of duties and so on. However, limited permissions are required to be executed by a certain sequence, that is, the permission owned by a user is controlled by other users'. To solve this problem, this paper proposed an improved model on the base of the original RBAC, not only to retain the original characteristics of RBAC but also solve a specific problem of some permissions which are needed to executed by sequential order, and the analysis shows that this scheme has better security, better flexibility, and can be well applied to the workflow system.**

***Index Terms*—RBAC, least privilege, duty separation, dynamic constrain**

I. INTRODUCTION

With the continuous development of computer networks and the use of much distributed technology, the companies are increasingly focused on information management and data sharing, which leads to a great challenge to data security. Accessing the data if the user is not permitted will lead to serious problems, especially in large systems [1]. This makes the access control become a focus of attention. Due to increasing complexity of data availabihtv and protection requirements, many modern systems incorporate a complex set of access control policies The defacto approach to modeling these access control requirements is Role-based access control (RBAC),The access control mechanisms in computer systems define the permission that users or processes have to access protected resources in a computer system. In a role-based access control (RBAC) mechanism, these rights are defined based on the role that individuals are assigned to in an organization. The advantage of assigning access rights to roles instead of individual users is that roles have more permanence in an organizational context than users [2]. Individual users can be assigned and de-assigned from roles without having to manage the access control permissions for each individual separately.Early access controls are divided into two types: Discretionary Access Control (DAC) and Mandatory Access Control (MAC) [3][4][5]. DAC is a strategy which is based on the identity or the group where the identity controls its access methods. DAC's core idea is that the object owner can independently control other objects' visit his objects, and can independently decide whether pass the permission to other subjects or groups. Although the idea of spreading the permissions of DAC is with good flexibility and scalability, it also has security problems, making it difficult to meet the demanding high security system. The MAC is based on the security level of subject and object to access control. Security level is mandatory assigned by the security administrator. Either subject or object can change the attributes of the security level. The property of MAC makes it applicable to high security system, but it lacks flexibility. Currently, the international popular access control model is RBAC [6][7], by introducing the concept of the role to achieve the logical separation of users and permissions to achieve the permissions of management. RBAC is considered to be the best one to instead of [8][9] DAC and MAC. In many studies, RBAC is extended according to the need, according to the specific application to access control, such as adding time features [10][11] or joining the task access control [12][13] and so on.

Reference [14] proposes a permission management mechanism based on a management mechanism with combination of static permissions and dynamic permissions, dynamically adjusting the permission according to the role's environment function and role's method, which increases the flexibility and dynamic. The permissions management mechanism has been put in the appropriate system into use and performed well.

Reference [15] proposes a separated RBAC model (Separation RBACS-RBAC), dividing the roles' permissions into basic permissions and dynamic permissions, user can get the basic permissions (BP) after getting the role, but other corresponding permissions are

Manuscript received November 20, 2010; revised December 10, 2010; accepted January 10, 2011.

© 2011 ACADEMY PUBLISHER
doi:10.4304/jsw.6.6.1096-1102

hanging, which is called dynamic permissions (DP). When the task instance arrives, activate these specified permissions by way of licensing authority. The role operates the data with the activated permissions in the task's lifetime. When the task is completed, the activated dynamic permission is hung again. This permission management adapts to the dynamic nature of the workflow, which has good adaptability and integrity. But the shortage is using task-based access control methods when realizing the workflow, which is complex to realize and did not present a detailed process of implementation.

The previous access control has solved some problems in some ways and improved the traditional role-based access control. But most of them did not mention the problem of the permissions which required to be executed by sequential order in RBAC. Although the roles and tasks based access control model can handle the task of the workflow, it is not suitable for dealing with vaguely, liquid, out of workflow task. This paper presents a new type of permission management which is based on RBAC model, and solves this problem and improves the security of the system as well as making the system much closer to the real world.

Ⅱ. ROLE-BASED ACCESS CONTROL MODEL

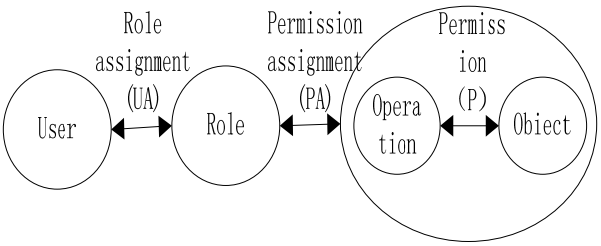
A. Basic Idea of Role-based Access Control

A user made its literal sense, it should be is a person. But in fact the concept can be extended to include machines, networks, or intelligent agent. And a role can be seen as a feature set that within the organization associated with the rights and obligations of the user. Permissions are allowed to perform one or more objects to execute one or more related operations.

Any access control technologies are intended to protect the system resources. In RBAC systems, its main purpose is to protect the objects. Access control model with the earlier agreement, an object is an entity containing or receiving information. RBAC for an implementation of the system, an object can be used as Resource Investigator (such as operating system files or directories, database management system table, column, row, view) or can be used to indicate the limited system Resources (such as printers, magnetic trick free 'space, CPU time).

The core concept in RBAC is the role relationships, role semantics is constructed in the access control policy management for the conduct.

RBAC model is defined in terms of three modelcomponents-Core RBAC,Hierarchical RBAC and Constraint RBAC. The core RBAC model includes five basic elements,i.e. U (users), R (roles), O (objects), OP (Operations) and P (permissions). The core RBAC also has some useful session sets, which is the mapping relationship between some users and some adaptable roles[16].The core idea of RBAC is that adds roles between users and permissions. It forms relationships among users, roles and permissions. Users get roles' corresponding permissions by getting roles to operate on the objects, as shown in Fig.1 [15].



Figuer 1. The core idea of RBAC

Basic defines [17] are shown as follows:

"User": The objects which issue the request in the system can be a person, equipment, networks, or intelligent agent device.

"Role": The entity which connects the user and the permissions, corresponding to the work functions in the organization's environment of the reality.

"Object": The entity which is modified or changed, being the ultimate carrier to receive and hold information.

"Operation": The type and the object of operation in the program execution depends on the systems and implementations, such as operations in the file system including read, write and execute, and operations in the database system including insert, delete, append and update.

"Permission": It means that the ability which can operate one or more objects protected by RBAC. It is constituted by a set of operations and objects.

Users are assigned appropriate roles to obtain the corresponding permissions to operate the corresponding object. The users associate with the roles, the roles associate with the permissions.

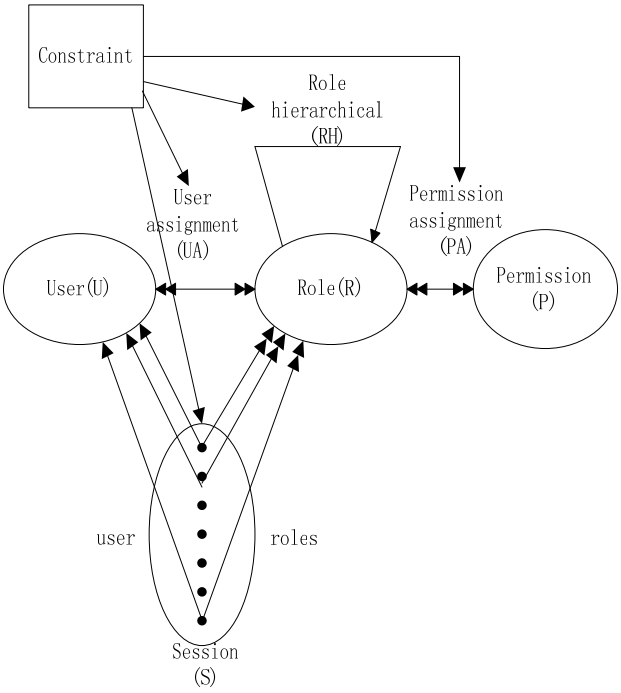
B. Structure Diagram of Role-based Access Control Model

In the traditional RBAC model, the user can not perform the operation on behalf of all those operater, in most cases ,the process (including the user processes and system processes) access files, directories and other data. Executives of all operations in system can not be accurate expressted by concept of the user in traditional model. Therefore, the concept of users need to extended in traditional model.

Currently, the set of the main session role is adjusted by the principal or the administrator himself, although you can support the principle of least privilege, but such adjustments are static, not automatically by the system. We hope to realize the set of the main session role dynamic adjustment, for example, the main role of the current session is a system administrator, if the principal implement a non-credible process, the session is automatically adjusted to the role of ordinary users, which can reduce user' errors or harm of the hobbyhorse. From two points of view, the dynamic role-based access control model has a certain significance.

The structure diagram of role-based access control model is shown in Fig.2 [18] as follows.

© 2011 ACADEMY PUBLISHER



Figuer 2. The structure diagram of role-based access control model

C. Formal Definition of RBAC

The formal definition [19] of RBAC is shown as follows:

$UA \subseteq U \times R$: It expresses the many-to-many associated relationship between the users and the roles.

$PA \subseteq P \times R$: It expresses the many-to-many licensing relationship between the roles and the permissions.

$RH \subseteq R \times R$: It expresses the hierarchical relationship in roles, which is a partial order.

$users : R \to 2^U$: It expresses the mapping functions which are mapping roles to users.

$perms: R \to 2^P$: It expresses the mapping functions which are mapping roles to permissions.

$roles: P \to 2^R$: It expresses the mapping functions which are mapping permissions to roles.

D. Role Hierarchical Relationship

Hierarchical RBAC describes hierarchical relation between roles. It goes beyond simple user and Permission role assignment by introducing the concept of a role for authorized users and authorized permissionsA new term called RH (Role hierarchy) was introduced into H-RBAC. RH is used to resolve the complex relationship among many organizations,which has the nature to map the given permissions to a suitable duty.

Organizing a role hierarchy according to a genericspecialized relation leads to several problematic consequences[20][21][22], among which the most important one is that senior roles acquire all permissions assigned to junior roles. In many organizations, senior roles are not qualified enough to undertake the activities of junior roles [21].

Role hierarchical relationship expresses the inheritance in roles' permissions, such as the role A inherits role B, and then B's permissions also belong to A. Role hierarchical relationship uses the partial order relation in discrete mathematics to represent. A role may inherit from multiple roles or be inherited by multiple roles. The use of role hierarchical relationship not only makes the system closer to reality, but also makes it easier to add and remove roles, easier to manage.

E. Role Constraints

In real life, sometimes require that certain functions can not be served by the same person, this is separation of duties. As a security principle, the concept of separation of responsibilities has long been widely used in the industrial, commercial and government. Its purpose is generally designated with different skills and different interests of the people to do a full business to different parts of behavior to prevent or reduce possible errors caused by fraud and accidental loss. This point the abstract to the RBAC system to get Constraint RBAC. Constraint RBAC model in RBAC adds separation of duty relations.

Constrained RBAC is used to set constraint condition in role assignment and activate roles in a session . Separation of duty relations include the static separation of duty (SSD) and dynamic separation of duty (DSD). SSD defines mutually disjoint user assignments with respect to sets of roles. DSD limits the permissions that are available for a user, its requirements limit the availability of the permissions by placing constraints on the roles that can be activated within or across a user's sessions. Both SSD and DSD is the guarantee for implementation of least privilege principle

Role constraints include least privilege, separation of duties and so on. The most important of them is separation of duties. Separation of duties includes static separation of duties and dynamic separation of duties. Static separation of duties refers to when assigns roles to users do not distribute mutually exclusive roles. Such as accountant and cashier are two mutually exclusive roles, assign roles to users only one of them, otherwise there will be serious security problems. Dynamic separation of duties means that a user has several roles, in one session not having the role of combination which can make security issues. Such as bank clerk and saver which are not mutually exclusive roles, however, if a user uses both of them in one session, it will come to very serious harm. At this time, it requires the user use one role at one session, such as using saver after exit the bank clerk, or vice versa.

F. Features of RBAC

Manage easily. The users' permissions changes easily, but roles' permissions are relatively stable. Because of the role's joining, making users can only get permissions from getting roles. RBAC adds, deletes and modifies the

© 2011 ACADEMY PUBLISHER

role according to the need, making management more flexible.

Close to the reality. Since the addition of the concept of role, RBAC makes the system closer to the real world, easier to understand and use for users.

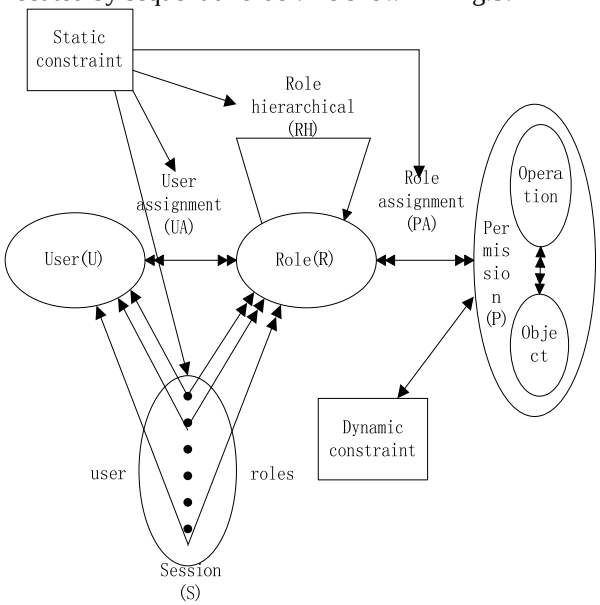
More secure. Because RBAC model derived from reality, so users' permissions are the same as the situation of reality, avoiding many problems of responsibilities and permissions, making the system more security. It follows the safety principles [19] of least privilege and so on.

III. DYNAMIC ROLE-BASED ACCESS CONTROL MODEL

A. Structure Diagram of Dynamic Role-based Access Control Model

Traditional RBAC is described as follows: if one subject accesses one object, the subject has the operation authority,which has access operation. Users have certain authority by role, and which has corresponding operation, without implementing operation environment, thus easily bringing security hidden trouble.

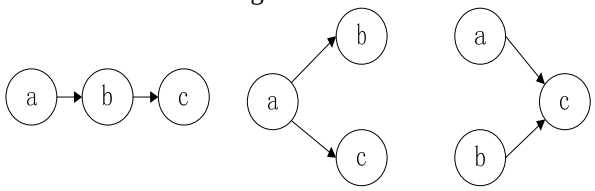
On the base of the original RBAC model, the dynamic role-based access control model increases a module of dynamic constraint, which makes the dynamic constraints executed by sequential order. As shown in Fig.3.



Figuer 3. Structure diagram of dynamic role-based access control model

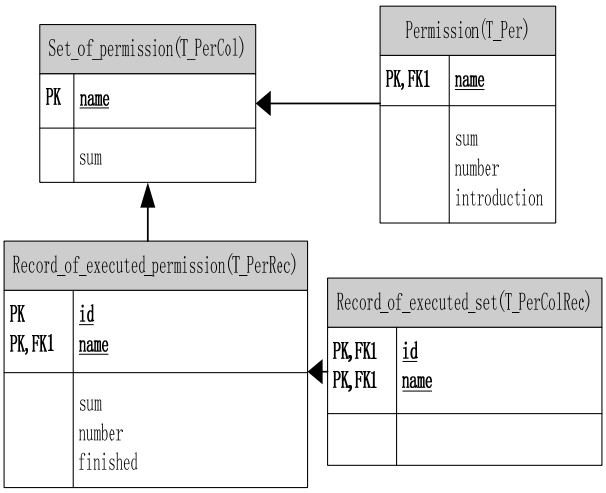
Although RBAC has many advantages, it also has some disadvantages. it ignores the need to make dynamic constraints executed on sequential order. Such as in real life, superior restricts subordinate on the implementation of subordinate's permission. Accountant is the cashier's supervisor, cashier has permission to remit the money to the customer, but it must have the consent of the accountant, that the cashier remits the money when accountant tells. This point is not reflected in the RBAC, when the role of the cashier enters the system, he has the permission of remittance, he can execute this permission, which would be big security risk.

To avoid the occurrence of this security problem, this paper introduces the concept of dynamic constraint. After static constraints determined by the administrator, the user can not make any changes to it. Dynamic constraint is that administrator provides a role which can change the state of permission. Such as the problems between accountant and cashier, accountant has the permission to control the cashier, the cashier has permission of remittance, it is necessary to order the implementation of the two rights, when the cashier check Dynamic constraints finding out the state of accountant's control permission of is true, then cashier can remit the money. The permissions which do not need to be executed on sequential order called static permission, which must be executed on sequential order called dynamic permission. There are three situations of the association between dynamic permission, a, b, c are three permissions, situations are shown in Fig.4 as below:



Figuer 4. Three situations of the association

The database design of dynamic constraint module is shown in Fig.5.

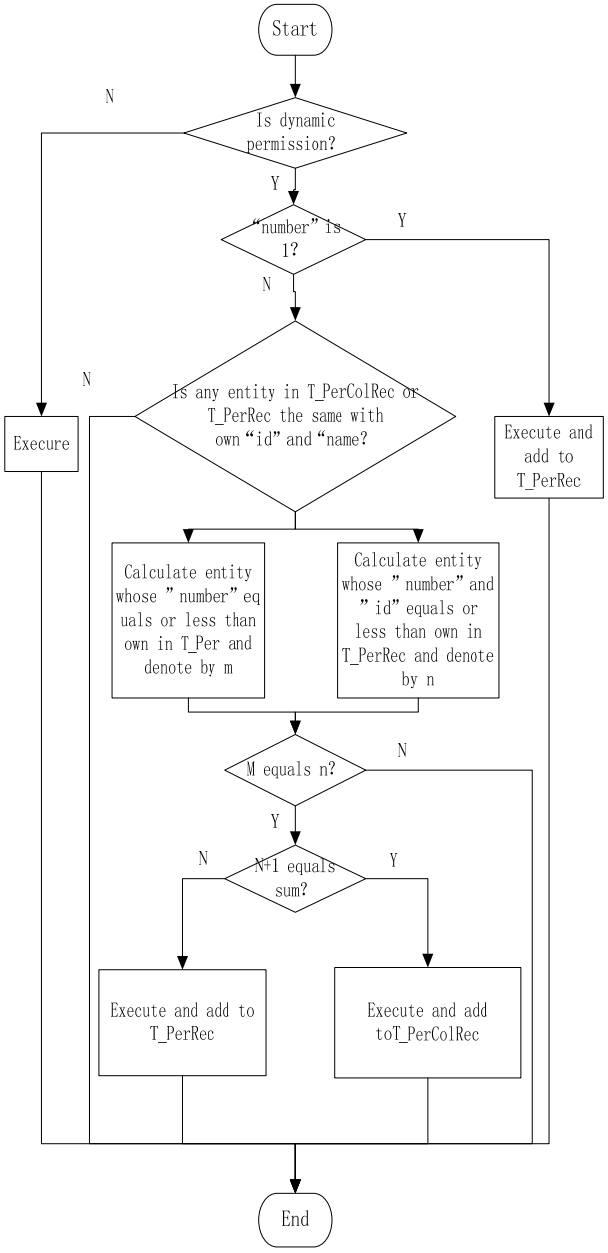


Figuer 5. Diagram of database design

In the Fig.5, "name" means the set of the dynamic permissions which have the sequential order relations, "sum" means number of permissions in the permission set, "id" means one digital code of the permission set, when "name" is same that "id" is unique, "number" is the first few permission in the permission set, "finished" means the "number" location of permission set is executed, "true" means that permission is executed, "false" means that permission is not executed, "introduction" means brief of the permission. Table T_PerCol and T_Per are created and added by the administrator, on behalf of all permission set. Table T_PerRec and T_PerColRec are dynamically added by the role. Specific algorithm flow is shown in Fig.6. Dynamic RBAC examines the current permission which will be executed on this flow, finding the result that the

© 2011 ACADEMY PUBLISHER

permission can be executed or not. The dynamic role-based access control model makes the system more security, more close to the real world.



Figuer 6. Flow diagram of algorithm

The paper implements a dynamic access control model based on roles and authentication control, inducing database values into RBAC, Access control system is independent of the all application system, which has good reusability.

Ⅳ. SECURITY AND PERFORMANCE ANALYSIS

A. Security Analysis.

The security of this model bases on the following two parts: The first is the security of the original traditional role-based access control model. The second is the security brought by the improved dynamic constraint module.

The constraints of role-based access control model embody a lot of protection in the real world, such as mutually exclusion. Complying with the principle of least privilege, user may activate the minimum required permissions while logging on, only be able to get the permissions required by completing his own work, and no extra permissions, so that the security problems resulted in the intruders' pretending will not happen by the errors due to negligence. To comply with segregation of duties, including static separation of duty and dynamic separation of duty, the basic principle is that do not allow any user to get permissions portfolio that privileged enough to abuse the system, Such as the combination of rights with the cashier and accountant, so that it can ensure the security of the system.

Improved constraints include static constraints and dynamic constraints. The traditional RBAC model is based on the role of the organizational structure to divide roles, such as the company's general manager, accountant and cashier duties are set the corresponding permissions, such as financial management, preparation of relevant reports, cash, remitting money. According to the characteristics of RBAC accountant or cashier logs that gets the corresponding permissions to operate. This will be a security problem, when the cashier logs he has the permission of remittance, but the system does not know at this time whether he should carry out the operation of remittance, if cashier can remit the money at any time, which will be a serious security risk. This requires a certain set such that when the accountant allows the cashier so that the cashier can execute the permission of remittance. This is a situation, the permission in front of the others has activated, so that the permissions back can operate, which is solved by dynamic constraint module, so the permissions required by the sequential order can be executed by order, ensuring when the workflow occurs can operate his dynamic permission, preventing abuse of the user's own permissions, making the system more security.

B. Performance Analysis

Dynamic RBAC bases on the classic model, includes static constraints and dynamic constraints, static permissions and dynamic permissions, compared with traditional access control, having the following advantages.

(1)Added to the classic constraints with the dynamic constraints, permissions divided into static permissions and dynamic permissions, the dynamic RBAC increases dynamic characteristics.

(2)Dynamic RBAC retains the original permissions which do not need to be ordered by dynamic constraint, namely static permissions. It retains the advantages of the traditional RBAC. It is more efficient compared with the pure dynamic model.

(3)Dynamic RBAC makes the permissions executed by sequential order which need to be in sequential order by adding dynamic constraints and dynamic permissions to the traditional RBAC.

(4)Dynamic RBAC overcomes the shortages of the traditional RBAC by adding with dynamic constraints

© 2011 ACADEMY PUBLISHER

and dynamic permissions, so that it makes the system easier to manage and more close to the real world.

The analysis shows that this scheme has better security, better flexibility, and can be well applied to the workflow system.

Ⅴ. CONCLUSION

The paper analyses RBAC which is widely used in access control model, However, limited permissions are required to be executed by a certain sequence, that is, the permission owned by a user is controlled by other users', Role-based access control is an access control which is concerned a lot. The dynamic RBAC in this paper has solved the problem that some permissions which are required to be executed by sequential order with adding dynamic constraints and dynamic permissions to the traditional RBAC. This paper shows the specific database design and algorithm flow and careful analysis the security and performance of the dynamic RBAC. After all the dynamic RBAC has high practical value.

ACKNOWLEDGEMENTS

This work is partially funded by the Key Laboratory of Intelligent Information Technology of Beijing, China.We thank our colleagues for helpful discussions.

REFERENCES

[1] R.Power.Tangled web: Tales of Digital Crime from the Shadows of Cyberspace[M], Que/MacmillanPublishing, August 2000.

[2] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models,"[C] IEEE Computer, vol. 29, pp. 38-47, 1996.

[3] Snyder L.Formal Models of Capability-Based Protection Systems[J].IEEE Trans on Computers,vol. 30,pp:172-181,March 1981.

[4] Solworth, J.A.; Sloan, R.H.. A layered design of discretionary access controls with decidable safety properties,[C] IEEE Symposium on Security and Privacy,pp: 56-67, May2004 .

[5] Ninghui Li. How to make Discretionary Access Control secure against trojan horses[C],Parallel and Distributed Processing, 2008, pp: 1-3 April 2008.

[6] Sandhu, R.Issues in RBAC.In: Proceedings of the ACM RBAC Workshop.MD: ACM Press, pp:21-24,1996.

[7] Sandhu R S,Cogne E J, Feinstein H L, etal. Role-Based Access Control Models[J].IEEE Computer, vol.29, pp:38-47, February1996.

[8] QIAO Ying, XU De, DAI Guo-Zhong. A New Role-Based Access Control Model and It's Implement Mechanism[J]. Journal of Computer Research & Development,vol.37,pp: 37-44, January2000.

[9] Ferraiolo D, Kuhn D R,Chandramouli R. Role based Access Control[M].[s.l.]: Artech House,2003.

[10] DONG Guang-yu, QING Si-han, LIU Ke-long. Role-Based Authorization with Time Character[J]. Journal of Software, vol.13,pp:1521-1527.August 2002.

[11] HUANG Jian, QING Si-han, WEN Hong-zi, Timed Role-Based Access Control[J]. Journal of Software, vol. 14,pp: 1944-1954, November2003.

[12] GUO Hui, LI Yangming, WANG Lifen. Design and Research of Access Control Model Based on Role and Task[J]. Computer Engineering,vol. vol.32,pp: 143-145,August2006.

[13] LUO An-de. Research and Practice on Task and Role-Based Access Control Model[D]. Zhejiang: Zhejiang Gongshang University.2009.

[14] YANG Fan, XUE Zhi-xin, SHI Yong-ge. A Dynamic Authority Management Mechanism Based on Role[J]. Computer Engineering,vol.7,pp:99-102, July2008.

[15] FANG Yu. The research and design of role based access control[D]. Anhui: HeFei University of Technology. 2009.

[16] Guang-liang Liu, Xin-you Li, Sheng-xian Xie, Hong-bin Luo, Jun-qing Li, Yu-ting Wang. Multi-granularity Time-constraint Role-based Access Control[C]. IEEE International Symposium on IT in Medicine and Education,pp:1024-1027,August 2008.

[17] JIANG Xue-wu. The research of role-based access control's policy[D]. Shanghai: Shanghai Jiao Tong University. 2005.

[18] CHEN Yi, GENG Guo-hua, LI Zhe. Research and Application of Dynamic Access Control[J]. computer technology and development,vol.16,pp:223-225, February2006.

[19] JIANG Tao, LI Xin-man, LIU Ji-ren. Research on information securoty mode [J]. MINI-MICRO SYSTEM,pp: 1076-1081, October 2000.

[20] J. Crampton,"On permissions, inheritance and role hierarchies,"in CCS '03: Proceedings of the 10th ACM conference on Computer and communications security. NewYork,NY,USA: ACM, pp:85-92, 2003,

[21] C. Goh and A. Baldwin,"Towards a more complete model of role," in RBAC '98: Proceedings of the third ACM workshop on Role-based access control. New York, NY, USA: ACM, pp:55-62,1998.

[22] J. D. Moffett and E. C. Lupu, "The uses of role hierarchies in access control,"in RBAC '99: Proceedings of the fourth ACM workshop on Role-based access control. NewYork, NY, USA: ACM, pp:153-160,1999.

Jun Zheng, born in 1969, Vice professor. Beijing Institute of Technology, Beijing, China. Her research interests include information security.

Qikun Zhang,born in 1980 . Ph.D. candidate. Beijing Institute of Technology, Beijing, China. His research interests include information security and cryptography.

© 2011 ACADEMY PUBLISHER

Shangwen Zheng, born in 1986, Now he is a graduate student in Beijing Institute of Technology. His research interesting includes computer networks and access control.

Yuan Tan, born in 1972 .Ph.D. Professor, Ph.D. Beijing Institute of Technology, Beijing,China . supervisor, senior member of China Computer Federation. His current research interests include Information Security and network storage.

© 2011 ACADEMY PUBLISHER