Journal of Software Engineering and Applications, 2016, 9, 57-62
Published Online February 2016 in SciRes. http://www.scirp.org/journal/jsea
http://dx.doi.org/10.4236/jsea.2016.92004

Role of Time-Domain Based Access Control Model

Chaoqun Liu, Zhen Peng, Lili Wu

Department of Information Management, Hunan University of Finance and Economics, Changsha, China
Email: liuchaoqun_cn@foxmail.com

Received 20 January 2016; accepted 23 February 2016; published 26 February 2016

Abstract

While Role-Based Access Control Model (RBAC) is being analyzed, the concept of Role of Time-domain Based Access Control Model (T-RBAC) is put forward. With time-domain added, both time-domain and authority control roles. The basic idea of T-RBAC is introduced and described formally, and the safely of this model is analyzed. The research shows that T-RBAC fulfills both rules of information security, which are principle of least privilege and separation of duties. With practical application of T-RBCA, it can handle most of the time-related or authority-related problems. What's more, it also increases the security level, flexibility and dynamic adaptation of the system and has lower complexity than system only handled by authority. This model also can solve conflicts caused by authority.

Keywords

Time-Domain, Role, Access Control, RBCA

1. Introduction

With the continuous development of computer network and distributed technology, enterprises are increasingly focused on information management and data sharing, leading to data security challenges. The access control has become a focus. Nearly, twenty years researchers have proposed many access control model. The paper puts forward a kind of RBAC model based on time domain (T-RBAC). User role permissions are controlled by time domain. The user can get permanent authority and be able to get a certain period of time to get some permissions. This is a task instance to reach the limits of time domain control. Control time domain activates these specify access permission. The role of activated permissions operation data and tasks of life cycle is the time domain. When the task is complete, the activation of temporal authority fails. This license management to adapt to the dynamic characteristic of the tasks in practical work has good adaptability and integrity. T-RBCA is a new kind

How to cite this paper: Liu, C.Q., Peng, Z. and Wu, L.L. (2016) Role of Time-Domain Based Access Control Model. *Journal of Software Engineering and Applications*, **9**, 57-62. http://dx.doi.org/10.4236/jsea.2016.92004

of permission management to solve the problem of processing task time, improve the security of the system and make the system more close to the real world.

2. Background and Related Work

Early access control model has HRU model which is proposed by Harrison, Ruzzo and Ullman [1] and Take-Grant model which is proposed by Jones etc., subsequently, discretionary access control model (DAC) and mandatory access control model (MAC) is proposed [2]-[4]. DAC strategy is based on the identity of the identity or the organization to control its access methods. DAC core idea is that the owner of the object can be independently controlled other objects access object, can independently decide whether through other subjects or group permissions. Although the idea spread DAC permissions have good flexibility and extensibility, it also has security problems, and it is difficult to meet the requirements of high security system. MAC is based on the subject and object of access control security level. Assigned by the security administrator security level is mandatory. Subject or object can change the security level of attributes. MAC features make it suitable for high security systems, but the lack of flexibility. In recent years hotspot of access control technology research focused on role-based access control (RBAC) which is proposed by Ferraiolo and Kuhn [5] and task-based access controls (TBAC) which is proposed by Kuhn [6]-[8], but there are also some other related research, such as dynamic role-based access control model [9], a suitable administrative model that governs changes to temporal policies [10], parameterized role-based access control [11], a framework using Budget-Aware Role Based Access Control (BARBAC) [12], adding time features [13] [14] or joining the task access control [15] [16] and so on.

The core of Role-Based Access Control is taking the user's access control into Role permissions. The user belongs to some kind of role and permissions are assigned to the user through the role by the administrator so that the user has certain permissions.

Model consists of users, roles and permissions three entities. The user is associated with the role and the permissions are separated. Users can not be directly related to permissions, Users can only be given the role to get some kind of permission [17]. A user can have multiple roles, and a role can be assigned to multiple users [18]. A role can have a variety of permissions. A permission can also belong to a number of roles. Its relation is shown in **Figure 1**.

Under RBAC, roles represent organizational agents that perform certain job functions, and permissions to access objects are grouped as roles. Users, in turn, are assigned appropriate roles based on their responsibilities and qualifications [19] [20]. This feature immediately reduces the operational costs of the system since the number of roles is usually much smaller than that of the permissions. The success of RBAC led the development of some useful extensions to satisfy new application domains. In particular, researchers preserve the basic idea of having roles in the model and add some additional dimensions, like time and space. Temporal RBAC (TRBAC) [21], Generalized Temporal RBAC [22], Spatial-Temporal RBAC [23] are some examples of these extensions.

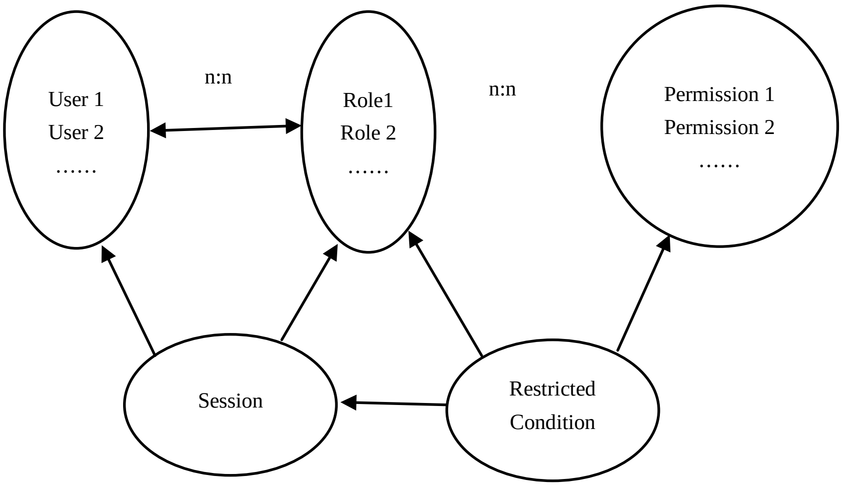

Figure 1. RBAC model.

3. Role of Time-Domain Based Access Control

In practical applications, due to the needs of management, through role assigned to the user's operating permission have time limit. Namely role only within a certain time-domain has some operating functions, and not in a time-domain, role permissions invalid and in the RBAC model, mainly to solve the user, roles and permissions authorization problem. But time problem of permission is not involved. In order to solve this problem, the time-domain is introduced on the basis of RBAC model, this makes the permissions of the roles have time limitation, the role of operating authority will be effective on the corresponding time-domain. That is to say, in a time-domain, the role can get some specific operating authority, and if not in the time-domain, the operating access control of the role is invalid. This is the Role of Time-Domain-Based Access Control Model (T-RBAC).

In this model, the role is authorized, but the permissions are not necessarily effective. Only the user when using this access within the prescribed time-domain permission is valid. The result of the common action of the authority and the time-domain to make the role obtain a certain operation permission. Because the user can only obtain the relevant permission by the role, the user's operation is also the result of the common function of the permission and the time-domain.

3.1. Formal Definition of T-RBAC

T-RBAC model is composed of the following units:

User set U, role set R, time-domain set T, permissions set P, time-domain permission set TP, and other permissions set OP.

1) The relationship between the user and the role for the user is granted the role of the relationship (UR).

UR: U → R. The user U was awarded role R.

2) Time-domain is used to control the permissions of the effective time. By the interaction between time-domain and permission, the specific and effective permission of the role could be determined.

3) According to the characteristics of time, the time is divided into effective time, the Time-domain and the Expiration time.

Effective time: Time is which permissions began to be allowed. At this time point users began to be given a permission.

Time-domain: The user has some operating authority and Time period which these user can operate some function.

Expiration time: Permissions for lost time point and at this time point users began to lose an authority.

4) Relationship of each unit of T-RBCA

$\mathrm{P} = \mathrm{TP} \bigcup \mathrm{OP}$: The permissions include permissions of time-domain and other permissions;

$\mathrm{TAP} \subset \mathrm{T} \times \mathrm{TP}$: It is to-many mapping relation between time-domain to permissions of time-domain;

$\mathrm{RP} \subset \mathrm{R} \times \mathrm{OP}$: Directly relations of role are assigned permissions;

$\mathrm{RT} \subset \mathrm{R} \times \mathrm{T}$: Directly relations of role is assigned time-domain;

$\mathrm{UR} \subset \mathrm{U} \times \mathrm{R}$: Directly relations of user is assigned role;

$\mathrm{UT} \subset \mathrm{U} \times \mathrm{T}$: Directly relations of user is assigned time-domain;

$\mathrm{URT} \subset \mathrm{U} \times \mathrm{UR} \subset \mathrm{U} \times \mathrm{R} \times \mathrm{T}$, URT: It is relationship which exists between users, roles and time-domain;

$\mathrm{UAO} \subset \mathrm{U} \times \mathrm{TAP} \subset \mathrm{U} \times \mathrm{T} \times \mathrm{TP}$: It is UAO relationship which exists between the user, time-domain and time-domain permission;

$(\mathrm{u}, \mathrm{t}, \mathrm{tp}) \subset \mathrm{UAO}, \mathrm{u} \in \mathrm{U}, \mathrm{t} \in \mathrm{T}, \mathrm{tp} \in \mathrm{TP}$: u, t and tp have the UAO's relationship;

$\mathrm{URAO} \subset \mathrm{URT} \times \mathrm{TAP} \subset \mathrm{U} \times \mathrm{R} \times \mathrm{T} \times \mathrm{TP}$: It is URAO relationship which exists between users, roles, time-domain and time-domain authority;

$(\mathrm{u}, \mathrm{r}, \mathrm{t}, \mathrm{tp}) \subset \mathrm{URAO}, \mathrm{u} \in \mathrm{U}, \mathrm{r} \in \mathrm{R}, \mathrm{t} \in \mathrm{T}, \mathrm{tp} \in \mathrm{TP}$: u, t and tp have the URAO's relationship;

$\mathrm{UA} \subset \mathrm{UAO} \bigcup \mathrm{UPO} \subset (\mathrm{U} \times \mathrm{TAP}) \bigcup (\mathrm{U} \times \mathrm{RP}) \subset (\mathrm{U} \times \mathrm{T} \times \mathrm{TP}) \bigcup (\mathrm{U} \times \mathrm{R} \times \mathrm{OP})$: It is dispatched relationship between user and permission, including users and time-domain permission's relationship associated with time-domain.

3.2. The Working Mechanisms of T-RBAC

The working mechanisms of T-RBAC model is: The user belongs to a specific position, users have been given a role by UR relationship, so the user can use has been granted the role of the login system. Since the main contents of the user's work does not change, this role as the basic role of the user. When the user need to finish the other work according to requirements of the boss, don't need frequent change the role of user, just by changing the time-domain associated with this role to get the permissions to complete another task need. Upon reaching the expiration time point, obtained additional permissions automatically disappear. Its relation is shown in **Figure 2**.

When companies have more business, working content changes frequently, using T-RBAC model can reduce unnecessary role change, you just need to Change the time-domain so that the role can get the permissions associated with time-domain. When the time-domain is set up, it does not need to change the user's role. Once the expiration time arrives, the permissions that are controlled by time-domain automatically lose. Doing so can reduce the frequent operation of the database administrator, and can simplify the administrator permissions management, facilitate optimal management database.

4. Safety Performance Analysis of T-RBAC

The time-domain expanded RBAC model has a wide range of analysis, and it can capture the time-domain user roles and permissions role assignment, and the role of time-domain hierarchy and enabling role. We put forward based on the analysis of time-domain sub-problems make RBAC problems easier to handle [24] [25]. T-RBAC model supports two well-known principles: the principle of separation of duties and least privilege principle. Role normally only have to complete the work of the most basic permissions, only when need to complete an additional work are endowed with certain permissions, it makes a clear division of responsibilities to each character, which conform to the principle of separation of duties and the principle of least privilege. When users log in through a role, if the role want to have some rights, must be in the permissions associated with time-domain within the effective time can have the authority, outside the valid time don't have the authority, so as to realize the dynamic separation and revoke the permission.

5. Conclusions and Application

In the enterprise, due to the work required, the user who has the role A needs to cooperate with staff of other departments (assuming the role B), and understand some of the internal dynamics of other departments. Role A sometimes needs to shoulder two jobs, to take on other people's work. (Assuming other people is role B). At this time, the T-RBAC model is very necessary. Role A to work with other departments or undertake the work of others, can be through the use of time-domain control permissions to make the role A obtain certain role B to complete the work required permissions. Administrators only need to give the role A some permissions that role B have, and set the time-domain for these permissions, such as viewing the file information, the signing of the relevant documents, etc. While the other permissions of role B do not give the role A, they can ensure the security of information and can avoid the role conflict. Starting from the valid time, the user of the role A would been granted to the part of the role B's permission. Then, the user has certain role B's permissions. For example,

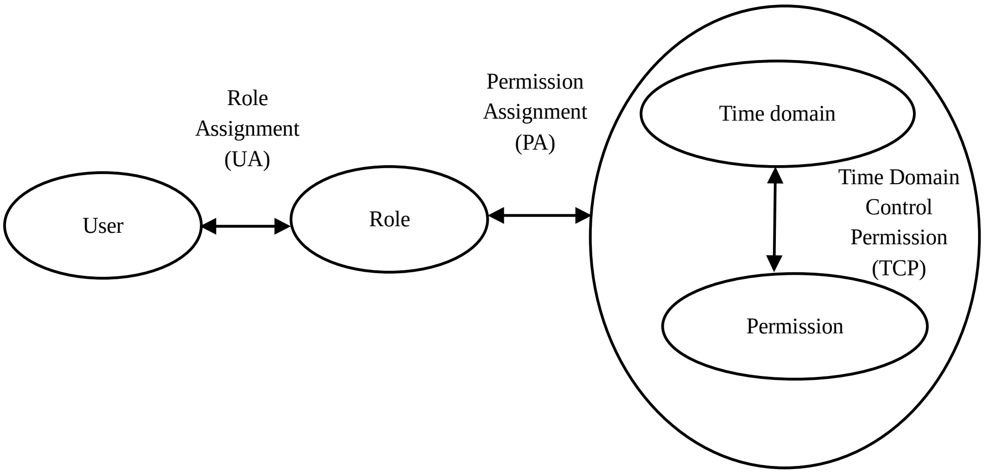

Figure 2. T-RBAC model.

the role B has the view documents and other relevant documents sign permission. When the time reaches the expiration time point, users have the appropriate permissions of role B which disappear automatically. Such as:

Basic assumption:

Role A: This is the developer's permissions, assuming that it can be related operations for project 1 source code.

Role B: This is agent's authority, assuming that it manages related documents of the project.

T: it is time-domain. Start time is 8:00, 2015-12-25; end time is: the 2015-12-30, 18:00.

In the work, clerk A leaves. During the clerk A leave, developer B serves as his work.

Start: the developer B has Role A; the clerk A has Role B.

During the clerk A leave: the developer B has Role A and Role B (T).

Note: B Role (T) is Role B that is controlled by time-domain T.

End: developer B has Role A; clerk A has Role B.

T-RBCA realizes the dynamic separation, revokes permissions, reduces the administrator frequent operation of the database and simplifies the management of the database.

Based on the analysis of the existing role access control model, the concept of time-domain is introduced. Time-domain is constructed role-based access control (RBAC), and the model gives the formalized description and the analysis of security. Through the model application in actual system, it shows that the T-RBAC satisfies the two famous safety principles: the principle of separation of duties and the principle of least privilege, and has good dynamic adaptability.

Acknowledgements

This work is funded by the key discipline of computer application technology of Hunan and science plan project in Hunan province (project number: 2014FJ6028), China. We thank our colleagues for helpful discussions.

References

[1] Harrison, M., Ruzzo, W. and Ullman, J. (1976) Protection in Operating Systems. *CACM*, **19**, 461-471. http://dx.doi.org/10.1145/360303.360333

[2] Snyder, L. (1981) Formal Models of Capability-Based Protection Systems. *IEEE Trans on Computers*, **30**, 172-181. http://dx.doi.org/10.1109/TC.1981.1675753

[3] Solworth, J.A. and Sloan, R.H. (2004) A Layered Design of Discretionary Access Controls with Decidable Safety Properties. *Proceedings*, 2004 *IEEE Symposium on Security and Privacy*, 9-12 May 2004, 56-67. http://dx.doi.org/10.1109/secpri.2004.1301315

[4] Li, N.H. (2008) How to Make Discretionary Access Control Secure against Trojan Horses. *International Parallel and Distributed Processing Symposium/International Parallel Processing Symposium—IPDPS* (*IPPS*), 1-3.

[5] Ferraiolo, D. and Kuhn, D.R. (1992) Role-Based Access Control. 15*th National Computer Security Conference*, Baltimore, 554-563.

[6] Chen, F.-Z. and Hong, F. (2003) Task-Based Access Control Model. *Mini-Micro System*, **24**, 621-624.

[7] Zhao X.F. and Guo, Y.B. (2007) An Access Control Model Based on Role and Task. *Information Security*, **3**, 63-64.

[8] Thomas, R.K. and Sandu, R.S. (1997) Task-Based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-Oriented Authorization Management. *Proceedings of the* 11*th IFIP WG* 11.3 *Conference on Database Security*, Lake Tahoe, August 1997, 166-181.

[9] Zheng, J., Zhang, Q.K., Zheng, S.W. and Tan, Y. (2011) Dynamic Role-Based Access Control Model. *Journal of Software*, 6, 1096-1102. http://dx.doi.org/10.4304/jsw.6.6.1096-1102

[10] Uzun, E., Atluri, V., Vaidya, J., *et al.* (2014) Security Analysis for temporal Role Based Access Control. *Journal of Computer Security*, **22**, 961-996.

[11] Müldner, T., Leighton, G. and Miziolek, J.K. (2009) Parameterized Role-Based Access Control. *Information Security Journal*, **18**, 282-296.

[12] Nirmalrani, V. and Sakthivel, P. (2015) Framework for Providing Access to Web Data Bases Using Budget Aware Role Based Access Control. *Journal of Theoretical and Applied Information Technology*, **76**, 296-308.

[13] Huang, J., Qing, S.H. and Wen, H.Z. (2003) Timed Role Based Access Control. *Journal of Software*, **14**, 1944-1954.

[14] Guo, H., Li, Y.M. and Wang, L.F. (2006) Design and Research of Access Control Model Based on Role and Task.

Computer Engineering, **32**, 143-145.

[15] Luo, A.-D. (2009) Research and Practice on Task and Role Based Access Control Mode. Zhejiang Gongshang University, Hangzhou.

[16] Yang, F., Xue, Z.-X. and Shi, Y.-G. (2008) A Dynamic Authority Management Mechanism Based on Role. *Computer Engineering*, **7**, 99-102.

[17] Zhou, J.C., Zhang, J.Q. and Leng, W.H. (2009) Extensible Access Control Based on RBAC Model in the System. *Computer Engineering*, **35**, 145-147.

[18] Liu, Y., Wei, R.Y. and Chen, C.B. (2006) Research on an Extended Role Based Privilege Management Model (E-RBAC). *Computer Science & Engineering*, **28**, 126-128.

[19] Ferraiolo, D., Sandhu, R., Gavrila, S., Kuhn, D. and Chandramouli, R. (2001) Proposed NIST Standard for Role-Based Access Control. *ACM Transactions on Information and System Security*, **4**, 224-274. http://dx.doi.org/10.1145/501978.501980

[20] Sandhu, R., Coyne, E.J., Feinstein, H.L. and Youman, C.E. (1996) Role-Based Access Control Models. *IEEE Computer*, **29**, 38-47. http://dx.doi.org/10.1109/2.485845

[21] Bertino, E., Bonatti, P. and Ferrari, E. (2001) TRBAC: A Temporal Role Based Access Control Model. *ACM Transactions on Information and System Security*, **4**, 191-233. http://dx.doi.org/10.1145/501978.501979

[22] Joshi, J., Bertino, E., Latif, U. and Ghafoor, A. (2005) A Generalized Temporal Role Based Access Control Model. *IEEE Transactions on Knowledge and Data Engineering*, **17**, 4-23. http://dx.doi.org/10.1109/TKDE.2005.1

[23] Aich, S., Sural, S. and Majumdar, A.K. (2007) STARBAC: Spatiotemporal Role Based Access Control. In: Meersman, R. and Tari, Z., Eds., *On the Move to Meaningful Internet Systems* 2007: *Coop IS*, *DOA*, *ODBASE*, *GADA*, *and IS*, Springer, Berlin/Heidelberg, 1567-1582. http://dx.doi.org/10.1007/978-3-540-76843-2_32

[24] Uzuna, E., Atluria, V., Vaidya, J., Sural, S., Ferrara, A.L. and Parlato, G. (2014) Security Analysis for Temporal Role Based Access Control. *Journal of Computer Security*, **22**, 961-996.

[25] Uzun, E., Atluri, V., Vaidya, J. and Sural, S. (2013) Analysis of TRBAC with Dynamic Temporal Role Hierarchies. In: Wang, L.Y. and Shafiq, B., Eds., *Data and Applications Security and Privacy XXVII*, Springer, Berlin, 297-304. http://dx.doi.org/10.1007/978-3-642-39256-6_22