MATEC Web of Conferences 22, 01011 (2015)
DOI: 10.1051/matecconf/20152201011
© Owned by the authors, published by EDP Sciences, 2015

Task-role-based Access Control Model in Smart Health-care System

Peng Wang & Lingyun Jiang
College of Telecommunications & Information Engineering, Nanjing University of Posts & Telecommunications, Nanjing, Jiangsu, China

ABSTRACT: As the development of computer science and smart health-care technology, there is a trend for patients to enjoy medical care at home. Taking enormous users in the Smart Health-care System into consideration, access control is an important issue. Traditional access control models, discretionary access control, mandatory access control, and role-based access control, do not properly reflect the characteristics of Smart Health-care System. This paper proposes an advanced access control model for the medical health-care environment, task-role-based access control model, which overcomes the disadvantages of traditional access control models. The task-role-based access control (T-RBAC) model introduces a task concept, dividing tasks into four categories. It also supports supervision role hierarchy. T-RBAC is a proper access control model for Smart Health-care System, and it improves the management of access rights. This paper also proposes an implementation of T-RBAC, a binary two-key-lock pair access control scheme using prime factorization.

Keywords: access control, permission, task, task-role-based access control (T-RBAC), smart health-care system

1 INTRODUCTION

A small family Smart Health-care System is needed for patients who need medical care. According to this system, patients, doctors, nurses and guardians of the patients can share the health-care information. Doctors and nurses are able to diagnose the status of patients by reading the files in the small health-care system. In the system, patients can authorize others to be guardians with full authorities. The guardians can view some of the information through the limited permission in the system. The patients can also ask for medical help through the system. The system has a high request for the limited permissions for users. Neither can the users visit the non-authorized information, nor cannot visit the authorized information. Access control plays an important role in the health-care environment, because of various kinds of users. Access control is the main method for the implementations of data confidentiality and integrity.

Users in the Smart Health-care System visit the records a lot, and the records are private, not available for non-authorized users. However, the traditional access control models fail to meet the needs of the health-care system, because they focus directly on the management of users' access right.

There are three main traditional access control models: discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC) [1-3]. The supervisor in DAC has the highest permission for access control, deciding who can or cannot visit the information. Once the users in the health-care system leave, it needs the supervisor to reset every detail of the user. When it happens to massive subjects, the changes of organizations are complex. It will need a lot of human resources, and it cannot realize the dynamic access control. MAC cannot deal with the level of access control properly between reality and the health-care environment, and it overemphasizes the confidentiality [4-5]. RBAC does not support the concept of task, not taking active access control into considerations.

The purpose of this paper is to propose a suitable access control model, T-RBAC [6-7], for the health-care environment. Task and role are main aspects of the proposed model, and they have various characteristics related to access control. It comes out that the proposed model meets the requirements of access control in the health-care environment.

The remaining parts of this paper are organized as follows. Section 2 introduces the factors related to access control in the health-care system. Section 3 introduces the Task-role-based access control model. Section 4 proposes a mathematical implementation of T-RBAC, a binary two-key-lock pair access control scheme using prime factorization.

2 FACTORS RELATED TO ACCESS CONTROL IN THE HEALTH-CARE SYSTEM

To build an access control model for the health-care system, the basic factors of the system are needed to be figured out. In the system, users want to visit some specific information, and the final goal of access control is to decide whether an access request is valid or not. There are several factors that are related to the system, and the main ones are: users, organization, medical positions, medical roles, tasks, medical processes, and medical rules. The details will be discussed in the following part.

User: Users are the subjects of access control. They can be patients, guardians, nurses, and doctors in the health-care system.

Historic records: Historic records are the objects of access control. They can be files, tables in the database.

Organization: An organization is a group of people work together to achieve some common goals. Doctors and nurses can form an organization to supervise the conditions of patients.

Medical position and Medical role: Medical position and Medical role are similar but not the same. Medical position emphasizes management of different users, and Medical role emphasizes the work activities. They are used to authorize the access right of users.

Task: Task is the basic aspect of health-care work or health-care activity. Checking patients status, making reports, diagnosing, are the examples of task. The permissions of access control are assigned to tasks, and tasks are assigned to roles. At last, roles are assigned to users. A user can have one or several roles.

Medical process: A medical process is a set of tasks that are connected to achieve a certain aim. In the health-care system, a medical process can be described: the portable health-care equipment on the patients causes an alarm, and the doctors receive the signal, checking the files of the patients, diagnosing the situation, taking measures to solve the health-care issue. According to medical process, the tasks in the health-care system can be divided into two main aspects: active access control and passive access control. Tasks related to a health-care process are the examples of active access control. The nurses monitor the condition of patients is the case of passive access control.

Medical rule: A medical rule is a formal regulation, which regulates the way an organization conducts its activity. Separation of Duty is an example of medical rule.

3 TASK-ROLE-BASED ACCESS CONTROL MODEL

The proposed access control model, T-RBAC, is based on the RBAC model, taking the concept of task into consideration. T-RBAC model is used in the health-care environment to fulfill the management of access control. T-RBAC is an improved access control model, and it achieves the aim of access control through tasks. It also supports dynamic real-time security management. Task is the minimum unit of health- care activities. In the RBAC model (see Figure 1), the permissions are assigned to roles, and roles are assigned to users. In T-RBAC model (see Figure 2), the permissions are assigned to tasks, and tasks are assigned to roles. Users achieve the permissions of access control through roles. Medical tasks are the core elements in the proposed health-care system, and they keep the health-care system running. Taking the main factors in the health-care environment into consideration, T-RBAC model performs well. It improves the management of access control.

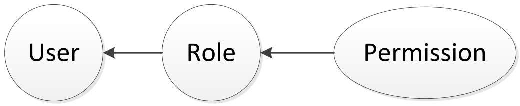

Figure 1. RBAC model

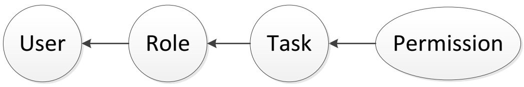

Figure 2. T-RBAC model

3.1 *Classification of tasks based on the health-care environment*

Tasks in the Smart Health-care System can be divided into four main categories: inheritable tasks, non-inheritable tasks, passive tasks and active tasks. Figure 3 shows the related factors for task classification in the system.

The concepts of inheritable or non-inheritable tasks are based on the structure of medical organization. The concept of role hierarchy is introduced in this model, and it has the connection with medical positions. In the medical organization, the doctor is in a higher position than nurses, but it does not mean doctors can inherit full access rights from nurses. T-RBAC emphasizes partial inheritable access right from lower medical positions. Inheritable tasks mean the higher position can inherit from lower position. Non-inheritable tasks mean the opposite way.

As discussed in section 2, passive or active tasks are distinguished from whether it belongs to a working process or not. If a task belongs to a medical process, it is active access control. The specific task categories are shown in Figure 4.

	Non-inheritable	Inheritable
Passive access	A	B
Active access	Null	D

Figure 3. Classification of tasks

Class A: The access permission of this task cannot be inherited to higher medical positions. The task does not belong to a medical process, either. Figure 5 shows a case of task A. In this case, doctors do not inherit access right from nurses, and the medical group can only visit some historic information stored in the database passively.

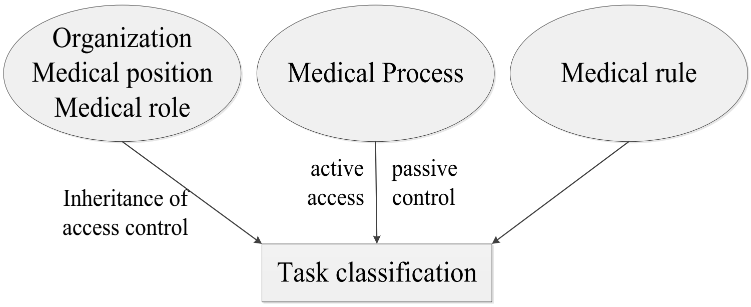

Figure 4. Related factors for task classification

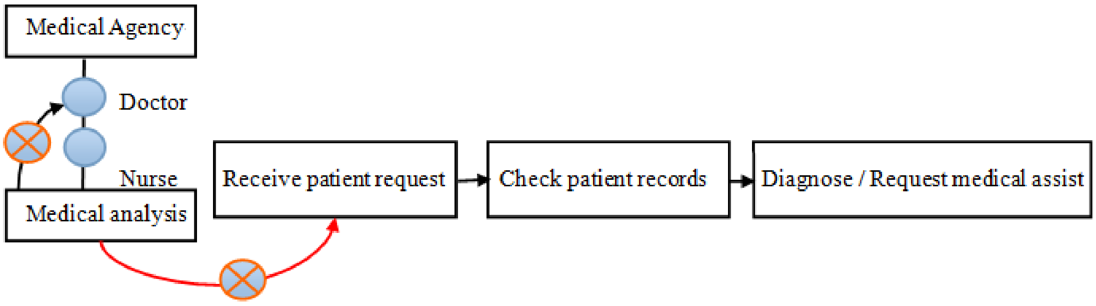

Figure 5. An example of class A

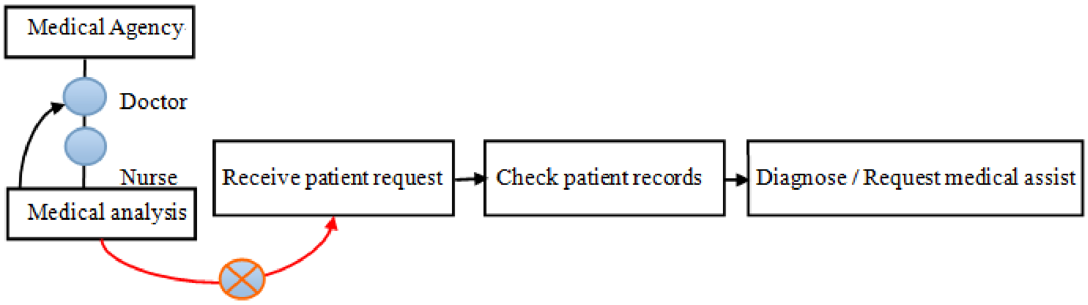

Figure 6. An example of class B

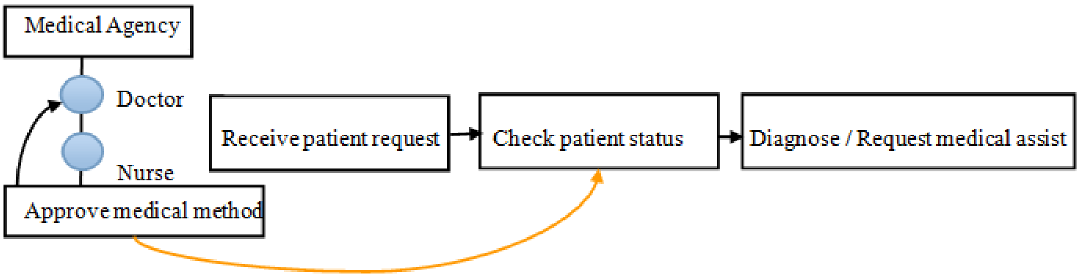

Figure 7. An example of class D

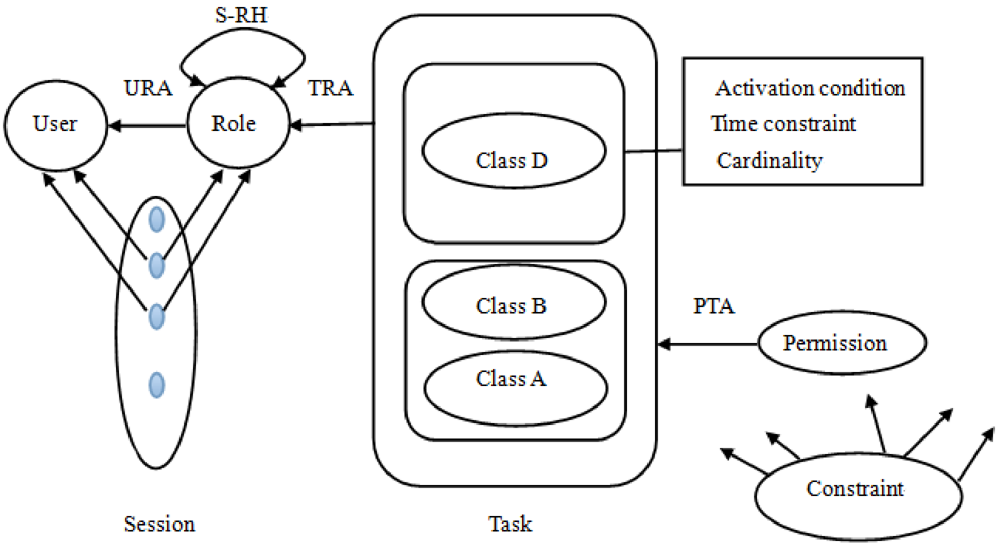

Figure 8. T-RBAC (URA: user-role assignment, S-RH: supervision role hierarchy, TRA: task-role assignment, PTA: permission-task assignment)

Class B: The access permission of task B can be inherited to higher medical positions. The task does not belong to a medical process. (Figure 6). Doctors extend part of access rights from nurses, but they still perform tasks passively.

Class D: The access permission of task D can be extended to higher medical positions. The task belongs to a medical process (Figure 7). During task D, medical staffs check patient status actively, and they approve medical method to give patients medical assist.

3.2 *Introduction of T-RBAC model*

Figure 8 shows an overview of Task-role-based access control model [8].

As shown above, there are three main traditional access control models, DAC, MAC, and RBAC. They are not appropriate for the Smart Health-care System, and the proposed T-RBAC has the advantages as follows: support task concept, access rights through tasks, partial inheritance from lower positions, support active access control, and so on.

From Figure 8, it shows how T-RBAC model works. Tasks are the most important issue in the Smart Health-care System. Almost all main activities are related to tasks. The permissions are assigned to tasks through permission-task assignment. Tasks are divided into four categories. There are three characteristics about active access control: Activation condition, Time constraint and Cardinality. Activation condition means the tasks belong to working process can be activated. Time constraint means the available time after tasks are activated. Cardinality means the maximal number of tasks activated at the same time.

Task-role assignment deals with the permissions between tasks and roles. S-RH means supervision role hierarchy, and it emphasizes the supervision between higher positions with lower positions, in case of the abuse of access control. User gets their access right through user-role assignment, and the user can access the characters of roles through sessions. Constraint means regulations and rules for the system, such as, separation of duty. It means the separation of responsibility and authority.

4 IMPLEMENTATION OF T-RBAC

4.1 *Implementation mechanisms of access control*

There are four main implementation mechanisms of access control, Access Control Matrix (ACM) [9], Access Control Lists (ACLs), Access Capabilities Lists, and Access Control Security Labels Lists (ACSLLs). Elements a_{ij} in Table 1 mean the specific access rights between the subjects (users) and objects.

Table 1. Access control matrix

	Object 1	Object 2	Object 3	Object 4
User 1	W	---	R	Own
User 2	---(**a_{ij}**)	R	---	---
User 3	R	Own	---	W

Note: W: Write, R: Read, Own: Ownership=full access right, ---: no access control right, m /n means the number of subjects/ objects in the system, aij means the access right between subjects with objects

4.2 Proposed implementation mechan*ism of T-RBAC*

In this paper, a new implementation mechanism, a binary two-key-lock pair access control scheme using prime factorization (TPB-2-KLP), is introduced to the implementation of T-RBAC. TPB-2-KLP uses access control matrix as the implementation method [10-11].

At the very beginning, the introduction of unique factorization theorem:

Every integer N (N>1) can be expressed as the product of some prime numbers, and the formula can be described: $N=P_1^{n1} \cdot P_2^{n2} \cdots P_r^{nr}$. ($P_i$ means different prime numbers. i=1,2......r, $P_1<P_2<.....<P_r$. n_i means how many time a prime number appears.)

In TPB-2-KLP, both subject and object are assigned a key and a lock. Data structure used in this mechanism: table of key-lock belongs to the subject or object, the stack of prime number belongs to the subject (PS) or the object (PO). In the prime stack, smaller prime numbers are stored at the top of stack, and they are prepared to be used as keys of subjects or objects by order (2, 3, 5, 7...). In the table of key-lock, it records the value of keys, lock vectors and time stamps. When the subjects or objectors enter the system, each of them will be assigned a unique time stamp, TS_i for subjects and $TS_j^{'}$ for objects. The PS/PO will assign a prime number for subjects/ objects (K_i/ $K_j^{'}$). The value of keys and lock vectors will be added into the key-lock table. The value of time stamp is determined by the time sequence of entering the system. Earlier entrance means smaller value of time stamp.

In Table 1, the element a_{ij} means the access right between subjects with objects. Thus, a_{ij} can be described in binary form (Equation (1)).

$$a_{ij}=\left(a_{ij}^{(b)}a_{ij}^{(b-1)}\cdots a_{ij}^{(1)}\right)2=\sum_{x=1}^{b}a_{ij}^{(x)}2^{x-1} \quad (1)$$

(b means the digits when a_{ij} is in binary form, $a_{ij}^{(x)} \in \{0, 1\}$)

The lock vectors of subjects (S_i) and objects (O_j) can be calculated by the formulas below:

$$L_{i(x)}=\prod_{j=1}^{n}(k_j^{'})^{a_{ij}(x)},\ (x=1,2,...,b,\ i=1,2,...,m) \quad (2)$$

$$L_{j(x)}^{'}=\prod_{i=1}^{m}(k_i)^{a_{ij}(x)},\ (x=1,2,...,b,\ j=1,2,...,m) \quad (3)$$

(L_i means the lock vectors of S_i, $L_j^{'}$ means the lock vectors of O_j, K_i means the key value of S_i, $K_j^{'}$ means the key value of O_j , $a_{ij}^{(x)} \in \{0, 1\}$, m /n means the number of subjects/ objects in the system)

The example of TPB-2-KLP is shown as follows:

In a given system, S_1, S_2, S_3 are the subjects, and O_1, O_2, O_3 are the objects. The access control matrix and its binary form are shown in Table 2. The number 1,2,3,4 mean the access right of read, write, execute and full-ownership. The time sequence of entering the system: S_1, O_1, S_2, O_2, O_3, S_3. Time stamps in Table 3 follow the entering sequence of subjects and objects.

Table 2. The access control matrix and its binary form

Object Subject	O_1	O_2	O_3
S_1	4 (100)	0 (000)	1 (001)
S_2	2 (010)	1 (001)	4 (100)
S_3	2 (010)	4 (100)	1 (001)

Table 2 shows the digits of a_{ij} in binary form, so the value of b in Equation (2)-(3) is 3. When S_1 enters the system, the PS assigns the prime number 2 to be Key value of K_1. L_1 is (0,0,0) in Table 3, because there are no objects in the system before S_1 enters. O_1 is the first object that enters the system, so the value of $K_1^{'}$ is 2. The value of $L_1^{'}$ can be figured out by Equation (3) by using the value of K_1. At the very moment, m=1 and n=1.

According to the analysis above, the value of K_i, TS_i, $K_j^{'}$, $TS_j^{'}$ are shown in Table 3. Using Equations (2)-(3), the lock vectors can be calculated in Table 3.

Table 3. Key-lock table of subjects and objects

	K_i	L_i	TS_i		$K_j^{'}$	$L_j^{'}$	$TS_j^{'}$
S_1	2	(0,0,0)	0	O_1	2	(2,1,1)	1
S_2	3	(1,2,1)	2	O_2	3	(1,1,3)	3
S_3	5	(3,2,5)	5	O_3	5	(3,1,2)	4

In the proposed implementation mechanism, Equations (2) (3) are used to verify the access right of subjects. If $TS_i < TS_j^{'}$, K_i, $L_j^{'}$ and Equation (3) are used to test whether the subject has the permission or not. On the contrary, $K_j^{'}$, L_i and Equation (2) are functioned.

To realize the T-RBAC model, three similar matrices are needed: permission-task matrix, task-role matrix, and role-user matrix. The elements in these matrices mean the right of access control. In the permission-task matrix, permission is the object, and task is the subject. Similarly, in the task-role matrix, task is the object, and role is the subject. In the role-user matrix, role is the object, and user is the subject. These three matrices work in the sequence of role-user matrix, task-role matrix, permission-task matrix. Users get their roles through role-user matrix, and then go on checking task-role matrix and permission-task matrix, otherwise the sequence breaks. These three matrices are applied into TPB-2-KLP mechanism for T-RBAC, and the mechanism proves to be effective.

REFERENCES

[1] R.S. Sandhu, E. J. Coyne, H. L. Feinstein, C. E. Youman. 1996. Role-based access control models. *IEEE Computer*, 29(20): 38-47.

[2] R.S. Sandhu, V. Bhamidipati, E. Coyne, S. Ganta, and C. Youman. 1997. The ARBAC97 model for role-based administration of roles: Preliminary description and outline. *Proceedings of the Second ACM Workshop on Role-Based Access Control*.

[3] D.F. Ferraiolo, D. R. Kuhn. 1992. Role based access control. *15th National Computer Security Conference*.

[4] Peiying Shao, Shuling Su. 1999. Security design and implementation based on traditional mandatory access control. *Computer Engineering and Applications*, (8): 58-60.

[5] Huaiyu Liu, Weiqing Li. 1999. The technology of access control. *Electronic Outlook and Decision-making*. 42-46.

[6] R.K. Thomas, Thomas, R. Sandhu. 1997. Task-based authorization controls (TBAC): a family of models for active and enterprise-oriented authorization management, *Proceedings of the IFIP WG 11.3Workshop on Database Security, Vancouver, Canada*.

[7] S.Oh, S. Park. 2000. Task-role-based access control model for enterprise environment, *J Korea Inst Information Security Cryptology*, 11 (1): 2.

[8] Sejong Oh*, Seog Park, 2003. Task-role-based access control model, *Information Systems*, 28: 533-562.

[9] Butler W. Lampson. 1971. Protection. Proc. 5th Princeton Conf. On Information Science and Systems, Princeton, pp: 437.

[10] Hwang, M.S., Tzeng, W.G., Yang, W.P. 1994. A two-key-lock-pair access control method using prime factorization and time stamp IEICET trans Inf & Syst, E77-D(9): 1042-1046.

[11] Hwang, M.S., Tzeng, W.G. & Yang, W.P. 1996 An access control scheme based on Chinese Remainder Theorem and time stamp concept. *Computers & Security*, 15(1): 73-81.