Efficient Role Based Access Control Method in Wireless Environment

Song-hwa Chae[1], Wonil Kim[2], and Dong-kyoo Kim[3*]

[1] Graduate School of Information and Communication, Ajou University, Suwon, Korea
portula@ajou.ac.kr
[2] College of Electronics and Information Engineering, Sejong University, Seoul, Korea
wikim@sejong.ac.kr
[3] College of Information and Computer Engineering, Ajou University, Suwon, Korea
dkkim@ajou.ac.kr

Abstract. As resource sharing is common practice in distributed and wireless network, authentication and authorization become important issue in the security field. Many access control mechanisms including Role-Based Access Control (RBAC) are widely used for authorization. The common use of the wireless network imposes not only existing problems such as secure system management but also new problems such as limited storage and transaction size. In this paper, we propose an access control method that solves these problems for wireless environment. The proposed system uses bit pattern to represent access control information hence reduces transaction size and enhances security level. This system employs neural networks instead of access control tables, which reduces storages for role-permission tables and extra mutual exclusive data tables.

1 Introduction

Recently wireless networking has become more common, through which provides various types of contents to users. As technology advances, wireless terminals provide in various forms of services such as multi media contents, mailing and banking services. For the secure communications in between, it is essential for service providers to know user's information such as '*who connect'* and '*what is user's rights*'. It can only be supported by proper authentication and authorization methods.

Wireless networks have several problems that are different from those encountered in wired network. Consequently implementing security service is more difficult than in wired network. Wireless network is more vulnerable to unauthorized access. Today, a mobile phone is a common terminal for wireless service. The mobile phone has limited memory and the power that is less than personal computer. For that reason, it is difficult to have full fledged security service to mobile phone. It is a formidable task how to make secure data with these reduced transmissions.

Much progress has been made on access control mechanism in information security. Generally access control mechanism is categorized into three areas, such as

* Author for correspondence +82-2-3408-3795

I. Niemegeers and S. Heemstra de Groot (Eds.): PWC 2004, LNCS 3260, pp. 431–439, 2004.

mandatory access control (MAC), discretionary access control (DAC) and role-based access control (RBAC). MAC is suitable for military system, in which data and users have their own classification and clearance levels respectively. DAC is another access control method on the objects with user and group identifications. RBAC has emerged as a widely acceptable alternative to classical MAC and DAC [2][5]. It can be used in various computer systems. Since service provider should support different levels of service to users according to user's level, access control is important security service.

In this paper, we propose an efficient authorization method in wireless environment. In the proposed system, access control information is represented by bit patterns which are obtained via neural network. It reduces the size of access control information and enhances security level of wireless communication in which small data size for transaction size is preferable. We employ neural network for role-based access control mechanism instead of fixed tables, hence the proposed system uses bit pattern to represent access control information. In addition, it enables to eliminate the search time of relation tables and easily detects mutual exclusive roles.

This paper is organized as follows Chapter 2 explains the basic concept of RBAC and the neural network. Chapter 3 describes the role based access control method in wireless environment. Chapter 4 simulates the proposed system and Chapter 5 concludes with future works.

2 Background

2.1 RBAC

RBAC uses the concept of *role*. It does not allow users to be directly associated with permissions, instead each user can have several roles and each role can have multiple permissions. There are three components of RBAC: users, roles, and permissions. Each group can be represented as a set of user U, a set of role R, and a set of permission P.

- $U = \{u_1, u_2, \ldots, u_i\}$
- $R = \{r_1, r_2, \ldots, r_j\}$
- $P = \{p_1, p_2, \ldots, p_k\}$

Two different types of association must be managed by the system; one is the association between user and role, the other is the association between role and permission. It is characterized as user-role (UR) and role-permission (RP) relationship. Consequently, in order to have proper management, the system needs to maintain two separate association tables.

- $UR = \{u \in U \mid u \rightarrow 2^{|R|}\}$
- $RP = \{r \in R \mid r \rightarrow 2^{|P|}\}$

Conflicts of interest in a role-based system may arise as a result of a user gaining authorization for permissions associated with conflicting roles [4]. For example, if one role requests expenditures and another role approves them, the system must prohibit the same user from being assigned or active to both roles. In order to solve these conflict problems, there have been many researches since middle of 1990's.

Finally, National Institute of Standards and Technology (NIST) proposed two Separation of Duty (SOD) reference models in 2001; Static Separation of Duty (SSD) and Dynamic Separation of Duty (DSD). To implement these reference models, the system must have extra tables to protect against activating mutual exclusive roles. According to the NIST reference models, SSD should check the mutual exclusive role in every role assignment, and the role-permission in every user's session request. DSD should check all the three relations for every user's session request. SSD is rarely used in practice and DSD imposes a lot of overload in a system with many users due to excessive table accessing time. In fact, general processes do not always use mutual exclusive roles.

2.2 Neural Network

Artificial neural networks refer to computing systems whose central theme is borrowed form the analogy of biological neural networks [3]. It is composed of a large number of highly interconnected processing elements that are analogous to neurons and are tied together with weighted connections. These connection weights store the knowledge necessary to solve specific problems. Artificial neural networks are being applied to an increasing number of real world problems of considerable complexity, control problems, where the input variables are measurements used to drive an output actuator, and the network learns the control function. They are often good at solving problems that are too complex for conventional technologies and are often well suited to problems that people are good at solving, but for which traditional methods are not [4].

The proposed system employs backpropagation algorithm. It is one of method of neural network learning algorithm, which uses input data and desired output data for supervised learning. The weights between nodes are updated to reduce the difference of actual output and desired output by iterative learning process.

3 Role Based Access Control in Wireless Environment

Wireless network is popular way to use Internet. As technology advances, various services are possible in handheld terminals such as tablet PC, mobile phone and PDA. Most of wired service providers now offer wireless Internet services on banking and stock trading. These services should be processed in secure environment. Especially, authentication and authorization are important security service to achieve safe transaction. ID/password checking method is widely used authentication method whereas role-based access control is popular authorization method.

The resources of wireless network are limited hence a system developer must consider both the capability of the system and the handheld terminal. For that reason, implementing security service in wireless network is more difficult than in wire network. It is important issue that how to make smaller secure data and reduce the number of transactions.

In this paper, we propose an access control method to alleviate the mentioned problems. This system employs neural networks for authorization which represents access control information using bit patterns. This pattern reduces the size of access

control information. In order to achieve efficient access control, we also propose a new implementation method for RBAC. It uses neural networks instead of access control tables. In addition, it enables to eliminate the search time of relation tables and easily detects mutual exclusive roles which was an inherent problem in RBAC.

3.1 System Architecture

When the users log into a system, they should be authenticated by that system. The system should use minimal authentication transactions for wireless environment. The ID/password method is a simple authentication method. After authenticating user, the system generates user's access control information from user information in the system. The user is given access control information that is represented by bit pattern. The user submits this bit pattern to use specific services from system. The system checks user's right of resources using neural network whenever the user wants to access a resource.

The proposed system represents all the access control information by bit patterns. Generally for a system employing RBAC, it needs at least 3 fixed tables for a session, such as user-role table, role-permission table and mutual excusive role table. It requires extra storage as well as checking time for both role-permission and mutual exclusive role tables. To cope with these problems, the proposed RBAC system uses neural networks instead of fixed RBAC relation tables. By employing neural network in RBAC, the system can check the user's permissions without using relation tables in each corresponding session. This method does not only reduce access time for authorization but also prevent a user from being activated with mutual exclusive permission.

It is assumed that roles, permissions and their associations are static information, whereas associations between user and role are dynamically changed. User can have several roles and role may have multiple permissions too. The process of this system consists of the following three phases: 1) neural network learning phase, 2) role assignment phase, 3) permission extraction phase. Depending on whether a user's role set contains mutual exclusive roles or not, two cases are considered in system processing.

3.2 Non-mutual Exclusive Role Case

This case is SSD in RBAC. Users do not contain mutual exclusive roles. Thus, the system checks only user's role and permission.

1. neural network learning phase
   In the learning phase, the training data is the role-permission relation provided by the system administrator. Each role and permission is represented by input and output respectively. The value of input (role) and output (permission) is either '1' (active/permit) or '0' (non-active/denial). Since the proposed system should be able to accommodate hierarchical RBAC, the high level role may contain the low level permissions too. After the neural network learns the relation, the system should be able to respond user's permissions for access control.

2. role assignment phase
   In this system, a user is defined as a human being and a role is a job function within the context of an organization [4]. Therefore, the system can assign multiple roles to the user according to the required job. The association of the user and the role can be changed dynamically. Our RBAC system can successfully respond to these changes. It produces the proper set of permissions dynamically even though the user-role association changes.
3. permission extraction phase
   When the user tries to access data, the system makes decisions such as permit or denial. The proposed system makes the decision using the user's permission set. This permission set is generated by the neural network in the user logging phase. This set has the user's whole permissions. Since all the permissions do not contain any mutual exclusive role, mutual exclusive resolution is not necessary.

3.3 Mutual Exclusive Role Case

This case uses DSD in RBAC. The user can have multiple roles, potentially including mutually exclusive roles, such as applying for expenses and approving those same expenses. These two permissions come from two different roles. The main point of this process is to reduce the role set, so that the reduced role set does not have any mutual exclusive permission. With this process, the neural network will be able to produce the reduced permission set according the reduced role set. The process of producing the reduced permission set is as follows.

1. neural network learning phase
   In this case, we represent permissions with three types of values; '0','1', and '0.5'. The '0' and '1' has the same meaning as defined in non-mutual exclusive role case. Especially, '0.5' means mutual exclusive permission. An example of this is shown in Table 2. If there is a high level role containing low level mutual exclusive permission, that node (permission) is also set to '0.5'. In this case, second neural network is employed to produce the reduced role set. It will lean the relation between permissions and roles. Each permission and role will be represented by input and output respectively. An example of this is shown in Table 3.
2. role assignment phase
   Same as in non-mutual exclusive case.
3. permission extraction phase
   The DSD system must decide permit or denial on the given request in every session. The proposed system makes the decision using the user's permission set. This permission set is generated by the neural network in the user logging phase. This set has the user's whole permissions including mutual exclusive permission. The process of making the whole permission set is similar to non-mutual exclusive case. When the user tries to access data defined as mutual exclusive permission, the system recognizes mutual exclusion case using permission's value, which is approximately '0.5'. In this case, the system should make a least user's permission set for the session. This permission set is a reduced set which does not contain mutual exclusive permission. Second neural network is employed to produce reduced role set. In order to limit user's permission, it changed a bit to '1' in user's permission set and others to '0'. This changed user's permission set is used to

produce the limited role set. The limited role set is used to produce the reduced permission set using the first neural network for this session. After this process, the user has reduced permission set which is not containing mutual exclusive permission. In any session, if the request permission is found to be the mutual exclusive permission, the system does the same process recursively. After the session, it will return to the previous permission set. This process protects from executing mutual exclusive permission in any given session.

4 Simulation

The proposed system was evaluated on a typical customer class hierarchy in Fig 1. It consists of 2 Internet services in a wireless terminal that performs stock trading and remote banking service. The customer class has 10 roles and 6 mutual exclusive roles. This system can be extended to accommodate unlimited number of users depending on services. The evaluation result showed that the proposed system was able to detect mutual exclusive role activation and produced the user's permission set using reduced role set. The role-permission relationship of Fig 1 is represented in Table 2. The wireless terminal does not need to contain user's whole access control information. It holds just small size of bit pattern which is user's whole role set. When user needs service, he/she submits this bit pattern to server which supports specific service.

For instance, if the system has 8 roles and a user assigned 2 roles, it can be represented as Table 1. In this case, User1's access control information is [0100000100].

Table 1. Example of roles

Role	FC1	GC1	GC3	VIP1	Admin	VIP2	GC4	GC2	Studt1	Customer
Bit	0	1	2	3	4	5	6	7	8	9
User	0	1	0	0	0	0	0	1	0	0

We assumed that VIP1 and VIP2 had mutual exclusive roles. GC1 and GC3, GC 2 and GC4 had mutual exclusive roles too. Therefore, the permissions of these roles are set to '0.5'.

We trained two neural networks using Table 2 and Table 3 respectively, with learning and the momentum rates are 0.001. The proposed neural network had one hidden layer (30 nodes) and used sigmoid functions for hidden and output nodes. The five sample users and their role set (representations) are given below;

- User1 : {GC1, GC2} : (0100000100)
- User2 : {GC1, GC4} : (0100001000)
- User3 : {GC1} : (0100000000)
- User4 : {VIP1, GC2} : (0001000100)
- User5 : {Admin} : (0000100000)

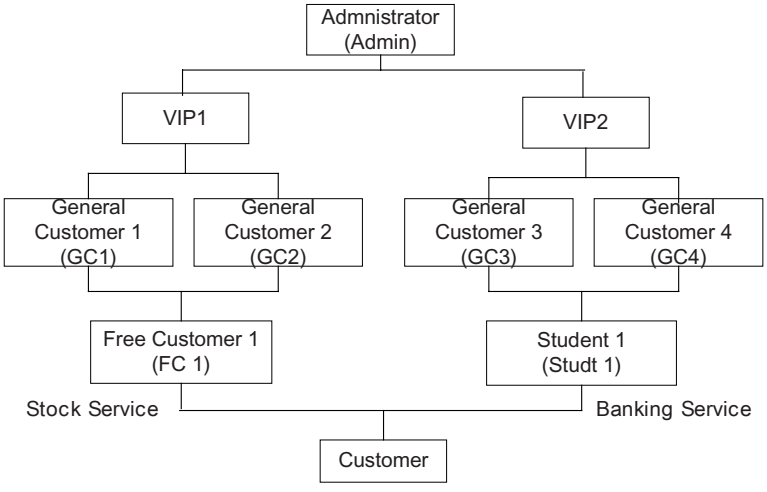

Fig. 1. Example of a role structure for wireless service

Table 2. Input and output data for first neural network training

	Input data	Out data									
	Role	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10
Customer	0000000001	0	0	0	1	0	0	0	0	0	0
FC 1	1000000000	0	0	0	1	0	0	1	0	0	0
Studt1	0000000010	0	1	0	1	0	0	0	0	0	0
GC1	0100000000	0	0	0	1	0	0	1	0	1	0
GC2	0000000100	0	1	0	1	0	0	0	0	0	1
GC3	0010000000	1	0	0	1	0	0	1	0	0	0
GC4	0000001000	0	1	0	1	0	0	0	1	0	0
VIP1	0001000000	0.5	0	1	1	0	0	1	0	0.5	0
VIP2	0000010000	0	1	0	1	0	1	0	0.5	0	0.5
Admin	0000100000	0.5	1	0.5	1	1	0.5	1	0.5	0.5	0.5

The system produces user's whole permission set using first neural network. If the user tries to access any mutual exclusive permission, it produces reduced role set using second neural network. For example, user5 is assigned as Admin, the first neural network will produced the whole permission set of {p1, p2, p3, p4, p5, p6, p7, p8, p9, p10} with access values between 0.0 and 1.0. If Admin tries to access any mutual exclusive permission, such as p9, the system recognizes its mutual exclusive case and produces the reduced role GC1 using second neural network. As a result, the role of user5 which was originally defined as Admin, has reduced to GC1 in this

particular session and the permission sets as {p4, p7, p9} accordingly. The whole role and permission set and reduced role and permission set of User1~ User5 are shown in Table 4.

Table 3. Input and output data for second neural network training

	Input data										Out data
	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10	Role
Customer	0	0	0	1	0	0	0	0	0	0	0000000001
FC 1	0	0	0	1	0	0	1	0	0	0	1000000000
Studt1	0	1	0	1	0	0	0	0	0	0	0000000010
GC1	0	0	0	1	0	0	1	0	1	0	0100000000
GC2	0	1	0	1	0	0	0	0	0	1	0000000100
GC3	1	0	0	1	0	0	1	0	0	0	0010000000
GC4	0	1	0	1	0	0	0	1	0	0	0000001000
VIP1	0	0	1	1	0	0	1	0	0	0	0001000000
VIP2	0	1	0	1	0	1	0	0	0	0	0000010000
Admin	0	1	0	1	1	0	1	0	0	0	0000100000

Table 4. The whole role set and reduced role set

Case	Whole Role Set	Whole permission Set	Requested Job(permission)	Reduced Role Set	Reduce Permission Set
user1	GC1,GC2	{p2,p4,p7,p9,p10}	p9	GC1	{p4,p7,p9}
user2	GC1,GC4	{p2,p4,p7,p8,p9}	p8	GC4	{p2,p4,p8}
user3	GC1	{p4,p7,p9}	p9	GC1	{p4,p7,p9}
user4	VIP1,GC2	{p1,p2,p3,p4,p7,p9,p10}	p10	GC3	{p2,p4,p10}
user5	Admin	{p1,p2,p3,p4,p5,p6,p7,p8,p9,p10}	p9	GC1	{p4,p7,p9}

5 Conclusion and Future Works

Wireless network becomes common in these days as many people use Internet service in wireless environment. As wireless technology advances, users can access various types of contents such as multi media, bank account and stock trading. However, users' terminals such as mobile phone and PDA still have limited memory and computing power. Consequently they are equipped with limited security feature. Therefore, reducing data and transaction size is very important in wireless Internet. In addition, both authentication and authorization should be well defined and properly controlled for secure Internet service. Access control method such as RBAC is a popular method used to satisfy these security requirements.

In this paper, we proposed a novel access control method in wireless environment. In order to reduce access control information, we use bit pattern and process this pattern to neural networks. This reduced amount of information in wireless communication enhances security level. The proposed methods can be applied dynamically with user's role change. It has advantages of not using multiple storages for role-permission tables and extra mutual exclusive data tables. It also reduces access time by eliminating excessive table search for mutual exclusive roles. This method can be easily extended to various access control mechanisms and suitable for wireless network environment.

References

1. Rumelhart, D. E., Hinton, G. E., and Williams, R. J. Learning representations by back-propagating errors. Nature, 323, (1986) 533-536
2. E.H.Choun, A Model and administration of Role Based Privileges Enforcing Separation of Duty. Ph.D. Dissertation, Ajou University(1998)
3. K.Mehrotra, C.K.Mohan,S.Ranka, Elements of Artificial Neural Networks, MIT Press (1997)
4. D.F.Ferraiolo, R.Sandhu, E.Gavrila, D.R.Kuhn, R.Chandramouli, Proposed NIST Standard for Role-Based Access Control, ACM Transactions on Information and System Security, Vol4, No3 (2001) 224-274
5. G.Ahn, R.Sandhu, Role-Based Authorization Constraints Specification, ACM Transactions on Information and System Security, Vol3, No4,207-226 (2000)
6. D.FFerraiolo, J.F.Barkley, D.R. Kuhn, A Role-Based Access Control Model and Reference implementation Within a Corporate Intranet, ACM Transactions on Information and System Security, Vol2, No1 (1999) 34-64
7. S. Farrell, An Internet Attribute Certificate Profile for Authorization, RFC 3281,(2002)