Malaysian Journal of Computer Science, Vol. 14 No. 2, December 2001, pp. 20-25

ROLE-BASED ACCESS CONTROL IN KIDNEY DIALYSIS INFORMATION SYSTEM

Boon Peng Lim, Omar Zakaria and Mustaffa Kamal Mohd Nor
Faculty of Computer Science & Information Technology
University of Malaya
50603 Kuala Lumpur
Tel: 603-79676341 / 6383
Fax: 603-79579249
email: boonpeng@hotmail.com
omar@fsktm.um.edu.my
mustaffa@fsktm.um.edu.my

ABSTRACT

Role-Based Access Control in Kidney Dialysis Information System (RBAC-KDIS) uses the role-based access control mechanism to control unauthorised access to patient medical information in KDIS. This RBAC is a flexible and policy-neutral access control technology. Its properly administered system enables users to carry out a broad range of authorised operations. For example, permissions are not assigned to users but to the roles, thus providing great flexibility in administration and cost reduction. This system was developed using Microsoft Visual InterDev and the Web server is Personal Web Server under the Windows '98 platform. Two major sections in RBAC-KDIS are the administrator and the patient record sections.

Keywords: ***RBAC, Administration RBAC (ARBAC), Kidney Dialysis Information System***

1.0 INTRODUCTION

Computer security is the protection of the confidentiality, integrity and availability of automated information. Security mechanisms are used to prevent all the security services that are provided in computer system and networking. Today, most of these security mechanisms are used by computer systems for authentication, access control, audit trail and cryptography.

In a traditional medical system, the protection of patient records information is the responsibility of individual institutions such as hospitals, medical centers, physicians and nurses. Now using highly information technologies such as the Internet, World Wide Web and high-speed networking, patient information can be shared among patients, physician's offices and other related organisations.

This will bring health care industry to move towards to a more open medical information infrastructure and to improve the quality of health care. At the same time, health care industry also presents a number of new challenges in enforcing a patient medical information to keep it in confidentiality and availability. An open health care delivery system like Tele-Medicine requires integrated security management techniques to prevent the existence of serious potential breaches of privacy and security.

Role-Based Access Control (RBAC) is one of the access control mechanisms to address many of the requirements of security management in distributed information systems. Therefore, this paper focuses on how to implement RBAC in Tele-Medicine. An example of Tele-Medicine application is Kidney Dialysis System.

2.0 OBJECTIVE

From the survey that has been done [1], it was found that many organisations currently attempting to incorporate an RBAC capability within one of their products are lacking a complete prototype of RBAC. This is because RBAC is more flexible and suitable to control unauthorised access rather than other access control mechanisms.

Therefore, the objectives of this paper are to:

i) define basic ideas of RBAC and Administration of RBAC (ARBAC).
ii) perform a case study by using RBAC in a selected Tele-Medicine application, i.e. a kidney dialysis system, after a thorough risk analysis.
iii) configure three types of situation for roles and permissions such as assignable, assigned and unassignable.
iv) develop the RBAC-KDIS as a part of control against unauthorised access to patient medical information.

3.0 METHODOLOGY

The problems are viewed from five different perspectives on how to develop an access control mechanism to enhance security in patient medical information.

i) There are three parts that must be considered. They are role-based access control, administration role-based access control and Tele-Medicine.
ii) Analysis process is implemented by using the role-based access control mechanism of the targeted Tele-Medicine's security. This includes defining the assignable, assigned and unasssignable situations to achieve the completed access control mechanism. Consequently, RBAC-KDIS is designed as the solution for access control in patient records.
iii) Designing the RBAC in Kidney Dialysis Information system (RBAC-KDIS) is based on the concepts of RBAC and analysis of kidney dialysis system.
iv) Coding the RBAC-KDIS is done by using Microsoft Visual InterDev.
v) Testing the RBAC-KDIS that has been developed.

4.0 ARCHITECTURE OF RBAC-KDIS

The development framework for the RBAC-KDIS follows along five phases mentioned above which will be described in full in this section.

4.1 Literature Review

The concept RBAC has been used with a multi-user computer system and multi-application online system since the late 1960s and early 1970s. However, RBAC has rapidly emerged in the 1990s as a promising technology for managing and enforcing security in large-scale enterprise-wide systems, largely because of the non-existing enhancement in the traditional Mandatory Access Control (MAC) and Discretionary Access Control (DAC) used in many computer systems and networks. Thus, RBAC is an alternative to traditional MAC and DAC policies that is currently attracting increasing attention, particularly for commercial applications [2].

RBAC [4] is a family of reference models in which permissions are associated with roles, and users are assigned to appropriate roles. This greatly simplifies management of permissions. Roles are created for the various job functions in an organization and users are assigned roles based on their responsibilities and qualifications. Users can be easily reassigned from one role to another. Roles can be granted new permissions as new applications and systems are incorporated. Besides that, permissions can be revoked from roles if necessary.

A role hierarchy defines the roles that have uniquely attributes and may "contain" other roles, that is, one role may implicitly include the operation, constraints, and objects that are associated with another role. Role hierarchies are a natural way of organising roles to reflect authority responsibility and competency [3]. Constraints are an important aspect of RBAC, which can apply to the preceding components that include users, roles, permissions, or sessions. A common example is the mutually disjoint roles, such as, a purchasing manager and an accounts payable manager as the same user, is not permitted to be a member of both roles because this creates a possibility for committing fraud.

A major purpose of RBAC is to facilitate access control administration and review. This RBAC idea greatly simplifies management of authorisation while providing opportunities with great flexibility in specifying and enforcing enterprise-specific security policies, and for streamlining the security management process. RBAC is able to support a number of products that can be directly formed or combined within one of their products.

Administration RBAC (ARBAC) involves control over components such as roles, users, and permissions. These include creations and deletion of roles, creation and deletion of permissions, assignment of permissions to roles and their removal, creation and deletion of users, assignment of use to roles and their removal. Moreover, definition and maintenance of the role hierarchy, definition and maintenance of constraints; all of these in turn are for administrative roles and permissions. It has three components or sub-models called user-role assignment (URA97), permission-role assignment (PRA97) and role-role assignment (RRA97) [4, 5, 6, 7, 8].

Imaging Science and Information System (ISIS) system, Department of Radiology, the Clinical Economics Research Unit (CERU) and the Division of Nephrology in the Department of Medicine at Georgetown University Medical Center, Washington DC, have joint together to implement the kidney dialysis system project, named as Phoenix [9]. The objectives of this project are to provide Tele-Medicine services for kidney dialysis patients including creating, managing, transferring, and using electronic health data to provide decision support and information services for care-givers.

4.2 System Analysis

In this section, analysis has been done to the entire possible requirements to implement role-based access control mechanism. It consists of two main sections, which are the RBAC section and ARBAC section in Tele-Medicine: Kidney Dialysis Information System. In the RBAC section, examination of the basic task and permissions of the roles such as nurse, nurse supervisor, physician, engineer, secretary and patient is done. It also takes into consideration the role hierarchy and constraints.

Users and roles in this kidney dialysis information system are small, so assigning a security officer for administrator RBAC only requires the security administrator role. A single security administrative role is enough to avoid skirmish in the scope of the administrative authority vested in administrative roles. The security administrator must be able to perform administration of the RBAC model such as assigning and revoking of permissions and roles to or from the users, definition and maintenance of role hierarchies and constraints.

4.3 System Design

A whole RBAC in Tele-Medicine: Kidney Dialysis Information System is divided into two major components, i.e. Administrator and Patient Records (See Fig. 1 and Fig. 2).

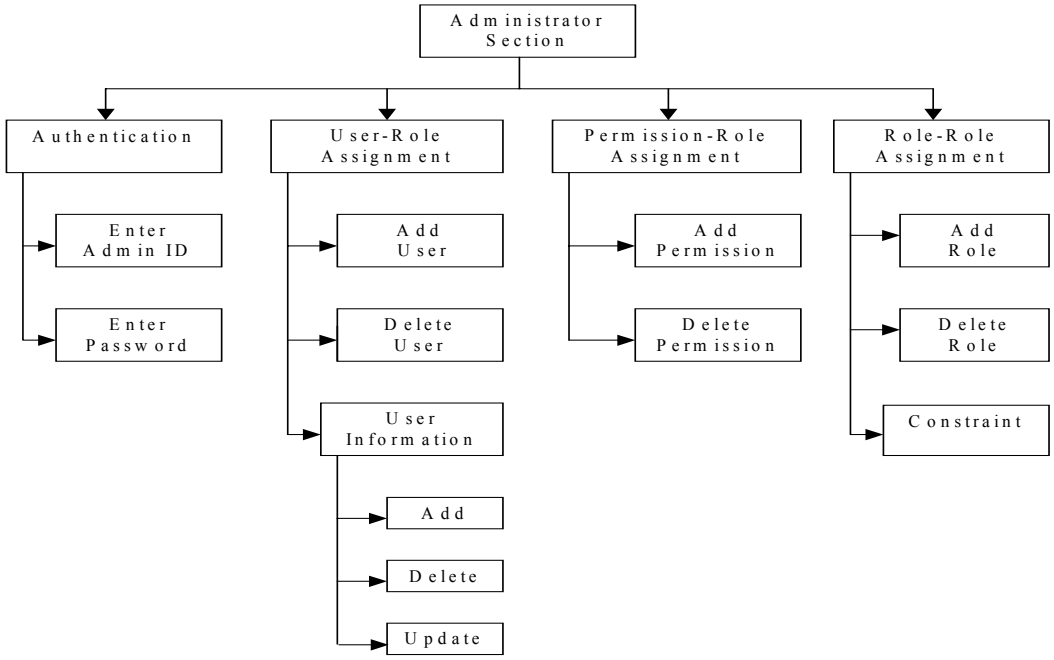

Fig. 1: Structure chart for RBAC - Administrator Section

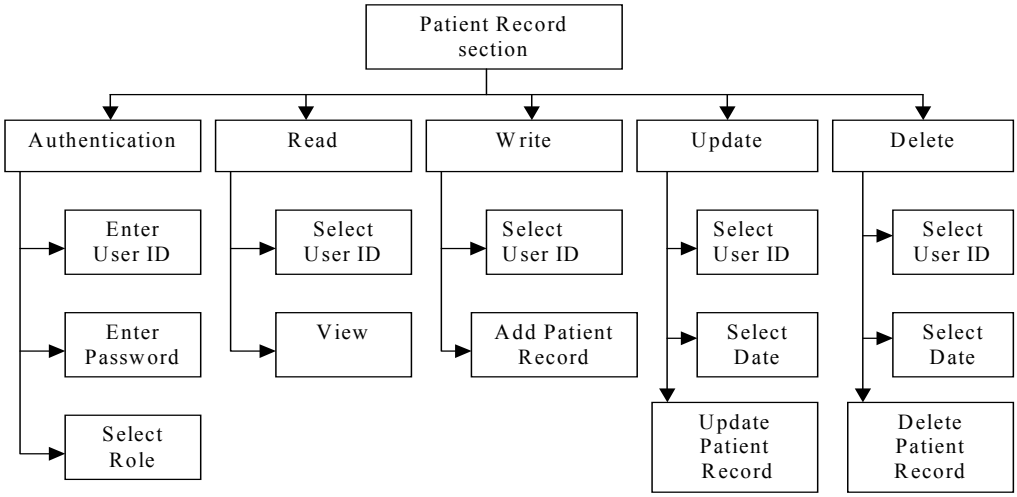

Fig. 2: Structure chart for RBAC - Patient Record Section

Since RBAC-KDIS is a web-based system, the web page design considerations are taken into account, as stated in the following:

i) Design an effective user interface to enable users to be effective in accomplishing their tasks.
ii) Provide a common consistent look and feel across the application. The pages should reflect a consistent page font, colour, image, page background and page layout.
iii) Give a navigational way to provide proper guidance to users in their journey to make sure that they are informed when performing the navigation.

The first step in the user interface design is to define the overall look and feel of the site. This is followed by determining the user's accessibility and restrictions. The public sites for user viewing and sites for configuration of RBAC administrator have to be differentiated. Navigation links need to be provided on all pages so that the user can move between different pages easily as in Fig. 3.

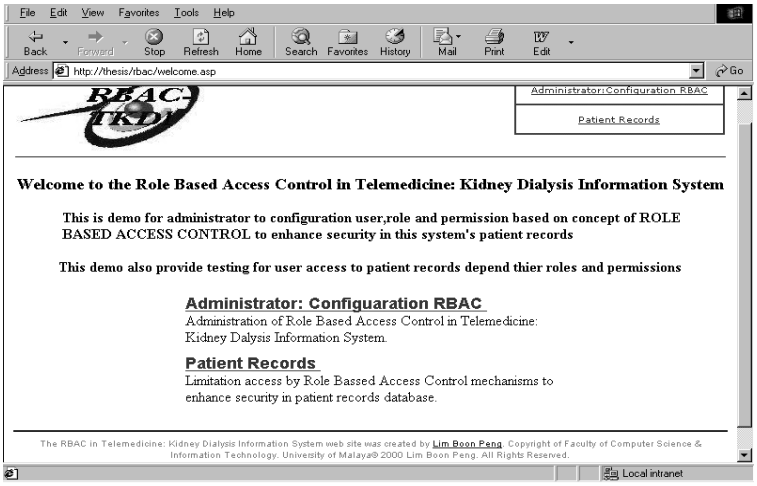

Fig. 3: Welcome as Main View

4.4 System Implementation

The tool used to implement the RBAC-KDIS is Microsoft Visual InterDev 6.0. It enables easy performance of the many complex programming and database tasks required in the creation of a Web site, as well as the incorporation of Active Server Pages (ASP), HTML formatting and layouts, graphics and other multimedia components.

One of the most valuable features of ASP is its ability to insert up-to-date database data into any HTML document just before it is sent to the browser. ASP documents use the ActiveX Data Object (ADO) to execute SQL statements against any ODBC-compliant database. In this system, the database is placed on the Web server and an ODBC DSN was created that points to its location and named as Role_Based.

4.5 System Testing

System testing can uncover different classes of errors in a minimum amount of time. Testing strategy should be flexible enough to promote the creativity and customisation necessary to adequately test all parts of the system. Thus, the strategies used for testing in this system are unit testing and integration testing. Verification of each unit in the main modules, sub modules and sub functions was done in unit testing. The integration testing was then carried out for the entire system.

5.0 DISCUSSIONS

Usage of role-based access control mechanism in a web-based application to control the patient medical information by enhancement security with controlled, unauthorised user access to patient records has been described. Role-based access control is more flexible for the administrator compared to other access control mechanisms.

The user interface in RBAC-KDIS is easy to understand and also user friendly. The web pages are designed to suit a wide spectrum of users and administrator - from the patient record section to the administrator section. Users can easily access the patient records database depending on their roles. The security administrator can access through the Web pages to configure the role hierarchy and assign permissions. Moreover, as a web-based application, it can be accessed easily from the Web browser.

In the authentication session, the author has provided a password-protected site by giving the administrator an AdminID and password. Password-role-protected for users (non-administrator) by giving a UserID, roles and password. Unauthorised users are prohibited from accessing the Web pages, thus making the system safe and secure.

Future enhancement can be recommended for the system to make it more advanced and easier to use, such as implementation of encrypted password or biometrics mechanism. A full RBAC-KDIS shall combine with the real Tele-Medicine Kidney Dialysis System to achieve a complete Tele-Medicine system. These combinations will provide further pointers on real Tele-Medicine application systems with a strong security protections.

The data process was merely covering the dialysis parameter from the dialysis machine, patients' blood pressure and weight before and after the dialysis process. Research can be extended to cover a wider range of data such as the sounds from electronic stethoscope, conversations between patient and physician, x-ray and video image.

Both concepts of ARBAC99 [10] and RSL99 [11] are not included in this paper. ARBAC99 considers mobility and immobility in user-role assignment (URA99); a user's membership in a role can be mobile or immobile. RSL99 focuses on Separation of Duty (SoD) technique for the prevention of fraud and errors. This paper has adopted the concepts of SoD from D. Richard Kuhn [12]. The basic ideas of RSL99 was also derived from D. Richard Kuhn. RSL99 is new and more complex. Its formal syntax and semantics are also given. For future enhancement, it is possible to apply these concepts into RBAC-KDIS to achieve a complete ARBAC.

REFERENCES

[1] C. Smith, "A Survey to Determine Federal Agency Needs for a Role Based Access Control Security Product", in *Proceedings of the 3rd International Software Engineering Standards Symposium (ISESS '97), Walnut Creek, CA,* 1-6 June 1997.

[2] R. Sandhu et al., "Role-Based Access Control". *IEEE Computer,* Vol. 29, No. 2, February 1996, pp. 38-47.

[3] D. Ferraiolo et al, "Role-Based Access Controls", in *15th NIST-NCSC National Computer Conference*, Baltimore, MD, 13-16 October 1992, pp. 554-563.

[4] R. Sandhu et al., "The RRA97 Model for Role-Based Administration of Role Hierarchies", in *Proceeding of 14th Annual Computer Security Application Conference*, 1998.

[5] R. Sandhu et al., "The ARBAC97 Model for Role-Based Administration of Roles". *ACM Transaction on Information and System Security*, Vol. 2, No. 1, February 1999, pp. 105-135.

[6] R. Sandhu et al., "Role-Based Administration of User-Role Assignment: The URA97 Model and Its Oracle Implementation". *The Journal of Computer Security*, 1999.

[7] R. Sandhu et al., "The ARBAC97 Model for Role-Based Administration of Roles: Preliminary Description and Outline", in *Proceeding of 2nd ACM Workshop on Role-Based Access Control,* Fairfax, VA, 6-7 November 1997.

[8] R. Sandhu et al., "The URA97 Model for Role-Based User-Role Assignment", in *Proceeding of IFIP WG 11.3 Workshop on Database Security,* Lake Tahoe, CA, 11-13 August, 1997.

[9] M. Meissner et al., *Risk Analysis of a Computer-Based Tele-Medicine Patient Management System*. The Cyberspace Policy Institute, 1997.

[10] R. Sandhu et al., "The ARBAC99 Model for Role-Based Administration of Roles", in *Proceeding of 15th Annual Computer Security Application Conference,* 1999.

[11] Gail-Joon. Ahn et al., "The RSL99 Language for Role-Based Separation of Duty Constrains", in *Proceeding of 4th ACM Workshop on Role-Based Access Control*, ACM, 1999, pp. 43-53.

[12] R. Kuhn, "Mutual Exclusion of Roles as a Mean of Implementing Separation of Duty in Role-Based Access Control Systems", in *Proceeding of IEEE Symposium on Research in Security and Privacy*, Oakland, CA, May 1998, pp. 172-183.

BIOGRAPHY

Boon Peng Lim received his Master of Computer Science from University of Malaya in 2001. He is currently attached to one of the private companies in Klang Valley.

Omar Zakaria obtained his Master of Science in Information Security from Royal Holloway, University of London in 1996. Currently, he is a lecturer at the Faculty of Computer Science and Information Technology, University of Malaya. His research areas include information security management, computer personnel research and business continuity plan.

Mustaffa Kamal Mohd Nor holds a Master in Computing from the University of Northumbria, Newcastle Upon Tyne, UK. He is presently a lecturer specialising in Information System and Strategic Planning at Faculty of Computer Science and Information Technology, University of Malaya.