International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

Role Security of It Industry with RBAC

Hnin Yu Hlaing[1], Hlaing Phyu Phyu Mon[2] & War War Myint[3]
[1]University of Computer Studies (Meiktila), Faculty of Information Science
[2,3]University of Computer Studies (Meiktila), Faculty of Information Science

Abstract:

A key issue in any information security is to protect information about all forms against unauthorized access. Innovation access control model is now becoming a need for application on systems due to emerging acts. RBAC is the standard and most important access control model and provides a great way to fulfill the access control needs. Role based access control is a feasible alternative to traditional. This study focused on IT Company by using Role Based Access Control (RBAC). The design architecture is based on RBAC concepts that only the administrator has the privilege to manage or administer the data. The administrator controls the largest information, including access to the IT Company's workers' files and has the sole access to all potential workers and their assigned duties. Study is integrated into the RBAC which is appropriate for managing system of IT Company. RBAC is used to control the access to company staffs' project file records, files and the company resources and eliminates security violations.

Keywords

RBAC Concept, Security Policy, IT Company Management.

1. Introduction

The principal motivations behind RBAC are the ability to articulate and enforce enterprise-specific security policies and to streamline the typically burdensome process of security management. RBAC represents a major advancement in flexibility and detail of control from the present-day standards of discretionary and mandatory access control. The policies enforced in a particular stand-alone or distributed system are the net result of the precise configuration of the various components of RBAC. RBAC framework provides administrators with the capability to regulate who can perform what actions, when, from where, in what order, and in some cases under what relational circumstances.

Security is a major concern in today's digital world. Role based access control provides a mechanism for protecting the digital information in an organization by assigning roles to the individual user and giving permissions to the assigned roles for accessing any resources. This paper describes the importance of roles in an organization and the evolutionary changes that occurs with respect to the organizational roles. Here the role is defined as an entity and the attributes of the roles have been identified with their related operations.

RBAC is the standard and most important access control model and has been a most important research topic since last two decades. Role Based Access Control model provides a great way to fulfill the access control needs. An access control policy is a statement which specifies the rules about who can access the resources and how much access is given to each user. In RBAC main Focus is on Role. Main idea behind the RBAC is that a role is an intermediate module between users and permissions. In RBAC roles are assigned to the users (many-to-many assignments) and permissions are associates with each role (many-to-many assignments), and thus indirectly assigns users to permissions. [6]

For efficiency, roles can be structured hierarchically so that some roles inherit permissions from others. RBAC simplifies access control compared with the administrative burden that would be required for a direct mapping from individual users to access control lists attached to resources. Once roles with their permissions have been defined, user provisioning simply requires that office staff assign users to roles as authorized by management.

RBAC is also well suited to separation-of-duty requirements, where no single individual has all permissions needed for critical operations such as expenditure of funds. Proper operation of RBAC requires that roles fall under a single administrative domain or have a consistent definition across multiple domains, so distributed applications might be challenging. [3]

In RBAC system data access is provided to the user according to their role. The roles are mapped to access permissions and users are mapped to appropriate roles. The Administrator assigned the roles to users based on their responsibilities and qualifications in their organization. Permissions are assigned to roles as per their qualifications instead of users. In RBAC, role hierarchy structure is used. The roles can inherit permissions from other roles. The RBAC system provides flexible control and management by having two mappings of user to role and roles to privileges on data objects.

Once an individual has been properly identified and that identification authenticated, the individual chooses a role that has been assigned and accesses information according to the operations assigned to the role.

2. Roles & Role Hierarchy

With RBAC, roles can have sometimes overlapping responsibilities and privileges; i.e. Users belonging to different roles might need to perform common activities. Some general operations might be performed by all employees. In such a situation, it would be inefficient and administratively difficult to specify repeatedly these

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

general activities for each role that gets created. Role hierarchies can be established to provide for the natural structure of the organization. A role hierarchy defines roles that have unique attributes and that might contain other roles. In project case, a role specialist could contain the roles of Project Manager, Team Leader and Team Members. This implies that members of the role specialist are implicitly associated with the activities associated with the roles Project Manager and Team Leader and Team Member without the administrator having list the activities of them. Role hierarchies are a natural way of organizing roles to reflect authority, responsibility, and competency.

In the case of company management, the role in which the User is gaining membership is not exclusive mutual, with another role for which the User already possesses membership. These activities and roles are usually subjected to management or administrative policies and constraints. When these activities intersect, hierarchies of roles can be established. Rather than costly auditing to monitor access, management can put in constraints on access through the use of RBAC. This might seem sufficient to allow physicians to have access to all patients ‟ data records if their access is monitored carefully. Applying RBAC, constraints can be placed on physician access so that only those records that are related to the physician can be accessed.

3. Company Management Environment

The IT Development environment is a complex mixture of IT professionals (CEO, System Analyst), electronic and non-electronic systems, clients, users, HR, administrator, Receptionist etc. Data processed in this environment are valuable and might have a negative outcomes attached to them if not handled well enough. The security of this sensitive data is of most importance to software development company staff, management, users, client and probably the supporting other specialists. In this paper, we focus on the basic privacy, security mechanism (RBAC application) that is fundamental of IT Software Development Company's information management. Company's essential and non-essential records keeping are particularly complex due to the highly sensitive nature of the records and the need to provide maximum protection, while allowing access to the data by a large number of users in the company who might need access for specific purposes. Records in company is heavily regulated; due to the sensitive and privacy implications [5].

In this paper the following are defined in relation to the IT industry environment:

An Administrator (CEO): The system administrator is responsible for managing each user and authority in the system. Its specific management functions mainly include creating users and roles and defining and assigning various operation rights of the system, and according to the user's level and responsibility.

User Authentication: Company staffs including software engineers, system analyst, business analyst, technical support, network engineer, technical consultant, technical sales, web developer, HR manager and software tester at all levels use their own account number (e.g. Staff-ID) for system login. Only users with identity and password authentication during logon can perform their own privileges in the system.

It also defines the identification and authentication of each role. In this model, policies define which permissions are established to roles in figure 3.1 in the software development company's information management. Permission related to role allows the appearance of access authorization in the generic way. Consequently, it is not required that only anyone who has access to get some records. Instead anyone is identified to have right access to get records he/she wants. The hierarchy of company organization, roles and associated permission of RBAC comprises the organization confidential policies. In this context, the company management structure is introduced, the implementation and illustrations of the role, sub-system function by data flow diagram.

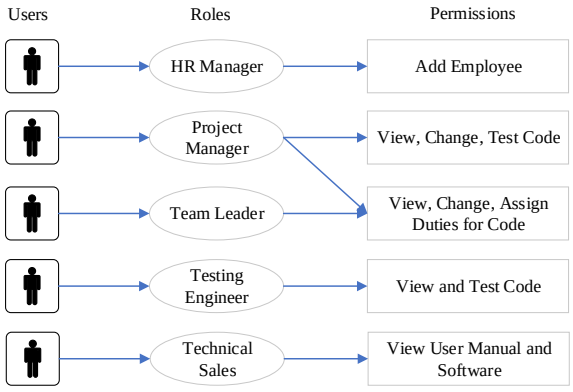

Figure 3.1 Relationship between IT member and Privilege

This model illustrates how workers in the company are managed, according to their role or job function, the privilege that is assigned. As explained earlier company information security management involves thorough analysis of how the management operates and include input from a wide spectrum of users in the company. It would be desirable to have a simpler solution that is easier to configure, maintained and reliably executed.

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

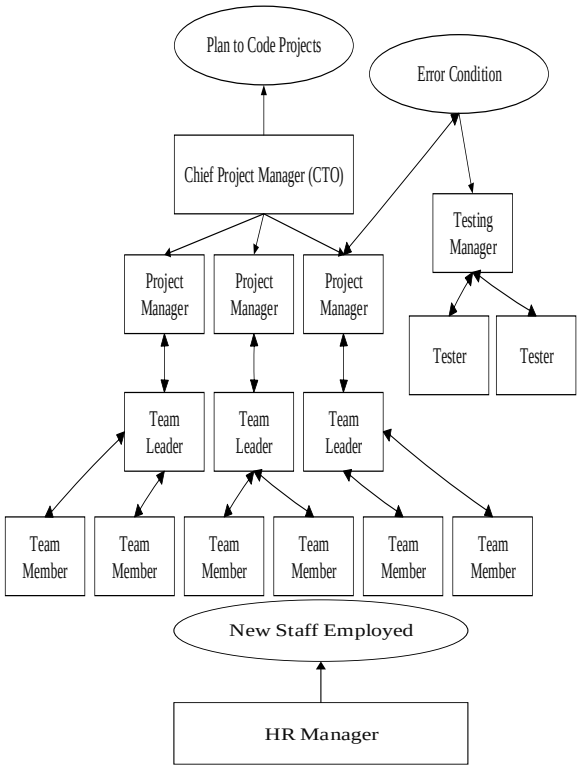

Figure 3.2 Relationship between IT member and Privilege

The figure 3.1 shows the hierarchy of assigning roles and partitioning company management into activities as required by company management in the implementation of Role-Based-Access Control. It also illustrates the relationship between the working partners (users), subjects, roles which operate in RBAC system.

The basic idea underlying company's whole process management technology is a system that explains the roles, and manages the activities of workflow through the use of designing software. In this model, an administrator manages the system in such a way that it can control the employee using the RBAC method as shown in the figure 2 hierarchy. The workflow specified in this model, describes and managed by a workflow management system which enacts each segment in the order specified by the process definition input. The RBAC is used to define company membership of the individual working in the company by assigning individuals to roles, assign permissions to roles, and now activate the job function or role with respect to the appropriate points in the sequence. Each user is assigned one or more "ROLES" and each "ROLE" is assigned one or more "PERMISSION" that is authorized for the users in that role by the administrator. In this model, permission consists principally of the opportunity to perform operations within an activity of the company workflow. Objects, such as files and processes, can be organized into hierarchies. In such object hierarchies, it is important to know not only the access of role group to an object, but also to know whether the path in the hierarchy could be traversed [11].

4. Model Database for the IT Company

In the IT industry, all the company information and process information is personal and are stored in the database system. The data must only be accessed by the users who are defined or authorized. This is the first step for any information stored and any secure data. To make the queries simple and provide an easy to administer, a decent database must reduce data redundancy.

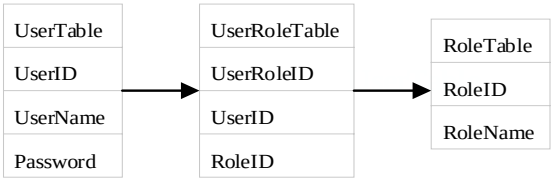

Figure 4.1 RBAC Database

Role-Based Access Control (RBAC) Based in Company Management Figure 3.1, their role tables, user tables and user role table. In the user table, every user has a unique User ID and User Name. Also, in Role Table, every role is determined by a unique Role ID and Role Name.

The relationship between a role and a user is managed by the User Role Table. It may include that one role can comprise many users. If the user decides to have two or more different roles, he/she should have two or more different User Name's, because one user with a single User Name can only be accepted for one role.

According to the figure 4.1, it is employed three roles: software engineer, system analyst, and testing engineer. With the different roles, when the user tries to log into the system, the overall system will check first the user's role, then his/her username and his/her password. If one user tries to log in one domain that he does not have an access, one message will appear directly (the system denied your request because of lack of rights) according to a program that will be installed in the database. A user is able or has the access to change his password once he is already accepted by the system in the data. According to the request imputed correctly, means username and password accepted, the system will appear in the windows. Different functionality is provided by each window.

In order to advance the security, the machine that the user logs in will turn automatically off if there is no action within on period time. This action can be defined by the administrator at any time. It avoids the leaking of certain information that is stored in the data as personal information and employee's private record. For instance, at the moment that one user forgot to log off in the system

and left his/her office, other can have access by using his/her machine to get some information or to alter a document. There is some information on company data that is private, only who has right access should modify.

5. CONCLUSION

Information systems in IT Company have unique specific security and privacy requirements. If management would like to apply RBAC in this information system to reduce the administrative tasks and manage the smooth running of the company, then must be adopted. Other issues that should be looked at are control of data sharing in an open distributed environment. We therefore propose this model of RBAC; this approach increases the data availability, confidentiality, integrity, accountability, which is the most important requirement in the company management. In addition, we have also proposed a program that takes permission evaluation when conflicting roles are present.

Managing the company has come a long way from serving principally as a means of making it easier to manage access to applications. As the growing number of employees‟ roles-driven projects indicates, RBACs are increasingly likely to address critical management objectives such as greater cost efficiencies, improved compliance, and reduce security exposure. Working as part of an integrated, automated role-management and identity-management solution, RBAC can go a long way toward helping avert potential management catastrophes in increasing collaborative and complex company environments.

6. Acknowledgements

I would like to take this opportunity to express my sincere thanks to all my senior and associates who gave me a lot of valuable advice and information. I am also graceful to all respectable people who directly or indirectly contributed towards the success of this research. I especially also thank to my parents. I owe my respectful thanks to Dr. Mie Mie Khin, Rector of the University of Computer Studies, Meiktila for allowing me to develop this research and giving me general guidance during the period of studying time.

I owe a great debt of gratitude to Dr. Hlaing Phyu Phyu Mon, Professor and Head of Faculty of Information Science, University of Computer Studies, Meiktila, for giving advices.

REFERENCE

[1] Ms. Sunita, Prachi, “Efficient Cloud Mining Using RBAC (Role Based Access Control) Concept”, Volume 3, Issue 7, July 2013.

[2] Edwin Okoampa Boadu, Gabriel Kofi Armah, “Role-Based Access Control (Rbac) Based In Hospital Management”, Volume 3, Issue 9 (September 2014), PP.53-67.

[3] Suganthy.A, Dr.T. Chithralekha (Associate Prof.), “Role-Evolution in Role-based Access Control System”, July 2017, ISSN: 2278-9359 (Volume-6, Issue-7).

[4] LIU Dongdong, XU Shiliang ,ZHANG Yan, TAN Fuxiao, NIU Lei, ZHAO Jia, “Role - based Access Control in Educational Administration System”, MATEC Web of Conferences 139, 00120 (2017).

[5] Nicola Zannone, “Role Based Access Control (RBAC)”.

[6] Anthony Rhodes, William Caelli, “A Review Paper Role Based Access Control”.

[7] Ed Coyne, Timothy R. Weil, “ABAC and RBAC: Scalable, Flexible, and Auditable Access Management”, 1520-9202/13/$31.00 © 2013 IEEE.

[8] H.B. Klasky, P.T. Williams, S.K. Tadinada, B.R. Bass ORNL, “A Role-Based Access Control (RBAC) Schema for REAP”, September 2013.

[9] “A best practice case implementing Role Based Access Control at ABN AMRO, KCP first European Identity Management Conference Munich, May 7-10.

[10] T. Finin, A. Joshi, L. Kagal, Niu, R. Sandhu, W. Winsborough, “ROWLBAC - Representing Role Based Access Control in OWL”, SACMAT’08, June 11–13, 2008, Estes Park, Colorado, USA.

[11] Hui Qi, Hongxin Mat, Jinqing Li and Xiaoqiang Di ” Access Control Model Based on Role and Attribute and Its Applications on Space-Ground Integration Networks” IEEE 2015.

[12] Cecilia Ionita and Sylvia Osborn. Privilege administration for the role graph model. In Research Directions in Data and Applications Security, IFIP WG 11.3 Sixteenth International Conference on Data and Applications Security, July 28-31, 2002, Kings College, Cambridge, U.K., volume 256 of IFIP International Federation for Information Processing, pages 15–25. Kluwer Academic Publishers, 2003.

[13] Liang Chen “Analyzing and Developing Role-Based Access Control Models”, 2011.

[14] Role-based access control policy administration, March 2004 URL: *http://www.cl.cam.ac.uk/TechReports/*UCAM-CL-TR-586.pdf

[15] David W. Chadwick and Alexander Otenko. The PERMIS X.509 role based privilege management infrastructure. In Seventh ACM Symposium on Access Control Models and Technologies (SACMAT’02), pages 135–140. ACM Press, 2002.

[16] Michael D. Schroeder Jerome H. Saltzer. The protection of information in computer systems. IEEE, 63(9):1278–1308, September 1975.

[17] Michael Hitchens and Vijay Varadharajan. Tower: A language for role based access control. In Policies for Distributed Systems and Networks, International Workshop (POLICY'01), Bristol, UK, pages 88–107, 2001.

[18] Ravi Sandhu and Pierrangela Samarati. Access control: Principles and practice. IEEE Communications Magazine, 32(9):40–48, 1994.

[19] Ravi Sandhu. Roles versus groups. In Proceedings of the First ACM Workshop on Role-Based Access Control (RBAC'95), pages I–25–26, 1995.

[20] Ravi Sandhu, Edward Coyne, Hal L. Feinstein, and Charles E. Youman. Role-based access control models. IEEE Computer, 29(2):38–47, 1996.

[21] Ravi Sandhu. Role activation hierarchies. In Proceedings of the Third ACM Work shop on Role-Based Access Control (RBAC'98), pages 33–40, 1998.

[22] Ravi Sandhu and Qamar Munawer. How to do discretionary access control using roles. In Proceedings of the Third ACM Workshop on Role-Based Access Control (RBAC'98), pages 47–54, 1998.

[23] Ravi Sandhu, David Ferraiolo, and Richard Kuhn. The NIST model for role-based access control: towards a unified standard. In Proceedings of the Fifth ACM Work shop on Role-Based Access Control (RBAC'00), pages 47–63, 2000.

[24] Richard T. Simon and Mary Ellen Zurko. Separation of duty in role-based environments. In PCSFW: Proceedings of the Tenth Computer Security Foundations Workshop, pages 183–194. IEEE Computer Society Press, 1997.

[25] Tor Didriksen. Rule based database access control – a practical approach. In Proceedings of the Second ACM Workshop on Role-Based Access Control RBAC'97), pages 143–151, 1997.

[26] http://www.emeraldinsight.com/doi/abs
Web Banking and performance

[27] The role graph model and conflict of interest. ACM Transactions on Information and System Security (TISSEC), 2(1):333, 1999.

[28] Privilege administration for the role graph model. In Research Directions in Data and Applications Security, IFIP WG 11.3 Sixteenth International Conference on Data and Applications Security, July 28-31, 2002, Kings College, Cambridge, U.K., volume 256 of IFIP International Federation for Information Processing, pages 15–25. Kluwer Academic Publishers, 2003.

[29] A comparison of commercial and military computer security policies. In Proceedings of the 1987 IEEE Symposium on Security and Privacy (SSP'87), pages 184–195, Los Angeles, CA, April 1987. IEEE Computer Society Press.

[30] Privacy and Security of Electronic Health Information Guiding, Theinformation contained in this Guide is not intended to serve as legal advice nor should it substitute for legal counsel. The Guide is not exhaustive, and readers are encouraged to seek additional detailed technical guidance to supplement the information contained herein, version 2.0, april 2015.