

Integrating Event-Driven-Based with Grey Relational Analysis for Role Engineering

Me-Yu Wu
Department of Information Management, Chung Hua University, Hsinchu, Taiwan, ROC
Email: mywu@chu.edu.tw

***Abstract*—Role-based access control (RBAC) has become the well-known and widely used access control model. However, role engineering is an important process to go through before using RBAC. Role engineering is the process of defining roles and related information as they pertain to the user's functional use. Role engineering is a critical success factor in implementing RBAC. This study proposes event-driven-based role engineering. An event is a routine task, and activities are triggered by events. Roles are created by many overlapping events. Among the roles, events and activities form many to many relationships. Our approach adopts the relationships to define the roles and assign permissions to them. Furthermore, we integrate the grey relational analysis (GRA) into the proposed model to refine the access control model. The proposed approach is suitable for organizations attempting to achieve refined role-permission planning, no matter whether or not they are using RBAC.**

***Index Terms*—RBAC, Role Engineering, Event-Driven, Grey Relational Analysis**

I. Introduction

In order to deal with complex permissions in large organizations, many small and medium size enterprises (SMEs), large enterprises and most organizations have changed their authorization approach to the role-based access control (RBAC) model proposed by Sandhu et al. in 1996. [15] The traditional access control is to authorize permissions for users. However, intuitive authorization generates huge amounts of authorization-related management data and is not easy to manage. Besides, large and complex data can easily result in inconsistent or conflicted access rights. Role-based access control minimizes problems with permission assignments and reduces the authorization management effort. Due to the advantage of simplified access control administration, RBAC has become a well-known and popular approach for enterprise access control management. However, "role" is the most important element in RBAC. In RBAC, the permission assignments are not assigned to users but to roles.

Roles can reflect essential business functions or correspond to the hierarchical organization in an enterprise. Role engineering is a critical success factor in the successful implementation of the RBAC model. The concept of role engineering was proposed by Coyne [4]. Role engineering discipline refers to the set of methodologies and tools used to define roles and to assign permissions to roles according to the actual needs of the company. More and more researchers have addressed the different types of role engineering: scenario-driven role engineering [13][17], graph optimization role engineering, [21] and aspect-oriented requirements engineering, [6] etc. Each approach captures, depicts and organizes diverse permissions under different situations. However, the existing approach must be based on a case or scenario that aggregates the set of permissions. Some situations may have been ignored or permission may have been assigned inadequately. Although few literatures adopted executed events to explore permissions to a role, strict counting numbers of event is not enough to express the real operating environment.[20]

Therefore, this research proposes activities and event-driven-based role engineering and integrates the grey relational analysis into the proposed model to refine the access control model. The proposed approach captures and assigns reasonable permission rights to corresponding roles in role engineering. The remainder of this paper is organized as follows. Section 2 reviews related works on access control, role-based access control, role engineering and grey relational analysis. Section 3 introduces the proposed event-driven-based role engineering approach and adopts grey relational analysis to refine the approach. A real case discussion is offered in Section 4. Finally, Section 5 presents our conclusions.

II. Related Work

A. Access Control

There are diverse permissions in an organization. According to their degree of importance, operational objects and executable tasks for each permission are very different. If there are many different permissions in an enterprise, the enterprise needs an adequate access control mechanism. Access control is an authorization management uses to decide whether permissions can be possessed or executed, as well as when and for whom. Traditional access control policy includes access control lists (ACL), mandatory access control (MAC) and discretionary access control (DAC). In access control list, each object will generate an independent list with authorized subjects and related permissions. In mandatory access control, all permissions are controlled be

doi:10.4304/jsw.8.9.2142-2146

administrator. All subject and objects are labeled according to their security level. The security labels are divided into four levels including top secret, secret, confidential, and unclassified. In discretionary access control, the owner of resource has the discretionary for its resource that is different from MAC. These access control policies are suitable for small-size organizations [16].

When SMEs grow into large enterprises, the permission structures may become complex. Some permission may cause inconsistencies and conflicts due to overlapping projects or systems. Using traditional access control policies in a large-size organization can make access control management difficult. Therefore, role-based access control has become a well-known and recognized flexible security model for enterprise access control management.

B. Role-Based Access Control

Role-based access control (RBAC) was proposed by Sandhu et al. in 1996 [15]. In RBAC, a user can play several roles, and a role can be assigned to several users. Unlike traditional access control, the permission assignments of RBAC are not assigned to users but rather to roles. Therefore, RBAC, as compared to traditional access control policies, can have several advantages, such as simplifying the complexity of authorization management, reducing the huge permission rights data and providing understandable access control. Moreover, RBAC supports other related security targets, such as constraints and role hierarchy, where a higher role can inherit a lower role's permission. Fig. 1 presents the structure of the model.

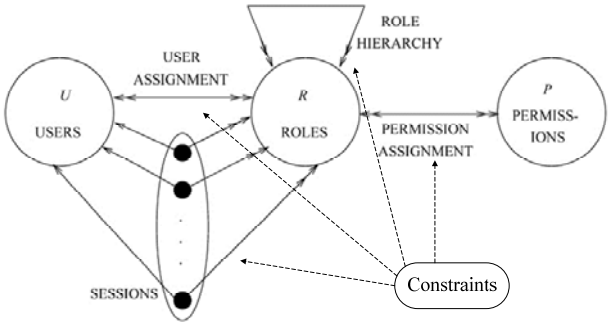

Figure 1. Role-Based Access Control Model[15]

RBAC reduces the complexity and effort required to manage authorization data in large systems. Several researchers have proposed extended RBAC models to enhance access control mechanisms, such as owner-based role-based access control (OB-RBAC) [14] and group-based role-based access control (GRBAC) [12]. The core concept of these models is "role." For this reason, role engineering is an important research issue.

C. Role Engineering

The concept of role engineering was proposed by Coyne [4]. Role engineering is a set of methodologies used to define roles and produce the sets of permissions to roles. The main purpose of role engineering is to find the most adequate permissions for each role. Several researches have investigated the reasonability of the permissions assigned to each role [6][10][17][20][21]. The steps for identifying roles may contain collecting activities performed by system users, naming each activity cluster, comparing the candidate roles with one another, identifying the minimal set of permissions, and simulating the user's activities. [4]

Some researchers have classified the existing role engineering approaches into two categories: top-down and bottom-up [3][8][18]. The former seeks the adequate permissions of a role using the role as the starting point. In other words, it carefully identifies which features or rights are necessary to carry out specific tasks of a role. The latter, based on the analysis of existing access controls permissions, elicits a set of roles that correctly describe the existing user-permission assignments.

For using RBAC organization, some researchers proposed agent to keep all objectives satisfied security [10]. Due to there are complex permissions in an organization, using agent to realize the condition determination. Role mining is one kind of bottom-up role engineering. Researchers adopted bipartite graph to optimize the collected permissions or discovered the optimal role hierarchies. [3][7]

Role is the most important element of the role-based access control. A user is given permissions according to the authorized roles. The reasonability of role-permission assignments is based on role engineering. The existing role engineering approaches are based on specific scenarios or cases that may cause some specific permission to be ignored or introduce permission conflicts. Therefore, this study proposes activities and event-driven-based role engineering with the aim of achieving better role-permission assignments.

D. Grey Relational Analysis

A system having incomplete information is called Grey system. The grey relational analysis (GRA) is an important method in the grey system theory [5][19]. The GRA have been widely used in a number of areas, such as manufacturing [1], the building material [2], transportation [9] and software estimation [11]. The grey theory is based on the random uncertainty of small samples which developed into an evaluation technique to solve certain problems of system that are complex and having incomplete information [1]. Grey relational analysis is a normalization evaluation technique and extended to solve the complicated multi-performance characteristics optimization effectively.

Although many enterprises have adopted role-based access control model, there are still ambiguous in the user-role-permission assignments. In RBAC, a user has permissions according to the assigned roles and the role-permissions assignments should be clarity. But in actual operation environment, the same role name, otherwise known as job position, may have different executing tasks and permissions. Therefore, this research attempts to integrate grey relational analysis to refine the role-permission assignment. Grey relational analysis is suitable for simple and uncertainty sample to find the actual assignments of roles and permissions.

III. Event-Driven Role Engineering Process

A. Element Definition

This study proposes an event-driven-based role engineering approach and integrates grey relational analysis to refine the approach. There are five main elements to the approach: user, role, event, activity and permissions. Each element is described in detail as follows:

- **User (U):** A user is an employee in an organization assigned a specific role in order to gain a specific permission. In role engineering, appropriate permissions are assigned to roles based on each user's work-related activities. A user, if authorized an appropriate role, will be verified by corresponding activities.
- **Role (R):** Roles can reflect essential business functions or correspond to the hierarchical organization of an enterprise. Each role has a specific set of permissions. In RBAC, role is the set of permissions. However, in this research, role signifies assigned permissions according to corresponding events and activities.
- **Event (E):** Event in this study does not refer to unexpected events or incidents in daily life. Events here refer to the daily need to perform routine jobs or tasks in each position in an enterprise. Each routine job or task is called an event. According to the frequency of actual events, a role may be derived from the aggregation of events.
- **Activity (A):** All routine tasks or sudden jobs are regarded as events in this study. Furthermore, each task or job contains several steps or phases. These steps or phases are called activities in this study. In accordance with comparisons to actual implemented activities and expected activities in the organization, the role-permission assignments are verified.
- **Permission (P):** Permissions are the privileges to execute systems or operate objects. According to the events and corresponding activities, a set of permissions will be derived.

Definition 1. The activities and event-driven-based role engineering model has the following components:

- U, R, E, A, and P (users, roles, events, activities, and permissions respectively),
- $PA \subseteq P \times R$, a many-to-many mapping permission-to-role assignment relation,
- $UA \subseteq U \times R$, a many-to-many user-to-role assignment relation,
- assigned_permissions($r : R$) $\rightarrow 2^P$, the mapping of role r onto a set of permissions,
- User: $E \times A \rightarrow U$, a function mapping events and related activities to the single user $user(e_i, a_i)$, and
- Role: $E \times A \rightarrow 2^R$, a function mapping events and related activities e_i, a_i to a set roles $roles(e_i, a_i) \subseteq \{r \mid (user(e_i, a_i), r) \in UA\}$ (which can derived from events and refined by activities) and has the permissions $\cup_{r \in roles(ei, ai)} \{p \mid (p, r) \in PA\}$

We expect each derived role to be assigned at least one permission and each user to be assigned to at least one role. The main elements of the proposed activity and event-driven-based role engineering model are illustrated in Fig. 2. The relationship between activity, event and role are all 'many to many'.

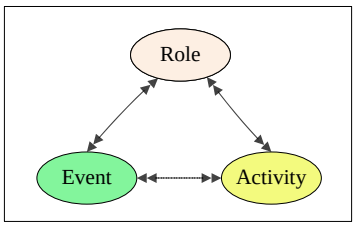

Figure 2. Element relationship of the proposed role engineering model

B. Event-Driven Model

Role engineering has to work before implementing RBAC. Defining an accurate and complete set of roles is the main purpose of role engineering. This study proposes activities and event-driven-based role engineering. An event may trigger several activities, and an activity may be caused by different events. The relationship between activity and event is 'many to many'. A role can be derived from many overlapping events and refined by activities. The relationship diagram example of role, event and activity in the proposed role engineering approach is shown in Fig. 3.

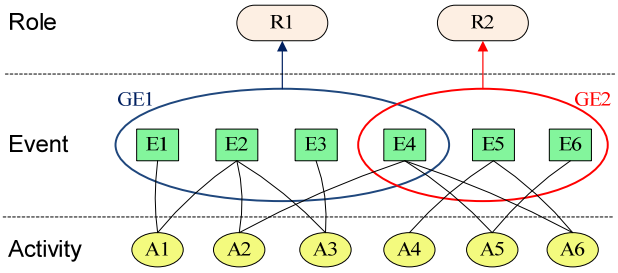

Figure 3. Relationship diagram example of role, event and activity

The relationship diagram of the proposed approach contains three layers. From the top-down they are role, event and activity. In the event layer, many events may be performed by one person, as in E1, E2, E3 and E4 in Fig. 3. We can aggregate the events into a group, such as GE1. Then a role could be derived from the event group, such as R1.

From the event layer to the activity layer, each event may trigger several activities. There may be duplicate activities between events. For example, event E1 and E2 are different events; however, they both have the same activity, A1. In the activity layer, many events may contain duplicate activities. However, in the relationship diagram, duplicated activities only appear once. Each event group contains several events and some events may also be included in another event group. For example, event E4 belongs to both event group GE1 and GE2. Nevertheless there are events which exist in overlapping event groups; this does not affect the derived role. After the formation of a role, a new role may be derived and hence role hierarchy is formed indirectly.

Let GE_i represent an event group and e_j denotes a base event. $S^r_{GE_i}$ is used to derive the event aggregate of GE_i

for deriving role r. The formal equation of $S^r_{GE_i}$ is shown in (1).

$$S^r_{GE_i} = \{\, e_j \mid e_j \in GE_i : e_j \text{ is specified in the needed event aggregation of } GE_i \text{ for deriving role } r \,\} \quad (1)$$

$\mathcal{D}^r(GE_i)$ denotes the aggregate information of GE_i to derivate role r; $\mathcal{D}(e_j)$ denotes the executed event information handled by e_j; and $\boldsymbol{F}$ denotes an aggregate function. The formal equation to derivate the role is illustrated in (2).

$$\mathcal{D}^r(GE_i) = \boldsymbol{F}(\{\mathcal{D}(e_j) \mid e_j \in S^r_{GE_i}\}) \quad (2)$$

These aggregate functions are used in simple statistical computations, for example, SUM, AVERAGE, MAXIMUM and MINIMUM, that summarize information from events handled by the a user. In this study, we count and sum executed times of each event. A user executed some events frequently and furthermore, we can derive suitable role for the user by the related events in an event group.

C. Refined Model by Grey Relational Analysis

Through collecting practical events and activities, we may finish the role-event-activities relationship diagram as shown in Fig 3. Furthermore, we can adopt grey relation analysis to analyze the most important system factors. We may analyze the associated factors of role-permission assignment depending on the related events and activities executed by users who have the same role. We can filter out what events or activities are most executed. What permissions are worth for a role and what is needed to give up. The discarded permissions may generate a new role with new permissions. For example, we suppose event E4 and E5 in Fig. 3 are the most executed tasks and the most corresponding performed activities are A4, A5 and A6. Therefore, we may aggregate a new event group and derive a new role.

Enterprises may collect the related information of role-permissions and the actual executed permission of roles. Then administrator used grey relational analysis to analyze the correlation of the role-permissions. Perhaps enterprise will find inadequate role-permission assignment. A new refined role may be generated. Besides, the original roles and refined roles may form a role hierarchy. For example, the role "Professor" may be derived by event-driven based role engineering. But when we further analyze the most frequent performing activities, the new roles of "Vice Professor" and "Assistant Professor" may be derived.

IV. Case Discussion

In the study, we use the roles "chairman" and "professor" in a department of a university as examples. We suppose that the department has adopted role-based access control to perform security management. We may collect and capture all roles, events and activities in the department. The role-event-activity relationship diagram is illustrated in Fig. 4.

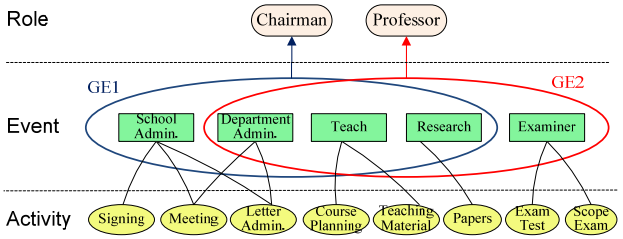

Figure 4. The relationship diagram of a department

The collected events in a department contain school administration, department administration, teaching, research and exams. Each event may consist of several activities. For example, the "teach" event consists of two activities, course planning and preparing teaching material. In Fig.4, we can see the frequent events, i.e. GE1, executed by role chairman are school administration, department administration, teaching and research. The formal equation for role "Chairman" is shown in (3).

$$\mathcal{D}^{Chairman}(GE_1) = \boldsymbol{F}\{\mathcal{D}(school\ administration), \mathcal{D}(department\ administration), \mathcal{D}(teach), \mathcal{D}(research)\} \quad (3)$$

Although the department has adopted role-based access control to perform security management, we can adopt the equation to verify the reasonable of role-permission assignments. In our proposed approach, we may further analyze related events and activities. We can determine the most executed events and activities of each user to refine the role-permission assignments. For example, the role-event-activity relationship diagram of "professor" role is shown in Fig. 5.

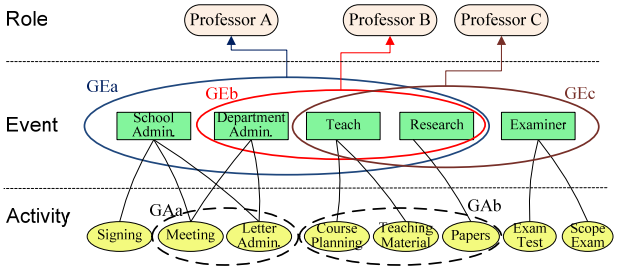

Figure 5. The relationship diagram example of the professor role

By referring to the times of performed activities for one user, we can aggregate an activity group, such as GAa, consisting of meeting and letter administration. Therefore, we may refine the role to generate a new role, called "Assistant". The other activities group, GAb, contains three activities; course planning, preparing teaching materials and publishing papers. We make sure the role "Professor" is appropriate. Moreover, if the role "chairman" does perform the "teach" and "research" events and related activities, we may refine the user-role assignment. The proposed activities and event-driven based role engineering may verify the suitable role-permission assignment for the organization that the adopted role-based access controls. Even if the organization has not yet adopted role-based access control model, the proposed approach is still applicable.

V. Conclusions

This research proposes an integrating event-driven-based with grey relational analysis for role engineering approach which is suitable for organizations whether or not they use RBAC to achieve refined role-permission planning. The proposed approach adopts the concept of event to enumerate a routine task or job and further uses grey relational analysis to improve role-permission planning. Through the refined model based on activities, a role may be created, modified or deleted in accordance with reasonable control management.

In future work, we will keep using event-driven based architecture to investigate comprehensive role engineering. We hope to obtain the actual data to verify the effectiveness of combining grey relational analysis. Furthermore, fuzzy or mining approaches to events and activities may be adopted to refine the role-permissions planning.

References

[1] S. Balasubramanian, S. Ganapathy, "Grey Relational Analysis to determine optimum process parameters for Wire Electro Discharge Machining (WEDM)," *International Journal of Engineering Science and Technology*, vol.3, no.1, pp. 95-101, 2011.

[2] W. C. Chang, K. L. Wen, H. S. Chen, and T. C. Chang, "The Selection Model of Pavement Material via Grey Relational Grade," *In Proceeding of IEEE International Conference on System, Man, and Cybernetics*, pp.3388-3391, 2000.

[3] A. Colantonio, R. D. Pietro, A. Ocello and N. V. Verde, "Mining Stable Roles in RBAC," *IFIP Advances in Information and Communication Technology*, vol.297, pp. 259-269, 2009.

[4] E. J. Coyne, "Role Engineering," *Proceedings of the first ACM Workshop on Role-Based Access Control*, pp. I-15 - I-16, 1996.

[5] J. Deng, "Grey Information Space," *The Journal of Grey System*, vol.1, pp.103-117, 1989.

[6] S. Gao, Z. Dai and H. Yu, "Improving Scenario-Driven Role Engineering Process with Aspects," *Aspect-Oriented Requirements Engineering and Architecture Design Workshop*, 2004.

[7] Q. Guo, J. Vaidya and V. Atluri, "The Role Hierarchy Mining Problem: Discovery of Optimal Role Hierarchies," *Computer Security Applications Conference*, pp. 237-246, 2008.

[8] C. Giblin, M. Graf, I. Molloy, J. Lobo and S. Calo, "Toward an Integrated Approach to Role Engineering," *SafeConfig '10 Proceedings of the 3rd ACM Workshop on Assurable and Usable security configuration*, 2010.

[9] Y. T. Hsu, C. B. Lin, and S. F. Su, "High Noise Vehicle Plate Recognition using Grey System," *The Journal of Grey System*, vol.10, pp.193-208, 1998.

[10] C. Huang, J. Sun, X. Wang and Y. Si, "Role Engineering with SKAOS for Systems Employing RBAC," *2009 International Conference on Network and Digital Society*, pp. 56-60, May 2009.

[11] S. J. Huang, N. H. Chiu, and L. W. Chen, "Integration of the Grey Relational Analysis with Genetic Algorithm for Software Effort Estimation," *European Journal of Operational Research*, vol.188, no.3, pp.898-909, 2008.

[12] Q. Li, M. Xu and X. Zhang, "Towards a Group-based RBAC Model and Decentralized User-Role Administration," *The 28th International Conference on Distributed Computing System Workshops*, pp. 441-446, 2008.

[13] G. Neumann, M. Strembeck, "A Scenario-Driven Role Engineering Process for Functional RBAC Roles," *Proceeding of the 7th ACM Symposium on Access Control Models and Technologies*, pp. 33-42, 2002.

[14] M. Saffarian and B. Sadighi, "Owner-Based Role-Based Access Control OB-RBAC," *2010 International Conference on Availability, Reliability and Security*, pp.236-241, February 2010.

[15] R. S. Sandhu, E. J. Coyne, H. L. Feinstein and C. E. Youman, "Role-Based Access Control Models," *IEEE Computer*, vol.29, no.2, pp. 38-47, 1996.

[16] R. S. Sandhu and P. Samarati, "Access Control: Principles and Practice," *IEEE Communication Magazine*, pp. 40-48, September 1994.

[17] M. Strembeck, "Scenario-Driven Role Engineering," *IEEE Security and Privacy*, vol.8, no.1, pp. 28-35, January 2010.

[18] S. Vanamali, "Role Engineering: The Cornerstone of Role-Based Access Control," *CA Transforming IT Management*, July 2009.

[19] H. H., Wu, *The Introduction of Grey Analysis*, Gauli Publishing Co., Taipei, 1996.

[20] M. Y. Wu, "Activities and Event-Driven-Based Role Engineering", *Sixth International Conference on Genetic and Evolutionary Computing, Kitakyushu*, pp.550-553, 2012.

[21] D. Zhang and K. Ramamohanarao and T. Ebringer, "Role Engineering using Graph Optimisation," *SACMAT '07 Proceedings of the 12th ACM Symposium on Access Control Model and Technologies*, pp. 139-144, 2007.

Mei-Yu Wu received the MS and the PHD degree from the Institute of Information Management, National Chiao Tung University, Taiwan, in 1999 and 2005. She is currently an assistant professor of the Department of Information Management, Chung Hua University. Her research interests include information security management, role-based access control, workflow process, and knowledge management.