行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※
※ ※
※ 工作流程授權管理模式之研究 ※
※ ※
※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：☑個別型計畫 □整合型計畫
計畫編號：NSC 89-2416-H-009-041
執行期間：89 年 8 月 1 日至 90 年 7 月 31 日

計畫主持人：劉敦仁

共同主持人：

本成果報告包括以下應繳交之附件：
- □ 赴國外出差或研習心得報告一份
- □ 赴大陸地區出差或研習心得報告一份
- □ 出席國際學術會議心得報告及發表之論文各一份
- □ 國際合作研究計畫國外研究報告書一份

執行單位：國立交通大學資訊管理研究所

中 華 民 國 90 年 9 月

工作流程授權管理模式之研究

Research on Authorization Models for Workflow Management

計劃編號：**NSC 89-2416-H-009-041**
執行期間：89 年 8 月 1 日至 90 年 7 月 31 日
主持人： 劉敦仁 交通大學 資訊管理研究所
計劃參與人員：吳美玉、沈民新、柯志坤 交大資管所

一、摘要

網路的開放性使企業資源包括工作流程處理及資訊系統之資料，更亦遭到不當的存取。因此在一個開放的環境中，如何對工作流程之執行與存取相關系統資源的使用者予以適當的安全控管與授權管理，是重要的議題，本研究即是要探討工作流程的存取控制與授權管理。存取控制主要是判斷使用者是否有權執行工作流程之工作及存取流程相關資源，而授權管理主要是規範使用者與角色之權限，管理工作流程各項工作之指派授權予適當角色及使用者。存取控制之研究主要是以角色或工作為存取控制依據，而以權責區分作為授權角色與使用者權限之規範。權責區分主要是將衝突的權責予以區分授權予不同的角色或使用者負責，避免權責不分、舞弊之情形。本計畫探討工作流程存取控制及建立符合權責區分準則之工作流程授權管理機制。本計畫主要包括下列研究成果：(1) 分析並定義企業工作流程環境下的工作權責衝突關係，並進而制訂工作流程環境下之權責區分準則；(2) 設計符合權責區分準則之工作流程授權管理模式；(3) 發展授權管理雛形系統，並以實際企業流程案例進行驗證與應用分析。

關鍵詞：工作流程管理、權責區分、存取控制、授權管理

Abstract

The openness of the Internet makes workflow and related business information more vulnerable to insecure access. It is necessary to provide secure mechanisms for workflow management. The aim of this project is to investigate the access control and authorization management in workflow management systems. In this context, access control determines whether a user has the privilege to execute tasks and access workflow-related information, while authorization management enacts the assignment of workflows and tasks to roles and users. The research on access control mainly makes access decisions based on access permissions associated with roles or tasks. Authorization rules for the assignment of permissions to roles and users are designed to achieve separation of duty. Separation of duty is a security principle to prevent fraud and errors by assigning duty-conflict responsibilities to different roles or users. In this project, we investigate the issues related to access control, separation of duty and authorization management in workflow-based environments. Our research achievements include the following. (1) We analyze and define several duty-conflict relationships among tasks. Authorization rules that achieve separation of duty are then designed based on the duty-conflict relationships. (2) With the incorporation of authorization rules, an authorization model is proposed to support authorization management of workflow systems. (3) A prototype system is developed to realize the proposed authorization model. Finally, we analyze a practical case of business process to demonstrate how authorization management is conducted in the developed system.

Keywords：Workflow Management, Separation of Duty, Access Control, Authorization Management

二、緣由與目的

As an effective process management tool, workflow management systems (WfMS) allow a business to analyze, simulate, design, enact, control and monitor its overall business processes [3,8,14]. With the prevalent use of Internet, conducting workflow management on the Internet is an inevitable trend for business commerce [13]. However, the openness of the Internet makes workflow and related business information more vulnerable to insecure access. To provide secure mechanisms for workflow management, an adequate authorization management is required to manage all users' access to ensure that workflow related data and tasks are under a secure and effective access control management.

Considerable work has been done on access control in enterprise resource management. In role-based access control (RBAC), roles are assigned to users [1,5,6,9]. The authorization of access to a user is determined according to the access privileges of role activated by the user. To ensure secure access, authorization rules for separation of duty need to be defined to enforce legal assignment of access privileges to roles and roles to users. Separation of duty (SoD) is a secure principle to control secure access in multi-user environments [7,11]. The purpose

of separation of duty is to authorize conflict duties to different roles or users in order to avoid fraud.

The dynamic changing environments of industry necessitate the addition of new task or rearrangement of tasks. The permission or operation specified in RBAC is not adequate to model the concept of "task" in enterprises. Comparing to an operation, a task is a more high level expression of access privileges [4]. To adapt to the modification of tasks and flexibly adjust the authorization of tasks to roles or users, RBAC needs to be enhanced to incorporate the concept of task.

Some work has been done on task-based access control and authorization management [2,10,12]. Sandhu et al. proposes task-based authorization control to manage the execution states of tasks [12]. Schier has also proposed a role and task based security model [10]. Although authorization rules for SoD have been designed based on mutual exclusive (duty-conflict) tasks, the proposed work is merely an extension of RBAC model. Bertino et al. discuss the specification and enforcement of authorization constraints in workflow management systems [2]. A logical authorization language is proposed to express authorization constraints. They do not consider the variations of SoD arising from different duty-relationships between tasks.

The objective of this research is the following. (1) Analyze and define various duty-conflict relationships among tasks; Design authorization rules to achieve separation of duty; (2) Design an authorization model to support authorization management of workflow systems. (3) Develop a prototype system to realize the proposed model for authorization management in workflow systems.

三、研究方法及成果

The main research results are summarized as follows.

(1) This work analyzes and further defines different duty-conflict relationships between tasks from the aspect of how enterprises design and plan tasks. Furthermore, this work designs authorization rules for SoD based on the defined duty-conflict relationships.

(2) This work proposes an authorization model to verify the assignments of roles/users to tasks of a workflow that ensures the authorization constraints for SoD are not violated.

(3) This work designs and implements a prototype system capable of conducting authorization management in task-based workflow environments. An analyzed procurement process is deployed into the system to demonstrate the proposed authorization management..

3.1 Analyzing duty-conflict tasks

A task defined by an enterprise represents a set of task-related privileges to be assigned to roles or users. Assigning a task to a role or a user enables the role or the user to own the duty of performing the task, i.e. task-duty. In general, the corresponding duty relationship between two tasks is called duty-conflict relationship, as if assigning the two tasks to the same user or role will result in fraud. Several duty relationships have been defined, including duty-conflict, duty-balancing, duty-supervising, coordinating duty, and non-proprietary duty relationships.

[Work-dependency] Two tasks T_i and T_j are execution-dependent tasks, if they are correlated, i.e. the execution (processing) of one task (T_i) depends on the execution (processing) of the other task (T_j).

[Duty-Conflict Tasks] Two tasks T_i and T_j are duty-conflict tasks, if their implicitly defined task-duties are conflict.

Duty-conflict relationships can be further distinguished into duty-balancing and duty-supervising relationships.

[Duty-Balancing Tasks] Two tasks T_i and T_j are duty-balancing tasks, if the implicit task-duty of T_i (T_j) is to review task T_j (T_i). T_i and T_j have equal level of task duty.

[Duty-Supervising Tasks] Task T_i supervises task T_j, if the implicit task-duty of T_i is to supervise task T_j. T_i has a higher level of task-duty than T_j does.

3.2 Task-based separation of duty

Based on the defined duty relationships, this work further designs authorization rules for SoD on role-task and user-role assignments. The authorization rules contain static, dynamic, execution-dependent, and object-based SoD for duty-conflict and duty-supervising tasks. Two categories of SoD variations are static SoD and dynamic SoD variations, as described in the following.

Static SoD: Static SoD strictly enforces that two duty-conflict tasks cannot be assigned to the same role or user. The validations of the authorization constraints on user-role/ role-task assignments are performed during the design phase to enforce SoD.

Dynamic SoD variations: Static SoD is too strict to reflect real world security principles. The constraints for dynamic SoD variations are weaker than the constraints for static SoD. Dynamic SoD variations provide flexibility by allowing two duty-conflict tasks to be assigned to different roles and then be assigned to the same user. The validations of the authorization constraints on role/task/object activations are then conducted during the run-time phase to enforce SoD.

The authorization rules for dynamic SoD variations include authorization rules for dynamic SoD and execution-dependent SoD. Authorization rules for dynamic SoD specify whether a user (subject) is authorized to activate several roles, execute several tasks and access several objects at the same time. The

authorization rules for execution-dependent SoD mainly enforce SoD in the execution of work-dependent tasks. For example, the tasks of the same workflow have work-dependent relationships.

[Execution-Dependent SoD] Task T_i and task T_j are duty-conflict and execution-dependent tasks. Subject S executed task T_i under role R_x, and task T_j is authorized to role R_y. Subject S can activate R_y, but subject S can not execute task T_i under role R_y.

[Dynamic SoD for Duty-Supervising Tasks] Subject S_A and S_B play role R_x and R_y to activate task T_i and T_j, respectively. Task T_i and T_j have duty-supervising relationship, $T_i \succ T_j$. Role R_x must have a higher position than role R_y.

3.3 Authorization model for workflows

A workflow contains various tasks of a business process. These tasks need to be executed by users with authorized roles. The proposed authorization model handles the assignments of roles/users to tasks of a workflow. The assignments need to satisfy the authorization constraints for SoD defined in Section 3.2. The proposed authorization model contains the planning phase and run-time phase. The planning phase generates initial workflow activation plans in advance, i.e., a set of valid roles/users assignments to tasks that satisfy the constraints for SoD. The planning phase is conducted before the workflow execution starts, while the run-time phase is executed upon the actual activation of each task during the workflow execution. The enactment of a workflow decides the current task to be activated. According to the selected role/user activation plan (current plan) generated by the planning phase, the run-time phase determines the user authorized to activate the current task under a certain role. Since dynamic SoD variations are more realistic security policies. Both the planning and run-time phase are designed to find roles/users assignments to tasks that satisfy the dynamic SoD variations.

Notably, the current activation plan may need to be modified during the run-time phase due to the following reasons. The planned user, authorized to activate the current task according to the current plan, may not be available to execute the task. Furthermore, the activation of current task by the planned user may violate the constraints for dynamic SoD variations. Since the activation plan is generated by the planning phase before the workflow execution starts. The planning phase can only consider the assignment of those tasks of the workflow being planned and is not able to verify run-time activations of tasks in which a user may activate several tasks from more than one workflow execution. Therefore, the activation of current task by the planned user needs to be verified to ensure that constraints for SoD are not violated. If the authorization check fails, the current activation plan needs to be modified. The run-time phase determines an available user authorized to activate the current task, and generates a new activation plan based on the current activation plan.

3.4 System implementation

Figure 1 shows the system architecture integrated with a workflow management system. The user authentication module provides user authentication to validate the user identity and enable the user to conduct authorized operations such as activating roles, executing tasks, and accessing objects. The authorization controller provides the authorization control of role-task and user-role assignments. Role activations and task executions conducted by users are verified to ensure that authorization constraints for SoD are not violated. The activation controller manages role/task activations and the interactions with users and WFMS. The activation controller handles users' requests for role/task activations and issues an authorization request to the authorization controller to verify authorization constraints for SoD.

The workflow management system (WFMS) supports the design and the enactment of workflows. The design module assists a workflow designer with the specification of a workflow in the design phase. In addition, the design module supports the assignment of roles/users to each task in a workflow. The run-time module is responsible for the enactment of workflows. The run-time module controls the task execution flow and assigns a user to perform the current task. The assignment needs to be validated by the interactions with the authorization controller to verify authorization constraints for SoD.

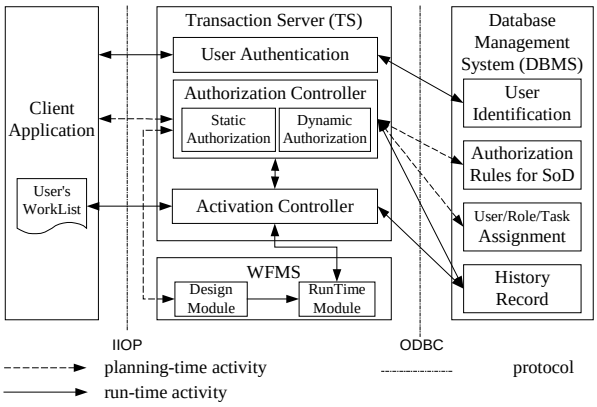

Figure 1. The system architecture

We use the Sybase's EAS (Enterprise Application Server) 3.0 to develop the system. The prototype system is a three-tier architecture with the transaction server (TS) as the middle tier between the client application and the DBMS server. The client application program provides the interface between the user and system. The DBMS stores authorization data and process/task data. The PowerDesign 7.0 is used to develop databases managed by the Sybase SQLAnywhere 6.0 DBMS. The application program of the client side communicates with the Transaction Server

by IIOP (Internet Inter-ORB Protocol). The TS retrieves the required data from DBMS server by ODBC. The system provides various business functions to support task execution, authorization control and activation control. These business functions are developed as business objects using the object-oriented approach. Finally, we use a procurement process to demonstrate the application of our system to conduct authorization management of business processes.

四、結果與討論

This work contributes to provide a novel view to analyze different duty-conflict relationships from the aspect of how enterprises organize tasks. Based on the analysis, this work defines duty-conflict relationships among tasks and further defines the authorization rules for SoD according to the duty-conflict relationships. Furthermore, an authorization model and a prototype system are developed to conduct authorization management of tasks in workflow environments.

The proposed work facilities effective authorization management of workflows on the authorization of tasks to roles or users with the enforcement of SoD. Secure task-based access control to workflow related data is enforced via effective authorization management.

五、計畫成果自評

We have accomplished 90% of the work described in the proposal. The research achievements include (1) proposing a novel approach: Novel duty-conflict relationships among tasks and authorization rules for SoD are analyzed and defined. Moreover, an authorization model for task-based authorizations in workflow environments is proposed; (2) analyzing a procurement process to illustrate the proposed approach; and (3) deploying a prototype system.

Authorization management and access control are crucial for supporting secure workflow management systems. Our work will be a basis for further research on designing secure business commerce. Our work not only contributes to further research on secure workflow systems but also contributes to the application of workflow-enabled electronic commerce. In summary, we have proposed novel idea, investigated new technology and developed a prototype system.

六、參考文獻

[1] J. Barkley, "Implementing Role Based Access Control Using Object Technology", *First ACM Workshop on Role Based Access Control*, November 1995.

[2] E. Bertino, E. Ferrari, V. Atluri, "A Flexible Model Supporting the Specification and Enforcement of Role-based Authorizations in Workflow Management Systems", *RBAC 97 Workshop*, 1997.

[3] A. Cichocki, A. Helal, M. Rusinkiewicz, D. Woelk, *Workflow and Process Automation: Concepts and Technology*, Kluwer Academic Publishers, 1998.

[4] G. Coulouris, J. Dollimore, M. Roberts, "Role and Task-based Access Control in the PerDis Groupware Platform", *Third ACM Workshop on Role-Based Access Control*, October 1998.

[5] D. F. Ferraiolo, J. Cugini, R. Kuhn, "Role-Based Access Control (RBAC): Features and Motivations", *Proc. of 11th Annual Computer Security Application Conference*, pages 241-248, December 1995.

[6] D. F. Ferraiolo, R. Kuhn, "Role-Based Access Control", *In Proceedings of 15th NIST-NCSC National Computer Security Conference*, pages 554-563, October 1992.

[7] V. D. Gligor, S. I. Gavrila, D. Ferraiolo, "On the Formal Definition of Separation-of-Duty Policies and Their Composition", *Proceedings of IEEE Symposium on Security and Privacy, IEEE Computer Society*, May 1998.

[8] G. Kappel, P. Lang, S. Rausch-Schott, W. Retschitzegger, "Workflow Management Based on Objects, Rules, and Roles", *IEEE Bulletin of the Technical Committee on Data Engineering*, Vol. 18/1, March 1995

[9] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models", *IEEE Computer*, 29(2), pp.38-47, February 1996.

[10] K. Schier, "Multifunctional Smartcards for Electronic Commerce — Application of the Role and Task Based Security Model", *14th Annual Computer Security Applications Conference*, December 1998.

[11] R. T. Simon, M. E. Zurko, "Separation of Duty in Role-Based Environments", *10th Computer Security Foundations Workshop*, June 10-12, 1997.

[12] R. K. Thomas, R. S. Sandhu, "Task-Based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management", *Proc. of the IFIP WG11.3 Workshop on Database Security*, August 11-13, 1997.

[13] W. Weitz , "Workflow modeling for Internet-Based Commerce: An Approach Based on High-Level Petri Nets", *Proc. of Intl. IFIP/GI Working Conference TREC'98*, Hamburg, Germany, June 1998.

[14] *Workflow Management Coalition*, "Workflow Management Coalition: Workflow Reference Model", at URL http://www.aiim.org/wfmc/standards/docs/tc003v11.pdf