論文2002-39TE-4-15

확장된 과업 역할기반 접근제어 모델의 구현

(Implementation of Extended Task Role-Based Access Control Model)

任 黃 彬 *, 朴 東 圭 *

(Hwang-Bin Yim and Dong-Gue Park)

요 약

본 연구에서는 워크플로우 환경에서 정적 및 동적 의무 분리 요구 사항의 명세에 대한 과업 역할 기반 접근제어 모델과 상충하는 엔티티 관리 패러다임의 통합을 통하여 기업 환경에서 접근제어 시행을 위한 개선된 접근제어 모델을 구현한다. 본 논문에서 구현한 확장된 과업 역할기반 접근제어 모델은 워크플로우 지향 과업에 대하여 상충하는 엔티티들을 다룰 수 있고 기업의 특성에 따라서 기업 세션의 분류를 통하여 기업 환경에서 과업에 정교한 의무 분리 정책을 지원할 수 있다.

Abstract

This paper implements an improved model for access control enforcement in enterprise environments. The integration of the task role-based access control model and the "conflicting entities" administration paradigm supply a specification of static and dynamic separation of duty requirements in the workflow environment. The implemented Extended Task Role-Based Access Control model can deal with the conflicting entities for workflow oriented tasks. It will support elaborate separation of duty policy to tasks in enterprise environment through the classification of enterprise sessions according to their characteristics.

Keyword : ET-RBAC, workflow, access control

Ⅰ. 서 론

인터넷과 웹의 활성화로 정보자원들을 액세스하는 것이 훨씬 더 쉬워졌다. 그러나 이로 인하여 몇 가지의 중대한 보안 문제들을 생기게 하였다.

접근제어를 위해 개발된 보안 정책으로는 임의 접근제어(DAC), 강제적 접근제어(MAC), 역할 기반 접근제어(RBAC) 및 과업 역할기반 접근제어 모델(TRBAC) 모델 등이 있다[1-4]. 그러나 이들 모델들은 모두 기업 환경에 대한 애플리케이션에서 제약들을 가지고 있으며, 특히 사용자와 사용자 상충(user-user conflicts)과 연관된 복잡한 작업 처리 요구 사항 등은 지원하지 않는다[5-8]. 이에 대한 해결 방법으로 확장된 과업 역할기반 접근제어(Extended Task Role-Based Access Control) 모델이 소개 되었다[9-11].

본 연구에서는 워크플로우 환경에서 정적 및 동적 의무 분리를 해결하기 위한 접근제어 모델인 ET-RBAC 모델을 구현한다.

본 논문의 구성으로 Ⅱ장에서는 새로운 접근제어 모

* 正會員, 順天鄕大學校 情報技術工學部
(Dept. Information & Communication Engineering, Soonchunhyang Univ.)

※ 본 연구는 정보통신부의 ITRC 사업에 의해 수행된 것임

接受日字:2002年8月22日, 수정완료일:2002年12月9日

델인 확장된 과업 역할기반 접근제어 모델에 대해 살펴보고 Ⅲ장에서는 이 모델의 구현과 기능에 대해 설명한 후 Ⅳ장에서 결론을 유도한다.

Ⅱ. 확장된 과업 역할기반 접근제어 모델

<그림 1>은 확장된 과업 역할기반 접근제어 모델의 개념을 표현한 것이다.

확장된 과업 역할기반 접근제어에서의 세션은 W세션과 세션 두 종류로 분류된다. 확장된 과업 역할기반 접근제어의 W세션은 한 사용자를 W 클래스에 해당하는 과업에 할당된 역할들 중 최하위 역할로 매핑하고, 워크플로우 환경에서 과업 인스턴스에 기반을 둔 역할의 활성화를 통제한다. W세션은 사용자가 특별한 과업으로 사용 중일 때에만 존재한다. 즉 사용자가 작업 목록(work-list)에서 하나의 과업으로 작업을 시작할 때부터 그 사용자가 같은 과업에서 작업을 마치거나 일시적으로 중단할 때까지의 시간동안만 존재한다. 사용자가 과업 인스턴스를 일시적으로 중단하거나 완료할 때 과업 인스턴스에 대한 모든 권한은 취소되며 W세션은 파괴된다[11].

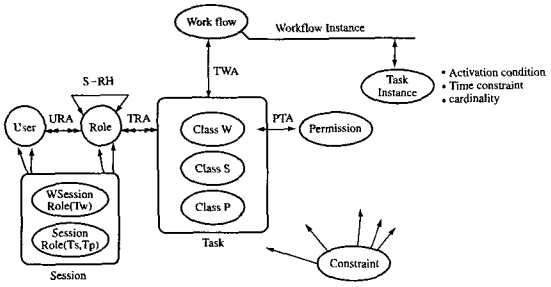

그림 1. 확장된 과업 역할기반 접근제어 모델
Fig. 1. Extended Task Role-Based Access Control (ET-RBAC) model.

Ⅲ. 확장된 과업 역할 기반 접근제어 모델의 구현

<그림 2>는 구매 워크플로우의 예이다.

<그림 2>에서 고딕체는 과업을 나타내고, 이탤릭체는 과업을 수행하고자 하는 사용자의 직위를 나타낸다.

<그림 3>은 워크플로우 예에 대하여 하나의 역할 계층을 묘사한 것이다. 이 그림에서 S 클래스에 속하는

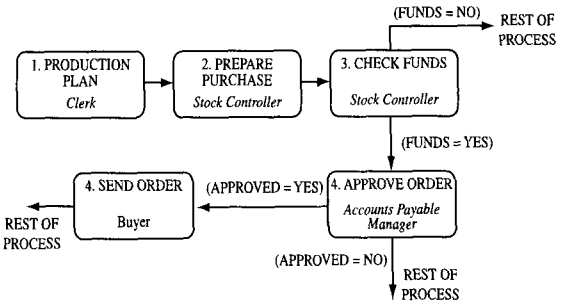

그림 2. 워크플로우의 예
Fig. 2. Example of Workflow.

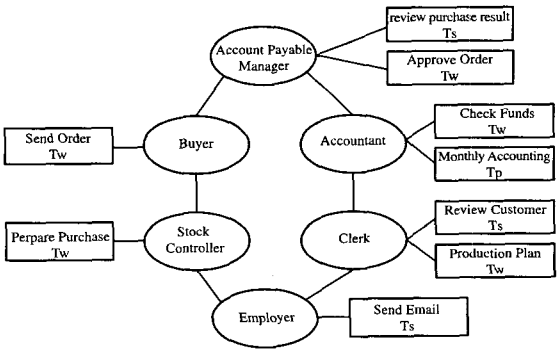

그림 3. 역할계층의 예
Fig. 3. Example of Role Hierarchy.

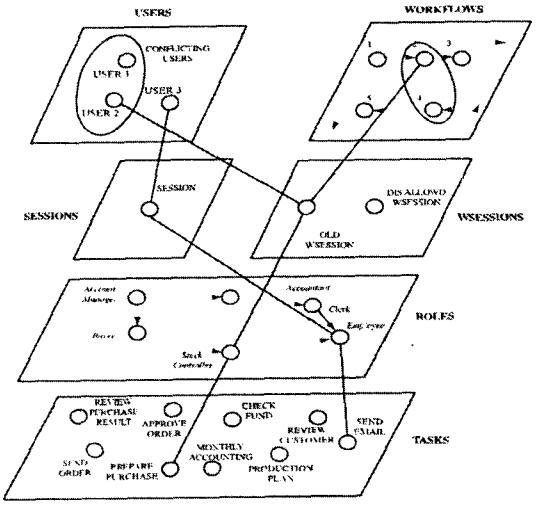

그림 4. 상충 과업과 상충하는 사용자와 W-Session개념의 예
Fig. 4. Example of enforcing the business rule through conflicting tasks and conflicting users and W-Session concept.

과업들은 역할 계층에서 상위 역할로 상속이 이루어지나 P 클래스에 속하는 과업들은 상속이 되지 않는다.

<그림 4>는 상충 과업과 상충하는 사용자, 그리고 W세션에서 업무 규칙이 어떻게 시행하는가에 대해 도표로 묘사한 것이다. 사용자1과 사용자2가 같은 가족 멤버인 경우 이 조건은 상충하는 사용자로써 지정될 수 있다.

과업2와 과업4는 업무 규칙에 의해 동적으로 상충 과업으로 지정되어진다. <그림 4>의 실선으로 연결된 사용자2는 과업2에 할당된 재고관리자(stock controller) 처럼 행동하고 이 사실은 처리 인스턴스의 일부로써 기록된다. 이때 점선으로 연결된 사용자1이 계정관리자(account manager)로서 행동할 수 있는 과업 4를 수행하려고 하면 사용자1과 연관된 W세션은 허가되지 않아야 한다. 만약 사용자1이 과업4를 수행할 수 있는 계정관리자로 행동하면 사용자1과 사용자2는 상충하는 사용자로서 공모할 수 있을 것이다. 이 예를 통하여 워크플로우에서 복잡한 동적 의무분리를 처리하는 것이 가능하다는 것을 알 수 있다. 확장된 과업 역할기반 접근제어 모델을 구현하기 위해 <그림 5>와 같은 ER 다이어그램을 작성하였다. <그림 5>는 can-assignTs-M과 can- assignTs-IM, can-assignTp , can-assignTw의 경우이며 can-revokeTs-M과 can- revo- keTs-IM, can-revokeTp , can- revokeTw도 <그림 5>와 같은 형식의 ER 다이어그램으로 작성할 수 있다.

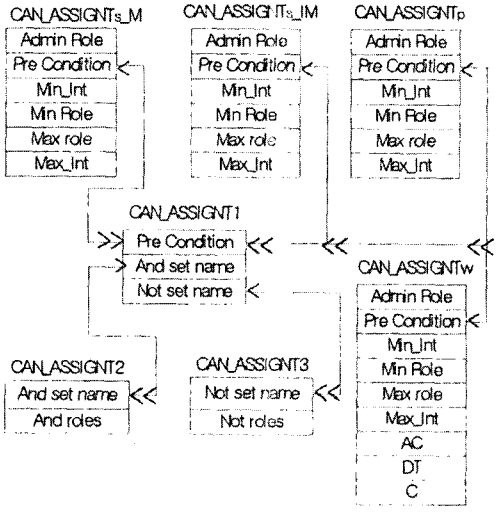

그림 5. can-assignTs-M과 can-assignTs-IM, can-assignTp, can-assignTw 관계의 ER 다이어그램

Fig. 5. ER-Diagram of can-assignTs-M, can-assignTs-IM,can-assignTp, can-assignTw *Relation.*

표 1. can_assignTs_M 테이블의 예

Table 1. Example of can_assignTs_M Table.

AR	PC	Min_Int	Min_R	Max_R	Max_Int
DSO	C1	[	$PL1_s$	$PL1_s$	]
DSO	C1	[	$PL2_s$	$PL2_s$	]
PSO1	C2	[	$PE1_s$	$PE1_s$	]
…	…	…	…	…	…

표 2. can_assignTs_IM 테이블의 예

Table 2. Example of can_assignT_s_IM Table.

AR	PC	Min_Int	Min_R	Max_R	Max_Int
DSO	C1	[	$PL1_s$	$PL1_s$	]
DSO	C1	[	$PL2_s$	$PL2_s$	]
PSO1	C2	[	$PE1_s$	$PE1_s$	]
…	…	…	…	…	…

표 3. can_assignTp 테이블의 예

Table 3. Example of can_assignT_p Table.

AR	PC	Min_Int	Min_R	Max_R	Max_Int
DSO	C11	[	$PL1_p$	$PL1_p$	]
DSO	C12	[	$PL2_p$	$PL2_p$	]
PSO1	C21	[	$PE1_p$	$PE1_p$	]
…	…	…	…	…	…

표 4. can_assignTw 테이블의 예

Table 4. Example of can_assignT_w Table.

AR	PC	Min_ Int	Min_ R	Max_ R	Max_I nt	AC	DT	C
DSO	C11	[	$PL1_p$	$PL1_p$	]	AC1	DT1	C1
DSO	C12	[	$PL2_p$	$PL2_p$	]	AC2	DT2	C2
PSO1	C21	[	$PE1_p$	$PE1_p$	]	AC3	DT3	C3
…	…	…	…	…	…	…	…	…

표 5. can_assignT1 테이블의 예

Table 5. Example of can_assignT1 Table.

PC	*and_set_name*	*not_set_name*
C1	ASET1	null
C2	ASET2	NSET1
C3	ASET2	NSET2
…	…	…

다음의 <표 1, 2, 3, 4, 5>는 <그림 5>의 ER 다이어그램을 이용하여 테이블을 작성하고 작성된 테이블에 관리역할에 대한 데이터를 입력한 예이다.
can-assignT2와 can-assignT3 테이블도 <표 5>와 같은 형식으로 작성할 수 있다.

확장된 과업 역할기반 접근제어 모델을 구현하기 위해 Oracle8i 에서 SQL을 확장한 PL/SQL을 사용하여 관리 도구를 저장 프로시저로 작성하였다. 작성한 저장 프로시저는 다음과 같다.

- share_assignT(role, ttask, arole, mobile)
- share_weak_revokeT(role, ttask, arole, mobile)
- share_strong_revokeT(role,ttask,arole, mobile)
- private_assignT(role, ttask, arole)
- private_revokeT(role, ttask, arole)
- workflow_assignT(role, ttask, arole, ac, dt, c)
- workflow_revokeT(role, ttask, arole)
- conflict_user(user, user)
- conflict_role(ttask, ttask)

저장 프로시저는 역할에 과업을 할당하고 과업을 취소하는 기능을 한다. 파라미터 role은 과업이 할당되거나 취소될 역할이고 ttask(target task)는 역할에 할당되거나 취소될 과업이다. arole(administrative role)은 role에 ttask 과업을 할당하거나 취소할 관리역할이다. mobile 파라미터는 ttask에 입력되는 과업이 이동자격을 가지는지 부동자격을 가지는지를 표시한다. 저장 프로시저중 share_assignT, share_weak_revokeT, share_strong_revokeT는 여러 역할들에 할당될 수 있는 과업 Ts에 대한 과업-역할 할당과 취소 저장 프로시저이고 private_assignT, private_revokeT는 다른 역할들에 할당할 수 없고 특정 역할에만 할당되는 과업 Tp에 대한 과업-역할 할당과 취소 저장 프로시저이다.

저장 프로시저 workflow_assignT, workflow_revokeT는 과업 Tw에 대한 과업-역할 할당 취소 저장 프로시저이다. ac는 role에 할당된 ttask가 활성화 될 수 있는 조건을 의미하며, dt는 활성화된 과업이 유지될 수 있는 시간을 의미하고, c는 동시에 활성화 될 수 있는 과업의 최대 개수를 의미한다. 저장 프로시저 conflict_user와 conflict_role은 상충되는 사용자와 상충되는 과업을 저장하는 프로시저이다.

파라미터 user는 사용자를 의미한다. 저장 프로시저

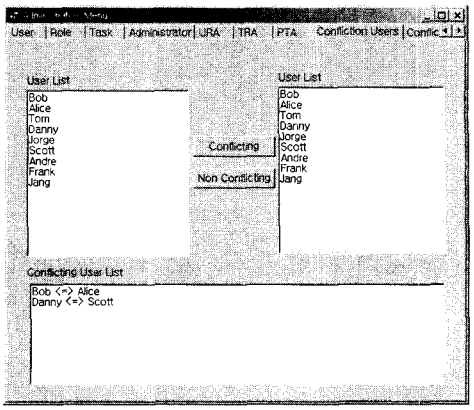

그림 6. 상충되는 사용자 리스트의 예
Fig. 6. Example of Conflicting User List.

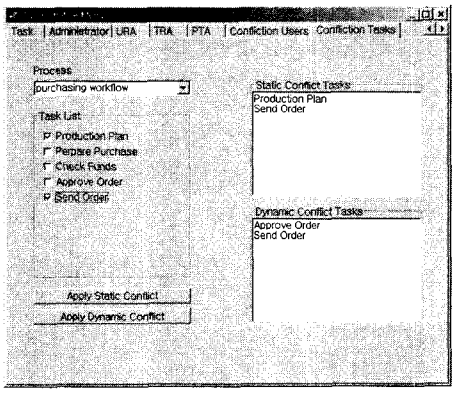

그림 7. 상충되는 과업 리스트의 예
Fig. 7. Example of Conflicting Task List.

표 6. 구현 환경
Table 6. Implementation Environments.

시스템 구현 환경	
OS	Windows 2000
Database	Oracle 8.1.5
개발툴	Borland Delphi 6
H/W	펜티엄III 800MHz 256M RAM, 40G HDD

conflict_user와 conflict_ role을 제외한 저장 프로시저에 의해 할당된 역할과 과업은 시스템에서 사용자에 역할이 할당되는 세션에 의해 사용되며, conflict_user와 conflict_ role에 의해 저장된 상충되는 사용자와 상충되는 과업은 W세션에 의해 사용된다. 위 <그림 6, 7>은 저장 프로시저를 호출해서 사용할 수 있는 관리도구의 GUI이다. <그림 6>은 관리 도구에서 상충되는 사용자

를 입력하는 화면의 예이고, <그림 7>은 정적, 동적으로 상충되는 과업을 입력하는 예이다.

관리 도구를 개발하고 실행하기 위해서는 여러 가지 프로그램이 필요하게 된다. 구현환경은 위 <표 6>과 같다.

Ⅳ. 결 론

시스템에 수많은 사용자, 역할, 권한이 존재하는 경우 이를 관리하는 관리역할을 두어 시스템을 효율적으로 관리할 수 있는 방법이 필요하다. 워크플로우 시스템에서 과업을 고려한 접근통제 방식으로 과업 역할기반 접근제어가 제안 되었으나 이 모델은 동적 의무 분리 요구 사항, 특히 사용자와 사용자간의 상충과 관련된 복잡한 작업 처리를 지원하지 않는다. 이 논문은 상충되는 실체간의 상충 문제를 해결하기위한 개선된 접근제어 모델인 확장된 과업 역할기반 접근제어 모델에 대한 구현 예를 보인 것이다.

이 구현된 모델은 기업 환경에서 기업의 특성에 따라 워크플로우 지향 과업을 세션별로 분류하여 접근제어를 시행함으로서 상충하는 실체들을 다룰 수 있다는 장점을 갖는다.

구현된 관리 도구를 실제 기업 환경의 시스템에 적용해 보고 향후 워크플로우 시스템의 접근통제를 위한 범용 컴포넌트를 구현하고자 한다.

참 고 문 헌

[1] C.P.Pfleeger, "Security in Computing", second edition, Prentice-Hall International Inc. 1997.

[2] R.S.Sandhu, E.J.Coyne, H.L. Feinstein, C.E. Youman "Role-Based Access control Method", IEEE Computer, vol. 29, Feb. 1996.

[3] D.Ferraiom J.Cugini, R.Kuhm, "Rolebased Access Control(RBAC) : Features and motivations", Proc. of 11th Annual Computer Security Application Conference, Dec.1995.

[4] E. Bertino, E.Ferrari, V.Atluri "Specifica tion and Enforcement of Role-based Authorization Constraints in Workflow-Management Systems", ACM Transactions on information and System Security, pp. 65~104, February, 1999.

[5] W.K.Huang, V.Atluri "Secure Flow : A Secure Web-enabled Workflow-Management System", Proc. of 4th ACM Workshop on Role-Based Access Control, 1999.

[6] M.S.Oliver, R.P.Reit, E.Gudes "Specifying Application-level Security in work flow Systems", Proc. of 9th International Workshop on Database and Expert Systems Applications, 1998.

[7] S. Oh and S. Park, "Task-Role Based Access Control(T-RBAC) : An Improved Access Control Model for Enterprise Environment," Proceedings of the 11th International Conference on Database and Expert Systems Appli cations, DEXA 2000, pp. 264~273, 2000.

[8] M. H. Kang, J. S. Park, and J. N. Froscher, "Access Control Mechanisms for Inter-Organizational Workflow," Proceedings of the 6th ACM Symposium on Access Control Models and Technologies SACMAT 2001, Cha ntilly, VA 3-4 , pp. 66~74, May , 2001.

[9] G.-J. Ahn, R. S. Sandhu, M. Kang, and J. Park, "Injecting RBAC to Secure a Web-Based Workflow System," Proceedings of the 5th ACM Workshop on Role-Based Access Control, Berlin,July 26~28, 2000.

[10] R.A.Botha, J.H.P.Eloff, "Separation of duties for access control enforcement in work flow environments," IBM Systems Journal. Vol 40, No 3, pp. 666~682. 2001.

[11] Dong Gue Park, Yu Dong Hwang, Sun Hyung Kim, Extended Task Role-Based Access Control Model For Access Control Enforcement in Enterprise Environments, EALPIIT, 2002.

저 자 소 개

任 黃 彬(正會員)

1983년 : 명지대학교 전자과 학사. 1985년 : 건국대학교 대학원 전자공학과 석사. 2002년 : 순천향대학교 전기전자공학과 정보통신 전공 박사수료.

朴 東 圭(正會員)

한양대학교 대학원 전자공학과 공학박사. 1992년~1995년 : 순천향대학교 정보통신공학과 전임강사. 1995년~1998년 : 순천향대학교 전기전자공학부 조교수. 1999년~현재 : 순천향대학교 정보기술공학부 부교수.