RBAC 에서 권한 할당 제약사항들 간의 충돌 탐지 모델

임현수*, 조은애**, 문창주***

The Model of Conflict Detection between Permission Assignment Constraints in Role-Based Access Control

Hyun-Soo Im, Eun-Ae Cho, Chang-Joo Moon

Abstract

Assuring integrity of permission assignment (PA) constraints is a difficult task in role-based access control (RBAC) because of the large number of constraints, users, roles and permissions in a large enterprise environment. We provide solutions for this problem using the conflict concept. This paper introduces the conflict model in order to understand the conflicts easily and to detect conflicts effectively. The conflict model is classified as a permission-permission model and a role-permission model. This paper defines two type conflicts using the conflict model. The first type is an inter-PA-constraints (IPAC) conflict that takes place between PA constraints. The other type is a PA-PAC conflict that takes place between a PA and a PA constraint (PAC). Also, the conditions of conflict occurrence are formally specified and proved. We can assure integrity on permission assignment by checking conflicts before PA and PA constraints are applied.

Key Words: RBAC, constraint, permission assignment

* 고려대학교 컴퓨터학과, fribirdz@gmail.com

** 고려대학교 컴퓨터학과, eacho99@swsys2.korea.ac.kr

*** 건국대학교 컴퓨터응용과학부, cjmoon@kku.ac.kr

1. 서론

1RBAC의 개념은 다수의 응용프로그램을 다수의 사용자가 사용하는 온라인 시스템에서 시작 되었다. RBAC의 기본 개념은 역할을 생성한 후에, 역할에 적합한 권한들을 할당하고, 사용자를 역할에 할당하므로 사용자가 자신이 속한 역할들에 할당된 권한을 소유하는 것이다[1]. 이러한 개념은 사용자에 대한 권한 할당을 간단하게 해주며, 관리적인 측면이 매우 중요하다. RBAC의 관리에 관한 기존의 연구들은 주로 관리자의 관리 범위와 관리 권한에 대해 다루고 있고, 할당 제약조건에 기반한 역할에 대한 사용자 혹은 권한 할당의 무결성(integrity)에 대해서는 논하지 않고 있다.

본 논문은 RBAC을 관리하는 과정에서 발생하는 할당의 무결성 보장 문제를 충돌[2] 개념을 사용하여 해결 하고자 한다. 특히 권한 할당은 권한부여의 핵심적인 부분[3]임에도 불구하고 기존연구에서 자세히 언급되지 않고 있다. 따라서 본 논문에서는 권한 할당에 대해 집중적으로 다룬다.

논문의 나머지 부분은 다음과 같이 구성된다. 2장에서는 RBAC모델과 PA(Permission Assignment) 제약사항에 대해 설명한다. 3장에서는 본 논문에서 제안하는 충돌 탐지 모델을 기술한다. 4장에서는 제안한 충돌 탐지 모델을 바탕으로 IPAC(Inter-PA-Constraints) 제약사항과 PA 제약사항의 충돌을 탐지에 관해 논의한다. 마지막으로 5장에서는 결론을 기술한다.

2. 관련 연구

2.1 RBAC 모델

RBAC 모델은 사용자, 역할, 권한, 세션과 같은 4가지 구성요소를 갖고 있다. 그림 1은

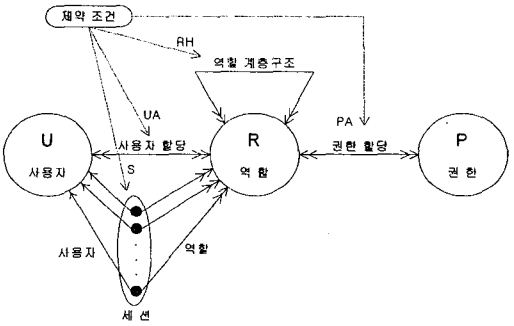

그림 1 RBAC 모델

RBAC96[1] 모델의 개념을 보여주고 있다. 사용자(User: U)는 인간의 행위나 자율적인 에이전트 등을 나타내고, 역할(Role: R)은 구성원들의 직책이나 책임 등을 고려한 일의 기능이나 직책을 나타낸다. 권한(Permission: P)은 하나 이상의 객체들에 대한 접근의 승인이나 특정 행위를 할 수 있는 특권을 나타낸다. 세션(Session: S)은 한 사용자에게 가능한 여러 역할을 나타낸다. 여기서 특정 세션 안에 있는 사용자는 자신이 속한 역할들의 일부분을 사용할 수 있다.

2.2 권한 할당의 충돌

이 장에서는 기존 논문[4]에서 연구되었던 대표적인 PA 제약조건들에 대해 알아본다.

1) 분리 권한(Disjoint Permission: DP) 제약조건

동일한 권한이 정적인 임무 분리가 선언된 두 개 이상의 역할에 할당되지 못한다[4].

2) 충돌 권한(Conflict Permission:CP) 제약조건

충돌 권한들은 동일 역할에 할당될 수 없다.

3) 선행 권한(Prerequisite Permission: PP) 제약조건

권한 q가 권한 p의 선행 권한이라고 할 때, 권한 p가 임의의 역할에 할당되려면 권한 q가 이미 그 역할에 할당되어 있어야 한다[1].

4) 단일 역할에만 권한 할당(Permission Assignmented to Single Role: PASR) 제약조건

권한의 집합인 pasr_ps에 속한 권한들은 어떤 역할 pasr_r에만 할당될 수 있다.

3. 충돌 탐지 모델

본 논문에서는 충돌 탐지 모델을 권한-권한 연관모델과 역할-권한 연관모델로 나누었다. 권한-권한 연관모델은 권한 간의 관계를 연결관계와 단절관계로 나눈다. 어떤 두 권한이 연결관계로 지정되어 있다면 역할에 이 권한들을 할당 할 때 반드시 두 권한을 같이 할당해야 한다. 반대로 두 권한 간의 관계가 단절관계로 설정되어 있다면, 이 관계들이 한 역할에 함께 할당될 수 없다. 역할-권한 모델은 역할과 권한 간의 관계를 포함관계와 배제관계로 나눈다. 어떤 역할과 권한이 포함관계이면 해당 권한은 반드시 그 역할에 할당되어야 한다. 반대로 배제관계이면 해당 권한은 그 역할에 할당될 수 없다. 그림 2는 충돌 탐지 모델을 보여주고 있다.

4. 권한 할당 제약조건 간의 충돌

4.1 IPAC 충돌

이 장에서는 충돌 모델을 사용해서 IPAC 충돌을 정의하고, IPAC 충돌 발생의 조건을 설명한다.

정의 1. 연결관계와 단절관계가 동일한 권한-권한 관계에 설정되어 있다면 IPAC 충돌이 발생한다.

정의 2. 포함관계와 배제관계가 동일한 역할-권한 연결에 설정되어 있다면 IPAC 충돌이 발생한다.

정의 3. 연결관계가 배제관계에 의해서 해제되면 IPAC 충돌이 일어난다. 그 역도 성립한다.

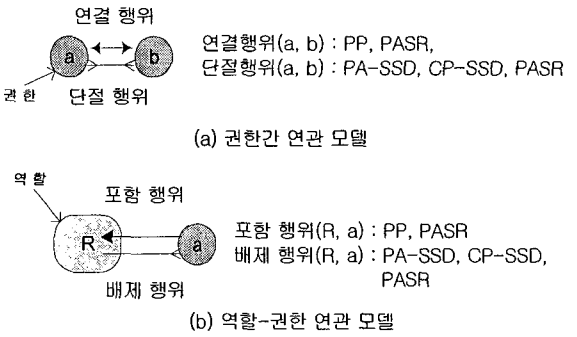

그림 2 충돌 탐지 모델

정의 4. 포함관계가 배제관계에 의해서 해제되면 IPAC 충돌이 일어난다. 그 역도 성립한다.

표 1은 2장에서 언급한 4개의 권한 할당 제약조건들의 가능한 조합을 보여준다. 각 조합은 3가지의 값(*No, Maybe, Yes*)을 가진다. *No*는 제약조건의 내용에 상관없이 IPAC 충돌이 발생하지 않는다는 것을 나타낸다. *Maybe*는 권한 할당 제약조건의 내용만으로는 충돌을 단정 지을 수 없고, 충돌의 가능성만을 판단할 수 있다는 것을 나타낸다. *Yes*는 제약조건의 내용만으로 충돌을 판단할 수 있음을 나타낸다.

표 1 권한 할당 제약조건간의 충돌 비교

	DP	*CP*	*PP*	*PASR*
DP	*No*	-	-	-
CP	*No*	*No*	-	-
PP	*Maybe*	*Yes*	*No*	-
PASR	*No*	*Yes*	*Maybe*	*Yes*

1) DP와 PP 사이의 충돌

정리 1. pp와 pp′ 가 있을때 pp.pps ∩ pp′.pps ≥ 1 이고 pp.pps ∩ pp′.pps ⊆ pa-ssd 이면, 충돌 가능성은 *Maybe*이다. 그리고 만일, pp.tp ∈r, pp′.tp∈r′, {r, r′}⊆ssd, 인 할당정보가 확

인되면 충돌 가능성은 *Yes*이다.

2) CP와 PP 사이의 충돌

정리 2. pp.tp ∈ cp-ssd 이고 pp.pps ⊆ cp-ssd 이면 충돌 가능성은 *Yes*이다.

3) PP와 PASR 사이의 충돌

정리 3. pasr.pasr_ps ∩ pp.pps ≥ 1 이면 충돌 가능성은 *Maybe*이다. 만일, pp.tp ∈ perms(cop_r_i) 인 할당정보가 확인되면 충돌 가능성은 *Yes*이다.

4) CP와 PASR 사이의 충돌

정리 4. cp와 pasr에서 pasr.pasr_ps ∩ cp ≥ 2이면, IPAC 충돌 가능성은 *Yes*이다.

5) PASR 사이의 충돌

정리 5. pasr과 pasr'가 있을 때, pasr.pasr_r 과 pasr'.pasr_r이 계층적인 관계를 갖고 있지 않고, pasr.pasr_ps ∩ cp ≥ 1이면 충돌 가능성은 *Yes*이다.

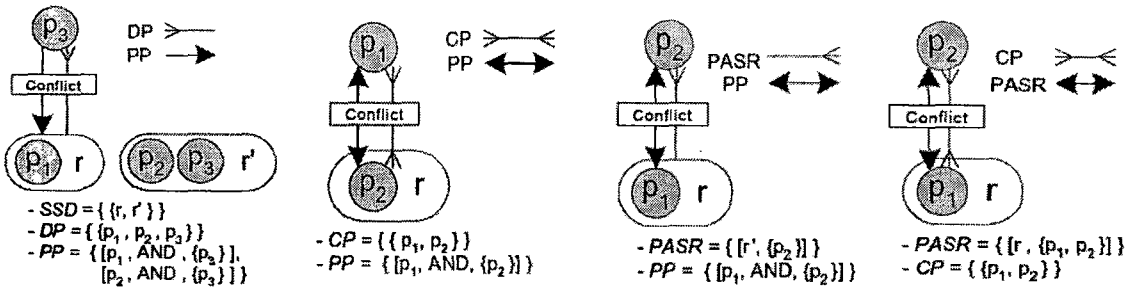

그림 3 제약 조건들 간의 충돌 : 왼쪽부터 DP와 PP, CP와 PP, PP와 PASR, CP와 PASR

4.2 PA-PAC 충돌

권한 할당이 권한 제약조건을 만족시키지 못할 때 PA-PAC 충돌이 발생한다. PA-PAC 충돌은 다음과 같은 두 가지 경우에 발생한다. 첫째, 제약조건이 새로 만들어지거나 변경되었을 때 기존에 할당되어진 권한이 새로 만들어진 제약조건을 만족하지 못할 때 발생한다. 둘째, 권한 할당이 새롭게 이루어지거나 변경되었을 때 기존의 제약조건이 새로운 권한 할당을 만족시키지 못할 때 발생한다.

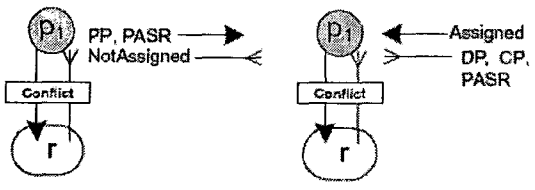

그림 4 정의 2에 의한 충돌

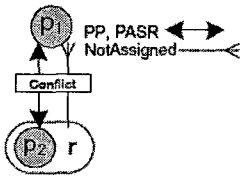

그림 5
정의 3에 의한 충돌

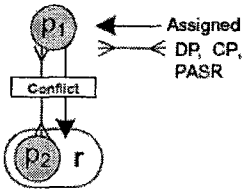

그림 6
정의 4에 의한 충돌

5. 결론 및 향후과제

본 논문은 권한 할당 제약조건을 가시적으

로 보여주는 충돌 탐지 모델을 제안했으며, 충돌들에 대해 정의하였다. 충돌 탐지 모델은 충돌을 쉽게 이해하고, 효과적으로 발견할 수 있게 해준다. 또한 본 논문은 충돌이 발생하는 조건들을 정형적으로 명세하였다. 이러한 연구들은 충돌 발생 여부를 명확히 판단할 수 있게 해준다. 그러므로 권한 할당을 하기 전에 충돌 여부를 검사하고 권한 할당 제약조건을 적용해서 권한 할당의 무결성을 보장할 수 있다. 따라서 본 논문에서 제안하는 충돌 탐지 모델은 권한 할당에서 발생할 수 있는 보안 관리자의 실수를 줄이고, 부적절한 권한 할당을 막아준다.

향후 연구로는 충돌에 대해 가능한 해결법을 자동화하여 제시하는 방안에 대한 연구가 필요하다.

참고문헌

[1] Ravi S. Sandhu, Edward J. Coynek, Hal L. Feinsteink , Charles E. Youmank, Role-Based Access Control Models , IEEE Computer, Volume 29, Number 2, February 1996, pages 38-47.

[2] Emil C. Lupu, Morris Sloman, Conflicts in Policy-Based Distributed System Management , IEEE TRANSACTION ON SOFTWARE ENGINEERING, VOL. 25, NO. 6, 1999

[3] Jason Crampton, George Loizou, Administrative Scope and Role Hierarchy Operations, SACMAT'02, June 3-4, 2002, Monterey, California, USA

[4] Chang-Joo Moon, Dae-Ha Park, Soung-Jin Park, Doo-Kwon Baik, Symmetric RBAC Model that Takes the Separation of Duty and Role Hierarchies into Consid-eration, Computers & Security, Vol.23, No.2, 2004 March, 126~136.