論文2002-39TE-3-13

다단계 보안통제가 가능한 확장된 역할 기반 접근통제 모델

(An Extended Role-Based Access Control Model with Multi-level Security Control)

任 黃 彬 *, 朴 東 圭 *

(Hwang-Bin Yim and Dong-Gue Park)

요 약

역할기반 접근통제(RBAC : Role-Based Access Control)는 사용자의 역할에 기반을 둔 접근통제 방법으로 다양한 컴퓨터, 네트워크 보안 분야에 있어서 유연성을 제공한다. 그러나 역할기반 접근통제는 역할이나 허가 등을 적용하는 대상으로 사용자만을 고려하고 있으므로 실제의 응용 시스템 상에서 정확한 접근통제를 위해서는 사용자뿐만 아니라 주체 및 객체를 추가로 고려할 필요성이 있다. 본 논문에서는 다단계 보안시스템을 위하여 역할기반 접근통제 모델에 사용자, 주체, 객체, 역할에 대한 보안등급을 추가로 고려하여 확장된 역할기반 접근통제 모델 $ERBAC_3$를 제안한다.

Abstract

RBAC(Role-Based Access Control) is an access control method based on the user's role and it provides more flexibility on the various computer and network security fields. But, RBAC models consider only users for roles or permissions, so for the purpose of exact access control within real application systems, it is necessary to consider additional subjects and objects. In this paper, we propose an Extended RBAC model, $ERBAC_3$, for access control of multi-level security system by adding users, subjects, objects and roles level to RBAC, which enables multi-level security control.

Keyword : multi-level security, Extended RBAC, RBAC, access control

Ⅰ. 서 론

역할기반 접근통제(RBAC : Role-Based Access Control)의 개념은 접근통제의 전통적인 강제적 접근통제(MAC : Mandatory Access Control) 및 임의적 접근통제(DAC : Discretionary Access Control)의 대안으로서 많은 관심을 집중시키고 있다.[1]

역할기반 접근통제는 역할(role), 역할과 관련된 행동을 나타내는 권한(permission), 사용자(user)의 관계로 표현된다.[4, 5]

역할기반 접근통제는 관리자에게 편리한 관리 능력을 제공하여 관리업무의 효율성을 꾀할 수 있고, 역할, 역할계층(Role hierarchy), 관계(relationship), 제약(constraint)의 정립을 통하여 사용자의 행동을 정적 또는 동적으로 규제할 수 있으므로 시스템 관리자에게 객체단위가 아닌 추상적인 개념으로 접근을 통제할 수 있어서 실제 환경에 자연스럽게 접목, 구현될 수 있는

* 正會員, 順川鄕大學校 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9月13日

장점과 분산 환경에서 사용되는 경우 역할기반 접근통제 관리자의 책임을 중앙과 국지 보호 영역으로 구분할 수 있어서 관리 책임을 분명히 할 수 있다는 장점이 있다.[8]

그러나 역할기반 접근통제는 역할이나 허가 등을 적용하는 대상으로 사용자만을 고려하고 있으므로 실제의 응용 시스템 상에서 정확한 접근통제를 위해서는 사용자뿐만 아니라 주체 및 객체를 추가로 고려할 필요성이 있다. 기 발표된ERBAC$_0$[7] 모델도 사용자, 역할, 주체 및 객체에 보안등급을 적용하여 다단계 보안이 가능하지만 역할 계층과 의무분리가 제공되지 않아 실제의 기업 환경에 적용하기에는 무리가 따른다.

본 연구에서는 역할의 보안등급에 따라 역할 상속이 가능한 역할계층과 정적, 동적인 의무분리를 할 수 있는 ERBAC$_1$, ERBAC$_2$ 를 추가로 고려한 확장된 역할기반 접근통제 모델 ERBAC$_3$ 를 새롭게 제안한다.

Ⅱ. 역할기반 접근통제 모델

역할기반 접근통제 모델은 특성에 따라 4가지 (RBAC$_0$, RBAC$_1$, RBAC$_2$, RBAC$_3$)형태의 역할기반 접근 통제 모델로 구분된다.

RBAC$_0$ 모델은 역할기반 접근통제를 다양한 시스템에 적용할 수 있도록 개발된 기본모델이다.

RBAC$_1$은 RBAC$_0$를 포함하고 다른 역할로부터 권한을 상속받을 수 있다는 역할 계층(role hierarchies)의 특성을 추가하였으며, RBAC$_2$는 RBAC$_0$를 포함하고 역할기반 접근통제 요소들의 설정에 제한조건을 설정할 수 있도록 제약(constraints)을 가하는 특성을 부가하였다.

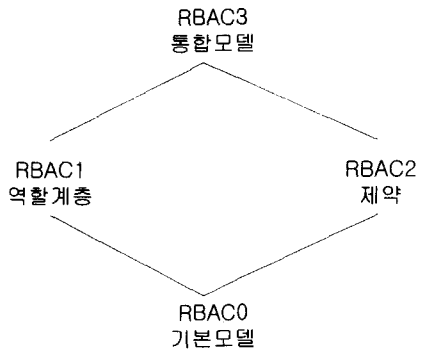


그림 1. 역할기반 접근통제 모델간의 관계
Fig. 1. Relationship of RBAC Models.

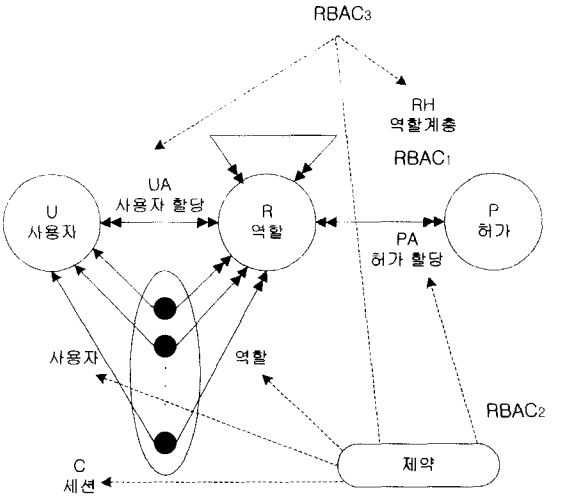


그림 2. RBAC 모델
Fig. 2. RBAC Model.

RBAC$_3$는 RBAC$_0$, RBAC$_1$, RBAC$_2$의 특성을 모두 포함하며 본 논문에서는 역할기반 접근통제 모델로 지칭한다.

그림 1은 4가지 역할기반 접근통제 모델간의 관계를 나타낸 것이고, 그림 2는 4가지 모델에 대한 개념도를 나타낸 것이다.

역할기반 접근통제 모델은 다음과 같이 정의 된다.

[정의 1] RBAC$_0$모델

- $PA \subseteq P \times R$
- $UA \subseteq U \times R$
- $user : C \rightarrow U$
- $roles : C \rightarrow 2^R$

$user$는 각 세션(session) C_i를 단일 사용자인 $user(C_i)$에 매핑(mapping)시키는 함수를 의미하며, $roles$는 각 세션 C_i를 임의의 역할 집합인 $roles(C_i)$에 매핑시키는 함수를 의미한다. 이때 다음의 관계가 성립한다.

- $roles(C_i) \subseteq \{r \mid (user(C_i), r) \in UA\}$
- 세션 C_i는 $\cup_{r \in roles(S_i)}\{p \mid (p, r) \in PA\}$에 해당하는 권한을 가진다.

[정의 2] RBAC$_1$모델

- RBAC$_0$모델 포함.
- $RH \subseteq R \times R$은 역할 계층이나 역할 포함 관계라 불리는 상에서 부분적인 순서이다.
- $roles : S \rightarrow 2^R$은 $roles(S_i) \subseteq \{r \mid (\exists r' \geq r)[(user(S_i), r') \in UA]\}$

를 요청하기 위하여 $RBAC_0$로 부터 수정되었으며, 세션 C_i는 권한 $\cup_{r \in roles(S)}\{p \mid (\exists r'' \geq r)[(p, r'') \in PA]\}$를 가진다.

[정의 3] RBAC2모델

- $RBAC_0$모델 포함.
- $RBAC_2$는 $RBAC_0$의 여러 요소들의 값이 허락되는지를 결정하는 제약의 집합을 요구한다.

Ⅲ. 확장된 역할기반 접근통제 모델

본 논문에서는 역할기반 접근통제 모델을 표현하기 위하여 다음과 같은 용어를 사용한다.

- U : U는 사용자의 집합을 의미한다.
- C : C는 세션의 집합을 의미한다.
- S : S는 주체의 집합을 의미한다. 여기서 주체의 집합 S는 사용자의 집합 U를 포함하는 것으로 정의한다.
- X : 임의의 사용자, 역할, 객체를 의미한다.
- S_{ji} : S_{ji}는 세션 c_j 및 사용자 u_i와 연관된 주체의 집합을 의미한다.
- R : R은 역할(Role)의 집합을 의미한다.
- R_{ji} : R_{ji}는 세션 c_j 및 사용자 u_i와 연관된 역할의 집합을 의미한다.
- SL : SL은 보안 등급(Security Level)의 집합을 의미한다.
- SL_u : SL_u는 사용자 u_i 에게 부여된 보안등급의 집합을 의미한다.
- SL_o : SL_o는 객체 o 에게 부여된 보안등급의 집합을 의미한다.
- SL_r : SL_r는 객체 r 에게 부여된 보안등급의 집합을 의미한다.
- CSL_{ji} : CSL_{ji}는 세션 c_j 및 사용자 u_i와 연관된 주체에게 부여된 현재의 보안등급(Current Security Level)의 집합을 의미한다.
- P : P는 권한의 집합을 의미한다. 예를 들면, READ 또는 WRITE 등이 권한에 해당한다.
- P_{ji} : P_{ji}는 세션 c_j 및 사용자 u_i와 연관된 권한의 집합을 의미한다.
- O : O는 객체의 집합을 의미한다. 여기서 객체의 집합 O는 주체의 집합 S를 포함하는 것으로 정의한다.
- UA : UA는 사용자와 역할의 연관관계 집합을 의미한다.
- PA : PA는 권한과 역할의 연관관계 집합을 의미한다.
- SA : SA는 주체와 역할의 연관관계 집합을 의미한다.
- OA : OA는 객체와 역할의 연관관계 집합을 의미한다.
- USL : USL은 사용자와 보안등급의 연관관계 집합을 의미한다.
- SSL : SSL은 주체와 보안등급의 연관관계 집합을 의미한다.
- OSL : OSL은 객체와 보안등급의 연관관계 집합을 의미한다.
- RSL : RSL은 역할과 보안등급의 연관관계 집합을 의미한다.

1. 확장된 역할 기반 접근통제 모델 설계

위에서 살펴본 바와 같이 지금까지 제안된 역할기반 접근통제는 역할이나 허가 등을 적용하는 대상으로 사용자만을 고려하고 있으므로 실제의 응용 시스템 상에서 정확한 접근통제를 위해서는 사용자뿐만 아니라 주체 및 객체를 추가로 고려할 필요성이 있다.

또한 다단계 보안을 위하여 사용자, 역할, 주체 및 객체에 보안 레벨을 적용할 필요가 있다. 이를 위해 기존의 역할기반 접근통제를 개선하여 다단계 보안이 가능하도록 한 확장된 역할기반 접근 통제 모델이 제안되었다[7]. 그러나 이 모델도 기존의 역할기반 접근 통제 모델들 중 ERBAC0만을 고려한 것으로 역할의 계층구조와 제약 등을 고려하지 못한 단점이 있다. 본 논문에서는 이런 단점을 개선하여 역할의 계층구조와 제약 등을 고려한 확장된 역할기반 접근 통제 모델을 제안한다.

확장된 역할기반 접근통제 모델을 그림으로 표현하면 그림 3과 같으며, 다음 정의들을 사용하여 확장된 역할기반 접근통제 모델을 $ERBAC_0$, $ERBAC_1$, $ERBAC_2$, $ERBAC_3$ 모델로 정의할 수 있다.

$ERBAC_0$ 모델은 다음 [정의 4]로 정의 할 수 있다.[7]

[정의 4] 확장된 역할기반 접근통제 모델 : ERBAC0 모델

U, R, P, S, O, C, X, SL에 대하여, $ERBAC_0$ 모델은 다음의 구성요소로 이루어진다.

- $PA \subseteq P \times R$,
- $UA \subseteq P \times R$,
- $SA \subseteq P \times R$,

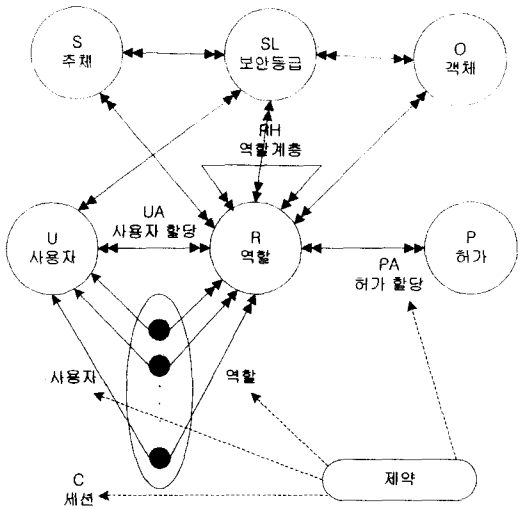


그림 3. 확장된 역할기반 접근통제 모델
Fig. 3. Extended RBAC Model.

- $OA \subseteq P \times R$,
- $USL \subseteq U \times SL$,
- $SSL \subseteq S \times SL$,
- $OSL \subseteq O \times SL$,
- $RSL \subseteq R \times SL$,
- $f_u: C \rightarrow U$,
- $f_s: (C, U) \rightarrow S$,
- $f_r: (C, U) \rightarrow 2^R$,
- $f_p: (C, U) \rightarrow 2^P$,
- $f_{SL}: X \rightarrow SL$,
- $f_{CSL}: (C, U) \rightarrow 2^{SL}$.

단, 여기에서 다음의 식1에서 식4 및 조건이 성립한다.

$$u_i = f_u(c_j) \quad \text{(식 1)}$$

$$S_{ji} = f_s(c_j, f_u(c_j)) = f_s(c_j, u_i) \quad \text{(식 2)}$$

$$R_{ji} = f_r(c_j, u_i) \subseteq \cup_{s \in S_{ji}} \{r \mid \text{RAssigned2U}(u_i, r) \wedge \text{RAssigned2S}(s, r)\} \quad \text{(식 3)}$$

$$P_{ji} = (c_j, u_i) = \cup_{r \in R_{ji}} \{p \mid (p, r) \in PA\} \quad \text{(식 4)}$$

[정의 5] 확장된 역할기반 접근통제 모델 : ERBAC1 모델

- $ERBAC_0$ 모델 포함
- $RH \subseteq R \times R$ 은 역할 계층이나 역할 포함 관계라 불리는 R상에서 부분적인 순서이다.
- $r_2 \geq r_1 \ (r_2) \geq (r_1)$

[정의 6] 세션 c_j 및 사용자 u_i와 연관된 역할의 집합을 결정하는 함수 f_r은 다음과 같다.

$$f_r: (C, U) \rightarrow 2^R$$

여기서, f_r은 세션 c_j와 세션 c_j에게 연관된 특정의 사용자 u_i를 역할의 집합인 $f_r(c_j, u_i)$에게 매핑시키는 함수를 의미한다. 이 함수 f_r은 $ERBAC_0$ 모델에서 정의된 함수를 확장된 역할기반 접근통제 모델 $ERBAC_1$ 을 설계하기 위하여 새롭게 정의하였다. 새롭게 정의된 함수 f_r은 함수 f_u 및 f_s를 이용하여 다음의 (식5)와 같이 임의의 세션 c_j 및 사용자 u_i와 연관된 역할의 집합 R_{ji}를 얻어낼 수 있다.

$$\begin{aligned} R_{ji} &= f_r(c_j, u_i) \subseteq \cup_{s \in S_{ji}} \{r \mid (\exists r' \geq r)\ [\text{RAssigned2U}(u_i, r') \wedge \text{RAssigned2S}(s, r')] \\ &= \cup_{s \in f_s(c_j, f_u(c_j))} \{r \mid (\exists r' \geq r)\ [\text{RAssigned2U}(u_i, r') \wedge \text{RAssigned2S}(s, r')] \\ &= \cup_{s \in f_s(c_j, u_i)} \{r \mid (\exists r' \geq r)\ [\text{RAssigned2U}(u_i, r') \wedge \text{RAssigned2S}(s, r')] \end{aligned} \quad \text{(식 5)}$$

[정의 7] 세션 c_j와 사용자 u_i와 연관된 허가의 집합을 결정하는 함수 f_p는 다음과 같다.

$$f_p: (C, U) \rightarrow 2^P.$$

여기에서, f_p는 세션 c_j와 c_j에게 연관된 특정의 사용자 u_i를 허가의 집합인 $f_p(c_j, u_i)$에게 매핑시키는 함수를 의미한다. 이 함수 f_p는 함수 f_r을 이용하여 다음의 (식6)과 같이 임의의 세션 c_j 및 사용자 u_i와 연관된 허가의 집합 P_{ji}를 얻어낼 수 있다.

$$P_{ji} = (C_j, u_i) = \cup_{r \in R_{ji}} \{(\exists r'' \leq r)[(p, r'') \in \text{PA}]\} \quad \text{(식6)}$$

[정의 8] 확장된 역할기반 접근통제 모델 : $ERBAC_2$ 모델

- SSD: ρ(Role × Role)

SSD : 정적인 의무분리(SSD : Static Separation of Duty)에 포함된 역할 쌍 $< r_i, r_j >$의 대칭집합, 따라서 대칭집합 $< r_i, r_j >$가 멤버이면, $< r_j, r_i >$도 멤버임.

- 정적인 의무분리(SSD : Static Separation of Duty) :

많은 기관에서 책임은 충돌을 피하기 위하여 여러 개의 역할들 간에 분리되어 있다. 역할의 그룹이 역할의 권한부여에 따라서 각각 상호 배타적인 정적인 의무분리 특성을 통하여 설계될 수 있다.

$\forall r_i \forall r_j \forall u_i$ RAssigned2U(u_i, r_i) $\wedge$ RAssigned 2U(u_i, r_j)

$\rightarrow < r_j, r_i > \notin SSD$

• Mutex-permission : ρ(Permission $\times$ Permission)

Mutex-permission은 사적인 허가 또는 사용자에게 인가된 역할 집합에 대해서 서로 배타적인 허가 쌍 <p, q> 의 대칭 집합임.

• *SOSD* : ρ(Role $\times$ Role)

SOSD : Mutex-permission 내의 허가에 따라서 정적인 운영상의 의무분리(SOSD : Static Operational Separation of Duty)에 포함된 역할 쌍 <i, j>의 대칭 집합

• 정적인 운용상의 의무분리(SOSD : Static Operational Separation of Duty) : 이는 비즈니스 업무는 다수의 오퍼레이션으로 구성되어 있다는 의미를 근거로 하고 있으며, SOSD는 객체 상에서 허용 가능한 오퍼레이션의 집합을 표현하기 위한 허가를 사용하여 시행된다.[2, 3]

$\forall r_i \forall r_j \forall u_i$ RAssigned2U(u_i, r_i) $\wedge$ RAssigned 2U(u_i, r_j) $\rightarrow < r_i, r_j > \notin$ SOSD

• DSD : ρ(Role $\times$ Role)

DSD : 동적인 의무분리(DSD : Dynamic Separation of Duty) 관계에 포함된 역할 쌍 $< r_i, r_j >$ 의 대칭 집합임.

• 동적인 의무분리(DSD : Dynamic Separation of Duty) : 역할의 그룹은 역할 활성화를 고려하여 상호 배타적으로 설계될 수 있다. 비록 DSD 역할이 사용자에 의해 동시에 활성화되는 것을 방지하지만 어떤 환경에서는 연속하여 활성화될 수도 있다.

$\forall r_i \forall r_j \forall c_j \forall u_i$ RAssigned2UC(c_j, u_i, r_i) $\wedge$ RAssigned 2UC(c_j, u_i, r_j) $\rightarrow < r_i, r_j > \notin$ DSD

• Mutex-perm : ρ(Permission $\times$ Permission)

Mutex-perm은 동일한 사용자에 의해 활성화된 서로 배타적인 허가 쌍 $< p_s, p_t >$의 대칭 집합임.

• DOSD : ρ(Role $\times$ Role)

DOSD : Mutex-Permission 내의 허가에 따라서 동적인 운영상의 의무분리(DOSD : Dynamic Operational Separation of Duty)에 포함된 역할 쌍$< r_i, r_j >$ 의 대칭 집합.

즉, $\forall r_i \forall r_j \forall c_j \forall u_i \forall p_s \forall p_t$ DOSD = {[$< r_i, r_j >$ | $f_{p_s}(c_j, u_i) \wedge f_{p_t}(c_j, u_i) \wedge < p_s, p_t > \in$ Mutex-perm }

$f_{p_s}(c_j, u_i) = \cup_{r_i \in R_n} \{ p_s / (p_s, r_i) \in PA \}$

$f_{p_t}(c_j, u_i) = \cup_{r_j \in R_n} \{ p_t / (p_t, r_j) \in PA \}$

• 동적인 운영상의 의무분리(DOSD : Dynamic Operational Separation of Duty) : 허가의 그룹은 임의의 사용자를 대신하는 주체에 의해 활성화되는 역할을 고려하여 상호 배타적으로 설계될 수 있다.

$\forall r_i \forall r_j \forall c_j \forall u_i$ RAssigned2UC(c_j, u_i, r_i) $\wedge$ RAssigned2UC(c_j, u_i, r_j) $\rightarrow < r_i, r_j > \notin DOSD$

• membership-limit : $Role \rightarrow N$

membership-limit[r_i] : 하나의 역할에 인가될 수 있는 최대 사용자 수. 디폴트 값은 시스템 사용자의 전체 수.

• authorized-members : $Role \rightarrow N$

authorized-members[r_i] : 역할에 인가될 수 있는 최대 사용자 수, 즉, $|\{r_i | \text{RAssigned2U}(u_i, r_i)\}|$, 여기서 집합의 멤버수 제한은 | |의 쌍에 의해 표기됨.

• 정적인 멤버 수 제한 : 하나의 역할에 인가된 사용자의 수가 일정 시간에 멤버쉽 제한을 넘을 수 없다는 특성이다.

$\forall r_i$ authorized-member[r_i] $\leq$ mem bership-limit [r_i]

• 선행 역할 : 선행 역할(prerequisite roles)의 개념은 능력과 선점에 기반을 두고 있다. 즉 사용자는 역할 B의 멤버이어야만 역할 A의 멤버가 될 수 있다는 것이다. 예를 들어 프로젝트 역할의 멤버였던 사용자가 테스팅 작업 역할에 할당될 수 있다는 것이다.[6]

r_i가 r_j의 선행역할일 경우, 다음과 같이 표현될 수 있다.

$\forall r_i \forall r_j \forall u_i \{ u_i | \text{RAssigned2U}(u_i, r_i) \rightarrow \text{AssignedR2U}(u_i, r_j)$

[정의 9] 확장된 역할기반 접근통제 모델 : $ERBAC_3$ 모델

$ERBAC_1$ 모델과 $ERBAC_2$ 모델을 합치면 $ERBAC_3$ 모델이 된다.

2. 역할기반 접근통제 모델과 확장된 역할기반 접근통제 모델의 비교

역할기반 접근통제는 기본적으로 응용 시스템 내에서 조직에서 정의된 임무나 작업기능 등과 같은 역할에 기반 하여 사용자의 자원에 대한 접근을 안전하게 통제하기 위한 수단을 제공하기 위한 것이다. 이때 사용자에 대한 역할이 정의되었다고 하더라도 정보보호 시스템 내에서 수행되는 사용자의 행위는 실행 가능한 작업(operation) 단위로 이루어지게 된다.

그러나 역할기반 접근통제는 역할이나 허가 등을 적용하는 대상으로 사용자만을 고려하고 있으므로 실제의 응용 시스템 상에서 정확한 접근통제를 할 수 없게 된다. 그러므로 다단계 보안시스템을 위하여 역할에 대한 보안등급을 고려하여 역할기반 접근통제 모델에 사용자 이외에 주체 및 객체의 역할과 역할에 대한 보안등급을 추가로 고려하여 정교한 역할기반 접근통제를 실현할 수 있게 되는 장점이 있다.

위 표1의 모델 특징 비교를 보면 ERBAC 모델은 다단계 보안통제 기능을 제공하며, 접근통제 대상도 다단계 보안통제를 고려했기 때문에 객체와 역할, 주체와 역할, 사용자와 보안등급, 주체와 보안등급, 객체와 보안등급, 역할과 보안등급이 추가되었다. 역할 적용대상도 사용자, 주체, 객체를 고려하여 좀더 상세수준에서의

표 1. 모델 특징 비교
Table 1. Comparison of Model Characteristics.

	RBAC	ERBAC
다단계 보안통제 기능	제공안함	제공함
접근통제 대상	- 권한과 역할 - 사용자와 역할	- 권한과 역할 - 사용자와 역할 - 객체와 역할 - 주체와 역할 - 사용자와 보안등급 - 주체와 보안등급 객체와 보안등급 - 역할과 보안등급
역할 적용대상	사용자	사용자, 주체, 객체
장점	- 기존의 DAC, MAC에 비하여 유연한 접근통제 정책제공 - 사용자에 대한 역할부여 기능	- 기존의 DAC, MAC에 비하여 유연한 접근통제 정책제공 - 사용자, 역할, 권한에 대한 다단계 보안통제 가능 - 주체 및 객체에 대한 역할 부여가 가능하므로 정교한 역할기반 접근통제 가능

표 2. $ERBAC_0$와 $ERBAC_3$의 특징 비교
Table 2. Comparison of $ERBAC_0$ and $ERBAC_3$ Characteristics.

	ERBAC0	ERBAC3
역할계층	역할계층 제공하지 않음(역할 상속이 이루어지지 않음)	- 역할 계층 제공(역할 상속됨) 하위 역할이 상위 역할로 상속 될 때에도 역할의 보안등급에 따라 상속이 결정된다.
의무분리	의무분리 제공하지 않음	- 정적 의무 분리 제공. - 동적 의무 분리 제공

역할기반 접근통제를 제공할 수 있다.

다음의 표2는 기존의 $ERBAC_0$[7]와 본 논문에서 제안하는 $ERBAC_3$의 특징을 비교한 것이다.

위 표1과 표2에서 알 수 있듯이 $ERBAC_0$ 모델도 사용자, 역할, 주체 및 객체에 보안등급을 적용하여 비교적 정교한 다단계 보안이 가능하지만 역할 계층과 의무분리가 제공되지 않아 실제의 기업 환경에 적용하기에는 무리가 따른다.

그러나 본 연구에서 제안하는 $ERBAC_3$ 모델은 역할의 보안등급에 따라 역할 상속이 가능한 역할계층과 정적, 동적인 의무분리를 할 수 있는 $ERBAC_1$, $ERBAC_2$를 추가하여 고려하였으므로 실제의 기업 환경에 적용하여 정교하고 정확한 다단계 보안통제가 가능한 확장된 역할기반 접근통제 기능을 제공한다.

Ⅳ. 결 론

역할기반 접근통제는 강제적 접근통제 및 임의적 접근통제에 이어 새로운 접근통제 방법으로서 각광을 받고 있으며 향후에도 정형적 설계 및 검증, 시스템 실용화 등의 측면에서 많은 발전이 있을 것으로 기대된다.

본 논문에서는 역할기반 접근통제 모델을 개선하여 사용자, 역할에 다단계 보안등급을 고려하고 주체 및 객체의 역할과 역할에 대한 보안등급을 추가로 고려하여 다단계 보안통제가 가능한 확장된 역할 기반 접근통제 모델을 제안하였다.

본 연구에서 제안하는 $ERBAC_3$ 모델은 기존의 $ERBAC_0$ 모델에 $ERBAC_1$, $ERBAC_2$ 모델을 추가하여 고려하였으므로 실제의 기업 환경에 적용하여 정교하고 정확한 다단계 보안통제가 가능한 확장된 역할기반 접근통제 기능을 제공한다. 이 모델은 또한 기존의 역할기반 접근통제 모델이 제공하지 못하는 작업(ope-

ration)단위의 정교한 접근통제 기능을 제공해 준다.

향후에는 본 연구결과를 토대로 다중등급보안 역할 기반 접근통제 모델을 다양한 형태의 응용 시스템에 적용하기 위한 연구가 계속 수행되어야 할 것으로 사료된다.

참 고 문 헌

[1] Matunda Nyanchama and Sylvia Osborn, "Modeling mandatory access control in role-based security systems", In Databvase Security Ⅷ : Status and Prospects, Chapman-Hall, 1996.

[2] LuigiGuiri and Pietro Iglio, "A formal model for role-based access control with constraints", In Proceedings of 9th IEEE Computer SecurityFoundations Workshop, pages 136-145, Kenmare, Ireland, June 1996.

[3] Ravi Sandhu, "Role Hierarchies and Constraints for Lattice-Based Access Control" Proc. Fourth European Symposium on Research in Computer Security, Rome, Italy, September 25-27, 1996.

[4] Ravi Sandhu, Edward J.Coyne, Hal L. Feinstein and Charles E. Youman, "Role-Based Access Control Models", IEEE Computer, pp.38-47, Volume 29, Number 2, February, 1996.

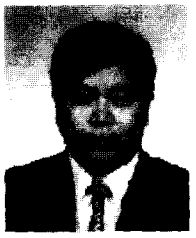
[5] C. Ramaswamy and R. Sandhu, "Role-Based Access Control Features in Commercial Database Management Systems", NISSC. 1998.

[6] W.A.Jansen, "Inheritance Properties of Role Hierarchies", 21th NCSC/NIST NISSC National Information Systems Security Conference, pp. 476~485, Crystal City, VA, October 5-8, 1998.

[7] 김학범, 홍기용, 김동규 "확장된 역할기반 접근통제 모델", 통신정보보호학회논문지, 1999. 3.

[8] D.F.Ferraiolo, R.Sandhu, S.Gavrila, D.R .Kuhn, R.Chandramouli, "Proposed NIST standard for role-based access control", ACM TIS-SEC Vol. 4, No.3, pp.224~274, 2001.

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)

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