역할계층을 포함하는 역할기반 접근통제 모델

김 학 범[1], 김 석 우[2]
드림시큐리티[1], 한세대학교[2]

요 약

역할기반 접근통제는 추상적 기본 개념의 임의적 접근통제나 강제적 접근통제에 비하여 응용 개념의 역할에 기반한 접근통제 모델이다. 모델은 BLP 모델에서 출발한 커널 단위의 액세스 제어의 제한적 기능과 달리 다양한 컴퓨터 · 네트워크 보안분야에 있어서 유연성과 적용성을 제공한다. 본 논문에서는 기존의 역할기반 접근통제 기본 모델인 $RBAC_0$ 모델에 주체 및 객체의 역할을 추가로 고려한 역할 계층을 포함하는 확장된 역할기반 접근통제 ($ERBAC_0$: *Exteded* $RBAC_0$) 모델을 제안하였다. 제안된 $ERBAC_0$ 모델은 기존의 $RBAC_0$ 모델에 비하여 주체 및 객체 수준에서의 역할을 계층적으로 정교하게 할당하고, 할당된 역할에 기반하여 접근통제 서비스를 보다 유연하게 제공할 수 있다.

Role Based Access Control Model contains Role Hierarchy

(Hak-Beom Kim[1], Seok-Woo Kim[2])

ABSTRACT

RBAC(Role Based Access Control) is an access control method based on the application concept of role instead of DAC(Discretionary Access Control) or MAC(Mandatory Access Control) based on the abstract basic concept. Model provides more flexibility and applicability on the various computer and network security fields than the limitted l functionality of kernel access control orginated from BLP model .

In this paper, we propose $ERBAC_0$(*Extended* $RBAC_0$) model by considering subject's and object's roles and the role hierarchy result from the roles additionally to $RBAC_0$ base model. The proposed $ERBAC_0$ model assigns hierarchically finer role on the base of subject and object level and provides flexible access control services than traditional $RBAC_0$ model.

Ⅰ. 서 론

역할기반 접근통제(*RBAC* : *Role Based Access Control*)개념은 지난 20여년 동안 꾸준히 연구되어 오다가 최근 들어 기존의 임의적 접근통제(DAC : Discretionary Access Control) 및 강제적 접근통제(MAC : Mandatory Access Control)의 대안으로서 관심이 집중되고 있다[1]. 역할기반 접근통제의 주요 동기는 수행이 어려운 보안관리 과정을 관리자가 능률적으로 처리하고 국방분야 이외의 상용분야에 적합한 보안정책을 정확히 표현하고 적용할 수 있도록 하는데 있다[2][3].

역할기반 접근통제에 대한 주요 연구는 NIST(National Institute of Standards and Technology)를 중심으로 조지메이슨 대학 및 Seta Corporation 등이 주축이 되어 활발한 연구를 진행해 오고 있다. NIST에서는 접근통제에 안전하고, 효과적이며 일관적인 메커니즘을 적용하기 위하여 역할기반 접근통제에 대한 정형적 참조모델(Formal Reference Model)을 개발하기 위하여 NSA(National Security Agency)와 메릴랜드 대학 등과 공동 연구개발을 추진하고 있다. 또한, Mach 운영체제에 기반한 안전한 플랫폼인 NSA의 Synergy 플랫폼 상에 RBAC을 구현 중에 있다[4]. 이런 노력의 결실로 RBAC은 SESAME(Secure European System for Applications in a Multi-vendor Environment) 분산 시스템과 Oracle의 SQL3 표준의 일부로 고려되었고, OMG(Object Management Group)의 CORBA(Common Object Request Broker Architecture) 보안명세서[5]에서도 OMG가 분산 객체 기술로 사용할 수 있는 접근통제 메커니즘의 하나로서 RBAC을 사용토록 하고 있다. 역할기반 접근통제 관련 기술을 구현하고 있는 제품도 Windows NT, ORACLE 7, NETWARE4 등 점차적으로 증가하고 있는 추세에 있다[6]. 이와 함께 '98년 5월에 국제공통평가기준(CC : Common Criteria)[7]이 발표되어 ISO를 통한 국제 표준 제정 과정에 있으며, 이를 기반으로 한 역할기반 접근통제 보호 프로파일(PP : Protection Profile)[8]이 발표되었다.

역할기반 접근통제 정책은 역할-허가, 사용자-역할, 역할-역할 관계와 같은 다양한 역할기반 접근통제 요소들로 구체화된다. 이러한 역할 및 역할 관계에 기반하여 어떤 특정 사용자가 시스템내의 자원이나 데이터에 대한 접근을 허용할 것인지가 결정되는 것이다. 접근허가 결정에 필요한 역할기반 접근통제 요소들은 시스템 관리자에 의해 직접적으로 설정되거나 또는 시스템 관리자에 의해 위임된 적절한 관리적 역할(administrative role)에 의해 설정될 수도 있다[9].

기존의 역할기반 접근통제 모델은 역할이나 허가 등에 사용자만을 고려하고 있으므로 실제의 응용 시스템 상에서 정확한 접근통제를 위해서는 주체 및 객체를 추가로 고려할 필요성이 있다. 이를 위하여, 본 논문에서는 Ravi S. Sandhu가 최초로 제안한 역할기반 접근통제 기본 모델인 $RBAC_0$ 모델[10]에 주체 및 객체의 역할을 추가로 고려하여 확장된 역할기반 접근통제($ERBAC_0$: *Extended* $RBAC_0$) 모델을 새롭게 제안한다.

Ⅱ. 용어 정의

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.

여기에서 주체의 집합 S는 사용자의 집합

U를 포함하는 것으로 정의한다.

- 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.
- P : P는 허가(Permission)의 집합을 의미한다.
- P_{ji}: P_{ji}는 세션 c_j 및 사용자 u_i와 연관된 허가의 집합을 의미한다.
- G : G는 신뢰된 주체(Trusted Subject)의 집합을 의미한다. 여기에서 신뢰된 주체의 집합 G는 주체의 집합 S에 포함되는 것으로 정의한다.
- O : O는 객체의 집합을 의미한다. 여기에서 객체의 집합 O는 주체의 집합 S를 포함하는 것으로 정의한다.
- PA : PA는 허가와 역할의 연관관계 집합을 의미한다.
- UA: UA는 사용자와 역할의 연관관계 집합을 의미한다.
- SA : SA는 주체와 역할의 연관관계 집합을 의미한다.
- OA : OA는 객체와 역할의 연관관계 집합을 의미한다.

III. 역할기반 접근통제 기본 모델

3.1 Ravi S. Sandhu의 역할기반 접근통제 모델

Ravi S. Sandhu는 4가지 형태의 역할기반 접근통제 모델 $RBAC_0$, $RBAC_1$, $RBAC_2$, $RBAC_3$을 최초로 제안하였다[10]. $RBAC_0$ 모델은 역할기반 접근통제를 다양한 시스템에 적용할 수 있도록 개발된 기본 모델이다. $RBAC_1$과 $RBAC_2$는 $RBAC_0$을 포함하지만 각각 고유한 특성을 보유하고 있다. $RBAC_1$은 다른 역할로부터 허가를 상속받을 수 있다는 역할 계층(role hierarchies)의 특성을 추가하였으며, $RBAC_2$는 역할기반 접근통제 요소들의 설정에 제한조건을 설정할 수 있도록 제약(constraints)을 가하는 특성을 부가하였다. 제약은 상위 레벨의 조직 정책을 정하기 위한 강력한 메커니즘이다. 어떤 역할이 상호 배타적으로 정해지면 역할에 대한 사용자의 할당은 조직의 전체적인 정책에 대한 손상을 두려워할 염려없이 분산시키거나 위임시킬 수 있다. 역할기반 접근통제의 관리가 완전히 보안 관리자에 의해 집중화되어 있을 경우 제약은 유용하게 활용될 수 있다. $RBAC_1$과 $RBAC_2$의 특징을 통합한 모델은 $RBAC_3$으로 (그림 1)에서와 같이 $RBAC_0$, $RBAC_1$과 $RBAC_2$를 수용한다. (그림 2)는 이 4가지 모델에 대한 개념도를 나타낸 것이다. 이들 중에서 $RBAC_0$ 모델은 $RBAC_1$, $RBAC_2$, $RBAC_3$ 모델들이 참조하는 기본 모델로 다음과 같이 정의된다.

【정의 1】 역할기반 접근통제 모델($RBAC_0$ 모델)

U, R, P, C 에 대하여 $RBAC_0$ 모델은 다음의 구성요소로 구성된다.

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

여기에서, $user$는 각 세션 c_i를 단일의 사용자인 $user(c_i)$에게 사상(mapping)시키는 함수를 의미하며, $roles$는 각 세션 c_i를 임의의 역할 집합인 $roles(c_i)$에게 사상시키는 함수를 의미한다. 이때, $RBAC_0$ 모델에서는 다음의 관계가 성립한다.

- $roles(c_i) \subseteq \{r \mid (user(c_i), r) \in UA\}$
- 세션 c_i는 $\bigcup_{r \in roles(c_i)} \{p \mid (p, r) \in PA\}$에 해당하는 허가를 지닌다.

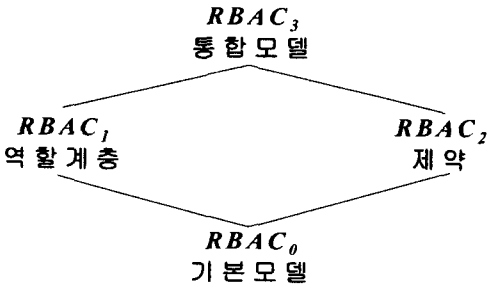

그림 1 역할기반 접근통제 모델간의 관계

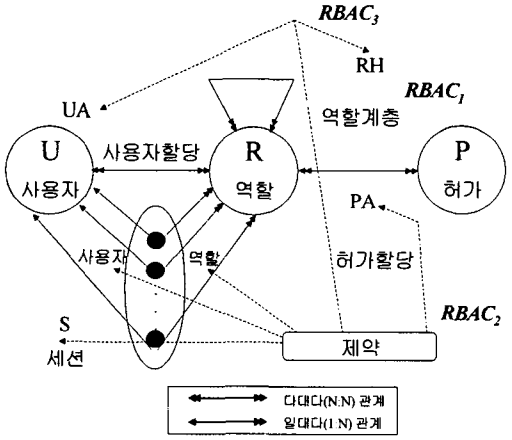

그림 2 역할기반 접근통제 모델

3.2 W. A. Jansen의 역할기반 접근통제 모델

W. A. Jansen의 논문에서는 역할 계층의 특징과 이 특징들이 의무분리(separation of duty)와 같은 기본적인 RBAC 특성에 미치는 영향을 분석하였다[11]. 기본적인 RBAC 모델의 특성은 역할의 멤버쉽에 대한 제약과 관련된 정적인 특성과 역할의 활성화(activation)에 대한 제약과 관련된 동적인 특성으로 구분된다. 이 논문에서는 두 가지 측면에서 역할 계층을 도입하였을 때 기본 특성들이 어떤 영향을 받는지를 분석하였다. RBAC 기본 특성 중에 역할 계층에 영향을 받는 특성에는 cardinality 상속성(inheritance), 의무분리의 계층적 일관성(separation of duty hierarchical consistency), 의무분리의 상속성(separation of duty inheritance) 등이 있다.

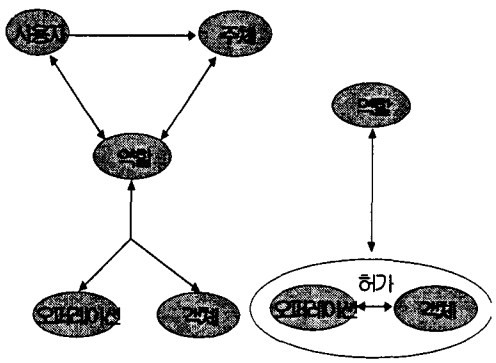

그림 3 (a) 모델 구성요소
(b) 객체를 고려한 허가

이 논문에서 사용된 모델 구성요소와 객체를 고려한 허가는 (그림 3)과 같다. 이 모델에서의 정적인 특성과 동적인 특성은 다음과 같다. 여기에서, u는 사용자의 집합, x, y는 주체의 집합, i, j, k는 역할의 집합, op는 오퍼레이션, p, q는 허가를 나타낸다.

- 정적 Cardinality :

$\forall i \; authorized-members[i] \leq$

$membership-limit[i]$

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

$\forall i \forall j \forall u \quad i \in authorized-roles[u] \wedge j \in authorized-roles[u] \rightarrow \langle i, j \rangle \notin SSD$

- 정적인 운용상의 의무분리(SOSD : Static Operational Separation of Duty) :

$\forall i \forall j \forall u \quad i \in authorized-roles[u] \wedge \in authorized-roles[u] \rightarrow \langle i, j \rangle \notin SOSD$

- 동적 Cardinality :

$\forall i \; active-members[i] \leq active-membership-limit[i]$

- 동적 의무분리(DSD : Dynamic Separation of Duty) :

$\forall x \forall y \forall i \forall j \quad i \in active-roles[x] \wedge j \in active-roles[y] \; active-roles[y] \wedge active-roles[y] \rightarrow \langle i, j \rangle \notin DSD$

- 동적인 운용상의 의무분리(DOSD : Dynamic Operational Separation of Duty) :

$\forall x \forall y \forall i \forall j \; i \in active-roles[x] \wedge j \in active-roles[y] \wedge active-user[x] \; active-user[y] \rightarrow \langle i, j \rangle \notin DOSD$

역할 계층의 개념을 제안한 모델에 적용하면 다음과 같은 영향을 미친다.

- 허용된 활동 :

$\forall x \forall op \forall o \; exec[x, op, o] \equiv \exists i \; (i \in active-roles[x] \wedge p \in authorized-permissions[i] \wedge \langle op, o \rangle \in p)$

- Cardinality 상속성(Cardinality Inheritance) :

$\forall i \forall j \; i \geq j \rightarrow (membership-limit[i] \leq membership-limit[j] \wedge (active-membership-limit[i] \leq active-membership-limit[j])$

- 의무분리의 계층적 일관성(Separation of Duty Hierachical Consistency)

$\forall i \forall j \quad (i \geq j \wedge \exists k \; (k \geq i) \wedge (k \geq j) \rightarrow \langle i, j \rangle \notin DSD \wedge \langle i, j \rangle \notin SSD \wedge \langle i, j \rangle \notin \wedge \langle i, j \rangle \notin DOSD)$

- 의무분리 상속성(Separation of Duty Inheritance) :

$\forall i \forall j \forall k \; i \geq j, \; \langle j, k \rangle \in SSD \rightarrow \langle i, k \rangle \in SSD$

$\forall i \forall j \forall k \; i \geq j, \; \langle j, k \rangle \in DSD \rightarrow \langle i, k \rangle \in DSD$

$\forall i \forall j \forall k \; i \geq j, \; \langle j, k \rangle \in SOSD \rightarrow \langle i, k \rangle \in SOSD$

$\forall i \forall j \forall k \; i \geq j, \; \langle j, k \rangle \in DOSD \rightarrow \langle i, k \rangle \in DOSD$

Ⅳ. 확장된 역할기반 접근통제 모델

4.1 모델 설계

Ravi S. Sandhu가 제안한 $RBAC_0$ 모델은 사용자에 대해서만 고려하고 있으므로 주체 및 객체에 대하여 추가로 고려할 필요성이 있다. W. A. Jansen이 제안한 역할기반 접근통제 모델에서는 주체 및 객체의 개념은 소개했으나 역할 계층(Role Hierarchy) 문제를 해결하기 위한 것에 초점을 둔 것으로 객체의 역할, 사용자와 주체 및 객체에 대한 바인드는 정확히 해결하지 못하고 있는 상태이다. 따라서 본 절에서는 새로운 확장된 역할기반 접근통제 모델($ERBAC_0$: *Exteded* $RBAC_0$)을 제안하기 위하여 먼저 사용자, 주체 및 객체와 역할간에 존재하는 관계성(Relationship)을 분석·제시하면 다음 (그림 4) 및 (그림 5)와 같다. (그림 4)는 사용자와 역할, 주체와 역할, 객체와 역할간의 관계성을 나타낸 것이다. 한 사용자는 여러 개의 역할을 할당받을 수 있고 하나의 동일한 역할에 대해서 여러 명의 사용자가 할당되어 있을 수 있으므로 사용자와 역할간의 관계는 다대다

(N : N) 관계가 성립한다. 또한 어느 한 주체(또는 객체)는 여러 개의 역할을 할당받을 수 있고 하나의 동일한 역할에 대해서 다수의 주체(또는 객체)가 할당되어 있을 수 있으므로 주체(또는 객체)와 역할간의 관계는 다대다(N : N) 관계가 성립한다.

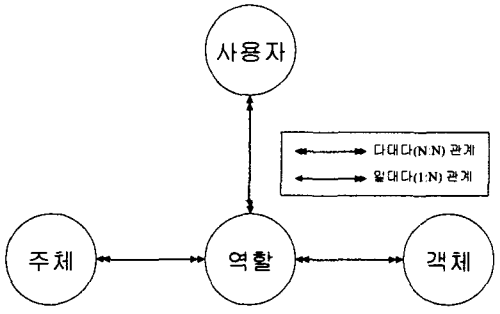

그림 4 사용자, 주체 및 객체와 역할간의 관계

다음 (그림 5)는 세션, 주체 및 사용자간의 관계성을 나타낸 것이다. 어느 한 사용자는 다수개의 세션을 유지할 수 있고 한 세션 동안에는 그 세션에 해당하는 단일의 사용자가 연관되어 있으므로 사용자와 세션간에는 일대다(1:N)의 관계가 성립한다. 또한, 어느 한 사용자는 세션을 유지하는 동안 다수의 주체를 생성하여 원하는 작업을 실행하게 되며 어느 한 주체는 반드시 단일의 사용자에게 연관되어 있으므로 사용자와 주체간에는 일대다(1:N)의 관계가 성립한다. 따라서 어느 한 세션은 그 세션에 해당하는 주체가 생성하여 실행시킨 다수의 주체들과 연관되므로 세션과 주체간에도 일대다(1:N)의 관계가 성립한다.

【정의 2】 (그림 1) 및 (그림 2)와 같은 관계성으로부터 U, R, P, S, O 에 대하여 다음 관계를 정리한다.

- $PA \subseteq P \times R$,
- $UA \subseteq U \times R$,
- $SA \subseteq S \times R$,
- $OA \subseteq O \times R$.

확장된 역할기반 접근통제 모델을 설계하기 위하여 주체와 역할의 연관관계 집합인 SA, 객체와 역할의 연관관계 집합 OA를 새롭게 추가하였다.

【정의 3】 임의의 세션과 연관된 사용자를 결정하는 함수 f_u는 다음과 같다.

$$f_u : C \rightarrow U.$$

여기에서, f_u는 각 세션 c_j를 단일의 사용자인 $f_u(c_j)$에게 사상시키는 함수를 의미하며 다음의 (식1)이 성립한다.

$$u_i = f_u(c_j) \quad \text{..... (식1)}$$

【정의 4】 임의의 세션 및 사용자와 연관된 주체의 집합을 결정하는 함수 f_s는 다음과 같다.

$$f_s : (C, U) \rightarrow S.$$

여기에서, f_s는 세션 c_j와 세션 c_j에게 연관된 특정의 사용자 u_i를 주체들의 집합인 $f_s(c_j, u_i)$에게 사상시키는 함수를 의미한다. 함수 f_u는 $RBAC_0$ 모델에서의 함수 $user$와 동일하며, 함수 f_s는 임의의 세션에 대하여 해당 사용자와 연관된 주체들의 집합을 결정할 수 있도록 하는 함수를 의미한다. 이 f_s는 $RBAC_0$ 모델에서는 정의되지 않는 함수로 확

장된 역할기반 접근통제 모델을 설계하기 위하여 새롭게 추가하였다. 새롭게 추가된 함수 f_s는 함수 f_u를 이용하여 다음의 (식2)와 같이 임의의 세션 c_j 및 사용자 u_i와 연관된 주체의 집합 S_{ji}을 얻어낼 수 있다.

$$S_{ji} = f_s(c_j, f_u(c_j)) = f_s(c_j, u_i)$$
..... (식2)

따라서, 사용자가 동작시킨 세션들은 무엇이며 어느 한 세션 동안에 실행한 주체들은 무엇인지를 파악할 수가 있다. 또한, 이러한 관계를 통하여 특정 사용자의 세션이 유지할 수 있는 역할을 결정할 수 있는 것이다. 이러한 관계는 (그림 5)에 나타낸 바와 같이 어느 한 사용자 u_i가 자신에게 속한 임의의 어느 한 세션 c_j 동안 원하는 작업을 수행하기 위하여 실행한 주체들은 s_l, s_m, ..., s_n이며 세션 c_j가 가질 수 있는 역할은 사용자 u_i에게 부여된 역할과 이 사용자 u_i가 생성한 주체들 즉, s_l, s_m, ..., s_n에게 부여된 역할에 의해서 결정된다. 즉, (그림 5)에서 임의의 세션 c_j 및 사용자 u_i와 연관된 주체의 집합 S_{ji}는 다음의 (식3)과 같음을 알 수 있다.

$$S_{ji} = \{s_l, s_m, \ldots, s_n\}$$
..... (식3)

【정의 5】 세션 c_j 및 사용자 u_i와 연관된 역할의 집합을 결정하는 함수 f_r은 다음과 같다.

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

여기에서, f_r은 세션 c_j와 세션 c_j에게 연관된 특정의 사용자 u_i를 역할의 집합인 $f_r(c_j, u_i)$에게 사상시키는 함수를 의미한다. 이 함수 f_r은 $RBAC_0$ 모델에서는 정의되지 않는 함수로 확장된 역할기반 접근통제 모델을 설계하기 위하여 새롭게 정의하였다. 새롭게 정의된 함수 f_r은 함수 f_u 및 f_s를 이용하여 다음의 (식4)와 같이 임의의 세션 c_j 및 사용자 u_i와 연관된 역할의 집합 R_{ji}를 얻어낼 수 있다.

$$\begin{aligned} R_{ji} &= f_r(c_j, u_i) \subseteq \\ &\bigcup_{s \in S_{ji}} \{r \mid (s, r) \in SA\} \\ &= \bigcup_{s \in fs(c_j, fu(c_j))} \{r \mid (s, r) \in SA\} \\ &= \bigcup_{s \in fs(c_j, u_i)} \{r \mid (s, r) \in SA\} \end{aligned}$$
..... (식4)

【정의 6】 세션 c_j 및 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 세션 c_j에게 연관된 특정의 사용자 u_i를 허가의 집합인 $f_p(c_j, u_i)$에게 사상시키는 함수를 의미한다. 이 함수 f_p는 $RBAC_0$ 모델에서는 정의되지 않는 함수로 확장된 역할기반 접근통제 모델을 설계하기 위하여 새롭게 정의하였다. 새롭게 정의된 함수 f_p는 함수 f_r을 이용하여 다음의 (식5)와 같이 임의의 세션 c_j 및 사용자 u_i와

연관된 허가의 집합 P_{ji}를 얻어낼 수 있다.

$$P_{ji} = \bigcup_{r \in fr(c_j, u_i)} \{p \mid (p, r) \in PA\}. \quad \text{(식5)}$$

이상의 【정의 2 ~ 6】 및 (식1 ~ 5)를 토대로 Ravi S. Sandhu가 제안한 $RBAC_0$ 모델을 확장한 역할기반 접근통제($ERBAC_0$: *Extended* $RBAC_0$) 모델을 제안하면 다음 【정의 7】과 같다.

【정의 7】 확장된 역할기반 접근통제 모델 : $ERBAC_0$ 모델 U, R, P, S, O, C에 대하여, $ERBAC_0$ 모델은 다음의 구성요소로 이루어진다.

- $PA \subseteq P \times R$,
- $UA \subseteq U \times R$,
- $SA \subseteq S \times R$,
- $OA \subseteq O \times R$,
- $f_u : C \rightarrow U$,
- $f_s : (C, U) \rightarrow S$,
- $f_r : (C, U) \rightarrow 2^R$,
- $f_p : (C, U) \rightarrow 2^P$.

단, 여기에서 다음의 식이 성립한다.

- $u_i = f_u(c_j)$,
- $S_{ji} = f_s(c_j, f_u(c_j)) = f_s(c_j, u_i)$,
- $R_{ji} = f_r(c_j, u_i) \subseteq \bigcup_{s \in S_n} \{r \mid (s, r) \in SA\}$
- $P_{ji} = \bigcup_{r \in fr(c_j, u_i)} \{p \mid (p, r) \in PA\}$.

4.2 모델의 비교

역할기반 접근통제는 기본적으로 정보보호시스템 내에서 조직에서 정의된 임무나 또는 작업 기능 등과 같은 역할에 기반하여 사용자의 자원에 대한 접근을 안전하게 통제하기 위한 수단을 제공하기 위한 것이다. 이때, 사용자에 대한 역할이 정의되었다고 하더라도 정보보호시스템 내에서 수행되는 사용자의 행위는 실행 가능한 프로그램(또는 객체), 즉 주체를 통하여 대신 이루어지게 된다. 그러므로 사용자는 정보보호시스템 내에서 허가된 임무를 수행하기 위하여 사용자를 대신하여 생성된 주체와 바인드(bind)가 이루어져야 한다. 바인드에 필요한 정보는 사용자의 식별자 및 접근권한 등으로 역할 정보가 반드시 이에 포함되어야 한다. 그러나 Ravi S. Sandhu가 제안한 기존의 $RBAC_0$ 모델은 이러한 주체 및 객체에 대한 역할 부여, 사용자와 주체 및 객체에 대한 바인드가 제공되지 않는다. 또한, W. A. Jansen이 제안한 모델은 주체 및 객체의 개념은 소개했으나 기존의 $RBAC_0$ 모델이 지원하지 못하고 있는 역할계층(Role Hierarchy) 문제를 해결하기 위한 주체의 역할에만 초점을 둔 것으로 이 모델 또한 객체의 역할, 사용자와 주체 및 객체에 대한 바인드가 제공되지 않고 있다. 그러므로 제안한 $ERBAC_0$ 모델을 사용할 경우 정보보호시스템은 사용자 뿐만 아니라 주체 및 객체에 대한 역할을 별도로 지원할 수 있게 되며 또한, 사용자가 이들 주체 및 객체에 대하여 접근을 시도할 때 사용자의 역할과 주체 및 객체의 역할이 상호 바인드되어 정교한 역할기반 접근통제를 실현할 수 있게 되는 장점이 있다.

V. 결 론

역할기반 접근통제에 대한 연구는 '70년대초 다중 사용자와 다중 응용을 위한 상용 온라인 시스템에 적용해 보기 위한 것으로부터 시작되

어 현재 기존의 접근통제 방법인 강제적 접근통제 및 임의적 접근통제에 이은 세 번째 접근통제 방법으로서 각광을 받고 있으며 향후에도 정형적 설계 및 검증, 시스템 실용화 등의 측면에서 많은 발전이 있을 것으로 기대된다.

본 논문에서는 Ravi S. Sandhu가 최초로 제안한 역할기반 접근통제 기본 모델인 $RBAC_0$ 을 개선하여 주체와 객체의 개념을 추가시킨 확장된 접근통제 모델($ERBAC_0$: *Extended* $RBAC_0$) 모델을 새롭게 제안하였다. 본 논문에서 제안한 $ERBAC_0$ 모델은 기존의 Ravi S. Sandhu가 제안한 $RBAC_0$ 모델 및 W. A. Jansen이 제안한 모델이 제공하지 못하는 주체 및 객체 수준에서의 역할기반 접근통제를 보다 정교하게 제공할 수 있다.

향후에는 본 연구결과를 토대로 $ERBAC_0$ 모델을 다양한 형태의 정보보호시스템 개발에 적용하기 위한 연구가 계속적으로 수행되어야 할 것으로 사료된다.

참고문헌

[1] David F. Ferraiolo and D. Richard Kuhn, "Role-based access controls", *15th NIST-NCSC National Computer Security Conference*, pp 554-563, Baltimore, MD, October 13-16, 1992.

[2] David F. Ferraiolo, Janet A. Cugini and D. Richard Kuhn, "Role-Based Access Control(RBAC) : Features and Motivations", *Annual Computer Security Applications Conference*, pp 554-563, IEEE Computer Society, 1995.

[3] David Ferraiolo, Dennis M. Gilbert, and Nickilyn Lynch, "An examination of federal and commercial access control policy needs", *16th NIST-NCSC National Computer Security Conference*, pp. 107-116, Baltimore, MD, September 20-23, 1993.

[4] Computer Systems Laboratory(CSL) Bulletin, "An Introduction to Role-Base Access Control", December, 1995.

[5] http://csrc.omg.org/corba/sectrans.htm#secl, "CORBAServices : Common Object Services Specification", 1998.

[6] Charles L. Smith, Edward J. Coyne, Charles E. Youman and Srinivas Ganta, "A Marketing Survey of Civil Federal Government Organizations ro Determine the Need for a Role-Based Access Control(RBAC) Security Product", NIST&SETA, *Small Business Innovation Research(SBIR)*, July, 1996.

[7] CCIB, *Common Criteria for Information Technology Security Evaluation,* Version 2.0, May, 1998.

[8] Jim Reynolds, Ramaswamy Chandramouli, *Role-Based Access Control Protection Profile*, Ver. 1.0, Cygnacom Colutions & NIST, July 30, 1998.

[9] 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.

[10] Ravi S. 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.

[11] 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.