다중 도메인 보안에서 RBAC의 상충문제

김형찬[O1], 이동익[1], 김형천[2], 강정민[2], 이진석[2]
[1]광주과학기술원 정보통신공학과, [2]국가보안기술연구소
{kimhc[O], dilee}@kjist.ac.kr, {khche, jmkang, jinslee}@etri.re.kr

Conflict analysis of RBAC in Multi-Domain Security

Hyung Chan Kim[O1], Dong Ik Lee[1], Hyoung Chun Kim[2], Jung Min Kang[2], Jin Seok Lee[2]
[1]Dept. of Information and Communications, Kwangju Institute of Science and Technology
[2]National Security Research Institute

요 약

역할기반 접근통제(RBAC)모델은 쉬운 관리성과 정책 적용의 유연성, 그리고 정책 중립적인 이점으로 인하여, 현재 많은 컴퓨팅 환경에서 적용되고 있다. 하지만 기존에 연구되었던 RBAC모델들은 대부분 단일 보안 관리를 가정하므로 최근의 협업 컴퓨팅 환경을 위한 접근통제를 설계하는 데 문제가 있다. 본 논문에서는 협업 컴퓨팅 환경을 다중 도메인 보안(Multi-Domain Security)으로 사상하고, 협업환경을 적절하게 고려하지 않은 RBAC의 적용이 야기할 수 있는 문제점들을 살펴본다.

1. 서 론

다중 도메인 보안(Multi-Domain Security)[1]은 다수의 컴퓨팅 단위가 서로 상호 작용하는 데 있어서의 보안 모델을 반영한다. 이는 정보 시스템들이 광대하게 연결되는 분산 시스템을 디자인 하는데 있어 필요한 개념이다. 다중 도메인 보안 시스템에서의 고려해야 할 문제점들로 다음과 같은 점들을 생각해 볼 수 있다[2]. 협업에 관여하는 시스템들 사이에서 같은 수준의 물리적 보안을 제공하기가 어려우며, 각 시스템들의 관리주체가 다를 수 있음으로 인한 협업의 어려움이 존재한다. 또한 서로 다른 수준의 보안이 적용되고 있는 임의의 두 시스템의 결합은, 각각의 시스템에서는 나타나지 않던 보안 결함(loophole)을 유발할 수 있다. 이러한 문제의 주요 원인은 각각의 도메인이 적용하는 정책의 다양성과 관리 주체의 이질성으로 요약될 수 있다.

기존의 접근통제 모델은 대부분 단일 보안 관리 도메인(Single Administrative Domain)을 가정한다. 따라서 이러한 모델을 반영한 시스템들은 분산 미들웨어, GRID Computing 및 편재형 컴퓨팅 기반과 같이 다중 보안 도메인의 범주에 속하는 어플리케이션들을 적절하게 지원하기가 어렵다. 따라서, 본 연구에서는 다중 도메인의 개념을 도입하여 협업 시스템에 알맞은 접근통제 모델을 고려한다.

기존의 역할기반 접근통제[3,4]는 관리의 용이함과 정책 중립적인 특성으로 인하여, 많은 분산 시스템에서 구현되고 있다. 하지만 RBAC을 협업시스템에 적용할 때, 다중 도메인 보안에 대한 고려가 미비하여 실제 발생한 접근이 통제정책과 상충되는 경우가 발생한다. 이러한 문제들로, 관심사의 상충(Conflict of interests), 업무의 상충(Conflict of duties), 규칙의 상충(Conflict of rules), 그리고 정책의 공백상태(Policy free states) 등이 충분하게 고려되지 않은 다중 보안 도메인 환경하에서 발생할 수 있다. 본 논문에서는 이러한 문제들을 살펴본다.

2. 다중 도메인 기반 접근통제

협업시스템에 대한 접근 통제를 설계하기 위해서는 모델이 보안 정책의 다양성과 서로 다른 권위(Authority)를 반영할 수 있어야 한다. 이러한 환경의 다양성을 구체화하여 반영하기 위해, 많은 연구들이 도메인(Domain)이란 개념을 도입하였다[1]. 일반적으로 도메인은 접근 주체와 객체의 집합 경계를 나타내는 개념을 반영하기 위해, 조직 경계의 추상적 개념으로 여겨져 왔다. 다른 관점에서 도메인은 보안 규칙이 적용되는 영역을 의미하기도 한다. 본 연구에서 도메인은 두 가지 관점에서 정의한다.

■정책 도메인(Policy domain): 접근 주체와 접근 객체의 그룹으로 하나의 보안 정책이 적용되는 영역이다.

■관할 도메인(Jurisdictional domain): 하나의 관할 도메인에는 한 명의 보안관리자 혹은, 하나의 보안 관리자 집단 계층이 존재한다. 보안 관리 계층의 존재 시, 상위 관리자는 하위 관리자의 관리 권한을 가진다.

관할 도메인의 개념에는 배타적 권위(Exclusive Authority)라는 개념이 내재되어 있다. 배타적 권위는 관할 도메인들의 집합에서, 서로간 관리 계층의 상하관계가 없을 때 정의된다. 이 개념은 한 도메인의 관리체계가 다른 도메인에 영향을 미치지 못하는 조직들을 표현할 때 유용하다.

정책 도메인은 관할 도메인과 동일 할 수 있다. 또 다른 경우로, 관할 도메인은 그 내부에 다수의 정책 도메인을 가지는 형태가 될 수도 있다. 접근 요청은 내부 접근의 형태로써, 하나의 정책 도메인 내부에서 이루어 질 수 있다. 도메인을 넘어선 접근 요청은 정책 도메인을 넘어서거나 또는, 관할 도메인을 넘어서 이루 어 질 수도 있다. 각 정책 도메인은 각자의 정책이 다를 수 있음을 유념한다.

3. 다중 도메인 하에서 RBAC의 적용

3.1 구성요소 간의 연관에 의한 적용방법

RBAC은 조직의 업무나 책임을 효과적으로 추상화 함으로써

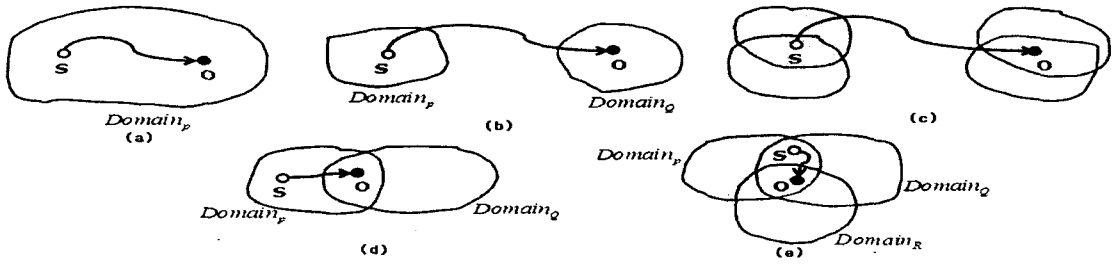

그림 1. 도메인 경계를 넘는 접근의 분류

많은 이점을 가져다 준다. 역할은 조직에 알맞은 보안 정책을 직접적으로 제공해 줄 수 있기 때문에 보안 관리에 많은 이점이 있다. 이에, 다중 도메인에서도 이러한 RBAC을 직접 적용하는 경우가 생길 수 있다. 직관적으로 다음과 같이 구성 요소간 직접적으로 연관하는 접근 방법을 생각해 볼 수 있다.

(i) 도메인 간 사용자 할당(Cross-domain user assignment).
(ii) 도메인 간 권한 할당(Cross-domain permission assignment).
(iii) (i),(ii)를 동시에 사용하는 방법.
(iv) 역할 대 역할 해석(Role-to-role translation).

다음 절부터는, 도메인 간 접근의 형태를 분류하고 이에 근거하여 위의 방법들이 가지는 문제점을 살펴본다.

3.2 도메인 경계를 넘는 접근의 분류

Kühnhauser[3]는 그의 연구에서 도메인 간 접근을 세가지로 분류하였다. 분류는 보안 정책이 파급되는 경계를 기준으로 이루어졌고, 도메인 간 접근의 원천적 속성으로 인한 보안 정책의 상충 조건(Conflict condition)을 제시하였다.

3.2.1 Class 1 접근

Class 1 접근은 하나의 정책 도메인 내부에서의 접근이다[그림1.(a)].접근 주체에서 객체로의 모든 임의의 접근(s,o)에 대하여; 해당 접근에 대한 규칙을 주는 정책은 단 하나이다. 정식으로 표현하자면 다음과 같다. 모든 접근 개체 $e \in \{s,o\}$는 모두 같은 정책하에 있다. $\Pi_e = \{P \mid e \in Domain_P\}$ 를 도메인 $Domain_P$ 하의 개체 e에 접근 규칙을 주는 정책의 집합이라 하자. 그러면 Class 1 접근은 다음과 같이 정의된다.

■Class 1 : $(|\Pi_S| = |\Pi_O| = 1) \wedge (\Pi_S = \Pi_O)$

3.2.2 Class 2 접근

Class 2 접근에서 모든 각 접근 개체는 서로 배타적인 정책 도메인에 속한다. 즉, 두 접근 개체에 대해 접근 규칙을 주는 정책이 존재하지 않는 경우이다. Class 2 는 다음 두 가지 형태로 나누어 진다. 하나는 접근(s,o)에서 각 접근 개체가 하나씩의 정책 도메인에 존재하는 경우이고, 다른 하나는 각 접근 개체가 하나 이상의 정책 도메인에 존재하는 경우이다. 물론 후자의 경우에도 각 개체는 서로 배타적인 정책 도메인에 속한다. Class 2 접근은 다음과 같이 정의된다.

■Class 2(a) : $|\Pi_S \cap \Pi_O| = 0 \wedge (|\Pi_S| = 1 \wedge |\Pi_O| = 1)$
■Class 2(b) : $|\Pi_S \cap \Pi_O| = 0 \wedge (\exists e \in \{s,o\} \wedge |\Pi_e| > 1)$

그림1.(b)와 그림1.(c)는 각각 Class 2(a)와 Class 2(b) 접근의 예를 보여주고 있다.

Class 2 접근에서 각 접근 개체 s와 o사이의 접근 규칙이 주어지지 않는 상태를 다음과 같이 정의한다.

□정의 1: 정책의 공백(Policy free)
도메인 간 접근 (s,o)에 대한 접근 규칙이 주어지지 않을 때, 이를 정책 공백 상태라 하며, 이 상태를 다음과 같이 정의한다.

$$|\Pi_S \cap \Pi_O| = 0$$

3.2.3 Class 3 접근

Class 3 접근에서는 두 접근 개체 s와 o에 대한 접근 규칙이 적어도 하나는 존재한다. 동시에 그 중 하나의 개체는 하나 이상의 정책 도메인에 포함된다. Class 3 접근도 Class 2와 같이 2가지 하위 분류가 존재한다. Class 3(a)는 접근에 대해 하나의 정책 도메인이 접근 규칙을 제공하는 경우이다[그림1.(d)]. Class 3(b)의 경우에는 둘 이상의 정책 도메인이 접근에 대해 규칙을 제공한다[그림1.(e)]. 두 하위 분류는 다음과 같이 정의된다.

■Class 3(a) : $(|\Pi_S \cap \Pi_O| = 1) \wedge (\exists e \in \{s,o\} \wedge |\Pi_e| > 1)$
■Class 3(b) : $(|\Pi_S \cap \Pi_O| > 1) \wedge (\exists e \in \{s,o\} \wedge |\Pi_e| > 1)$

Class 2(b), Class 3(a) 그리고 Class 3(b) 접근은 접근 개체 중 하나가 적어도 두 개 이상의 도메인에 속한다. 이를 도메인 상충(Domain conflict)라고 정의한다. 규칙의 상충(Rule conflict)은 둘 이상의 정책 도메인이 접근에 관여하여 둘 이상의 서로 다른 규칙을 하나의 접근에 대해 제공할 경우 발생한다.

□정의 2: 도메인 상충(Domain conflict)
도메인 상충은 접근(s,o)가 다음 정의와 같이, 적어도 하나의 개체가 두 개 이상의 도메인에 속할 때 발생한다.

$$\exists e \in \{s,o\} : |\Pi_e| > 1$$

□정의 3: 규칙의 상충(Rule conflict)
규칙의 상충은 접근(s,o)에 대하여, 두 개 이상의 정책 도메인이 서로 다른 규칙을 제공할 때 발생한다.

$$|\Pi_S \cap \Pi_O| > 1$$

3.3 직접연관 방법에 의한 문제점

RBAC에서 사용자는 사용자 할당 관계(UA)를 통해 역할에 할당 되고, 권한은 권한 할당 관계(PA)를 통해 역할에 할당 된다. 여기에서 정책 도메인 P하의 관계를 나타내기 위해 UA_P와 PA_P라는 표기를 사용하기로 한다. 여기에서는 (i)부터 (iv)의 방법들이 전 절에서 본 도메인 간 접근 분류에 근거해, 어떤 상충 문제들을 가질 수 있는지 살펴본다.

3.3.1 도메인 간 사용자 할당

방법 (i)은 접근 주체에 해당하는 한 도메인의 사용자가 다른 정책을 반영하는 도메인의 역할에 할당되는 상황이다. 이 경우, 접근 주체는 여러 정책 도메인에 포함되며 이는 도메인 상충을 발생시킨다. 그림2.(a)는 이것의 예제이다. 접근 주체 s2는 역할 R_A 와 R_B 에 할당되어 있으며, 이 두 역할은 각각 다른 정책 P1과 P2를 반영하는 도메인에 속해있다. 만약 s2가 역할 R_B 를 통해 접근 객체 o에 접근을 시도 할 경우, 접근 (s2,o)는 *정의 2*의 $|\Pi_{s2}| > 1$ 조건에 의해 도메인 상충을 일으킨다. 이 도메인 상충 조건은 $(s2, R_A) \in UA_{P1}$, 그리고 $(s2, R_B) \in UA_{P2}$에 의해 만들어진다.

관심사의 상충(Conflict of interest)은 경쟁조건에 있는 클래스들에 속해 있는 조직들의 자원에 대해, 한 사람이 경쟁조건에 관계없이 몇 조직에 대한 권한이 있을 때 발생한다. 그림2.(a)에서 주체 s2는 각 도메인에 대해 중복되어 있다. 따라서, 만약 이 두 도메인들이 경쟁관계에 있는 도메인 이라면, 도메인 간 사용자 할당은 관심사의 상충 문제를 일으킨다.

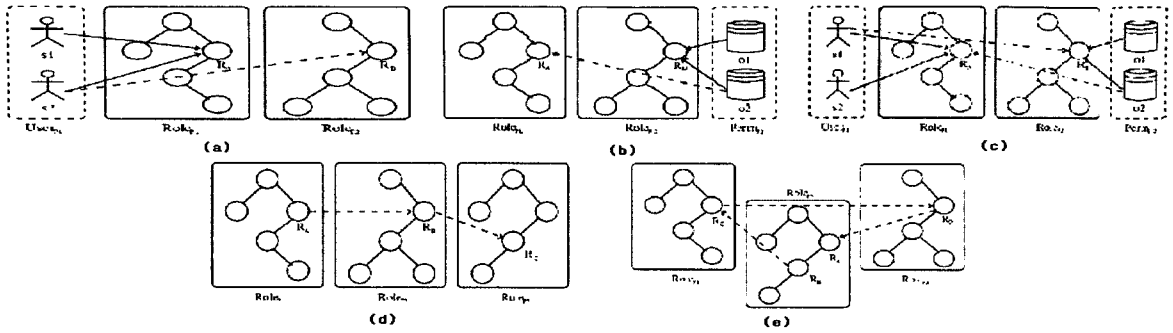

그림 2. 다중 도메인 환경에서 RBAC의 상충(Conflict)

3.3.2 도메인 간 권한 할당

방법 (ii)는 접근 객체가 서로 다른 도메인에 할당되어 있는 경우이다. 도메인 간 사용자 할당과 비슷한 경우로, 도메인 상충이 발생한다. 그림2.(b)에서 도메인 간 직접적으로 권한 할당 시 발생하는 도메인 상충 문제를 보여준다. 그림에서 나타난 상충 조건은 $|\Pi_{o2}|>1$ 로 이것은 $(o2,R_A)\in PA_{P1}$ 와 $(o2,R_B)\in PA_{P2}$ 관계로부터 파생된다.

도메인 간 권한 할당은 객체가 여러 도메인에 속하게 되기 때문에, 다수의 관리자가 해당 객체를 관리함에 따른 문제가 발생할 수 있다(Conflict from multiple managers). 이에 대한 몇 가지 상황에 대한 예를 들어볼 수 있다. 사용 가능성에 대한 상충(Conflict on availability)은 한 관리자가 객체를 사용 가능한 상태로 설정하였는데, 다른 관리자는 사용 불가능한 상태로 설정하는 데서 발생 가능하다. 유사한 상황으로써, 이 상충은 비밀성에 대한 상충(Conflict on Privacy)으로도 이해할 수 있다. 즉, 한 관리자는 객체가 읽기 가능한 상태로 두었는데, 다른 관리자가 해당 객체를 읽지 못하는 상태로 두게 한 경우이다. 만약 객체가 시간, 메모리, 디스크 사용 등 양으로써 측정할 수 있으며, 병행적으로 사용이 가능하다면 이기에 의한 상충(Conflict on self-interest)문제가 발생할 수도 있다. 예로써, 각자의 관리자들이 서로 많은 부분의 자원을 차지하기 위해 자원을 낭비해 버리는 경우이다.

3.3.3 도메인 간 사용자 및 권한 할당

그림2.(c)는 위에서 언급한 도메인 간 사용자 할당 및 권한 할당 두 가지 방법을 동시에 적용된 경우이다. 이 경우는 앞선 두 절에서 언급했듯이 각 접근 개체인 주체와 객체가 도메인 상충 문제를 각각 발생시킨다.

더욱이, 이 경우는 직무의 상충(Conflict of duties)을 유발한다. 왜냐하면, 한 접근 주체가 동일한 접근 객체에 대하여 각기 다른 도메인을 통하여 권리를 가지게 되는데, 이 때 주체가 서로 다른 직무로써 같은 객체에 접근할 수 있기 때문이다. 예를 들어 한 사람이 어떤 회사 A의 재무 담당으로써 주식을 매각할 수 있는 권한이 있고, 또 다른 증권 회사의 직원이라면, 회사 A의 주식을 평가절하된 가격으로 팔고, 그 자신이 증권 회사의 직원 신분으로 그 평가절하된 주식을 사들여 차익을 남기는 불법을 행할 수 있다.

위의 경우들에서 살펴봤듯이 도메인 상충(Conflict of domain)은 관할 도메인의 개념에서 더욱더 심각한 문제가 된다. 그 근본 이유는, 주체가 서로 경쟁적인 직무를 동시에 수행하거나, 혹은 객체의 완전한 소유권이 불분명 한데서 온다.

(i),(ii)에서 경쟁 클래스가 관할 도메인의 개념을 반영하며, (iii)의 예에서 회사 A의 재무 담당과 주식 거래 회사의 직원이 각각 서로 배타적인 관할 도메인에 있는 역할들을 반영한다.

3.3.4 도메인 간 역할 해석

마지막으로, (iv)의 접근 방법은 정책의 공백 상태 문제와 규칙의 상충 문제 두 가지를 발생시킬 수 있다. I-RBAC (Interop-erable RBAC) 모델[4]은 도메인 간 역할 해석 관계를 사용하는 모델이다. 서로 다른 도메인에 존재하는 두 역할($Domain_{p1}$의 R_X와 $Domain_{p2}$ 의 R_B)간 해석관계 $R_A \succ R_B$가 설정되면 다음 조건이 성립된다: $Domain_{p1}$의 모든 역할 R_X에 대하여, 만약 $R_X > R_A$ 이면 $R_X > R_B$가 성립한다. 결과적으로 역할R_X와 R_B 사이의 직접적인 연관이 없지만, $Domain_{p1}$의 역할 R_X는 $Domain_{p2}$의 역할 R_B 의 권한을 사용할 수 있게 된다. 이러한 역할 해석 관계를 통하여 도메인 간 접근을 할 수 있다. 하지만, 이 방법을 가지고 세 개 이상의 도메인이 관여하는 경우 다음과 같은 상황을 생각해 볼 수 있다.

그림2.(d)에서 세 도메인이 관여하여 역할 해석 관계를 적용하였다. 역할 R_A는 역할 R_B 에, 역할 R_B 는 역할 R_C 에 연관되었으며 각 역할은 서로 다른 도메인에 속한다. 이 경우 역할 R_A 는 역할 R_C 에 암묵적으로 해석되어 R_C 가 속한 도메인의 의지와는 관계없이 R_A가 해당 역할의 권한을 사용하게 되는 침투(Infiltration)공격이 가능하게 된다. 이것은 역할 R_A 와 R_C 사이에 명백하게 정의된 규칙이 없기 때문에 발생하는 규칙의 공백 상태에 해당된다.

그림2.(e)의 예제에서는 역할 R_B는 역할 R_C에, R_C는 R_D에, R_D 는 R_A에 각각 연관되었다. 역할 R_A는 같은 도메인의 역할 R_B 의 부모 역할이다. 그럼에도 불구하고, 역할R_B는 부모 역할R_A의 권한을 사용할 수 있는데, 이것은 여러 역할 해석관계들을 통해 생겨난 새로운 규칙 때문이다. 이 규칙은 내부 도메인의 정책인 역할간 상하관계와 서로 충돌하게 되어, 규칙의 상충(Conflict of rules) 문제를 일으킨다.

이러한 문제들 때문에, 역할 간 해석관계에 인한 도메인 간 접근은 세 개 이상 도메인을 안전하게 지원하지 못하며 따라서 확장성에 문제가 있다.

4. 결 론

본 논문에서는 다중 도메인 기반에서 협업환경을 고려하지 않는 역할기반 접근통제 방법이 여러 가지 상충 문제를 일으킬 수 있음을 분석하였다.

참고문헌

[1] Jose Vazquez-Gomez, "Multidomain Security," Computer & Security, Vol. 13, pp.161-184, 1994.

[2] R. S. Sandhu, E. J. Coyne, H. L. Feinstein and C. E. Younman, "Role-Based Access Control Models," IEEE Computers, Vol. 29, No. 2, pp. 38-47, Feb. 1996.

[3] W. E. Kühnhauser, "A Classification of Interdomain Actions,", ACM SIGOPS Operating Sys. Rev., Vol. 32, No. 4, pp. 47-61, 1998.

[4] A. Kapadia, J. Al-Muhtadi, R. Campbell, D. Mickunas, "IRBAC 2000: Secure Interoperability Using Dynamic Role Translation," The 1st International Conference on Internet Computing, Jun. 2000.