다중 접근제어 정책 모델에서 비명시적 권한을 보장하는 전파 정책

양주연° 박 석
서강대학교 컴퓨터학과 데이터베이스 연구실
{jyyang°, spark}@dblab.sogang.ac.kr

A Propagation policy for non-specific authorization in modeling multiple access control policies

Ju Yeon Yang° Seog Park
Database Research Lab., Dept. of Computer Science, Sogang University

요 약

일반적인 접근제어 모델이 메커니즘 내에 보안 정책을 미리 설계함에 따라 보안 요구사항의 추가나 변경에 어려움이 있는 반면에, 다중 접근제어 정책 모델은 기업 환경에 필요한 다양한 보안 정책들을 융통성 있게 지원하기 위해, 권한 명세 언어를 기반으로 positive/negative 권한을 모두 표현할 뿐만 아니라, 권한의 예외적 수행, 권한의 전파와 충돌 해결 정책 등을 구현함으로써, 접근제어의 권한 적용에 유연성을 강화하였다. 그러나, 기존의 권한 전파 및 충돌 해결 정책은 권한 전파의 모든 가능한 path를 고려하지 않거나, 충돌 문제를 해결하지 않는 부분이 있는데, 이것은 특히 서로 다른 정책의 어플리케이션 통합 환경에서 권한의 남용이나 상실 등 의도하지 않은 부당한 권한의 실행을 야기시킨다. 따라서, 본 논문에서는 다수의 정책의 영향을 받은 주체에 대해서 권한의 독립적 수행을 보장하면서, 추가적인 충돌 상황을 발생시키기 않는 권한 전파 정책을 제안한다.

1. 서 론

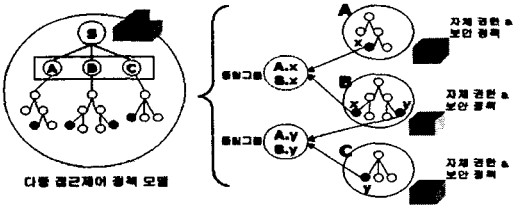
다중 접근제어 정책 모델이 단일 접근제어 모델[4]에 대한 가장 큰 차이점은 권한 모델과 메커니즘[5] 자체는 정책 중립적으로 설계하고, 추가/변경 되는 보안 정책들은 필요에 따라 매핑함으로써, 정책 적용의 유연성을 확보하였다는 것이다. 이러한 환경에서 접근 요청에 대한 결과(허가/부인)는 일련의 정책 평가 과정을 거쳐서 얻어진다.

다중 접근제어 정책 모델에서 사용되는 정책들은 그 기능에 따라서 전파 정책, 충돌 해결 및 결정 정책, 무결성 제약 등으로 나누어 진다[1]. 특히, 권한의 전파 정책은 권한 할당의 중복 작업을 줄일 수 있는 매우 유용한 정책이다.

그런데, 전파 정책을 통해서 권한을 할당 받는 경우, 상위 그룹으로부터 positive 권한과 negative 권한을 모두 전파 받게 되는 상황이 존재한다. 이 때, 둘 중 어느 것이 선택되느냐는 것은 적용된 전파 정책의 종류에 따라 달라지며, 전파 정책 내에 우선(overriding) 규칙이 내포되어 있는 경우, 충돌 문제는 전파 과정에서 해결되지만, 그렇지 않은 경우에는 다음 단계인 충돌 해결 및 결정 과정에서 이를 해결해야 한다.

따라서 보안 관리자는 올바른 권한이 전파될 수 있도록 전파 정책과 우선 규칙을 선택해야 한다. 이에, 본 논문에서는 기존의 전파 정책과 내포된 우선 규칙[1,2]을 이용할 때, 보안 관리자가 의도하지 않았던 권한이 전파되는 현실 세계의 상황이 존재함을 밝히고, 이러한 문제를 해결할 수 있는 새로운 규칙의 전파 정책을 제안한다. 새로운 전파 정책을 이용할 경우, 다양한 그룹에 동시에 소속된 사용자가 다른 그룹의 권한에 영향을 받지 않고 고유 권한을 수행할 수 있으며, 의도하지 않은 권한이 수행되는 것을 방지한다.

2. 서로 다른 정책의 어플리케이션 통합 환경



[그림1] 통합을 위한 권한 상태 그래프의 재구성

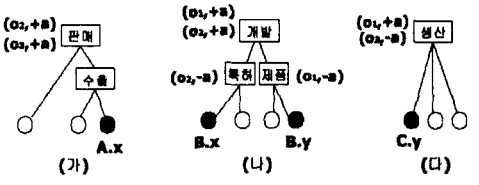
[그림1]에서 어플리케이션 시스템 A,B,C는 서로 다른 정

책에 의해 운영되고 있으며, 각각의 세부 그룹 계층은 그래프 형태로 표현된다. 일부 그룹 및 사용자는 둘 이상의 어플리케이션 시스템에 소속될 수 있고, 그래프의 각 노드는 개인 사용자 및 그룹을 나타내고, 권한의 할당은 노드에 해당 데이터와 연산을 레이블링하여 이루어진다. 시스템 통합 과정에서 얻게 되는 권한 상태 그래프는 다음과 같은 특징을 갖는다.

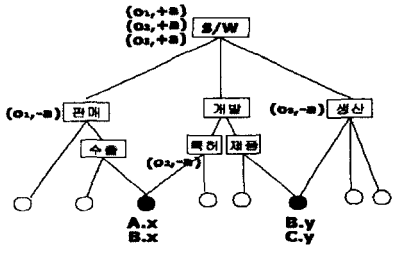
- 특징 1 : 서로 다른 정책의 하위 계층이 있고, 이들의 영향을 동시에 받는 공통 노드가 존재하다.
- 특징 2 : 어플리케이션 사이의 공통적인 권한은 최상위 노드에 할당하여, 권한 할당의 중복 작업을 줄인다.
- 특징 3 : 최상위 노드에 할당된 권한과 충돌하는 권한을 하위 노드에 할당할 수 있다.

위의 특징들로 인해, 통합 후 각 노드가 갖는 명시적 권한의 집합이 달라지고, 그래프의 path가 변경됨에 따라, 전파 정책으로 얻게 되는 암묵적 권한이 통합 전과 달라지게 된다. 따라서, 각 어플리케이션에 지정된 전파 정책을 적용하더라도 독립적으로 수행되던 때와 다른 권한이 사용자에게 전파될 수 있으며, 이는 의도하지 않은 권한의 상실 또는 권한의 남용이라는 결과를 초래한다.

3. 통합 환경에서 기존 전파 정책의 한계점



[그림2] 통합 전 권한 상태 그래프



[그림3] 통합 후 권한 상태 그래프

3.1 most-specific overriding(mso) 전파 정책 적용[1]

[그림2]에서 사용자 x는 ' 개발' 그룹에 속하므로, 데이터 o_1에 대해서 mso 전파 정책을 적용할 경우 positive 권한을 갖는다. 그러나, [그림3]에서, ' 개발' 그룹에 할당된 권한들은 상위 그룹으로 통합되었고, ' 판매' 그룹에서는 기존에 없던 권한이 전파 되는 것을 방지하기 위해, o_1에 대해서 negative 권한을 할당하였다. 이 상태에서 원래의 mso 전파 정책은 항상 사용자 x에게 negative 권한만을 전파하게 됨으로써, x가 원래 가지고 있던 positive 권한은 상실된다.

3.2 path overriding(po) 전파 정책 적용[1,2]

po 전파 정책은 mso 와 달리, 서로 다른 path로 상위 그룹의 권한이 전파되는 것을 허용한다. 따라서 x에서는 positive권한과 negative권한 사이에 우선 관계가 없으므로 충돌한다. 그러나 충돌 해결 정책은 어떤 path에 의해 전파된 것인지는 고려하지 않고, 무조건 positive를 우선하거나 negative를 우선하는 것이므로, 기존 권한을 유지하는 방법이 될 수 없다.

4. 권한의 독립적 수행을 보장하는 전파 정책

위에서 언급한 권한의 상실 문제는 서로 다른 어플리케이션의 영향을 받는 공통 노드에서 발생한다. 따라서 공통 노드의 전파 정책을 정할 때는, 해당 권한이 다른 어플리케이션의 path에 의해 영향을 받도록 하는 경우와 영향이 받지 않고 독립적으로 수행되기를 원하는 경우를 구별하여, 전자의 경우에는 기존의 mso 정책을 사용하고, 후자의 경우에는 본 논문에서 제안하는 비명시적 권한의 전파를 보장하는 전파 정책을 사용함으로써, 의도했던 권한이 수행되도록 한다.

4.1 비명시적 권한의 전파 (non-specific overriding: nso) 전파 정책의 의미

최상위 노드(또는 사용자에게 가장 인접한 내부 공통 노드)에 주어진 권한에 대해서 하위 노드에 충돌하는 권한이 없는 path가 존재한다면, 접근 요청 사용자는 최상위 노드(또는 사용자에게 가장 인접한 내부 공통 노드)에 할당된 권한을 전파 받을 수 있다.

4.2 nso 전파 정책의 표현

다중 접근제어 정책 모델의 권한과 정책들을 표현하기 위해 개발된 언어들은 다양하다. 특히, Jajodia[1]에 소개된 권한 명세 언어는 프레디키트를 사용한 논리적 언어이다. 권한과 정책을 표현하기 위한 최소한의 프레디키트를 미리 정의하여, 이들을 적절히 재배치 함으로써, 서로 다른 정책을 나타내는 규칙을 만들 수 있다. 본 논문에서 제안하는 전파 정책도 이들 프레디키트를 이용하여 아래와 같이 명세화할 수 있다. Dercando(o,s,+ a) 프레디키트는 주체 s가 객체 o에 대해서 연산 a를 수행할 수 있는 권한을 전파 받을 수 있다는 의미이다. 그리고 화살표 오른쪽에 나열된 프레디키트들은 선행되어야 하는 조건들이다.

이 중 어느 하나라도 만족하지 않으면, 해당 권한은 전파될 수 없다. ASH란, [그림3]과 같은 사용자 계층의 그래프를 의미하고, dirin 프레디키트는 주체 s가 s' 에 포함되는지를 확인한다.

```
Dercando(o,s,+a) ← cando(o,S,+a) & in(s,S,ASH)
        & dercando(o,s' ,+a) & dirin(s,s' ,ASH)
        & ~cando(o,s,-a).
Dercando(o,s,-a) ← cando(o,S,-a) & in(s,S,ASH)
        & dercando(o,s' ,-a) & dirin(s,s' ,ASH)
        & ~cando(o,s,+a).
```

4.3 nso 전파 정책의 조건 분석

nso 전파 정책을 이루는 각각의 조건은 상위그룹으로부터 해당 권한을 전파 받을 수 있는 path가 존재할 때, 이것이 다른 path에 의해 overriding되지 않도록 함으로써, 권한 전파의 독립성을 보장한다.

- L1 : cando(o,S,+a) = True

최상위 노드인 S에 (o,+a)의 명시적 권한이 할당되어 있어야 한다. 최상위 노드가 아니면, 다른 path에 의해 overriding 되지 않으므로, nso 정책을 사용하여 고유 권한을 보장할 필요가 없다.

- L2 : in(s,S,ASH) = True

주체 s는 S(최상위 노드)의 구성원이어야 한다. 이것은 base relation인 Authorization Subject Hierarchy를 통해 직접 확인할 수 있다.

- L3 : dercando(o,s' ,+a) = True

이 조건은 해당 주체의 직접적 상위 노드가 (o,+a)를 전파 받을 수 있는지를 조사하는 것이다. 주체의 직접적 상위 노드는 둘 이상이 될 수 있으므로-이것이 서로 다른 path를 발생시킴 - 그 중 한 개만 이 조건을 만족하여도 조건은 참 값을 가진다. 이 조건이 거짓 값을 갖는다는 것은 해당 권한에 대해서 사용자는 모든 path에 최상위 노드에 할당된 권한보다 most-specific 충돌 권한을 가진다는 의미이므로, non-specific 권한 전파의 보장이 무의미해지는 것이다. 따라서, 진리값을 False로 하고, 해당 전파 정책을 수행하지 못하도록 한다. 또한, L3 조건은 dercando 프레디키트의 특성상 다른 dercando를 검사해야 하므로 최종 조건이 만족되거나 만족되지 않을 때까지 반복적으로 수행된다.

- L4 : dirin(s,s' ,ASH) = True

L3를 수행하는데 주체가 되는 s' 이 접근 요청 주체인 s와 직접적인 상하위 관계를 갖는지 검사한다. 이것은 base relation인 Authorization Subject Hierarchy를 통해 직접 확인할 수 있다.

- L5 : ~cando(o,s,-a) = True

마지막으로 검사하는 것은 현재 접근 요청의 주체에게 (o,-a) 권한이 명시적으로 할당되어 있지 않은지를 검사하는 것이다. 다른 path로의 mso에 의한 overriding을 방지하기 위한 것이지, 현재 path의 mso에 의한 overriding을 방지하자는 것이 아니기 때문이다.

즉, L4 까지의 조건 검사가 주체보다 상위의 노드에 대한 검사였다면, L5는 주체에 대한 마지막 검사가 된다.

5. nso 전파 정책의 적용

nso 전파 정책의 적용은 다수의 그룹에 소속된 주체가 다른 path의 권한에 영향을 받지 않고, 최상위 노드(또는 상위 공통노드)의 권한을 전파 받고자 할 때 이용하는 것이다. nso 정책을 적용할 필요가 있는 객체와 주체에 대한 선별 작업은 독립적 수행을 원하는 해당 데이터에 대해서 다른 path에 명시적으로 할당된 권한 정보를 수시로 확인하는 작업보다 변경 가능성이 적고, 안전하기 때문에 보안 관리자는 자신의 관리 영역 내의 독립적 데이터에 대한 권한 관리를 용이하게 할 수 있다.

6. 평가 및 결론

이제까지 살펴본 바와 같이, 권한의 전파는 사용자 그룹 계층 그래프를 이용하기 때문에, 그래프의 path와 다른 권한의 존재에 따라 사용자에게 전파되는 권한도 달라지게 된다. 따라서, 그래프가 통합되거나 동적으로 권한이 할당/삭제 되는 상황에서 다른 path의 영향을 받지 않으면서 고유 권한을 유지시킬 수 있는 전파 정책은 중요한 기능을 한다. 본 논문에서는 권한의 할당과 그래프의 path가 동적으로 변경되는 상황에서 보안 관리자가 의도하는 권한이 항상 전파될 수 있도록 보장하는 전파 정책을 제안하였으며, 이는 추가적인 권한 할당 작업을 하지 않으면서도 다수의 path를 고려하였으므로, 기존의 전파 정책에 비교할 때, 다중 접근제어 정책 모델에서 보안 관리의 독립성과 효율성에 기여하였다.

참고 문헌

[1] Sushil Jajodia, Pierangela Samarati, Maria Luisa Sapino, V.S. Subrahmanian, " Flexible Support for Multiple Access Control Policies" , *ACM Trans.on Database Systems*, Vol.26, No.2, June 2001, pp 214-260

[2] Elisa Bertino, Sushil Jajodia, Pierangela Samarati, " Supporting Multiple Access Control Policies in Database Systems" , In *Proc. IEEE Symp. on Security and Privacy* ; Oakland, 1996

[3] Sushil Jajodia, Pierangela Samarati, V.S. Subrahmanian, " A Logical Language for Expressing Authorizations" , In *Proc. IEEE Symp. on Security and Privacy*, Oakland, CA, USA : IEEE Press, 1997, p.31-42

[4] Ravi S. Sandhu, " Role-Based Access Control." , *IEEE Computer*, Vol. 29, No. 2, February 1996, pages 38-47

[5] Sushil Jajodia, Pierangela Samarati, " A Unified Framework for Enforcing Multiple Access Control Policies." , In *Proc. SIGMOD' 97*, pages 474-485, Tucson,AZ,May 1997.