역할기반 접근제어에서 우선순위를 기반으로 한 동적의무분리 설계

A Design for Dynamic Separation of Duty based on priority

김은희, 조기천, 문호성, 신문선, 류근호(충북대학교 데이터베이스 연구실)
{ehkim,kicheon,hsmoon,msshin,khryu}@dblab.chungbuk.ac.kr

충북 청주시 흥덕구 개신동 충북대학교
TEL : 043) 267-2253
FAX : 043) 275-2254

요약

컴퓨터 통신 기술의 발전과 다양한 통신망의 개발로 인하여 데이터베이스에 저장되어 있는 개인 정보 뿐만 아니라 국가 기관 또는 군사 조직의 기밀 정보에 대한 보안 관리의 필요성이 증가되고 있다. 일반적으로 데이터베이스 보안에 대한 개념은 다음과 같은 세가지의 주요한 보안 목적들로 구성된다. - 정보의 보안성, 무결성, 가용성
첫째 정보의 보안성은 정보의 불법적인 노출(disclosure)을 방지하고자 함이고, 둘째 무결성은 정보의 부적절한 변경을 못하도록 하기 위한 것이다. 마지막으로 가용성은 정보 또는 시스템에서 제공하는 서비스에 대한 접근을 부당하게 거부하지 못하도록 처리하는 것이다.

정보의 비밀성, 무결성 그리고 가용성을 지원하기 위해서는 반드시 보안 정책이 필요하다. 보안 정책의 개념은 매우 광범위하며, 많은 분야에서 각각의 의미를 갖고서 다른 방법들로 이용되고 있다. 가장 많이 이용되는 방법은 특정한 정보 시스템이 조직의 보안 요구사항을 지원하기 위해서 처리되는 과정을 서술하는 시스템 보안 정책이며, 이는 접근 제어 정책으로 정의된다.

접근 제어 정책의 목적은 컴퓨터, 통신 그리고 정보 자원에 대한 권한이 부여되지 않는 접근을 방지하는 것이다. 접근 제어 정책의 종류는 임의적 접근 제어(discretionary access control:DAC)
와 강제적 접근 제어(mandatory access control:MAC)로 구분된다.

임의적 접근 제어 정책은 각 정보의 소유자들이 그들 임의의 판단으로 접근 권한을 다른 사용자에게 위임하거나 취소시킬 수 있어서 정보에 대해 유연하며 분산된 접근제어 기능을 수행할 수 있는 특성을 가진다. 반면에 강제적 접근 제어 정책은 군사환경이나 매우 제한적인 환경에서 제한된 수의 보안 관리자들에 의해 일정한규칙에 따라 사용자의 정보에 대한 접근 권한을 통제한다.
이러한 전통적인 접근 제어 정책의 대안으로 역할기반 접근제어 정책이 최근에 많은 관심을 받아오고 있다.

역할기반 접근제어 정책은 상업적으로 이용되는 환경에서 적용될 수 있는 보다 가치있는 보안 정책의 일종으로서, 시스템의 권한을 쉽게 관리할 수 있으며 또한 서로 다른 작업을 수행하는 사용자들에 대한 관리 작업을 단순화시키는 장점을 갖는다. 그래서 역할이 기본 단위가 되고 여러가지 역할들은 하나의 계층 구조를 형성한다. 특히 다양한 정책들을 구현할 수 있는 기법으로 그 중에서 많은 상업적인 응용에서 중요한 요구사항의 하나인 의무분리 정책을 위한 자연스런 메커니즘이다. 의무분리정책의 목적은 정보의 무결성을 필요로 하는 연산들을 여러 역할이나 사용자에게 분산시킴으로써 조직 내에서 관리하는 정보의 무결성 침해 가능성을 최소화하는 것이다. 이 논문에서는 역할기반 접근제어에서 역할을 작업단위로 세분화하여 각 작업에 대해 사용자 수준의 우선순위를 부여하여 동적 의무분리 정책을 수행하는 기법을 제안한다. 각 작업에 대해서 서로 다른 우선순위를 가지고 세션에서 활성화되며, 만약 동일한 우선순위를 가진다면 세션에서 활성화되지 않고 이로 인해서 정보의 무결성 침해 요소가 있음을 간접적으로 암시하게 된다. 그리고 작업단위로 동적 의무분리 정책을 수행하여 정보의 불필요한 유출을 막음으로서 정보에 대한 무결성과 비밀성 침해 가능성을 최소화시킨다.

keywords : Role-Based Access Control, security model, separation of duty