

HomeWork #3 연습문제

정보보안 이론과 실제

8장

1. 접근제어목록(ACL)에 대한 권한목록(Capability)의 장점 두 가지와 권한목록에 대한 접근제어목록의 장점 두 가지를 설명하라.

답변

권한목록은 접근제어목록에 비해 사용자 즉, 주체를 추가하거나 삭제가 용이하다. 접근제어목록에서 주체를 추가하거나 삭제하기 위해서는 각 객체에 있는 테이블 모두를 수정해야하는 반면 권한목록에서는 추가되거나 삭제된 주체가 가지고 있는 테이블만 수정하면 되기 때문이다. 그리고 Confused Deputy(대리 혼돈)을 방지하는 것이 용이하다. 접근제어목록에서는 각 주체가 특정 객체로의 접근 권한에 대한 정보를 가지고 있지 않기 때문에 때로는 어떤 특정 주체의 객체 접근 권한을 근거로 해야 할 때 다른 주체가 자신의 객체 권한을 근거로 동작하는 문제가 생긴다. 따라서 악의를 가진 주체는 자신에게 접근 권한이 없는 객체로 우회하여 접근이 가능하다. 하지만 권한목록에서는 각 주체가 객체로의 접근 권한 정보를 가지고 있기 때문에 주체끼리 전송하고 검사하는 단계를 거치면 Confused Deputy(대리 혼돈) 문제는 쉽게 방지할 수 있다.

접근제어목록은 권한목록과 반대로 각 객체가 권한 정보를 가지고 있기 때문에 객체의 추가 및 삭제가 용이하다. 권한목록에서 객체를 추가하거나 삭제하기 위해서는 각 주체가 가지고 있는 테이블을 모두 수정해야하지만 접근제어목록에서는 해당 객체가 가지고 있는 테이블만 수정하면 되기 때문이다. 그리고 권한목록에 비해 접근제어목록은 구현이 쉽고 오버헤드가 적어 현실적으로 많이 사용되며 많은 운영체제에서 채택하고 있는 권한 관리 방식이다.

11. 이 책에서 권한목록을 사용하면 위임이 용이함을 보았다. 접근제어목록 (ACL)을 사용하여 권리 위임이 가능한 방법을 설명하라. 앨리스가 빌에게 권리를 위임하고 빌은 나중에 다시 찰리에게 권리를 위임한다고 가정하라. 권한목록을 사용해 이것을 수행하는 방법을 설명하라. 접근제어목록을 사용해 이것을 수행하는 방법을 설명하라. 어느 방법이 더 쉽고 그 이유를 설명하라.

풀이

접근제어목록을 사용해서 권리 위임이 가능하기 위해서는 각 객체가 가지고 있는 권한 테이블에서 자신의 권한에 대한 정보를 가져와서 위임하는 것이다. 이는 권한목록에 비해 오버헤드가 크다.

앨리스가 빌에게 다시 빌이 찰리에게 권리를 위임하는 것을 구현하기 위해 권한목록을 사용하면 앨리스가 가지고 있는 각 객체에 대한 권한 정보 테이블을 빌에게 보내고 빌은 그 테이블 정보를 자신의 테이블에 덮어 쓴다. 같은 방법으로 빌은 자신이 가지고 있는 테이블을 찰리에게 보낸다.

접근제어목록을 사용하려면 앨리스는 각 객체가 가지고 있는 권한 테이블에서 자신의 권한에 대한 정보를 가져온 다음 그 정보들을 빌에게 보낸다. 빌도 앨리스가 했던 과정을 그대로 거쳐 찰리에게 정보들을 보낸다.

14. BLP는 “상향 읽기 금지, 하향 쓰기 금지”라고 말할 수 있다. 비바 모델은 비슷한 말로 무엇이라고 할 수 있을까?

풀이

“상향 쓰기 금지, 하향 읽기 금지”라고 할 수 있다. BLP는 비밀성을 주요 전제로 한다. 즉, “하급 비밀 취급자는 상급 비밀을 절대 알면 안 된다.”라는 것을 전제로 하기 때문에 자신보다 등급이 높은 비밀은 읽는 것은 당연히 안 되기 때문에 상향 읽기 금지, 자신이 알고 있는 내용이 하급 비밀에 쓰여 질 수 있기 때문에 하향 쓰기 금지라고 말한다.

반면에 비바 모델은 무결성을 주요 전제로 한다. 즉, “등급이 높은 비밀에 가짜 정보가 들어가서는 안 된다.”라는 것을 전제로 하기 때문에 자신보다 높은 비밀을 쓰는 것은 가짜 정보가 쓰여 질 수 있기 때문에 상향 쓰기 금지, 자신보다 낮은 비밀을 읽는 것은 가짜 정보에 대해 오염될 수 있기 때문에 하향 읽기 금지라고 말한다.