SPKI를 이용한 DB 접근통제 방안에 관한 연구

(A Study on The Access Control Model for Database Using SPKI)

김장성*, 장영달**, 김인성***, 김지홍****

(Kim JangSeong*, Jang YoungDal**, Kim InSung***, Kim JiHong****)

초 록

접근통제(Access Control)의 목적은 여러 자원들에 대하여 허가되지 않은 접근을 막는 것이다. 허가되지 않은 접근이란 자원의 불법적인 사용, 노출, 수정, 파괴 등을 포함한다. 즉, 접근통제는 각 자원에 대한 기밀성, 무결성, 가용성 및 합법적인 이용과 같은 정보보호 서비스에 직접적으로 기여하게 되며, 이러한 서비스들의 권한부여를 위한 수단이 된다. 본 논문에서는 X.509 계층구조의 한계점을 극복하기 위해 인터넷 드래프트 표준으로 제안된 SPKI(Simple Public Key Infrastructure) 인증서를 분석하고, 이를 DB 접근통제 수단으로 이용하는 방안을 제시한다.

키 워 드

공개키 암호화, SPKI 권한 인증서, SPKI 이름 인증서, SDSI 이름 인증서, 접근통제, 데이터베이스

1. 서 론

데이터베이스 환경에서 다양한 응용 시스템을 사용하는 사용자들은 데이터베이스가 지니고 있는 강력하고 편리한 인터페이스를 통하여 상호 연관되고 통합되어 있는 대량의 데이터를 손쉽게 검색할 수 있다. 따라서, 데이터베이스 환경에서의 정보보안에 대한 요구사항은 데이터베이스 관리 시스템(DBMS, Database Management System)의 중요한 기능으로써 명확히 정의되어야 한다.

데이터베이스 보안은 데이터베이스에 저장되어 있는 데이터에 대한 인가되지 않은 접근, 의도적인 데이터의 변경이나 파괴 및 데이터의 일관성을 저해하는 우발적인 사고 등으로부터 데이터 혹은 데이터베이스를 보호하는 것이다. 일반적으로 데이터베이스 보안에는 세 가지 중요한 특성이 포함된다. 첫째로, 비밀성은 정보의 부적절한 노출을 예방하고 감지하는 것을 의미하며, 둘째로 무결성은 정보의 부적절한 변경을 예방하고 감지하는 것을 의미한다. 셋째로 가용성은 정당한 방법으로 권한이 주어진 사용자에게는 정보 서비스를 거부하여서는 안 된다는 것이다.

데이터베이스에 대한 보안 요구사항으로는 부적절한 접근으로부터의 데이터베이스 보호, 통계적인 데이터 값으로부터 개별적인 데이터 항목에 대한 정보를 추적하지 못하도록 하는 추론 방지, 데이터의 내용 변경을 위한 인가되지 않은 접근과 저장 데이터를 손상시킬 수 있는 시스템 오류 등으로부터의 무결성 보장, 데이터에

* 세명대학교 전자공학과 석사과정
** 세명대학교 전자공학과 석사과정
*** 세명대학교 전자공학과 학부과정
**** 세명대학교 전자공학과 부교수

대한 모든 접근의 감사 기록 보장, 사용자 인증, 비밀 데이터의 관리 및 보호 등을 들 수 있다.

일반적으로 데이터베이스 보호는 흐름 통제(flow control), 추론 통제(inference control), 접근 통제(access control)의 세 가지 보안 통제를 통해 이루어질 수 있으며, 이외에 암호화 기법을 이용할 수 있다. 흐름 통제는 허용 가능한 정보 흐름에 근거하지 않은 데이터의 전송 요청을 거부하는 것이며, 추론 통제는 간접적인 데이터 노출로부터 데이터를 보호하기 위한 것이다. 본 논문에서 다루게 될 접근 통제는 컴퓨팅 자원, 통신 자원 및 정보 자원 등에 대하여 허가되지 않은 접근을 방어하는 것이다.

2. 접근통제의 개념

접근 통제는 일반적으로 비인가 된 사용자의 위협으로부터 정보 자원을 보호하는 것으로써, 컴퓨터와 정보통신망 기술의 발전으로 원격 분산 사용자들이 손쉽게 시스템 자원에 접근할 수 있게 됨에 따라, 시스템 및 통신망을 보호하기 위해 사용되는 수단이다. 이러한 접근 통제 서비스는 각종 시스템 자원에 대한 불법적인 접근을 방지함으로써, 각 자원에 대한 기밀성, 무결성, 가용성 보안 서비스를 제공하며, 사용자의 신분확인 절차를 통해 인가된 사용자가 정보 자원에 대해 어느 정도의 권한을 가지고 있는지를 결정한다. 대부분 컴퓨터 시스템의 사용자들은 시스템을 사용하기 위하여 식별과 인증이라는 검증 과정을 거쳐야 한다. 식별과 인증은 각 시스템 자원을 보호하기 위한 일차적인 보호단계라고 할 수 있다. 접근통제 결정은 이러한 식별과 인증을 통해 요청자의 신분이 완전히 인증되기 전까지는 수행될 수 없다. 인증이 성공하면 각 시스템 자원에 대한 사용자의 요청은 보안 정책이 적용된 접근통제 절차에 따라 허용된다.

접근통제 시스템은 보안 규칙과 정책의 구현 기능을 갖는 보안 메커니즘에 종속적이다. 보안

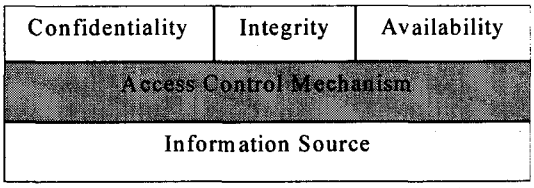

그림 1. 접근 통제의 개념

메커니즘은 부당한 접근의 예방(접근통제 메커니즘)과 부당한 접근의 방지(감사와 침입탐지 메커니즘)에 관련이 있다. 이러한 강력한 예방과 탐지를 위해서는 인증 기술이 필수적인 요소이다. 사용자 신분의 인증은 어떤 동작에 대한 사용자 권한을 통제하기 위하여 정당한 사용자를 검증하는 토대가 된다.

3. SPKI(Simple Public Key Infrastructure)

SPKI는 접근통제를 위한 공개키 인증서를 정의하고 있는 인터넷 드래프트 표준이며, 개체의 이름 대신에 공개키의 광범위한 사용과 분산을 강조하고 있다. SPKI 인증서의 전체적인 아이디어는 공개키 암호화에 기반을 두고 있으며, 서로 다른 허가권을 자유롭게 정의할 수 있다. 이러한 SPKI 인증서의 기본적인 요구사항은 다음과 같다.

- 발행의 자유
- 권한의 위임
- 자유로운 허가권 정의와 분배
- 유효기간의 명확한 기재
- 공개키의 광범위한 사용
- 공개키 획득을 위한 진보된 메커니즘제공

또한 SPKI는 X.509 계층구조의 한계점을 보완하기 위해 제안된 표준이다. X.509 계층구조는 최상위 CA(Certification Authority)를 두고, 이 최상위 CA가 신뢰된 개체를 선택하여 인증서를

발행해 주면, 그 인증서에 해당하는 개체가 새로운 CA가 되는 계층구조로 이루어지며 최하위 CA는 사용자에게 인증서를 발행한다. 이러한 X.509 계층구조가 가지는 한계점을 요약해 보면, 우선 최상위 CA의 하위 CA선정에 문제가 발생할 경우 하위 CA 역시 잘못된 이름 인증서를 발급할 수 있다. 또한 이름 인증서 사용을 원하는 모든 사용자들이 같은 계층구조에 속하거나 신뢰된 연결을 유지해야 하며, 이 사용자들이 유일한 이름(DN, Distinguished Name)을 사용한다고 가정하고 있다. 이러한 여러 가지 문제점들은 SPKI를 통해 해결될 수 있다. SPKI에서는 이름 대신 공개키의 광범위한 사용을 강조하고 있다. 공개키는 전세계적으로 유일하기 때문에 이름이 가지는 한계점을 극복할 수 있으며, SPKI/SDSI 이름 인증서를 이용함으로써 X.509 계층구조에서 이름을 이용하여 찾아야 하는 인증서 획득 문제를 해결할 수 있다.

SPKI 인증서는 기본적으로 이름 인증서(Name Certificate)와 권한 인증서(Authorization Certificate)로 구분된다. 이름 인증서는 발급자 이름 영역 내의 이름과 principal 또는 principal 그룹의 결합이며, 권한 인증서는 권한(허가)과 principal 또는 principal 그룹의 결합이다. 이름 인증서는 SPKI WG에 의해서 SPKI 표준의 일부로 채택될 예정인 SDSI(Simple Distributed Security Infrastructure) 이름 인증서를 사용한다.

(1) SPKI 권한 인증서

SPKI 권한 인증서는 5개의 엘리먼트로 구성되는 서명된 메시지이다. 이 인증서에서 서명문을 제외한 나머지를 5-tuple이라고 한다.

5-엘리먼트는 다음과 같다.

• Issuer(발급자) : 인증서 발행자 또는 서명자의 공개키나 키의 해쉬값을 의미한다. 발급자 영역에는 공개키가 위치하게 되며, 다른 사람들이 이것을 볼 수 있다. 개인키는 서명에 이용된다. 인증서가 키에 의해 직접적으로 발행되기 때문에 사람이나 개체의 이름이 언급될 필요가 없다.

• Subject(주체) : 인증서에 주어진 권한을 얻는 개체. 이 주체 영역에는 공개키나 공개키의 해쉬값, 또는 이름이 위치한다. 이것의 의미는 해당 공개키나 이름이 이 인증서를 소유하며, 다른 사람이 사용할 수 없음을 의미한다.

• Delegation(위임) : 위임 영역은 발급자가 주체에게 발행한 권한을 재 위임할 수 있는 권리를 주체에게 부여하는 영역으로, 부울 값으로 표현된다. 해당 인증서의 주체가 다른 주체에게 권한을 위임할 수 있도록 발급자가 허용하면, 부울 값은 "true"가 된다.

• Authorization(허가) : 허가 영역은 접근 권한을 의미하며, 종종 tag라고도 불린다. 발급자가 주체를 위해 인증서에 서명하면, 이것은 통상 주체가 가지게 될 권한을 정의하는 것이다. 권한은 인증서 발급자에 의해 자유롭게 정의될 수 있으며, 이 영역의 내용은 전적으로 어플리케이션에 달려 있다.

Validity Dates(유효기간) : 유효기간 영역은 발급자가 지정한 인증서의 유효기간을 정의하는데 사용된다. 이 영역의 형태는 not-before date와 not-after date를 사용하도록 제안되어 있다.

이 다섯 개의 엘리먼트 중 필수 엘리먼트는 Issuer와 Subject이고, 나머지 Delegation, Authorization, Validity Dates는 옵션 엘리먼트이다. 이 5가지 요소들은 SPKI와 SDSI에서 특별히 사용되는 S-expression으로 표현된다. 이 S-exp는 메시지 포맷을 정의하는 Lisp같은 표기법이다. SPKI에서는 ASN.1을 사용하지 않는데, 이는 S-exp가 적은 메모리와 느린 프로세서를 가진 디바이스에 더 적합하기 때문이다.

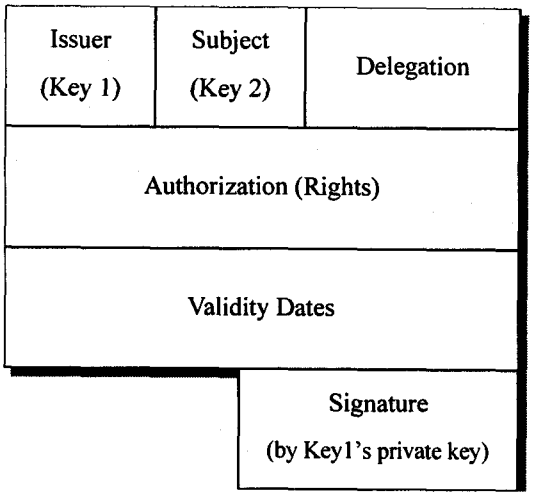

그림 2. SPKI 인증서 구조

인증서와 5-tuple간의 관계는 다음과 같다.

- 인증서 내의 서명이 검증되고 나면, 인증서는 5-tuple로써 컴퓨터 메모리에 저장된다.
- 5-tuple은 신뢰된 컴퓨터 프로그램에 의해서 인증서의 검증이나 축소 과정이 진행될 때 사용된다.
- 인증서의 모든 보안 관련 정보는 5-tuple 내에 저장된다.
- 5-tuple은 인증서의 수학적 모델이다.

5-tuple은 다음의 형태로 표현된다.

<I, S, D, A, V>

I : Issuer

S : Subject

D : Delegation

A : Authorization

V : Validity Dates

SPKI 인증서는 공개키 암호화에 기반을 둔다. PKI에서는 개인키의 분실이나 훼손의 경우에 대한 인증서 폐지 목록(CRL, Certificate Revocation List)이 유지되어야 한다. 그러나 SPKI에서는 PKI에서와 같이 인증당국에 의해 유지되는 큰 용량의 키 폐지 리스트가 요구되지 않는다. 대신에 모든 인증서 발급자들은 인증서 내에 허가와 유효기간 필드를 조정함으로써 CRL의 크기를 최소화할 수 있다. 그러나 이것은 필수 사항은 아니며, 인증서 발급자들은 개인키의 분실이나 훼손으로 인한 피해를 줄이기 위해 유효기간을 짧게 정의할 수 있다.

주체가 자신의 권한을 위임할 수 있는 권한을 가지게 되면, 다른 주체에게 해당 인증서를 재위임할 수 있다. 또한 다른 주체에 대한 새로운 인증서에 서명할 수 있다. 이러한 방법으로 계속적인 위임이 가능하며, 인증서 체인이 길어지면 길어질수록 최종 개체가 가지는 권한은 적어진다.

(2) 5-tuple Reduction

접근권한은 종종 인증서 체인으로 표현되기 때문에, 그것을 확인하는 방법과 간결화하는 문제가 매우 중요하다. SPKI 인증서를 가진 사람이나 공개키(이를 prover라고 부른다)가 서비스에 액세스하고자 할 때는, 서비스 제공 서버에게 인증서를 보여야 한다. 서버(verifier)는 검증자(prover)가 적절한 권한을 가졌을 경우에만 요구를 수용한다. 5-tuple reduction은 검증자의 권한을 계산하기 위한 것으로, 서버에 의해 주로 사용된다. 또한5-tuple reduction rule을 사용함으로써, 인증서 집합을 하나로 만들 수 있다.

발급자는 또한 단순화된 CRC(Certificate Result Certificate)를 검증자에게 발행한다. 이 간결화된 인증서는 서비스 제공자에 의해 직접적으로 발행된다. 이 인증서는 이전 인증서 집합과 정확하게 동일한 권한을 가진다.

5-tuple reduction에 대한 예로서, 주체 S1이 발급자 I1에 의해 발행된 인증서를 가지고 있고, 그 인증서의 권한이 A1, 유효기간이 V1, 위임권한이 D1이라고 하자. 이것을 5-tuple로써 표현하면, 다음과 같다.

<I1, S1, D1, A1, V1>

S1이 자신에게 발행된 권한을 다른 주체 S2에게 위임하고, 그 유효기간이 V2라면, 5-tuple은 다음과 같다.

<S1, S2, D2, A2, V2>

축소 규칙(reduction rule)에 의해서, 이 두 인증서(depth 2인 인증서)는 다음의 5-tuple로써 표현되는 하나의 인증서와 동일하게 된다.

<I1, S2, D2, AIntersect(A1, A2),
VIntersect(V1, V2)>

이 축소된 인증서는 I1에 의해 S2에게 발행되었고, 권한이 A1과 A2의 교차부분, 유효기간이 V1과 V2의 교차부분, 그리고 위임권한이 D2인 인증서와 동일하다.

5-tuple 축소 규칙에 의한 효과는 다음과 같다.

- 인증서 체인의 의미를 정의
- 검증자에게 부여될 인증서 체인의 권한을 간략화하기 위해 서버에 의해서 사용 가능
- 인증서 체인의 간결화를 위해 사용 가능
- 인증서 체인 내 intermediate key(중간 키)의 익명성을 보장한다. 인증서 체인 소유자는 중간 발급자의 권한을 읽을 수 있다. 그러나 인증서 체인의 단일화 이후에는 인증서 소유자가 더 이상 그 권한을 읽을 수가 없다. 축소 규칙과 함께 인증서의 암호화와 temporary key를 이용하여 익명성을 보호할 수 있다.

(3) 인증서의 사용

앨리스의 공개키 Kpa에 의해 밥의 공개키 Kpb에게 인증서가 발행되었다면, 인증서는 앨리스의 개인키 Ksa로 서명되어 있다. 따라서, 누구도 앨리스를 위장해서 잘못된 인증서를 발급할 수 없다. 밥이 앨리스의 디렉토리에 있는 파일을 읽고자 할 때, 밥은 자신의 개인키(Ksb)로 서명한 요구 메시지를 작성하고 인증서 체인과 함께 서명된 요구 메시지를 앨리스의 파일 서버에 보낸다. 파일 서버는 앨리스의 이름을 알지 못한다. 단지 공개키 Kpa가 어떤 파일을 관리한다는 것만을 알고 있다. 이 파일들에 대한 동작 요구를 파일 서버가 수신하면(이 요구는 개인키에 의해 서명되어 있다), 해당 요구를 수행한다.

앨리스의 파일 서버가 밥의 요구를 수신하면, 밥의 디렉토리 액세스를 허용하기 전에 인증서와 그의 요구를 확인한다. 유효성 검증 과정은 여러 가지 방법으로 수행될 수 있다.

① 앨리스의 파일 서버는 발행자 확인을 위해 발급자 영역을 조사한다. 앨리스의 파일 서버는 발급자가 Kpa임을 알아낸다. 파일 서버 고유의 ACL을 통해 Kpa가 액세스 권한을 승인하는 권한을 가지고 있음을 알 수 있다. 파일 서버는 서명문을 확인한다.

② 파일 서버는 인증서 주체 영역의 공개키 Kpb를 이용해 요구 메시지 상의 서명문을 검증한다.

③ 요구된 서비스가 서버 내의 Kpa에 대해 허용된 것임에 틀림이 없고, 해당 요구가 인증서 허가 영역의 권한 내에 있다는 사실을 확인한다.

④ 위의 모든 과정이 수행되고 나면, 앨리스의 파일 서버는 Kpb가 디렉토리에 액세스할 권한이 있음을 확인하게 된다.

모든 인증서는 발급자의 개인키로 서명된다. 인증서 사용 시에는 사용자가 주체의 개인키로 서명된 요구 메시지를 보내야만 한다.

SPKI 인증서는 접근통제뿐만 아니라 여러 다양한 응용 분야에 이용될 수 있다. 이러한 인증

서 사용에 대해서 SPKI 메일링 리스트에 모아진 브레인스토밍(brainstorming) 리스트를 요약해보면, 다음과 같다.

- 유권자 등록 카드
- 의약 처방 카드
- 보험 카드
- 운전 면허(운전 권한, 주류 구입 권한)
- ATM 카드
- 전자적 장비에 대한 소유 증명
- 타임 스탬핑/공증 서비스
- DNS 이름이나 서브트리에 대한 합법적 소유 증명 등

(4) SDSI(Simple Distributed Security Infrastructure)

SPKI WG는 SPKI 표준의 일부로 SDSI 이름을 채택하고 있다. SDSI 이름 인증서는 개체의 이름이나 속성에 따라 공개키를 찾는 데 이용된다. SPKI 인증서는 5-tuple에 매핑되는 반면에, SDSI 이름 인증서는 4-tuple에 매핑된다. 이름 인증서는 공개키나 키의 해쉬값에 대한 이름을 정의하고 있는 서명된 메시지이다. 4-tuple의 엘리먼트는 Issuer, Name, Subject, Validity Dates이다. 5-tuple과 비교해 허가 영역이 이름 영역으로 대체되어 있고, 위임 영역이 존재하지 않는다.

SDSI 이름은 반드시 사람 이름일 필요는 없으며, 어떠한 개체의 이름이나 또는 그러한 개체의 속성일 수 있다. SDSI 이름은 많은 참조(reference) 때문에, 예를 들어 "Alice's boyfriend's sister"와 같이 매우 길어질 수 있다.

SDSI 이름 인증서의 형태는 그림 3과 같으며, 이를 4-tuple에 매핑시키면 다음과 같다.

<Key 1, "Name", Key 2, Validity Dates>

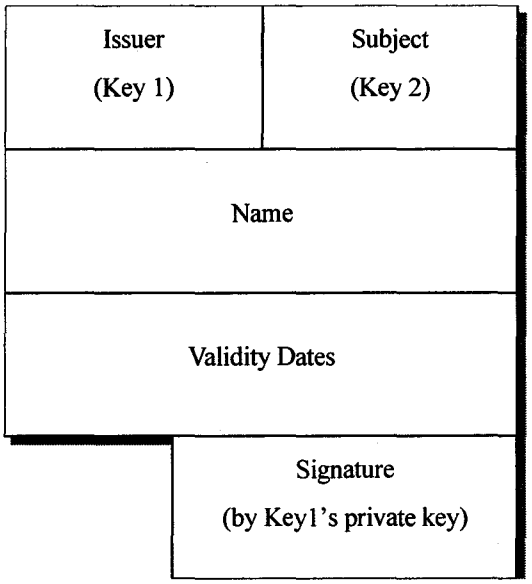

그림 3. SDSI 이름 인증서

(5) 키와 인증서의 보관

SPKI 인증서는 DNS Security Working Group에서 제안하고 있는 효율적인 키 저장과 분배 메커니즘인 KEY Resource Record (RR)에 보관될 수도 있으며, SPKI 인증서를 위한 새로운 RR을 구축할 수도 있다. 또한 웹 페이지 구동 서비스나 전자 우편 서비스에 모두 동작하는 MIT의 PGP 키 서버도 효율적인 키 저장과 복구 메커니즘을 제공해 준다. SDSI v1.0에서는 각 개체의 고유의 워크스테이션에서 구동될 수 있는 개별적 인증서 서버를 설명하고 있다. SPKI WG에서는 이와 유사한 SDSI/SPKI 인증서 서버를 검토 중에 있다.

4. SPKI를 이용한 접근통제 모델

SPKI를 이용한 접근통제 모델의 설계에서 가장 먼저 이루어져야 할 일은 인증서와 키를 생성해 주는 메커니즘을 설계하는 것이다.

사용자가 발행하는 인증서의 형태는 앞에서 논의한 권한 인증서와 이름 인증서, 그리고 부

가적으로 멤버쉽 인증서의 세 가지로 구분한다. 또한 발급자는 자기 자신에게 발행한 자가 인증서(Auto-Certificate)를 반드시 가져야 한다.

이러한 키 및 인증서 생성과 보관을 위해서는 각 개체가 개별적으로 SPKI/SDSI 서버를 보유할 수도 있으며, 그러한 생성 능력이 없는 경우에는 신뢰된 전문 서버의 일부를 할당 받아 자신의 서버로 사용할 수 있을 것이다. 이 두 가지 경우에 대해 사용자의 서버가 가져야 하는 공통적인 기능은 다음과 같다.

- 타 서버에 접속하기 위한 기능(인증서 검색과 query 생성 기능)
- 사용자 캐쉬와 서버 포함 기능(캐쉬 내 인증서의 디스플레이 기능, 자가 인증서 관리 기능)

인증서는 두 가지 형태로 보관이 가능하다. 첫째는 사용자 캐쉬 내에 지역적으로 보관하는 방법이고, 둘째는 SPKI/SDSI 서버에 원격적으로 위치하는 경우이다. 후자의 경우에는 획득하고자 하는 인증서가 위치해 있는 적절한 서버에 query를 보냄으로써, 인증서를 획득할 수 있다.

SPKI를 이용한 접근통제 모델은 그림 4와 같다. SPKI에서는 공개키와 개인키를 가진 모든 개체는 인증서를 발급하고, 자신의 권한을 위임할 수 있다. 예를 들어, 서버 내에 저장되어 있는 임의의 파일을 사용할 수 있는 권한을 가지고 있는 개체가 다른 사용자에게 자신의 권한 중 일부를 위임한다. 권한을 위임 받은 사용자는 해당 데이터베이스에 접근하여 자신이 원하는 정보를 이용할 수 있다. 일반적으로 데이터베이스에 접근하려는 사용자의 요구 메시지는 데이터베이스에서 처리 가능한 query문으로 변환되어 DBMS로 입력되고, 이 DBMS에서 모든 처리 과정이 수행된다. 따라서, SPKI 인증서를 이용하여 DB에 접근하는 사용자들을 위해 SPKI 인증서를 query문으로 변환해 주는 어플리케이션이 필요하게 된다. 권한을 위임 받은 사용자가 요구 메시지와 인증서를 보내면, 어플리케이션에서는 이를 DBMS로 전달한다. 또한 이 어플리케이션에서는 인증서의 reduction을 수행하며, 이 축소된 인증서를 보관하는 저장소의 기능도 하게 된다.

DBMS에서는 해당 인증서 발급자의 공개키와 ACL을 비교하여, 이 비교가 성공하면 해당 요구에 대한 오퍼레이션을 수행한다.

일반적으로, DBMS에 적용되는 접근통제 방식은 MAC(Mandatory Access Control)이다. MAC(강제적 접근통제)는 객체에 포함된 정보의 비밀성과 이러한 비밀성의 접근 정보에 대하여 주체가 가지는 권한에 근거하여 객체에 대한 접근을 제한하는 방법이다. 이 방식은 하위 비밀 등급 객체로의 정보 흐름을 차단하기 때문에 흐름 제어 정책으로 정의될 수 있으며, 한 주체가 객체를 읽고 그 내용을 다른 객체에게 복사하는 경우에 원래의 객체에 내포된 MAC 제한사항이 복사된 객체에 그대로 전파된다. 또한 MAC 정책은 모든 주체 및 객체에 대하여 일정하며, 어느 하나의 주체나 객체 단위로 접근 제한을 설정할 수 없다.

SPKI 인증서를 이용한 접근통제 방식은 MAC와는 다른 개념인 DAC(Discretionary Access Control) 방식이다. DAC 방식은 주체나 그것이 속해 있는 그룹의 ID에 근거하여 객체에 대한 접근을 제한하는 방식으로, SPKI 인증서에서 주체의 공개키에 대하여 접근권한을 설정하는 방식과 유사하다. 그러나 SPKI 인증서를 이용하는 방식은 자유로운 권한 설정과 위임이 가능하다.

어떤 조직에 구축되어 있는 DBMS에서 사용하는 ACL은 그 조직의 전체적인 구조를 반영해야 한다. 즉, 키 홀더의 이름 리스트와 그 각각의 이름에 대해 허용되는 접근 형태 목록을 포함해야 하므로, 규모의 문제가 발생할 수 있

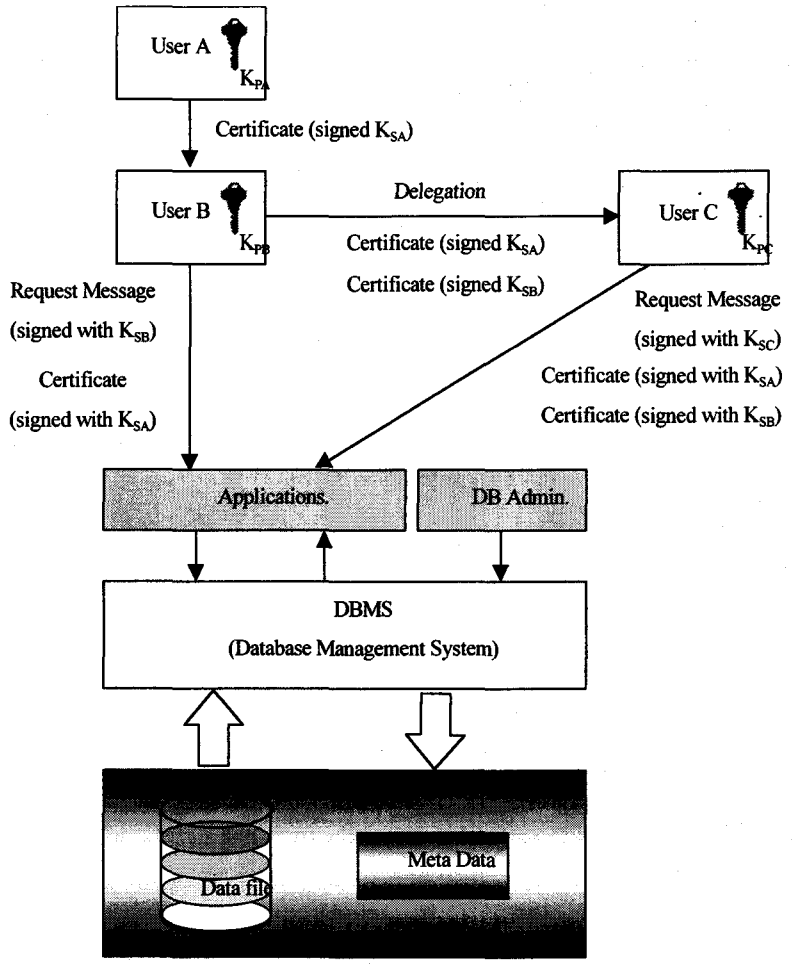

그림 4. 접근통제 모델 (SPKI 인증서 이용)

다. 또한 접근 통제 결정 뿐 아니라 ACL의 업데이트 시에도 액세스 요구를 수용할 수 있어야 한다. 그러나 그러한 접근이 권한 인증서에 의해 통제된다면, DBMS는 하나의 엔트리에 대한 ACL만 가지면 된다. 이 엔트리는 DB에 접근할 수 있는 권한을 위임해 주는 키에 대한 키 홀더에 해당한다. 이 키 홀더는 자신의 하부 개체에 인증서를 발급해 준다. 이렇게 생성된 인증서들은 ACL 집합과 같이 전체 조직 구조를 반영하지만, 하나의 DB에 보관되거나 또는 여러 DB에 복사(replication)되어 관리될 필요가 없다.

5. 결 론

SPKI 인증서의 특징을 요약해 보면, 우선 SPKI 인증서는 접근통제에 주로 사용되며, 공개키 암호화에 기반을 두고 있다. SPKI 인증서는 하나의 안전한 서버에 의해 관리되는 것이 아니라 공개키와 개인키를 가진 사용자나 컴퓨터에게 분산되며, 다른 개체의 승인 없이 누구나 발행할 수 있다는 특징을 가진다. 그리고, 이름 대신 공개키를 사용함으로써 신뢰된 공개키 획득 방법을 제공해 주며, 공개키 기반구조

(PKI, Public Key Infrastructure)의 구성 요소 중 하나인 인증 기관(CA, Certification Authority)의 필요성을 배제해 준다. 또한 SPKI의 한 부분에 SDSI를 결합함으로써, SPKI 이름 인증서는 이름과 키의 결합에 대한 보다 유연한 메커니즘을 제공해 준다.

이러한 특징들에 근거하여, SPKI 인증서를 사용함으로써 분산 DB 시스템 관리를 위한 DBMS에서의 ACL을 관리하는데 필요한 비용과 시간을 절감할 수 있으며, 또한 DBMS와는 별개의 응용 프로그램으로 동작됨으로써 암호 및 인증 메커니즘을 도입한 DB 접속권한 제어 방식으로 사용될 수 있다.

GIS는 각종 자연물과 인공물에 대한 위치정보와 속성정보를 포함하는 정보 시스템이므로, 이에 따른 군사적 기밀 정보 등이 포함될 수 있다. 따라서 이러한 정보를 보관하게 될 GIS DB에 대한 정보보호는 필수적이라고 말할 수 있으며, SPKI 및 암호화를 통해 GIS DB에 대한 강력한 접근통제를 실현할 수 있을 것으로 본다.

참고문헌

[1] William Stallings, *Network and Internerwork SecurityPrinciples and practice*, Prentice Hall, 1995

[2] M.Y. Rhee, *Cryptography and Secure Communications*, McGraw-Hill, 1993

[3] C.J. Date, *데이터베이스 시스템*, 홍릉과학출판사, 1998.9

[4] 김계현, *GIS 개론*, 대영사

[5] SPKI/SDSI 관련 문서

1) Internet Draft
- *SPKI Examples*, 1998.3
- *Simple Public Key Certificate*, 1998.3
- *SPKI Requirements*, 1999.5
- *SPKI Certificate Theory*, 1999.5

2) Yulian Wang, SPKI, 1998.7

3) Ronald L. Rivest, SDSI－*A Simple Distributed Security Infrastructure*(v1.0), 1996.9

4) Ronald L. Rivest, SDSI－*A Simple Distributed Security Infrastructure*(v1.1), 1996.10

5) Ronald L. Rivest, SPKI/SDSI 2.0－*A Simple Distributed Security Infrastructure*

6) Gillian D. Elcock, Web－*Based User Interface for a Simple Distributed Security Infrastructure(SDSI)*, 1997.7

김 장 성

1998년 세명대학교 전자공학과 졸업(공학사)
1998년～현재 세명대학교 대학원 전기전자공학과 석사 과정
관심분야 : PKI, 암호 프로토콜, 인증 기술