정보학연구 제6권 제1호 2003년 3월(pp.11-20)
The Journal of Information Technology, Vol.6, No.1

인증서를 이용한 역할기반 접근제어방안

박종화*, 김지홍**

요 약

정보통신기술의 발달로 최근 인터넷의 급격한 성장에 따라 공개키 인증서를 사용한 전자상거래가 활성화되고 있다. 또한 인터넷상의 웹서버, 데이터베이스에 접근하기 위한 접근통제시스템에 대한 연구도 활발히 진행되고 있다. 본 논문에서는 접근통제방식으로는 최근 주목되고 있는 역할기반의 접근제어(RBAC: Role-Based Access Control) 기법에 기존의 속성인증서를 적용한 방법과 SPKI 인증서를 적용한 접근제어 방식을 제안하고 이를 비교한다.

Ⅰ. 서론

정보통신 기술의 발달로 사회의 모든 분야에서 인터넷의 활용이 급속히 확산되어 전자결제, 전자상거래, 인터넷 뱅킹 등의 편리한 서비스가 제공되고 있다. 그러나 인터넷을 이용한 모든 거래는 거래 당사자간 비접촉, 비대면을 특징으로 하기 때문에, 온라인상의 편리함을 추구할 수 있는 반면에 거래 당사자간의 상호신뢰에 있어서 취약성을 가진다. 이러한 단점을 해결하기 위하여 전세계적으로 공개키기반구조(PKI : Public Key Infrastructure)라는 인증기반 구조[13]를 도입함으로서 거래당사자들 간의 신뢰성과 안전성을 추구하고 있다. 공개키기반구조는 계층구조 형식의 인증기반구조를 채택함으로서, 하위 계층의 인증기관 혹은 사용자에게 공개키 인증서를 발급하고, 이를 이용하여 온라인상의 안전한 전자거래를 할 수 있도록 하는 방식이다. 따라서 공개키기반구조 상에서의 모든 사용자는 공인인증기관으로부터 사용용도에 부합되는 공개키 인증서를 발급받고, 이를 이용하여 자신이 정당한 사용자임을 입증할 수 있다. 그러나 이러한 공개키 인증서를 이용한 기술은 공개키 정보를 이용하여 사용자 인증정보를 제공하므로 비대면 인터넷 통신에서의 사용자 신원을 입증하기 위해서 유용하게 사용될 수 있지만, 실제 시스템에서의 접근통제를 위한 정보는 포함하고 있지 않으므로, 접근통제를 필요로 하는 분야에서는 속성인증서 혹은 SPKI 인증서와 같은 별도의 형태의 인증서를 이용한 구조가 제안되고 있다.

속성인증서는 사용자의 속성정보를 저장하는 인증서로서, 사용자의 지위, 권한, 임무 등과 같은 다양한 권한정보를 제공한다. 속성인증서에 대한 연구는 ITU-T, IETF 등에서 진행되고 있으며, IETF에서는 Internet Draft 문서[5]와 RFC 3281[6]를 통하여 표준화가 진행되고 있다.

* 세명대학교 소프트웨어학과 조교수
** 세명대학교 정보보호학과 부교수

이러한 속성인증서는 사용자의 속성정보와 같은 유용한 정보를 저장하고 있지만, 사용자에 대한 공개키 정보를 가지고 있지 않다. 따라서 속성인증서를 접근통제 분야에 적용하기 위하여, 공개키 기반구조상의 PKI 인증서와 함께 속성인증서를 첨부하여 접근하거나, 혹은 PKI 인증서와 속성인증서를 결합하여 사용하는 방법에 관한 많은 연구가 진행되고 있다[10,11].

면에 SPKI 인증서 방식은 PKI 인증기반구조가 매우 광범위한 규모로 진행되고 있기 때문에 이에 대한 문제점을 보완하기 위해 제안된 방식으로서, 사용자의 공개키정보와 권한과 관련된 속성정보를 결합하는 방식을 사용하고 있다.

반 SPKI 인증서에 관한 연구는 IETF에서는 RFC 2692[7], RFC 2693[8]을 통하여 현재 표준화가 계속 진행되고 있다.

본 연구에서는 접근통제 기술로서 최근 부각되고 있는 직무기반의 접근통제기술(Role Based Access Control) 방식에 적용하기 위하여, 속성인증서를 사용한 방법과 SPKI(Simple PKI) 인증서를 사용한 방법을 제안하고, 이를 비교 분석하였다.

II. 기초이론

2.1 접근통제이론

접근통제(Access Control)는 외부사용자로부터 내부 네트워크 혹은 시스템을 보호하기 위해 사용되는 기술로서, 외부 사용자가 내부 네트워크로 또는 내부 사용자가 인터넷 등과 같은 외부 네트워크로 통신하기 위해 접근요청을 할 때, 통신 대상이 되는 목적지 시스템에 대한 접근 권한이 있는지를 검사하여 허용여부를 결정한다. 내부 네트워크를 보호하기 위한 기술로는 라우터와 같은 네트워크 장비에 ACL(Access Control List)을 설치하여 운용하고 있는 침입차단시스템을 대표적인 예로 들 수 있으며, 내부 시스템을 보호하기 위한 기술로는 웹서버, 데이터베이스 등을 보호하기 위하여 MAC(Mandatory Access Control), DAC(Discretionary Access Control) 등의 기술을 이용한 접근통제 시스템을 들 수 있다.

이러한 접근통제시스템에는 일정한 보안정책들이 적용된다. 미국 국방성에서 사용된 MAC 정책은 자동적으로 시행되는 일정한 규칙에 기반하고 있다. 그러한 규칙을 실제로 시행하기 위하여 사용자와 타겟에 대해서 광범위한 그룹형성이 요구된다. DAC 정책은 특별한 사용자별로 정보에 대한 접근을 제공하고 추가적 접근통제를 그 사용자에게 일임한다.

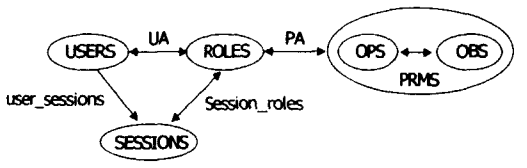
역할기반 접근제어(Role-Based Access Control) 방식은 1970년대 온라인시스템 상에서 다중사용자와 다중응용으로부터 시작되었다. RBAC의 기본개념은 MAC, DAC과는 달리, 역할(Role) 중심제어 방식이다. 이는 조직내의 다양한 작업을 역할단위로 구분하고, 사용자는 그들의 자격과 책임에 기초하여 역할에 지정된다. 또한 역할과 관련된 제어대상인 객체와의 관계를 규정해 주는 방법이다. 이는 조직내의 사용자들의 역할이 작업단위 혹은 프로젝트 단위로 수시로 변경될 수 있는 현실적인 문제점에 착안한 방법이라고 볼 수 있다. 그러므로 최근에는 RBAC 방식이 MAC, DAC의 대안으로 부각되고 있다.

역할기반 접근제어의 기본 개념은 접근 권한이 역할에 부여되고 사용자는 그들의 자격과 책임에 의해 역할에 지정됨으로써 사용자의 직무변경과 관계없이, 권한에 대한 관리를 매우 용

이하게 한다. 역할은 조직내의 특성에 의해 생성되고, 사용자는 그들의 특성에 따라 역할에 지정된다. 사용자는 역할 사이에서 재 지정이 용이하고, 역할은 새로운 응용으로부터 새로운 권한을 부여받을 수 있으며, 때에 따라 역할의 권한은 사용자로부터 회수될 수도 있다. 이러한 연구는 NIST(National Institute of Standards and Technology)를 통해 기존의 접근제어 모델에 비하여 역할기반 접근제어(RBAC: Role-Based Access Control)모델이 상업적이고 행정적인 분야에서 가장 적합하다는 것을 보여 주고 있다[1].

RBAC 모델에는 RBAC1, RBAC2, RBAC3 등 다양한 종류[1]가 있으나, 본 연구에서는 1998년 Jasen 이 제안한 개선된 RBAC 모델[3]을 사용한다. RBAC 기본모델은 사용자(users), 역할(roles), 허가(permission)와의 관계를 기본으로 하고, 객체(object), 주체(subject), 작용(operation), 세션(session)등을 이용하여 구체화하고 있다.

역할은 역할의 멤버 즉 사용자의 책임과 권한에 관련된 의미를 가진 조직내의 역할 기능이나 역할의 이름을 나타내며, 역할은 많은 허가(permission)를 할당받을 수 있으며, 허가는 조직 내에 하나 이상의 객체에 특별한 접근 모드를 승인하는 것을 말한다. 또한 Core RBAC은 사용자 세션(user-session) 개념을 포함한다. 사용자는 역할을 활성화 혹은 비-활성화하기 위해 세션을 이용하여 접근 할 수 있다.



(그림 2-1) RBAC 기본모델

- USERS : 사용자(user) 집합
- ROLES : 역할(role) 집합
- OPS : 동작(operation) 집합
- OBS : 객체(object) 집합
- UA ⊆ USERS × ROLES : 다대다(many to many) 사용자 대 역할 할당관계
- assigned_user(r) = { u ∈ USERS | (u, r) ∈ UA} : UA 에 의해 역할이 할당된 사용자
- PRMS = $2^{(OPS \times OBS)}$: 허가(permission) 집합
- PA ⊆ PRMS × ROLES : 다대다(many to many) 역할 대 허가 할당관계
- assigned_permissions(r : ROLES) → 2^{PRMS} : PA 에 의해 역할이 할당된 허가
- SESSIONS : 세션(session) 집합
- user_sessions(u : USERS) → $2^{SESSIONS}$: 사용자와 세션간의 매핑
- sessions_roles(s: SESSIONS) → 2^{ROLES} : 세션과 역할간의 매핑

2.2 인증서

인증서(certificate)란 여권과 같이 자기 자신의 신분을 증명하기 위해 사용되는 증서로서, 인터넷상에서 신뢰성있는 통신을 위하여 개개인을 입증하기 위해 사용된다. 이와같이 인터넷상에서 사용되는 인증서는 크게 PKI 인증서, 속성인증서, SPKI 인증서로 분류할 수 있다. PKI 인증서란 현재 범용적으로 사용되고 있는 공개키 기반구조에서 사용되고 있는 공개키 인증서를 말한다. 본 논문에서는 PKI 인증서[13]에 관한 설명은 생략한다.

2.2.1 속성인증서

속성인증서(Attribute Certificate)는 사용자의 속성정보를 저장하는 인증서로서, 사용자의 지위, 권한, 임무 등과 같은 다양한 권한정보를 제공하며, 속성인증서에 대한 형식[5,6]은 표 2-1과 같다.

〈표 2-1〉 속성인증서 형식

기본 영역	사용용도
버전	X.509 V2.0과 호환성을 가진 v2이면 "2"
서명 알고리즘	서명 알고리즘 ID 및 관련 파라미터
사용자(holder) 이름	속성인증서 사용자 이름(X.500 이름)
발급자(Issuer) 이름	속성인증서 발급자 이름(X.500 이름)
서명 알고리즘	서명알고리즘 ID 및 관련 파라미터
일련번호	속성인증서 일련번호
유효기간	UTCTime(시작날짜, 만료날짜)
속성정보	사용자에 대한 속성정보
발급자 고유 ID	발급자에 대한 부가정보(선택영역)
확장자	속성인증서에 대한 부가정보
서명문	인증서 발급자의 서명문

속성인증서의 구성은 PKI 인증서의 형식과 유사하다. 그러나 사용자의 공개키를 포함하고 있지 않으며, 사용자의 속성정보는 다음과 같다.

- Service Authentication Information : 사용자 ID 및 비밀번호
- Access Identity : 속성인증서 holder에 대한 정보
- Charging Identity : 과금을 위한 정보
- Group : 사용자가 속한 그룹
- Role : roleAuthority, 사용자의 역할
- Clearance : 보안인가등급

속성인증서는 서버 혹은 데이터베이스 등 시스템 자원에 대한 접근통제를 목적으로 하기 때문에, 인증서 발급주기를 가급적 짧게 하고, CRL(Certificate Revocation List)은 가능하면 사용하지 않는 것을 권장하고 있다.

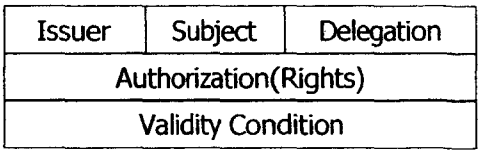
2.2.1 SPKI 인증서

SPKI 인증서[7,8]는 다음과 같은 공개키기반 구조에서의 문제점으로 인하여 제안되었다.

- 상위 CA의 오류가 전체 하부 구조에 전파된다.
- 상이한 PKI 구조간의 인증서 검증방법이 복잡하다.
- X.509 고유이름(DN: Distinguished Name)을 요구하기 때문에 현실적으로 문제가 많다.
- 대부분의 조직에서는 고용인의 이름이 공개되는 것을 원하지 않는다.

이러한 문제점을 해결하기 위하여 제안된 SPKI 기술은 현실적으로 요구되는 사용자의 권한에 관한 정보를 포함하고, 사용자간의 권한위임방법을 제안하고 있다.

SPKI 인증서는 기본적으로 그림 2-2와 같이 구성된다.

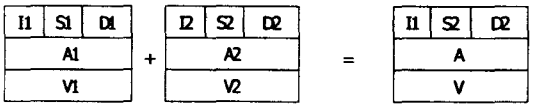


(그림 2-2) SPKI 인증서 형식

- Issuer : 발급자의 공개키 혹은 공개키 인증서
- Subject : 사용자 주체의 공개키 혹은 공개키 인증서
- Delegation : 사용자 주체에게 주어진 위임권한 여부
- Authorization : 사용자 주체에게 주어진 권한
- Validity : 유효기간

이러한 SPKI 인증서는 발급자의 공개키와 사용자의 공개키를 포함하여, 사용자에게 권한의 일부를 위임하는 5 tuple 구조로 형성된다. 마지막으로 발급자는 자신의 개인키로 인증서를 서명하고, 사용자에게 발급한다.

SPKI 인증서에서 사용되는 권한위임방법은 다음과 같다. 먼저 사용자 혹은 시스템에서 ACL에 저장된 사용자에게 최초의 권한을 지정한다. 최초의 권한을 가진 사용자(I1)는 자신의 권한 중 일부를 다른 사용자(S1)에게 위임하고, 다시 사용자(I2)는 또 다른 사용자(S2)에게 자신에게 할당된 권한 중 일부를 위임하기 위하여 SPKI 인증서를 발급한다.



(그림 2-3) SPKI 인증서를 이용한 서버접속

그림 2-3과 같이 권한위임이 2단계로 이루어진 경우에는 SPKI 인증서 확인자(verifier)는 다음과 같은 절차로 권한을 확인하고, SPKI 인증서 축소과정(reduction process)를 수행할 수 있다.

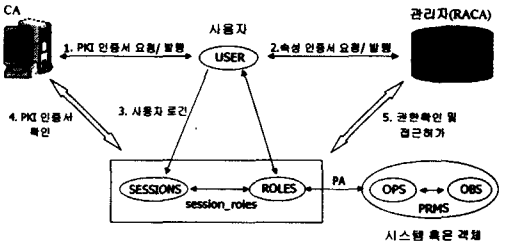
<I1,S1,D1,A1,V1> + <I2,S2,D2,A2,V2>
= <I1,S2,D2,A,V>

이러한 절차는 S1과 I2가 동일하여야 하며, 권한위임에 대한 D1 > D2이어야 하며, Authority와 Validity 필드는 다음과 같이 교집합부분으로 형성된다.

A = intersection(A1,A2)
V = intersection(V1,V2)

Ⅲ. 속성인증서를 이용한 RBAC 적용

2장에서 설명된 바와 같이 RBAC 시스템에 적용하기 위해서는 사용자의 인증정보를 필요로 한다. 지금까지는 RBAC 시스템에 사용자의 인증정보를 전달하기 위한 방법은 그림 (3-1)과 같다.



(그림 3-1) 인증서와 속성인증서를 이용한 접속방법

① RBAC 시스템에 접근하고자 하는 사용자는 기본적으로 PKI 기반시스템 사용자이어야 한다. 따라서 PKI 인증당국에 접속하여 PKI 인증서를 요청하고, 신원확인 과정을 거쳐, PKI 인증서를 발급받아야 한다.

② 사용자가 RBAC 시스템에 접속하기 위해서는 RACA(Role Attribute CA)에서 발급하는 속성인증서를 발급받아야 한다. 이 때 RACA는 속성인증서를 발행하는 인증기관을 말하며, 일반적으로 RACA는 시스템관리자가 시스템접속 권한을 가진 사용자에게 속성인증서를 발급하기 위해 운용된다.

③ 시스템에 접속하고자 하는 사용자는 자신의 PKI 인증서와 속성인증서를 이용하여 시스템에 로긴한다.

- PKI 공개키인증서 : 사용자 이름과 공개키

간의 결합관계를 나타내는 인증서

- 속성인증서 : 사용자 이름과 사용자의 권한 간의 결합관계를 나타내는 인증서

④ 서버에서는 사용자의 PKI 공개키인증서를 이용하여 CA 서명을 확인하고, CRL 검증절차를 수행한다. 사용자 인증이 완료되면, 사용자의 권한 사항을 확인하기 위하여 사용자의 속성인증서를 이용하여 RACA 서명을 확인하고, 권한 데이타베이스(Authorization Database)에 기록된 ACL(Access Control List)를 이용하여 사용자에 주어진 권한을 확인한다.

⑤ 사용자에 대한 PKI 인증서, 속성인증서에 대한 모든 사항이 체크된 후, 사용자의 접속을 허용한다.

이와같은 방법은 접근통제를 원하는 서버에서 인증서 검증절차를 두 번해야 된다는 단점이 있다. 그러므로 최근 발표된 논문에 의하면, 이러한 절차를 간략화시키기 위하여 공개키인증서와 속성인증서간의 결합(Binding) 방법을 연구한 논문들이 있다[9,10,11]. 최근 발표된 논문[11]에 의하면 속성인증서에 공개키인증서를 결합하기 위한 방법으로서, 다음과 같은 방법이 제안되고 있다.

① Monilithic Signature 방식 :

CA와 RACA의 역할을 동일한 인증기관에서 행하여 지는 경우에 적용될 수 있는 방법으로서, PKI 인증서의 확장자 영역에 속성인증서를 포함하여 1개의 인증서를 이용하는 형태이다.

② Automatic Signature 방식 :

CA와 RACA가 서로다른 별도의 인증기관으로 구성되며, 이를 결합할 수 있는 방법으로서, PKI 인증서와 결합하기 위하여 PKI 인증서의 일련번호, 발급자 ID 등의 일부정보를 속성인증서에 포함시키는 방법이다.

③ Chained Signature 방식

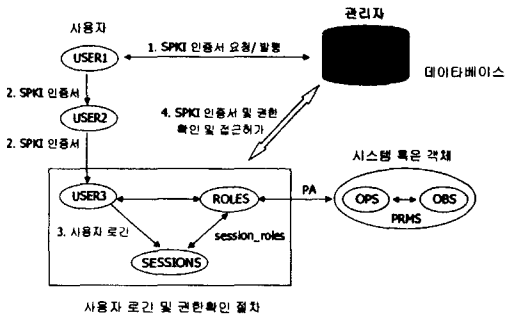
Automatic Signature 방식과 마찬가지로 CA와 RACA가 서로다른 별도의 인증기관으로 구성되며, 이를 결합할 수 있는 방법으로서, PKI 인증서의 서명문부분을 속성인증서의 확장자 영역에 포함시키는 방법이다.

이러한 방법들은 모두 그림(3-1)에서 제시된 기존의 PKI 인증서에서 역할, 책임과 관련된 속성정보를 포함할 수 없다는 단점에 기인하여, PKI 인증서와 속성인증서를 결합시킬 수 있는 방법으로 제시되고 있다. 이와는 별도로 PKI 인증서의 확장자 영역에 다중 속성인증서 기능을 할 수 있도록 여러 개의 RACA에서 발행한 속성인증서를 다중으로 첨부할 수 있는 스마트인증서(Smart Certificate) 라는 방법도 제시되고 있다[10].

이와같이 제시된 많은 논문과는 별도로 PKI 인증서의 확장자 영역의 주체대체이름(Subject Alternative Name)필드와 주체 디렉토리 속성(Subject Directory Attribute) 필드에 속성정보를 포함시키는 방법도 제안할 수 있다.

Ⅳ. SPKI 인증서를 이용한 방법

본 논문에서는 이와같은 연구발표 내용과는 별도로, 기존의 공개키기반구조의 한계성으로 인하여 제시되고 있는 SPKI 인증서를 이용하여 RBAC 방식에 적용할 수 있는 방안을 제시한다. 이와같은 SPKI 인증서를 이용하여 시스템에 접근하는 방법은 그림 4-1과 같다.



(그림 4-1) SPKI 인증서를 이용한 서버접속

그림 4-1에서와 같이 ACL에 저장된 시스템 접속허가자인 사용자 1은 사용자 2에게 자신의 권한 중 일부를 위임한 경우이고, 사용자 2는 사용자 3에게 자신의 권한 중 일부를 위임한 경우이다. 이에 대한 서버 접속절차는 다음과 같다.

① 사용자 1은 자신의 SDSI 이름 인증서를 제시하고, SPKI 인증서 발급을 요청한다.

시스템 관리자, 즉 인증서버는 사용자의 신원확인과정을 거치고, 시스템 접속권한을 포함하는 SPKI 인증서를 발급한다.

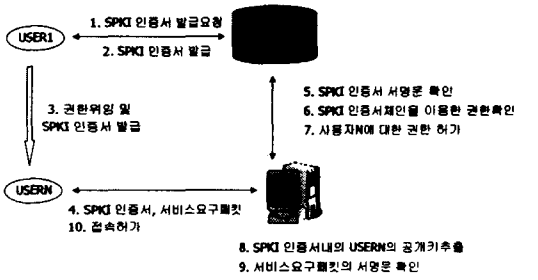
② 사용자 1은 자신의 권한 중 일부를 사용자 2에게 위임하며, 이에 대한 SPKI 인증서를 발행하고, 마찬가지로 사용자 2는 사용자 3에게 권한위임을 표시하는 SPKI 인증서를 발행한다.

③ 사용자 3은 사용자 1로부터 자신에게 위임된 권한을 행사하기 위하여 시스템에 로긴한다. 이때 사용자 3은 SPKI 인증서 체인과 서버접속 요구(Request) 패킷을 자신의 개인키를 이용하여 서명하여 서버로 전송한다.

④ 서버는 수신된 사용자의 SPKI 인증서 체인를 이용하여 Authorization Database에 접속하여 권한여부를 확인한다. 이때, 인증서 체인을 이용하여 인증서 축소과정을 거치고, 이를 이용하여 사용자 3에 대한 권한여부가 ACL에 등록된 권한리스트에 합당한 지를 체크한다. 만일 합당한 경우에는 3의 과정을 수행하고, 합당하지 않은 경우에는 접속이 허가되지 않는다. 만일 ②의 과정을 통하여 사용자의 접속권한이 인정되면, 사용자 3의 공개키를 추출하고, 이를 이용하여 사용자의 요구 패킷을 확인한다.

서버는 사용자의 요구 패킷을 분석하고 이를 처리한 후 , 이에 대한 결과를 사용자에게 전송한다.

이에 대한 상세한 절차는 그림 4-2로 표시된다.



(그림 4-2) SPKI 인증서를 이용한 서버접속

V. 두 방식의 비교

기존의 공개키기반구조에서 제공되지 않는 사용자의 속성 인증정보를 처리하기 위한 방법으로 속성인증서를 이용한 방법과 SPKI 방식을 이용하여 사용자의 속성인증정보를 처리하는 방법을 제안하였다.

일반적으로 속성정보를 가져오는 방법에는 user pull 방식과 system pull 방식이 있다. user pull 방식이란 속성인증서를 발급받은 후, user가 보관하고 있는 방식이며, system pull 방식이란 사용자가 접속하고자 하는 서버에서 직접 사

용자의 속성정보를 취하는 방식이다. 본 논문에서는 user pull 방식을 이용한 서버접속방법을 2가지 방법(속성인증서 이용방법, SPKI 인증서 이용방법)으로 제안하였다.

속성인증서는 PKI 공개키 인증서에서 처리할 수 없는 사용자의 속성정보를 가지고 있기 때문에 일반적으로 시스템에 대한 접근통제 알고리즘에 적용될 수 있다.

〈표 5-1〉 속성인증서와 공개키 인증서와의 비교

	공개키 인증서	속성 인증서
인증개념	사용자와 공개키	사용자와 속성정보
인증기관	공개키기반구조상의 CA	시스템 관리자(RACA)
속성정보	처리 불가	처리 가능
발급주기	길다	짧다
CRL	필요	불필요

표 5-1에서는 기존의 공개키 인증서와 속성인증서와의 차이점을 비교하였다. 이와같이 속성인증서는 사용자의 공개키 정보를 포함하지 않으며, 기본적으로 짧은기간 동안 사용자의 권한을 할당하기 위하여 발급하므로, CRL이 필요없다. 속성인증서는 직무와 관련된 사용자의 속성정보를 포함하고 접근통제용으로 사용할 수 있기 때문에 웹서버, 데이터베이스 등에 대한 접근통제 분야에 많은 연구가 진행되고 있다.

본 논문에서 제시한 방법으로 SPKI 인증서를 이용하여 이들 방법을 대치할 수 있는 방법을 제안한 것이다. 본 논문에서 제시하고 있는 SPKI 인증서를 이용한 방법과 기존의 방식과는 다음과 같은 차이점을 들 수 있다.

표 5-2에서 설명된 바와 같이 속성인증서에는 사용자 공개키에 대한 정보를 포함하고 있지 않기 때문에 사용자를 인증하기 위하여 PKI 인증서를 요구하거나 혹은 두 개의 정보를 포함하는 스마트 인증서를 사용하여야 한다. 그러나 SPKI

〈표 5-2〉 속성인증서 사용방법과 SPKI 인증서 사용방법 비교

	속성 인증서 방법	SPKI 인증서 방법
사용자의 공개키	포함하지 않음	포함
속성정보처리	가능	가능
권한위임처리	불가	가능
인증서 확인방법	속성인증서 확인 PKI 인증서 확인	SPKI 인증서 체인을 이용한 확인

인증서는 기본적으로 이름보다 공개키를 이용한 위임관계를 설정하는 방식이므로, SPKI 인증서를 이용하여 서명문을 확인할 수 있을 뿐 아니라, 사용자의 속성정보를 이용하여 접근제어를 할 수 있다.

Ⅵ. 결론

본 논문은 기존에 제시된 속성인증서와 공개키인증서를 결합하기 위한 여러 가지 방법을 제시한 논문[10,11,12] 과는 달리, SPKI 인증서의 사용자의 속성정보와 공개키정보를 이용하여 접근통제 알고리즘에 적용할 수 있는 방법을 제시한 논문이다. 이러한 연구결과를 바탕으로 향후에는 최근 접근통제방법으로 주목되고 있는 직무정보에 기반한 접근통제방식인 RBAC(Role Based Access Control) 방식에 적용시키는 연구가 진행되어야 한다. 또한 RBAC 방식에서의 Role Hierachy 구조와의 관련성, 정적인 의무분할, 동적인 의무분할과 연계하여 연구가 진행되어야 할 것 이다. 그러나 현재 SPKI 인증서와 관련된 연구가 점차 진행되고 있으므로 향후의 추세를 지켜볼 필요가 있다.

참고문헌

[1] David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn and Ramaswamy Chandramouli , "Proposed NIST Standard for Role-Based Access Control", ACM Transactions on Information and Systems Security, Volume 4, Number 3 / August 2001

[2] Ravi S. Sandhu, "Role-Based Access Control", 1997.9

[3] W.A. Jansen "A Revised Model for Role-Based Access Control", NISTIR 6192, July 9, 1998.

[4] Ravi S. Sandhu, Pierangela Samarati, "Access Control : Principles and Practice", IEEE Communication Magazine, Sept, 1994.

[5] Internet Draft "An Internet Attribute Certificate Profile for Authorization", S. Farrel, June 2001.

[6] RFC 3281 "An Internet Attribute Certificate Profile", S.Farrell, April 2002.

[7] RFC 2692 "SPKI Requirement", C.Ellison, Sept 1999.

[8] RFC 2693 "SPKI Certification Theory", Sept 1999.

[9] Joon S. Park and Sandhu, "RBAC on the Web by Smart Certificates ", ACM RBAC / 1999

[10] Joon S. Park and Sandhu, "Smart Certificates: Extending X.509 for Secure Attribute Service on the Web", NISSC / 1999

[11] Joon S. Park and Sandhu, "Binding Identities and Attributes Using Digitally Signed Certificates", ACSAC / 2000

[12] Yulian Wang, "SPKI", Dec 1998. http://www.hut.fi/~yuwang/SPKI.htm.

[13] 이만영외, "전자상거래 보안기술", 생능출판사, 2000.

RBAC Method using Certificates

Chong-Hwa, Park*, Ji-Hong, Kim**

Abstract

With the development of Information Communication Technique, electronic commerce using PKIs is widely used over the Internet. The goal of access control is to counter the threat of unauthorized operations involving Web-server or data base systems. The RBAC(Role-Based Access Control) has recently received considerable attention as a promising alternative to traditional discretionary and mandatory access controls. In this paper we propose two methods, the RBAC system using attribute certificates and the RBAC ststem using SPKI certificates. And we analyze and compare the two methods.

* Department of Software, Semyung University
** Department of Information Security, Semyung University