2002년 한국정보처리학회 춘계학술발표논문집 제9권 제1호

PMI를 이용한 확장 권한위임에 관한 연구

이덕규*, 이임영*
*순천향대학교 정보기술공학부
e-mail : hbrhcdbrh@catholic.or.kr, imylee@sch.ac.kr

A Study on Expansion Delegation using PMI

Deok-Gyu Lee *, Im-Yeong Lee*
*Division of Information Technology Eng
SoonChunHyang University

요 약

인터넷이 급속히 발달하면서 초기에 제공되던 정보제공의 방법으로는 사용자 신원에 대한 인증으로는 부족하게 되었다. 이에 대해 PKI(Public-Key Infrastructure)에서 인증서를 기반으로 사용자의 신원을 제공하는 보안방법이 대두되었다. 하지만 시스템에 따라 각 사용자에게 다른 서비스를 제공하고 이용해야 할 경우가 발생하게 되는데, 이 경우 각 사용자의 권한이나 임무 등의 사용자 속성을 관리할 필요가 있다. 이때 기존에 사용된 PKI 의 확장 영역을 이용하지 않고, 새롭게 사용자 속성을 위한 인증서를 사용하게 되는데 이것을 PMI 라고 한다. 본 논문에서는 PMI(Privilege Management Infrastructure)를 이용한 효율적이고 검증 가능한 권한위임 프로토콜에 대하여 제안한다.

1. 서론

인터넷이 급속히 발달하면서 초기에 제공되던 정보제공이나 검색 등의 기능뿐만 아니라 전자상거래, 인터넷 금융, 증권 등 다양한 서비스가 제공되고 있다. 이러한 상황에서 사용자자들간의 신원을 증명하기 어렵다는 단점이 대두되면서 사용자들간의 신원을 확인해 줄 필요가 발생하였다. 이를 해결하기 위해 PKI(Public-Key Infrastructure)기반의 전자 서명 시스템이 구축 되었다.

최근 PKI 를 기반으로 한 각 사용자 간에 신원 증명을 할 수 있게 되었지만, 인터넷 서비스 제공자들이 각 사용자 별로 다른 서비스를 제공하기 시작하였고, 시스템 내의 사용자에 따라 서로 다른 리소스를 제공하는 등 이제 사용자의 신원만 파악하는 것이 아니라 사용자의 속성을 정의하는 것이 필요하게 되었다.

이에 대해 새롭게 PMI(Privilege Management Infrastructure)가 나타나게 되었다. PMI 는 사용자 속성을 정의하여, 그 속성에 따라서 사용자 별로 권한 및 역할을 관리하는 방법의 하나로 대두되고 있다.

본 논문에서는 이러한 PMI 기반의 속성인증서를 이용하여 효율적이고 검증 가능한 권한위임 프로토콜에 대해 제한하고자 한다.

2. PMI 개요

기존의 PKC(Public Key Certificate)는 정보보호 서비스를 사용하는 사용자의 신원을 인증하는 기능을 한다. 하지만 다양한 웹 상의 서비스는 사용자 권한에 따라 서로 다른 기능을 제공하려는 움직임을 보이고 있다. 이런 상황에서 사용자 신원의 확인은 물론 사용자의 속성 즉, 권한, 지위, 임무 등에 관한 정보를 기록할 필요가 발생했다.

사용자 속성의 정보를 제공하려는 방법의 하나로 기존의 PKI 기반에서 사용하던 X.509 인증서의 확장 필드를 이용하는 방안이 제안되어 있다. 하지만 이를 사용할 경우에 또 다른 문제가 발생한다. 일반적으로 각 개체에게 주어지는 권한에는 유효기간 존재한다. 하지만 사용자 신원에 비해 사용자에게 부여되는 권한은 더 자주 변하므로 인증서에 비해 사용자 속성의 유효기간이 더 짧다. 따라서 새로운 속성을 적용하기 위해서 이미 발급된 인증서를 폐기하고 새로운 인증서를 폐기하고 새로운 인증서를 재발급 받아야 한다.

또, 사용자 신원은 전체에게 신뢰 받는 하나의 대리기관에서 받아서 모두 적용할 수 있지만, 사용자의 속성은 적용하려는 곳 마다 다르기 때문에 기존의 인증서를 사용할 경우 적절한 인증서를 항상 재발급 받아야 하는 단점이 생긴다.

이러한 문제들을 해결하고자 AC(Attribute Certificate)를 사용한다. 이는 사용자의 속성을 기록하고 인증하는 또 다른 인증서에 해당한다. 표 1 은 AC 에 들어갈 내용을 나타낸다.

표 1. 속성 인증서(AC : Attribute Certificate)의 필드

필드 이름	내용
Version	AC 의 버전, Version 2 사용
Holder	AC 소유자
Issuer	AC 발급자 (AA : Attribute Authority)
Signature	서명에 사용된 알고리즘
SerialNumber	AC 에게 부여되는 일련번호
AttrCertValidityPeriod	AC 의 유효기간
Attributes	소유자에게 부여된 속성 정보
IssuerUniqueID	발급자를 구분하는 번호
Extension	차후의 확장에 대비

2.2 구성요소들

일반적인 권한 관리 모델은 객체, 권한 소유자, 권한 입증자 등으로 구성된다. 객체는 접근 제어 응용과 같이 보호되어야 할 자원을 의미하는데, 이러한 객체들은 각자의 메소드를 지닌다. 예를 들어 방화벽 같은 객체는 '개체 허용'과 같은 메소드를, 파일 시스템 상의 파일은 읽기, 쓰기, 실행 등의 메소드를 지닌다.

권한 소유자(asserter, holder)는 특정 자원을 사용하기 위한 권한을 가지며 그 권한을 사용하는 개체이다.

권한 입증자는 주장되어지는 권한이 그 상황에 적절한지 아닌지를 판단하는 개체이다. 그러한 판단은 다음의 네 가지 사항에 근거하여 이루어진다.

- ▶ 주장하는 개체의 권한
- ▶ 권한 정책
- ▶ 현재 환경에 대한 변수
- ▶ 객체 메소드의 보안에 대한 민감성 정도

어떤 사용자가 지닌 권한은 그 권한을 소유한 사람의 신임 정도를 반영한다. 각 개체에게 부여되는 권한은 AC(s)에 캡슐화 되어 있거나 PKC 의 확장영역에 하나의 필드로 기록된다.

권한정책은 객체가 지닌 메소드의 보안 민감도나 사용환경을 고려하여 각 개체에게 적합한 권한의 정도를 부여하는 방법을 제시한다. 권한 정책은 무결성과 인증 서비스가 제공되어야 한다. 전달 정책을 세우는데 있어서 여러 경우가 존재하는데, 권한이 실제로는 전달되지 않게 하고 입증자의 환경에 맞게 부분적으로 사용하게 할 수도 있고, 시스템 내의 모든 개체에게 알려지고 전달되게 할 수도 있다.

권한 정책은 각 서비스에 대한 권한들의 수용을 위한 경계를 제시한다. 즉 소유자가 객체에 접근하기 위해 적합한지를 판단해야 할 때 입증자는 그 정책을 사용하여 결정한다.

환경 변수들은 권한 입증자가 결정을 내릴 때 지역적으로 그 환경에 맞게 설정할 수도 있는데, 이를 나타내기 위해서 사용한다.

객체 메소드의 보안에 대한 민감도는 전달되는 문서나 처리해야 할 요구들의 속성을 의미한다. 예를 들어 문서 내용이 어느 정도의 보안사항인지를 나타내는 것을 의미한다. 이는 AC 나 연관된 보안 레이블 등에 기록될 수 있다. 객체가 사용되는 상황에 따라 메소드의 민감도는 사용되지 않을 수도 있다.

2.3 AA 와 SOA

AA(Attribute Authority)와 CA(Certification Authority)는 논리적인 경우와 대부분의 물리적인 경우에서 서로 완전히 독립적이다. 신원(Identity)을 만들고 유지하는 것은 PMI 와 구분되어 PKI 를 기반으로 이루어진다. 그러므로 전체 PKI 가 구축되고 나서 PMI 를 구축하게 된다.

SOA(Source of Authority)는 일련의 권한 할당에 책임을 지는 권한 주장자에 의해서 신뢰되는 개체이다. SOA 는 자신이 AA 가 되어서 다른 개체에게 인증서를 발급하기도 하며, PKI 기반에서의 root CA 와 같은 역할을 하므로, SOA 로부터 서명된 인증서는 권한 입증자에게 신뢰를 준다.

3. PMI 사용 모델

AC 를 이용하여 접근 제어 응용에 사용할 경우 처리해야 하는 여러 상황이 발생한다. 이를 어떻게 처리하는 지를 보여준다. PMI 에는 크게 관제모델, 권한위임모델, 역할 기반 모델로 나누어진다. 각각에 대해 살펴보면 다음과 같다.

3.1 관제 모델

관제 모델은 PMI 가 보안이 요구되는 객체 메소드에 대한 접근을 어떻게 관제하는 지를 보여준다. 권한 소유자, 권한 입증자, 객체 메소드, 권한 정책, 환경 변수 등이 이 관제 모델의 구성요소가 된다.

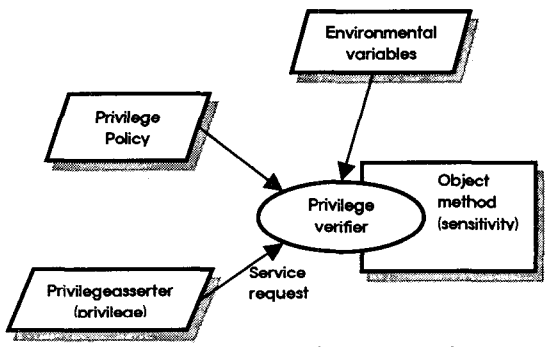

그림 1. PMI 관제 모델(Control model)

권한 소유자는 권한을 소유하고, 객체 메소드는 보안에 대한 민감도를 지닌다. 권한을 지닌 권한 소유자가 보안이 요구되는 객체 메소드에 접근하려는 것을 관제하도록 권한 입증자를 활성화 시킨다. 이때 권한 입증자는 권한 정책에 따라서 접근을 관제한다. 이때 권한과 보안 민감도는 다양한 값을 가지는 파라미터가 된다. 권한 소유자는 PKC 로 구분되는 개체이거나, 디스크 이미지의 요약(digest)에 의해서 구분되는 실행 가능한 객체가 된다.

3.2 권한 위임 모델

권한이 사용되는 환경에 따라서 임의적으로 권한의 위임이 필요하다. 권한 입증자, SOA, 또 다른 AA 들, 권한 주장자 등이 이 모델의 구성요소가 된다.

일반적으로 SOA 는 권한 소유자에게 권한을 할당하고 인증서를 발급하는 개체이지만, 이 경우에는 권한 소유자가 AA 의 역할을 할 수 있도록 인증하는 역할을 한다. 이때 AA 의 역할을 하는 권한 소유자는 자신이 소유한 원한의 일부나 똑같은 권한을 가지는 인증서를 발부하여 다른 개체에게 권한을 위임한다. 이때 SOA 는 위임에 경로 길이를 제한하거나 이름 공간을 제한하는 등의 제약을 둘 수 있다. 또 중간 단계의 AA 는 권한을 위임 받은 권한 소유자에 의해서 일어날 수 있는 이임에서 그 소유자가 AA 역할을 할 수 있도록 인증하는 역할도 한다. 자신이 가진 권한 이상의 것은 위임할 수 없다.

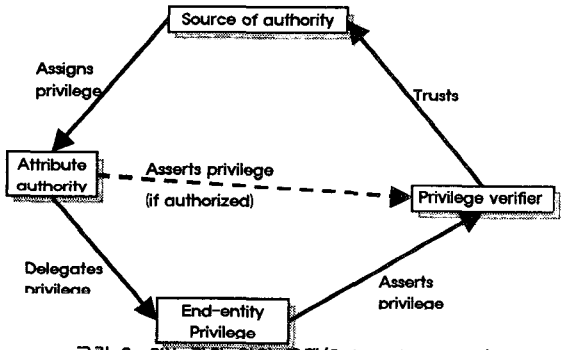

그림 2. PMI 권한 위임 모델(Delegation model)

3.3 역할 모델

역할은 각 개개인에게 권한을 직접적으로 부여하는 수단이다 개인들은 하나 또는 그 이상의 역할이 할당된 인증서인 역할 할당 인증서를 발급 받는다. 특정 권한들이 모여서 하나의 역할 이름을 할당 받는데, 이는 역할 명세 인증서를 통해서 이루어진다. 이렇게 함으로써 개인에게 할당된 인증서가 충돌하지 않고, 역할이 지니는 권한을 갱신할 수 있다. 만약 역할 명세 인증서를 사용하지 않으면 권한 입증자가 다음과 같은 방법들로 부분적으로 설정하여 사용할 수 있다.

- ▶ 임의의 수의 역할을 임의의 AA 가 정의
- ▶ 역할 자신이나 역할의 멤버를 서로 다른 AA 에 의해 각각 구분하여 정의 및 관리
- ▶ 역할의 멤버 위임 가능
- ▶ 역할이나 멤버에 적절한 수명 할당

만약 역할 할당 인증서를 AC 로 하면, 역할의 속성은 AC 의 attribute 영역에 포함된다. 그러나 이 경우에는 각 권한들이 인증 주체에는 추가적으로 할당 될 수 있어도 역할에는 추가적으로 할당 될 수 없다.

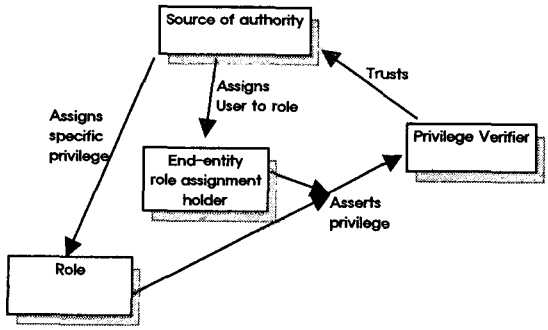

그림 3. PMI 역할 모델(Roles model)

4. 제안 방식

본 논문에서는 PMI 의 모델 중에서 권한 위임 모델을 바탕으로 제안되었다.

다음은 본 방식에서의 권한위임 모델을 나타내었다.

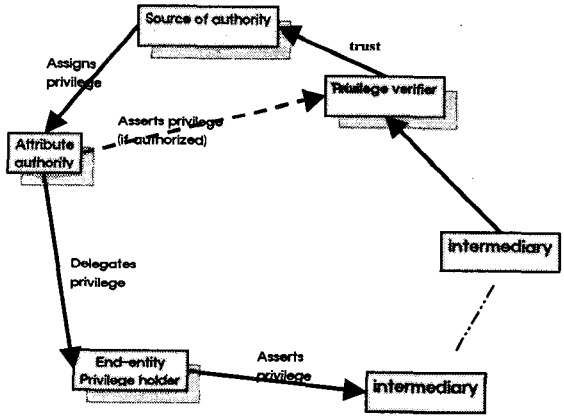

그림 4. 전체 시스템 모델

Source of authority : 사용자의 권한 인증서 발급개체이며 사용자의 권한을 인증서에 할당한다. 권한 소유자가 Attribute authority 의 역할을 하도록 설정한다.

Attribute authority : 권한 소유자의 권한 인증서를 전달한다. 여기서는 사용자와 같은 권한을 가진 것을 여긴다.

End-entity : 권한 인증서를 SOA 로부터 받으며 권한 인증서를 중개자에게 전달한다.

Privilege verifier : 실질적으로 권한 소유자가 서비스 받을 곳으로서 전달받은 SOA 에게 권한 인증서에 대한 사실 증명을 받는다.

4.1 시스템 계수

다음에서 설명하고 있는 것은 본 프로토콜에서 사용되는 시스템 계수이다.

· * : (EE : End-Entity, SOA : Source of authority, IM :

Intermediary, PV : Privilege Verifier)
· $IM_{(i)}$: i 개의 중개자(Intermediary)
· $Cert_{*}$: *의 공개키를 포함한 인증서
· DC_{PV} : EE 의 권한 위임 인증서
· n : 위임경로 길이
· AP : 유효기간(Available Period)
· Kpr_{*}, Kpu_{*} : *의 PKI 에서 만들어진 권한 위임을 위한 공개키와 개인키 쌍
· Kpr_{US}, Kpu_{US} : User 의 권한위임에 사용되는 공개키 개인키 쌍
· ID_{*} : *의 Identity
· R_{*} : *의 권한
· H() : 안전한 해쉬함수

4.2 프로토콜

권한 위임에 의한 순서는 결정되어 있지 않으며 권한 인증서에 따른 경로를 설정한다. 다음에서는 n 개의 중개자, 1 개의 사용자와 1 개의 목적지에 대하여 기술한다.

4.2.1 사용자 권한 위임 생성

SOA 는 사용자의 권한 위임을 위한 권한위임 인증서를 생성한다. 사용자 권한 위임 인증서에는 사용자의 ID, 권한, 경로제한 길이와 권한 인증서에 대한 유효기간으로 구성된다.

- SOA : $Cert_{EE}(DC_{PV}(ID_{EE}, R_{EE}, n, AP))$

4.2.2 사용자 권한 인증서 전송

사용자는 SOA 로부터 $Cert_{EE}$ 를 얻는다. 사용자는 권한 위임 인증서로부터 키 쌍을 획득한다. 획득한 키 쌍을 이용하여 중개자에게 권한 인증서를 포함하여 전송한다.

- EE : (Kpr_{US}, Kpu_{US})

- EE → $IM_{(1)}$: $Cert_{EE}$, $E_{KprEE}[Cert_{EE}]$, $E_{KpuIM(1)}[n]$

중개자는 전송 받은 인증서에서 다음에 전송할 중개자가 있을 경우 위임경로 길이 n 에서 1 을 뺀 후 다음 중개자에게 다음을 전송한다.

- IM(1) : $(Kpr_{IM(1)}, Kpu_{IM(1)})$

- IM(1) → IM(i) :
$Cert_{EE}$, $E_{KprEE}[Cert_{EE}]$, $E_{KpuIM(i)}[(n-i) \parallel H(Cert_{IM(1)} \ldots Cert_{IM(i-1)})]$, $Cert_{IM(i)}$

인증서를 받은 IM(i-1)는 이전 인증서를 검증하고 다음 중개자에게로 전송한다. IM(i-1)에서는 $Cert_{EE}$ 를 이용하여 사용자의 권한을 검증하고 다음 IM(i)에게 전송하게 되는데 이때 IM(i-1)은 사용자와 자신이 가지고 있는 권한보다 높은 권한을 가진 $IM_{(i)}$에게로 전송되지 않는다.

4.2.3 권한 인증서

PV(Privilege Verifier)는 IM(i)로부터 $Cert_{EE}$를 얻는다. 이때 PV 는 받은 $Cert_{EE}$ 와 $E_{KprEE}[Cert_{EE}]$, $E_{KpuPV}[(n-i) \parallel H(Cert_{IM(1)} \ldots Cert_{IM(i-1)})]$을 이용하여 경로에 대한 검증을 한다. 다음에는 $Cert_{EE}$ 를 이용하여 사용자의 권한 인증서를 획득하고 권한 인증서에 대한 검증을 요구한다. AA(Attribute Authority)로 받은 DC_{PV} 를 이용하여 검증된 $DC_{PV}(ID_{EE}, R_{EE}, n, AP)$에서 ID_{EE}, R_{EE}, AP 를 이용하여 사용자에게 서비스를 진행한다.

- IM(i) → PV :
$Cert_{EE}$, $E_{KprEE}[Cert_{EE}]$, $E_{KpuIM(i)}[(n-i) \parallel H(Cert_{IM(1)} \ldots Cert_{IM(i-1)})]$, $Cert_{IM(i)}$

- PV :
(n-i) → 이전 $Cert_{IM(i)}$를 이용하여 이전 $Cert_{IM(i-1)}$에 대해 검증

- AA → PV :
$Cert_{AA}$, $E_{KpuPV}[DC_{PV}(ID_{EE}, R_{EE}, n, AP)]$
Or E_{KpuEE}를 이용하여 $Cert_{EE}$ 검증

4.2 제안 방식 분석

본 제안 방식은 PMI 를 이용하여 확장된 권한위임을 제안하였다. 본 방식에서의 확장된 권한 위임 방법은 권한 위임에 대한 검증뿐만 아니라 권한 위인에 대한 경로를 검증할 수 있다.

권한 위임에 대한 경로 검증은 $IM_{(i)}$를 이용하여 이전 $IM_{(i-1)}$에 대한 경로 검증을 통해 이룰 수 있다. 이전에 대한 검증은 이전경로를 이용하면 해결할 수 있다.

권한에 대한 검증은 사용자의 권한 위임에 사용되는 공개키를 이용하는 방법과 AA 를 통해 권한위임 인증서를 받아오는 방법 두 가지를 통해 권한에 대한 검증을 할 수 있다.

5. 결 론

본 논문에서는 새로이 사용자 속성 정보를 관리해야 할 필요성과 기존에 사용하던 PKI 기반의 확장 영역을 사용할 경우의 단점에 대해여 새로운 방식인 PMI 를 이용하여 권한위임에 대하여 서술하였다.

새로이 제시되고 있는 PMI 의 모델 중에서 권한위임 모델을 가지고 제한하고자 한다. 권한 위임서는 경로 길이에 제약을 둘 수 있으며, 사용자에 의해서만 이임이 되며 권한위임 대상자는 자신의 권한 이상에는 위임을 하지 못한다.

향후 PMI 모델과 관련하여 역할 기반 모델(Roles model)과 관제 모델(Control model)에 관한 실제 서비스에서의 적용 가능성을 연구하고자 한다.

참고문헌

[1] ITU-T, Draft ITU-T RECOMMANDATION X.509 version4, ITU-T Publications, 2001. 5. 3
[2] A. Aresenault, S. Tuner, Internet X.509 Public Key Infrastructure, Internet Draft, 2000. 11
[3] S. Farrell, R. Housley, An Internet Attribute Certificate Profile for Authorization, Internet Draft, 2001.6
[4] Gun-Hee Lee, Jeong-Gak Yoo, Tae-Sik Shon, Song-Hwa Chai, Dong-Gyoo Kim, A Study about the PMI for Definition and Management of User Attribute, Korea Information Science Society, 2001. 10. 20, pp 742-744