사용자 속성의 정의 및 관리를 위한 PMI에 대한 연구

이건희[0] 유정각 손태식 채송화 김동규
아주대학교 정보 통신 공학과
(icezzoco, kagi, tsshon, portula1, dkkim)@madang.ajou.ac.kr

A Study about the PMI for Definition and Management of User Attribute

Gun-Hee Lee[0] Jeong-Gak Yoo Tae-Shik Shon Song-Hwa Chai Dong-Kyoo Kim
Dept. of Information Communication Engineering GSIC AJOU

요 약

인터넷의 서비스가 다양해 지면서 기존의 아이디와 패스워드를 이용한 사용자 신원 인증으로는 보안이 부족하게 되었다. 이에 대해서 인증서 기반으로 사용자 신원을 인증하는 강력한 보안 방법이 대두 되었다. 하지만 시스템에 따라서 각 사용자 별로 서로 다른 서비스를 이용해야 할 경우가 발생했다. 이 경우 각 사용자의 권한이나 임무 등의 사용자 속성을 관리할 필요가 생긴다. 기존의 PKI의 확장 영역을 사용하지 않고, 새롭게 사용자 속성을 위한 인증서를 사용하여 더욱 안전하고 안정적으로 정보보호 서비스를 제공한다.

1. 서 론

인터넷이 급격한 속도로 발달하면서 초기에 제공되던 정보의 공유나 검색 등의 기능 뿐만 아니라 전자상거래, 인터넷 금융, 증권, 관공서 업무 등의 다양한 서비스를 제공함으로써 실생활에서 인터넷의 효용가치가 더욱 높아지고 있다.

하지만 실제 생활과는 달리 인터넷 상에서는 상호간에 신원을 증명하기가 어려운 단점이 존재한다. 서로 보이지 않는 통신망 속에서만 모든 관계가 이루어지기 때문에 사용자들 간의 신원을 확인해 줄 필요가 발생하였다. 따라서 이를 해결하기 위해서 PKI를 기반으로 한 전자 서명 시스템이 구축 되었다.

이렇게 구축된 PKI를 기반으로 각 사용자간에 신원 증명을 할 수 있게 되었다. 그렇지만 인터넷 서비스 제공자들이 각 사용자 별로 다른 서비스를 제공하기 시작하였고, 시스템 내의 사용자에 따라 서로 다른 리소스를 제공 하는 등 이제 사용자의 신원만 파악하는 것이 아니라 사용자의 속성을 정의하는 것이 필요하게 되었다.

본 논문에서는 사용자 속성을 정의하여, 그 속성에 따라서 사용자 별로 권한 및 역할을 관리하는 방법의 하나로 대두되고 있는 PMI(Privilege Management Infrastructure)를 살펴보고자 한다.

2. PMI 구성요소

2.1 AC (Attribute certificate)

기존의 PKC(Public-key Certificate)는 정보보호 서비스를 사용하는 사용자의 신원을 인증하는 기능을 한다. 하지만 다양한 웹 상의 서비스는 사용자 별 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 유효기간이 존재한다. 하지만 사용자 신원에 비해 사용자에게 부여 되는 권한은 더 자주 변하므로 인증서에 비해 사용자 속성의 유효기간이 더 짧다. 따라서 새로운 속성을 적용하기 위해서 이미 발급된 인증서를 폐기하고 새로운 인증서를 재발급 받아야 한다.

또, 사용자 신원은 전체에게 신뢰 받는 하나의 대리 기관에서 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 AC를 사용한다. 이는 사용자의 속성을 기록하고 인증하는 또 다른 인증서에 해당한다. 표 1은 AC에 들어갈 내용을 나타낸다.

2.2 구성 요소들

일반적인 권한 관리 모델은 객체, 권한 소유자, 권한 입증자 등으로 구성된다.

표 1. 속성 인증서(AC, Attribute Certificate)의 필드들

필드 이름	내용
Version	AC의 버전. 현재는 v2 사용
Holder	AC 소유자
Issuer	AC 발급자 (Attribute Authority)
Signature	서명에 사용된 알고리즘
SerialNumber	AC에게 부여되는 일련번호
AttrCertValidityPeriod	AC의 유효기간
Attributes	소유자에게 부여된 속성 정보
IssuerUniqueID	발급자를 구분하는 번호
Extension	차후의 확장에 대비

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 주장 되어지는 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 PKC의 확장영역에 하나의 필드로 기록된다.

권한 정책은 객체가 지닌 메소드의 보안 민감도나 사용 환경을 고려하여 각 개체에게 적합한 권한의 정도를 부여하는 방법을 제시한다. 권한 정책은 무결성과 인증 서비스가 제공되어져야 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 전달되어지게 할 수도 있다.

권한 정책은 각 서비스에 대한 권한들의 수용을 위한 경계를 제시한다. 즉 소유자가 객체에 접근하기위해 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 AC나 연관된 보안 레이블 등에 기록될 수 있다. 객체가 사용 되는 상황에 따라 메소드의 민감도는 사용되지 않을 수도 있다.

2.3 AA와 SOA

AA(Attribute Authority)와 CA(Certification Authority)는 논리적인 경우와 대부분의 물리적인 경우에서 서로 완전히 독립적이다. 신원(identity)을 만들고 유지하는 것은 PMI와 구분되어 PKI(Public Key Infrastructure)를 기반으로 이루어 진다. 그러므로 전체 PKI가 구축되고 나서 PMI를 구축하게 된다.

SOA는 일련의 권한 할당에 책임을 지는 권한 주장자에 의해서 신뢰 되어지는 개체다. SOA는 자신이 AA가 되어서 다른 개체에게 인증서를 발급하기도 하며, PKI 기반에서의 root CA와 같은 역할을 하므로, SOA로부터 서명된 인증서는 권한 입증자에게 신뢰를 준다.

3. PMI 사용 모델

AC를 이용하여 접근 제어 응용에 사용할 경우 처리해야 하는 여러 상황이 발생한다. 이를 어떻게 처리하는 지를 보여준다.

3.1 관제 모델

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

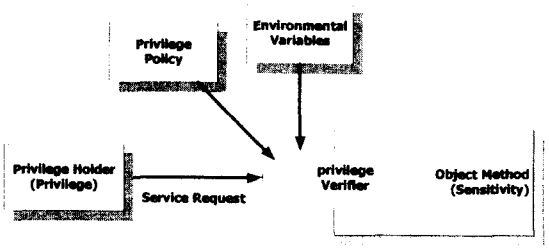

그림 1. PMI 관제 모델

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 PKC로 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 (Source of Authority), 또 다른 AA들, 권한 주장자 등이 이 모델의 구성요소가 된다.

일반적으로 SOA는 권한 소유자에게 권한을 할당하는 인증서를 발급하는 개체이지만, 이 경우에는 권한 소유자가 AA의 역할을 할 수 있도록 인증하는 역할을

한다. 이때 AA의 역할을 하는 권한 소유자는 자신이 소유한 권한의 일부나 똑 같은 권한을 가지는 인증서를 발부하여 다른 개체에게 권한을 위임한다. 이때 SOA는 위임에 경로 길이를 제한하거나 이름 공간을 제한하는 등의 제약을 둘 수 있다. 또 중간 단계의 AA는 권한을 위임 받은 권한 소유자에 의해서 일어날 수 있는 위임에서 그 소유자가 AA 역할을 할 수 있도록 인증하는 역할도 한다. 자신이 가진 권한 이상의 것은 위임할 수 없다.

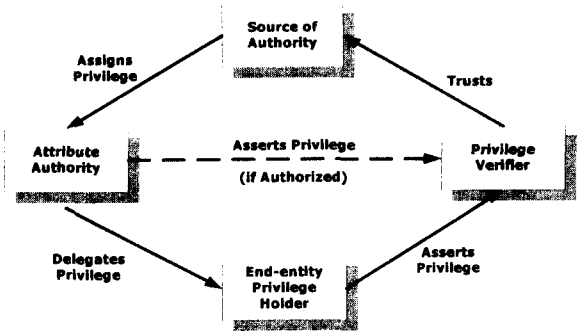

그림 2. PMI 권한 위임 모델

권한 위임이 시작되면, 권한 입증자는 자신의 권한을 위임할 SOA나 자신이 부여 받은 권한을 다른 소유자에 위임하려는 권한 소유자를 신뢰한다. 만약 권한 소유자가 발급 받은 인증서가 앞에서 신뢰한 SOA로부터 발급 받은 것이 아닌 경우에, 입증자는 그 소유자가 지닌 인증서가 어떤 SOA로부터 발급 되었는지 그 경로를 찾는다. 이 위임의 경로가 유효하다는 것은 각 AA가 적합한 권한을 지니고 있으며, 그러한 권한들이 온전하게 위임되었음을 정식으로 인증 받는 것을 나타낸다. AA나 입증자로부터 신뢰 받은 권한 소유자 만이 위임을 할 수 있고, 그렇지 않은 일반 개체들은 위임을 할 수 없다.

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 AA가 정의
- 역할 자신이나 역할의 멤버를 서로 다른 AA에 의해 각각 구분하여 정의 및 관리
- 역할의 멤버 위임 가능
- 역할이나 멤버에 적절한 수명 할당

만약 역할 할당 인증서를 AC로 하면, 역할의 속성은 AC의 attribute 영역에 포함 된다. 그러나 이 경우에는 각 권 한들이 인증 주체에는 추가적으로 할당 될 수 있어도 역할에는 추가적으로 할당 될 수 없다.

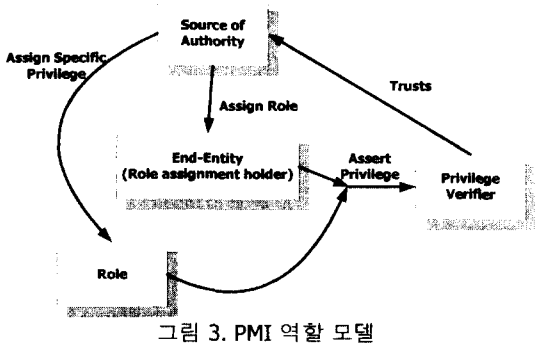

그림 3. PMI 역할 모델

역할 모델에서 권한 소유자에게는 특정 이름을 가지는 역할만을 할당 받게 되지만, 권한 입증자는 소유자가 객체에 접근하고자 할 때 접근 여부를 결정하기 위해서 그 역할에 연관되는 권한을 알고 있어야 한다.

만약 역할에 연관된 권한들을 역할 명세 인증서에 담게 되면, 그 역할과 연관된 역할 할당 인증서를 연결하기 위한 메커니즘이 필요하다. 역할 명세 인증서는 누구에게도 위임될 수 없고, 역할 명세 인증서의 발급자와 역할 할당 인증서의 발급자는 서로 달라야 한다. 그리고 그 둘은 폐기, 재발급 등등에서 완전히 다르게 관리되어 져야 한다.

4. 결론 및 향후 연구 방향

본 논문에서는 새로이 사용자 속성 정보를 관리해야 할 필요성과 기존에 사용하던 PKI를 기반의 확장 영역을 사용할 경우의 단점과 그에 따른 새로운 방식인 속성 인증서를 사용하는 PMI에 대해서 서술하였다.

기존에 사용하던 X.509의 확장영역으로 사용자 속성 정보를 정의하고 관리할 경우, 현재 대두하고 있는 사용자 속성 정보를 관리하는데 한계가 발생하게 된다. 따라서 이런 문제를 해결하기 위해서 기존 인증서와 구분되는 새로운 속성 인증서를 도입해서 사용자 속성을 정의하고 관리해야 한다.

앞으로는 이 PMI 기반의 속성 인증서를 실제 인터넷에 사용되고 있는 서비스에서 어떻게 적용할 수 있을지에 대해서 연구를 해 보고자 한다.

5. 참고 문헌

[1] ITU-T , Draft ITU-T RECOMMENDATION X.509 version 4, 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] Chadwick, D., Legg, S., Internet X.509 Public Key Infrastructure Additional LDAP Schema for PKIs and PMIs, 2000. 8