기존 인증서를 통한 PMI 연구

김건배*, 배두현*, 박세현*, 송오영*

*중앙대학교, 전자전기공학부

A Study of PMI based on Established Certificate

Keon Bae Kim*, Du Hyun Bae*, Se Hyun Park*, Oh Young Song*

*Chung-Ang Univ, School of Electrical & Electronics Engineering

요 약

본 논문은 PKC(Public Key Certificate)를 이용하여 Privilege Management를 제공하는 모델에 대해 다룬다. 권한관리는 PKC와 AC(Attribute Certificate)를 이용한 PMI가 제시되고 있으나, PMI를 구축하기 위한 비용이 들게 된다. 본 논문에서는 현재 구성되고 있는 PMI 모델과 본 논문에서 제시한 PSL(Privilege Status List)를 이용한 권한 관리 모델을 비교, 분석한다.

I. 서론

인터넷을 통한 E-mail이나 전자상거래, 중요 데이터의 전송이 많아지면서, 네트워크를 통한 정보의 암호화가 중요하게 되었다. 이러한 정보의 보호를 위해서 많은 연구가 시도되었으며, 최근에는 데이터의 암호화, 무결성, 전자서명, 부인방지 등을 제공하는 PKI(Public Key Infrastructure)에 대한 고려가 활발히 진행되고 있다.

그러나 이러한 정보보호 뿐 만 아니라, 정보에 대한 권한관리가 필요하다. 예를 들면 어떤 정보를 사용자가 요구했을 때 그 사용자가 그 정보를 요구할 자격이 있는지에 대한 그 사용자의 권한을 확인하는 작업이 필요하다. PKI를 이용하여 그 certificate의 소유자에 대한 권한을 나타내려 하였다. 그러나 공개키의 발급주체와 권한을 주는 주체가 서로 달라야하고, 공개키 인증서의 유효기간의 주기와 권한의 유효기간의 주기가 서로 다른 경우가 많으므로, PKI만을 이용한 권한부여/관리는 실제로 활용하기에는 무리가 있다. 그래서 제안된 것이 attribute certificate(AC)를 이용한 권한부여/관리이다.

Public Key Certificate를 통하여 Certificate Owner에 대한 identification을 하고, PKC와 AC를 연계시킴으로서 그 Certificate의 소유자에 대한 권한은 AC를 통하여 나타내게 된다. 이렇게 하여 위에 나열한 PKC만을 이용한 Privilege Management의 단점을 보안할 수 있다. 그러나, PKI와 같이 사용자의 속성에 대한 정보를 AA(Attribute Authority)에 넘겨주는 것은 기업의 입장에서 보면 그 기업의 인적정보라던가, 권한에 대한 여러 가지 정보를 넘겨주는 것이나 다름이 없으므로, 보통 AA는 PKI처럼 CA라는 공인인증기관에 PKC를 요구하는 것이 아니라, 사설 AA를 만들어 운영하는 것이 훨씬 바람직하다.

이와 같은 이유로 인해 기업은 PMI를 위해 AA를 따로 운영해야하는 부담과 함께, AC를 저장하기 위한 DB가 필요하게 된다. 또한 AC에 대한 CRL을 발행하고, 관리해야하는 부담이 있다. 또한 AC가 배포되고, network 상을 돌아다님으로서, AC 사용자의 권한정보의 유출이 용이해져서, 정보유출방지에 대한 고려도 필요하다.

이 논문에서는 위와 같이 새로운 Attribute Certificate를 이용하지 말고, 기존에 사용하던 PKC를 그대로 이용하고, target system에 대한 PKC의 권한을 기술한 Privilege Status List(PSL)를 만들어서 PMI를 구현할 수 있는 방법을 제시해 보고자 한다. 즉 사용자에 대한 인증은 PKC를 통해서 이루어지고, 그 PKC의 target system에 대한 권한부여 및 관리는 PSL을 통해서 이루어지는 모델을 제시할 것이다.

다음 장에서 보게될 내용으로 한 기업 내에서 기존의 certificate를 이용하여 PMI를 구축하는 모델을 예를 들어 설명할 것이다.

II. 구성요소

1) CA

Certificate에 대한 발행 및 관리를 하는 CA가 필요하다. 이 CA는 외부의 공인인증기관이 될 수도 있고, 기업내에 사설 CA가 될 수도 있다. 각 사용자의 Certificate를 발행하고, CRL을 발행한다. 그리고 PMS의 Certificate를 발행한다.

2) Repository

CA가 발행한 Certificate와 CRL의 저장장소이다.

3) Privilege Management Server(PMS)

각 Certificate의 소유자에 대한 Privilege를 관리하는 server 이다. certificate가 PMS에 등록이 되면 PMS는 등록된 certificate에 대한 권한을 설정하게 된다. 그리고 그 권한에 대한 Privilege Status List(PSL)를 발행하게 된다.

4) Privilege Status List(PSL)

Privilege Status List는 Target System에 대해서 각각 작성되며, 이것은 Certificate가 Target System에 대해 어떤 권한이 있는지를 나타내는 list가 되겠다. CRL은 폐기된 인증서의 목록인 반면, PSL은 Target System에 권한이 있는 목록과 어떤 권한이 있는지를 나타내는 것이므로, CRL과는 반대이다. 즉 PSL에 나타나지 않은 Certificate는 그 PSL에 해당하는 시스템에 대해서는 아무런 권한이 없다는 것이다. PSL은 PMS의 Certificate로 Sign되고, 발행된다. PSL의 구성은 아래와 같다.

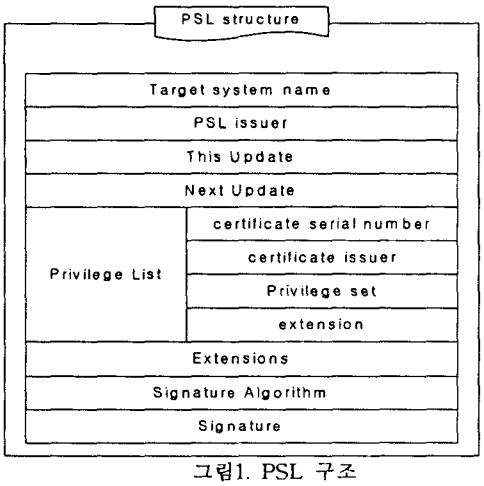

그림1. PSL 구조

Target System Name 은 Target System에 대한 고유이름을 말한다. PSL issuer 필드는 PSL을 발행하는 issuer의 DN이 들어가게 된다. Privilege List 필드는 Target System 에 대한 권한을 가지고 있는 인증서의 목록과 해당 권한에 대한 내용을 담고 있다. 인증서의 Serial Number와 인증서 발행자의 이름과 해당 인증서의 권한 목록과 추가될 확장영역이 있다. Signature Algorithm 필드는 PSL을 PSM이 서명할 때 사용한 알고리듬이 들어가게 되고, Signature 부분은 서명한 값이 들어가게 된다.

III. 모델링

한 기업의 사원이 들어오면 그 사원에 대한 인증서가 나오고, 또한 사원에 대한 권한이 부여되게 된다. PMS 관리자는 그 사원에 대한 인증서와 함께 인증서의 소유자에 대한 권한을 PMS에 등록하게 된다. PMS는 등록된 인증서에 대한 권한을 확인하여 해당 System의 PSL을 Update 한다. 인증서 소유자는 Target System에 access 하여 자신의 Certificate 요구권한을 Sign하여 보내면, Target System은 Certificate에 대한 검증과 클라이언트의 서명을 검증하고, 자신의 System에 해당하는 PSL을 보고 이 클라이언트가 요구하는 권한이 받아들일 수 있는 것인지 확인하게 된다.

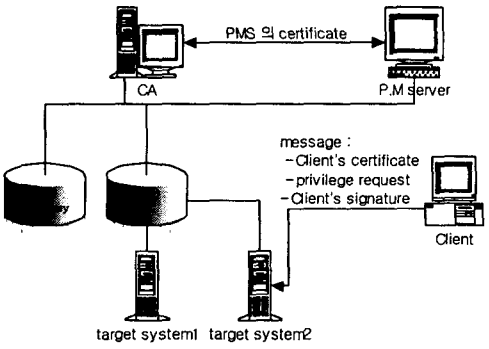

그림2. PSL 모델링

Target System은 client의 인증서에 대한 경로검증을 해야하고, 또한 client의 서명을 검증해야한다. 그리고 PSL에 대한 검증과 함께 권한 목록에서 client가 요구한 권한이 부여 가능한 것인지 살펴 봐야하기 때문에 target system에서의 network overhead와 system 성능이 떨어질 수 있다. 그리고 각각의 Target System들이 모두 위와 같은 검증 모듈과 처리모듈이 필요하게 된다. 그러나 client의 message에 대한 검증을 PMS server에 맡기고, PMS server에서의 응답을 통해서 권한 부여여부를 알게 된다면 각 Target System에서의 검증과정과 PSL 처리과정에서 생기는 overhead를 줄일 수 있게 된다. 다음 그림에서 보면 client의 request message를 받은 Target System은 받은 request message를 PMS에 보내게 되고 PMS에서 client 인증서 검증과 PSL 처리를 하여 Target System에 응답을 보내게 된다. target system은 응답을 받아서 client의 요구를 받아들일지 결정하게 된다. 이와 같이 PMS는 Target System에 대한 PSL을 발행하고, client의 Target System에 대한 권한 요구에 대한 검증을 비해줌으로써, client에 대한 권한 관리를 할 수 있게 된다.

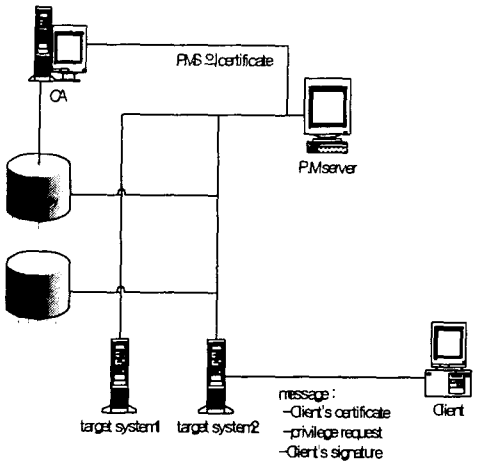

그림3. PSL 처리과정

IV. AC vs PSL

1) 권한변경

AC를 이용한 PMI에서는 PKC 소유자의 권한이 바뀌게 되면, 발행된 AC를 폐기하고 새로운 AC를 발행하여야 한다. 또한 PKC가 update되면 그에 따른 AC도 Update되어야한다. PSL을 이용한 PMI에서는 권한부여/변경이 훨씬 용이하다. 권한이 변경되었을 경우, 단지 PSL만 갱신해주면 되기 때문이다.

2) 확장성

Target System이 늘어날 경우에 AC를 새로 발행하여야 하는데 반해, PSL을 이용하면 새로운 Target System에 대한 PSL만 작성하면 되기 때문에 scalability 측면에서도 좋다.

3) 권한정보의 유출

AC를 이용한 PMI에서는 AC를 통한 PKC 소유자의 권한정보가 유출될 수 있다. PSL을 이용하면 이런 권한 정보의 유출을 막을 수 있다. PSL에 접속하는 것은 단지 PMS server와 Target System 뿐이므로, PSL의 저장소를 PMS server와 Target System만이 접속하도록 하면 권한정보의 유출을 AC를 사용할 때보다 줄일 수 있다. 그러나 PSL을 악의적 사용자가 획득하게 된다면, Target System에 대한 권한이 있는 모든 사용자의 정보를 알 수 있게 되므로, PSL을 안전한 곳에 저장해야 하겠다.

4) 기업간 co-work으로 인한 연동

기업 간 협력으로 인해 다른 domain의 client에 대한 권한을 부여할 때, AC를 이용하게 된다면, client에 대해 새로운 AC를 부여해야만 한다. 그러나, PSL을 이용하면 그 client에 대한 Certificate를 등록하고 PSL을 업데이트 해주면 되기 때문에 연동도 훨씬 쉬워지게 되고, 권한 부여/박탈의 관리가 용이해진다.

5) PSL의 크기와 처리시간

PSL에서 Target System에 대한 권한이 있는 사용자가 늘어나게 되면, PSL의 크기가 증가하게 된다. PSL에 대한 sign과 검증, PSL을 참조하여 권한부여여부를 결정하는 데도 그만큼 시간이 늘어나게 된다. PSL의 크기를 줄이기 위해서 PSL을 client의 Certificate나 정책을 통해 나누어서 작성해야 한다.

V. 결론

Client 에 대한 Identity는 기존의 client의 certificate를 통해서 이루어지고, certificate owner에 대한 권한 관리는 PSL을 통해 가능하다. 그리고 외부 사용자가 내부 네트워크가 데이터베이스에 접근을 위해서 새로이 AC를 받는 것이 아니고, 자신이 자기고 있던 certificate를 PM server에 등록하고, PM server로부터 권한을 부여받으므로 확장성이 좋아진다. 권한 정보의 유출도 AC를 이용할 때보다 안전하게 되고, 권한에 대한 management도 용이해진다. target system에 대한 권한이 있는 사용자가 늘어나게 되면, PSL의 크기가 증가하게 되므로, 그에 따른 처리시간이 늘어나게 되는 단점이 있다. 이것은 PSL의 분산을 통해 약점을 보안할 수 있다.

참고문헌

[1] Russ Housley and Tim Polk, Planning for PKI, Wiley, 2001.

[2] Andrew Hash and William Duane and Celia Joseph and Derek Brink, PKI:Implementing and Managing E-Security, McGraw-Hill, 2001

[3] R. Housley and W. Ford and W. Polk and D. Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC2459, 1999

[4] S. Farrell and R. Housley, An Internet Attribute Certificate Profile for Authorization, RFC 3281, 2002