E-PMI의 소개

김희선[0] 조상래 조영섭 진승헌
한국전자통신연구원
(sezsez[0], sangrae, yscho, jinsh)@etri.re.kr

Introduction of ETRI Privilege Management Infrastructure

Heesun Kim[0] Sangrae Cho Yeongsub Cho Seunghun Jin
Electronic and Telecommunication Research Institute

요 약

권한관리 기반구조(PMI)는 사용자의 권한 속성을 관리하기 위한 인프라로서 인가서비스를 제공한다. 전자상거래의 활성화와 더불어 인증, 기밀성, 무결성, 부인 방지 등의 보안 서비스의 필요성은 이미 중요하게 부각되어 왔다. 공개키 암호 기술은 이러한 보안 서비스의 제공에 핵심이 되었고, 이를 지원하기 위한 공개키 기반구조(PKI)가 주요 인프라로 제시되었다. 특히, 응용들에게 있어서 PKI는 인증서비스를 위한 필수 요소가 되었다. 그러나, 보안 서비스로서 사용자들의 권한인가에 대한 인가 서비스의 중요성이 증가함에 따라 권한 관리에 대한 연구가 활발해져 오고 있다. 이에 대한 해결방안으로 제시되고 있는 PMI 솔루션은 이미 네트웍상의 보안서비스를 위한 필수 요소로 인식되고 있다. 본 논문은 이러한 PMI 구축의 실례로서 ETRI에서 개발하고 있는 E-PMI를 소개한다.

1. 서 론

인터넷 응용 기술의 발전은 다양한 컨텐츠의 제공을 가져왔고, 고부가가치의 정보를 다루는 일이 증가함에 따라, 서비스를 위해 제공되는 리소스에 대한 접근 가능성, 즉 권한 확인에 대한 요구가 큰 관심사가 되어가고 있다. 이에 대한 해결방안의 하나로 권한관리 기반구조(Privilege Management Infrastructure : PMI)라는 개념이 등장하게 되었다.

PMI는 하나의 조직 혹은 여러 유사한 속성들을 지니는 응용환경들에게 있어서 리소스들에 대한 사용자의 권한 속성을 통합 관리하여 줌으로써, 응용들에 대해서는 권한 관리의 효율성과 리소스에 대한 안전한 관리를, 사용자들에게 있어서는 프라이버시 정보들의 안전한 관리를 제공하여 준다.

ETRI에서는 이와 같은 권한 관리 솔루션으로서 E-PMI를 개발 중에 있다. 이를 통해, 응용과 사용자들에게 효율적인 권한 인가 및 관리 서비스를 제공하고자 한다. 본 논문에서는 E-PMI의 구조 및 개괄적인 운영 시나리오를 통해 E-PMI를 소개하고자 한다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 PMI의 개요와 속성 인증서의 개념 및 필요성에 관하여 설명한다. 3장에서는 E-PMI의 구성 및 운영 시나리오를 소개하고, 4장에서 결론을 맺도록 한다.

2. PMI 개요

최근 인가 서비스는 인증 서비스와 함께 중요한 보안 요구사항으로 인식되고 있다. 여러가지 서비스를 제공하는 응용들에게 기존에는 서비스에 접근하고자 하는 사용자들이 누구인가의 문제, 즉 사용자를 인증하는 문제가 중요하게 인식되었다. 그러나, 리소스에 대해서 어떠한 접근 권한을 가지는 지에 대한 문제가 인증 못지않게 중요하게 인식되면서 이러한 권한을 보다 신뢰성 있고, 체계적으로 통합 관리하는 것에 관심을 기울이게 되었다. 즉, 권한 판단을 위한 데이타의 효율적인 관리 체계를 요구하게 되었다. PMI는 이에 대한 해결방안으로서 제시된 개념이다.

현재 PMI는 IETF와 ITU-T에서 표준화가 추진 중이며, 최근, 이러한 노력의 일환으로 RFC3281가 발표되었다 [1, 2].

2.1 AC의 개념

PMI의 핵심이라고도 불리우는 X.509 속성 인증서 (Attribute Certificate : AC)는 권한 속성을 관리하기 위한 구성요소로서, 사용자와 권한 속성을 AA(Attribute Authority)의 서명으로 바인딩하는 데이타 포맷이다. 반면에 같은 X.509 기반의 공개키 인증서 (Public Key Certificate : PKC)는 사용자와 공개키를 CA (Certification Authority)의 서명으로 바인딩한 구조를 지닌다.

X.509 기반의 인증서를 이용하여 권한 속성을 관리한다는 것은 단순한 속성 관리 수단 이외의 의미를 갖는다. 이는 속성 소유자와 그가 지닌 속성 간의 관계를 신뢰받는 인증기관의 서명으로 신뢰성을 보장한다는 것에 그 의의가 있다고 할 수 있다. X.509 PKC에서는 확장 필드를 이용하여 속성 정보를 저장할 수 있도록 지원하고 있다. 그러나, PKC를 이용하여 권한 속성을 관리하는 것은 공개키와 속성 정보의 서로 다른 lifetime으로 인해 잦은 인증서 폐기 문제를 야기시킬 수 있다. 그리고, 다수의 속성 정보를 위해 공개키를 여러 번 발급하지 않는다면 하나의 인증서에 여러 속성 정보를 저장하도록 해야 한다. 이것은 프라이버시 정보의 침해 가능성을 낳게 한다. 또한, 공개키와 속성 정보를 다루는 인증기관이 상이하다는 문제점을 갖는다. 따라서 X.509 AC를 도입하여 권한 관리 기능을 수행하려는 의견이 보다 설득력있게 제시된 것이다.

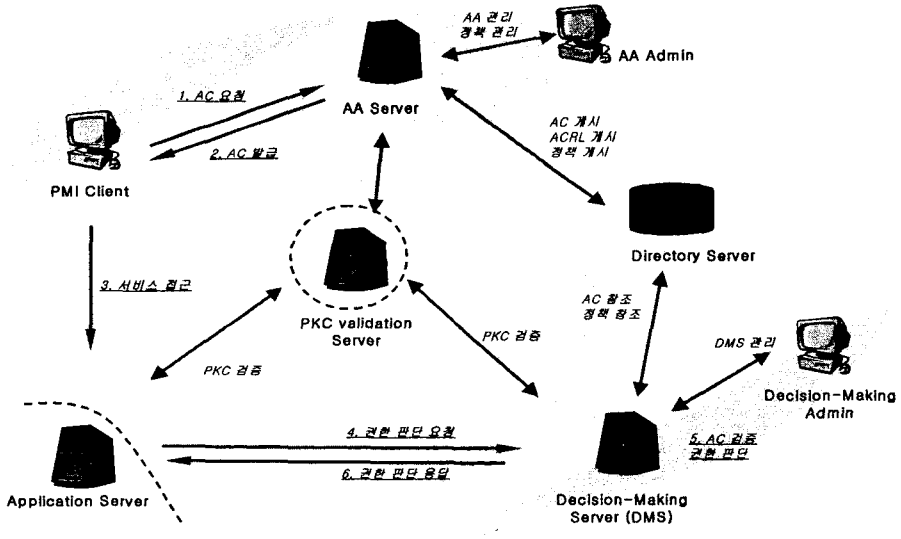
3. E-PMI 구성 및 운영 시나리오

이러한 PMI에 대한 연구의 한 실례로서 ETRI에서는 E-PMI (ETRI PMI)를 개발 중에 있다. 본 절에서는 E-PMI의 구조와 운영 시나리오에 관하여 간략히 소개하고자 한다.

3.1 E-PMI 구조

PMI는 기본적으로 권한 인가자, 권한 주체(주장자), 권한 검증자로 구성되어 있다. 권한 인가자는 일반적으로 AA가 되며, 권한 주체는 권한 속성을 인가받는 사용자들, 권한 검증자는 보호할 리소스에 대한 사용자들의 권한을 검증해 주는 주체를 말한다. 이를 기반으로 구성된 E-PMI의 구조는 [그림 1]과 같다. 사용자에게 권한을 부여하고 AC를 발행하기 위한 AA server, 권한 속성을 인가받고 이에 대한 AC를 소유하는 PMI client, AC를 검증하기 위한 Decision-Making Server, AC를 관리하기 위한 Directory server가 있다. E-PMI는 속성 인증서를 다루기 위해 이용되는 공개키 인증서의 검증을 위해 공개키 인증서 검증 서버 (PKC validation server)를 이용하여 검증 대행을 수행하도록 구성하고 있으며, 권한 관리의 대상이 되는 응용과 연동하여 운영된다 [3, 4].

E-PMI에서는 PMI client의 권한 속성을 X.509 AC를 이용하여 관리한다.



[그림 1] ETRI PMI 구조도

3.2 E-PMI의 권한관리 시나리오

앞의 [그림 1]과 같이 구성된 E-PMI는 다음과 같은 시나리오로 동작된다. E-PMI는 Push/Pull model을 모두 지원하나 본 절에서는 Push model를 기준으로 설명하도록 한다.

1) AC 요청

PMI client는 AA server에게 자신의 권한에 대한 AC를 요청한다. Client는 PKC를 이용하여 AA server에게 자신을 인증한다 (ID/Password를 이용한 인증도 지원).

2) AC 발행

AA server는 PMI client를 인증하고, 요청에 따라 X.509 AC를 발행하여, client에게만 속성 인증서를 전달한다.

3) 리소스 접근

PMI client는 Application server의 서비스를 이용하기 위해 자신의 AC와 함께 서비스를 요청한다.

4) AC 검증 요청

Application server는 서비스를 요청한 client를 인증한다. 그리고, client의 서비스 이용에 대한 권한을 체크하기 위해, Decision-Making server에게 AC을 전달하여 검증을 요청한다.

5) 권한검증 및 리소스 접근 허용

Decision-Making server는 AC의 유효성을 검증하고, 속성 정보를 통해 client가 요청한 서비스를 이용할 자격이 있는지의 권한 체크를 수행한다. 이에 따라, Decision-Making server는 Application server에게 서비스 요청 허용 여부에 대한 응답을 보내준다(허용/거부).

6) 권한 검증 결과에 따른 서비스 제공

Application server는 Decision-Making server의 응답에 따라 client에게 요청된 서비스를 제공하거나 혹은 거부한다.

4. 결론

지금까지 권한 관리 기능을 제공하는 E-PMI의 구조 및 운영 시나리오에 대하여 간략히 살펴보았다. E-PMI는 AA server, PMI client, Decision-Making server로 구성되어 있으며, X.509 AC를 이용하여 PMI client의 응용 환경 리소스에 대한 권한 관리를 수행하여 준다.

현재 PMI에 대한 연구가 매우 활발히 진행중이며, 많은 업체들이 개발에 뛰어들고 있다. 대부분의 보안 솔루션이 그렇지만, 특히 PMI는 PMI 자체로서는 어떠한 의미를 가지기 힘들다. 권한 속성들이 체계적으로 관리될 필요가 있는 적합한 응용에 PMI를 활용하는 것이 무엇보다 중요하다고 할 수 있다. 또한, 그러한 적절한 응용에 PMI를 이용하여 인가 서비스를 잘 제공한다고 하더라도, 인가 서비스 단독으로는 진정한 보안 서비스의 제공은 불가능하다. 이는 인가를 포함한 여러가지 보안 요구사항들을 함께 만족시킴으로서 얻어질 수 있는 것임을 명심해야 한다.

참고문헌

[1] ITU-T Recommendation X.509 | ISO/IEC 9594-8 : "Information Technology - Open Systems Interconnection - The Directory Public-Key and Attribute Certificate Frameworks", Draft ISO/IEC 9495-8, May 3, 2001

[2] S. Farrell, R. Housley, "An Internet Attribute Certificate Profile for Authorization", RFC 3281, April 2002

[3] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, June 1999

[4] 노종혁 김태성 최대선 진승헌 정교일, "Collaborative VA 모델", 제 28 회 한국정보과학회 추계학술발표회, 2001.