PMI 기반의 메시지 중계시스템에 관한 설계

채송화*, 이상하**, 김동규*

*아주대학교, 정보통신공학과, **동서울대학, 정보통신공학과

Design of Messaging Hub based on PMI

Song-Hwa Chae*, Sang-Ha Yi**, Dong-Kyu Kim*

*Department of Information Communication Engineering Ajou University.

**Department of Information Communication Engineering DongSeoul College.

요 약

엔터프라이즈 환경에서 데이터의 교환을 위해 메시지중계시스템을 사용하고 있다. 그러나, 현재 사용하고 있는 메시지중계시스템 자체에는 정보보호서비스가 적용된 예가 많지 않으며 일부 적용된 경우에도 접근제어 서비스를 제공하고 있지 못하다. 본 논문에서 제안하는 PMI(Privilege Management Infrastructure)기반의 메시지중계시스템은 기존의 구축되어 있는 PKI(Public Key Infrastructure)를 이용하여 정보보호서비스의 인증, 무결성, 기밀성, 부인방지 서비스를 제공하며 PMI을 적용하여 접근제어 서비스를 제공한다. PMI의 속성인증서를 사용하여 실시간적으로 변하는 접근제어 정보의 변화를 수용하며 SOA(Sorce of Authority)를 통해 중앙에서 접근제어정보를 관리한다. 교환되는 데이터는 S/MIME을 기본으로 하여 국제표준을 따르며 S/MIME의 보안 레이블을 이용 데이터의 변경없이 접근제어 정보를 전송할 수 있도록 하였다.

I. 서론

인터넷의 발달은 기업이나 조직에 정보화를 가져왔으며 이에 따라 종이로 이루어지던 모든 업무가 전자문서로 대체 되었다. 문서를 네트워크를 통해 전송하게 됨에 따라 전송하는 데이터에 대한 비밀성, 무결성, 접근 제어 등 정보보호서비스의 요구가 대두되었다. 특히, 일대일 통신이 아닌 일대다 통신인 경우에는 접근 제어가 필수적이다.

본 논문은 이러한 엔터프라이즈 환경에서 데이터 전송시 보안과 접근제어를 제공하고 중앙에서 접근 제어 정책을 관리할 수 있는 메시지 중계시스템을 제안하고자 한다.

II. 메시지 중계 시스템

1. 필요성 및 요구사항

엔터프라이즈 환경에서 데이터를 교환하기 위해서는 메시지 중계 시스템을 통해야 한다. 대표적인 메시징프로토콜은 SMTP를 들 수 있다. 엔터프라이즈 환경에서 교환되는 데이터의 무결성 및 비밀성 서비스를 제공하기 위해서는 암호와 전자서명을 이용할 수 있다. 그러나, 암호와 전자서명은 단순히 교환되는 데이터의 수신자 확인과 데이터가 변조되지 않고 유출되지 않도록 할뿐이다.

데이터 교환의 중요한 이슈는 데이터를 전송하고자 하는 개체가 그 데이터를 전송할 수 있는지에 관한 전송 권한의 소유 여부, 수신하는 개체가 수신할 수 있는지에 관한 수신권한의 소유 여부를 확인하고 적절한 서비스를 제공하는 접근제어이다. 접근제어서비스를 제공하기 위해서는 조직내부에서 접근제어에 필요한 권한, 주체, 객체를 정의하고 운영하여야한다. 따라서, 접근제어를 위한 중앙관리가 필수적이라 할 수 있겠다.

현재 제시되고 구현되어 있는 메시지 교환 서비스의 경우 PKI, S/MIME[4] 등을 적용하여 보안 서비스를 제공하고 있으나 중앙관리의 접근 제

어를 제공하고 있지 못하다. S/MIME[3][4]의 경우 버전3 의 보안 레이블을 이용하여 접근제어를 구현할 수 있으나 송신자가 모두 설정하도록 되어있어 중앙관리를 할 수 없다.

2. 설계 시 고려 사항

메시지중계시스템을 설계하기 위해서는 다음을 고려해야한다. 첫째, 메시지중계시스템을 이용하는 도메인내의 모든 개체에 대해 동일한 접근제어 정책을 제공하고 운영할 수 있어야한다. 둘째, 송신자와 수신자의 권한에 따른 적절한 접근제어를 제공하여야한다. 셋째, 실시간으로 변화하는 접근제어 정책을 바로 적용하고 운영할 수 있어야한다. 엔터프라이즈 환경에서 주체, 객체, 권한은 늘 추가되거나 삭제될 수 있으며 이에 따른 변화를 실시간으로 적용하여 원치 않는 정책 위반이 일어나지 않도록 해야 한다. 넷째, 메시지 재생성에 따른 보안문제를 해결할 수 있어야 한다. 메일링리스트를 이용하여 메시지를 전송할 경우 메시지중계시스템은 송신자가 전송한 메시지를 재가공하여 리스트의 사용자들에게 전송하게 된다. 따라서, 메시지 재생성시 메시지의 비밀성, 무결성을 제공하여야 한다. 다섯째, 전송하는 메시지가 표준을 따라야한다. 여섯째, 메시지중계시스템이 보안을 위해 사용하는 키에 대한 관리 기능을 가져야 한다.

III. PMI기반의 메시지 중계 시스템

본 논문에서 제시하는 메시지중계시스템은 비밀성 및 무결성 서비스를 위해 PKI를 기반으로 하며 접근제어 서비스를 위해 PMI를 기반으로 한다. 또한 메시지의 표준 규약으로 S/MIME을 채택하였다. 통신에 관여하는 각 개체는 다음과 같으며 개략적 구성은 [그림 1]과 같다.

- 인증기관: 인증서를 발급하는 신뢰성 있는 기관
- SOA : 속성인증서를 발급하고 접근제어 정책을 관리하는 기관
- 메시지중계시스템 : 접근제어 정책에 따라 도메인내의 메시지를 중계하는 시스템
- 주체 : 도메인내의 모든 서비스 요청자, 사람, 시스템 등
- 객체 : 도메인내의 모든 데이터와 서비스

1. PKI기반의 인증서비스

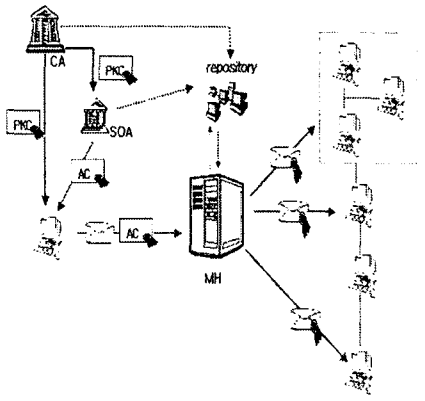

그림 1 : PMI기반의 메시지 중계시스템 구성도

도메인내의 각 주체가 메시지전송을 위해서는 우선 인증을 받아야한다. 인증서비스를 제공하는 매커니즘은 여러 가지가 있지만 신뢰성 있고 손쉬운 구현을 제공하는 방법은 PKI를 이용하는 것이다. PKI기반의 인증서비스를 제공하면 인증서를 사용함으로써 사용자의 공개키에 대한 신뢰성을 얻을 수 있다.

각 사용자는 자신의 공개키를 생성한 뒤 인증기관으로부터 공개키인증서를 발급 받아야 하며 사용자뿐만 아니라 메시지중계시스템도 공개키쌍을 생성하고 인증서를 발급 받아 사용한다. 메시지중계시스템에서 메시지 재생성시 전자서명을 사용하며 재생성된 메시지의 무결성과 기밀성 서비스를 제공할 수 있다.

2. PMI기반의 접근제어 서비스

제안하는 메시지중계시스템의 주요 기능은 실시간 접근제어 변화를 적용하며 중앙관리를 하는 것이다. 접근제어를 구현하는 방법은 여러 가지가 있지만 제안 시스템은 PMI[1][2]를 적용하였다.

일반적인 접근제어 기능을 구현하기 위해서는 중앙에 접근제어 정보를 가지고 있는 서버를 이용 트랙잭션마다 서버에 질의를 하거나 각 검증자가 접근제어정보를 가지고 판단을 하여야 한다. 그러나, 이러한 방식을 취하면 접근제어 서버에 통신이 집중된다. 그러나, PMI를 적용함으로써 권한의 변화를 쉽게 대응할 수 있다.

PMI는 기존 PKI가 인증서비스에 중점을 둔 것

에 반해 접근제어서비스를 제공하기 위해 제안된 기반구조이다. 이 구조는 단독적으로 운영되지 않으며 PKI와 함께 운영된다. PKI가 공개키정보를 공개키인증서에 담아 이용하는 것과 마찬가지로 PMI는 속성인증서에 접근제어 정보를 담아 접근제어서비스에 이용하도록 하고 있다.

도메인내에서 주체와 객체, 권한의 변화가 일어나면 속성인증서를 SOA에서 재발급하여 권한의 변화를 반영한다. 주체, 객체, 권한이 새롭게 생성되거나 삭제, 중지 등을 모두 적용할 수 있다.

각 사용자는 SOA에서 자신의 권한을 표기한 속성인증서를 발급 받고 사용자는 메시지전송시 속성인증서를 함께 보내어 메시지중계시스템이 권한을 검증하도록 한다. 검증이 올바로 이루어지면 메시지중계시스템은 접근제어 정책에 맞는 S/MIME의 보안레이블을 설정하여 메시지를 재전송한다.

3. 속성인증서와 보안 레이블 매커니즘

사용자가 전송한 속성인증서는 속성값을 사용하는 도메인의 접근제어 정책에 따라 역할, 그룹정보, ID등을 표기한다. S/MIME의 보안 레이블은 X.411의 표기에 따라 메시지 구조가 정의되었다.

속성인증서와 보안 레이블은 속성값을 표기하는 방법이 거의 비슷하여 변환에 큰 무리가 없다. 예를 들면 속성인증서의 보안 등급 ASN.1 표기는 다음과 같다.

```
ClassList::=BIT STRING{
        unmarked (0),
        unclassified (1),
        restricted(2),
        confidential(3),
        secret(4),
        topSecret(5)
}
```

S/MIME 보안 레이블의 경우는 아래와 같다.

```
SecurityClassification::=INTEGER{
        unmarked (0),
        unclassified (1),
        restricted(2),
        confidential(3),
        secret(4),
        topSecret(5)
}
```

예제의 경우는 데이터 구조가 비슷하여 특별한 논리적 변환 없이 바로 사용할 수 있다. 그러나, 모든 경우에 동일한 구조가 정의되어 있는 것은 아니며 도메인 환경에 맞게 속성을 정의하여 사용하는 경우 메시지중계시스템은 미리 정의된 변환 규칙에 따라 재전송하는 메시지에 대하여 보안 레이블링을 하여야한다.

보안 레이블링을 하여 메시지를 전송 할 때 보안성을 위하여 메시지중계시스템은 사용자가 보낸 메일을 열어보지 않고 보안 레이블 정보를 추가하여 서명하여 전송한다.

메시지중계시스템은 사용자의 임의적인 접근제어 정책에 따라 보안 레이블링을 하지 않고 SOA에서 정한 접근 제어 정책에 기반하여 보안 레이블링을 하게 된다. 따라서, SOA의 접근 제어 정책을 실시간으로 반영할 있으며 접근제어 정책에 대한 중앙관리가 가능한다. 또한, 속성인증서를 사용함으로서 접근 제어 정책을 직접 저장/관리하지 않는다.

4. S/MIME

안전한 메시지 전송과 표준화된 메시지 규약을 따르기 위해 본 메시지중계시스템은 S/MIME을 이용한다. S/MIME은 인터넷에서 사용하는 전자메일의 데이터 부분을 정의하는 MIME에 보안서비스를 추가한 프로토콜이다. 그러나, 전자 메일외에 MIME타입의 객체를 전송할 수 있는 모든 프로토콜에서 사용할 수 있다.

S/MIME 버전3 의 경우 보안 레이블을 두어 접근제어를 할 수 있도록 하였다.

5. 구조

제안하는 메시지 중계시스템의 구조는 [그림2]와 같다.

- 메시지 라우터 : 메시지 교환 모듈
- 인증서 검증 : 공개키인증서와 속성인증서 검증 모듈
- 인증서 및 키관리 : 메시지중계시스템의 공개키인증서 및 개인키 관리 모듈

- 변환기 : 속성인증서의 접근제어 정보를 S/MIME의 보안 레이블로 변화하는 모듈
- S/MIME : S/MIME 모듈
- 정보보호서비스 : 인증, 기밀성, 무결성, 부인방지를 위한 서비스 제공 모듈
- 인터페이스(I/F) : 각 외부 개체(디렉토리, 인증기관, SOA, 어플리케이션 등)와의 통신 인터페이스

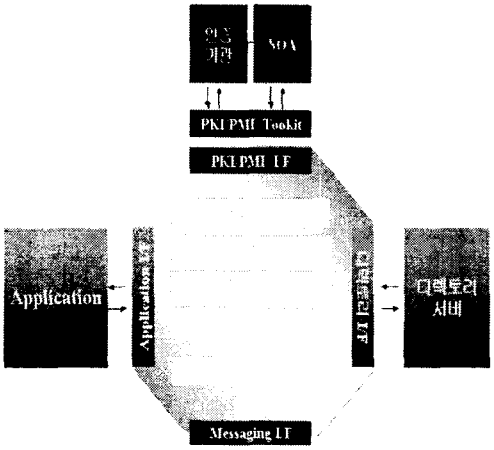

그림 2 .메시지중계시스템 구조

IV.결론 및 향후 연구과제

엔터프라이즈 환경에서 데이터의 교환 시 기밀성, 무결성, 인증, 부인방지, 접근제어의 정보보호 서비스의 제공이 필수적이다. 이러한 정보보호서비스를 제공하는 방법은 각 서비스 참여 주체에 프로그램을 새롭게 설치하고 제어할 수 있는 중앙 서버를 둘 수 있다. 그러나, 이러한 경우 실시간으로 변하는 접근제어 정보를 반영하고 운영하기가 쉽지 않으며 사용자에게 많은 부분을 부담 지워야 한다.

그러나, PMI의 기반의 S/MIME을 이용한 메지 중계시스템을 사용하고 기존의 구축된 PKI를 활용하여 정보보호서비스를 제공할 수 있다. 또한, SOA에서 접근제어 정보를 관리함으로써 중앙관리와 속성인증서를 이용 실시간 접근제어 정보의 반영이 가능하다. 현재 보안 메일 표준 규약인 S/MIME을 사용하여 향후 EAI(Enterprise Application Integration)/EIP(Enterprise Information Portal)등으로 확장이 용이하다.

향후 본 메시지중계시스템의 활용화를 위해서 속성인증서의 속성정보와 S/MIME의 보안 레이블의 연관관계에 대한 세분화된 연구와 아직 표준화되지 못한 PMI의 모델에 대한 연구가 필요하다.

참고문헌

[1] Draft revised ITU-T recommendation X.509 | ISO/IEC 9594-8 Information Technology The Directory: Public Key and Attribute Certificate Frameworks, May, 2001

[2] An Internet Attributed Certificate Profile for Authorization (draft-ietf-pkix-ac509prof-09.txt), IETF, July, 2001

[3] Implementing Company classification Policy with the S/MIME Security Label, (draft-ietf-smime-seclabel-0.4.txt), IETF, April,2001

[4] Enhanced Security Services for S/MIME(RFC2634), IETF, June, 1999