XML 기반의 SPKI 권한 인증서를 이용한 접근제어

*이영경° , **양수정, ***이경현
*부경대학교 전자계산학과
**부경대학교 정보시스템학과
***부경대학교 전자컴퓨터정보통신공학부

An access control using the SPKI authorization certificate based on XML

*Young-Kyung Lee° , **Soo-Jung Yang, ***Kyung-Hyune Rhee
*Dept of Computer Science, PuKyong Nat'l University
**Dept of Infomation System, PuKyong Nat'l University
***Division of Electronic, Computer & Telecommunication Engineering, PuKyong Nat'l University

요 약

SPKI 권한 인증서를 이용한 기존의 방식은 각 사용자마다 임의적으로 인증서를 발행할 수 있기 때문에 상위객체에 접근권한이 불가능한 데이터에도 접근권한을 줄 수 있다. 그래서 중요한 문서에 대한 보안이 완전하지 못하다. 따라서 본 논문에서는 강제적 접근제어 모델을 기반으로 하여 서버에서 보안레벨에 따라 등급을 나누고 인증서 내에 접근권한을 명시해 줌으로써 접근권한을 추가하거나 삭제할 수 있다. 이는 강제적 모델에 유연성을 제공해주고 서버에서 하는 역할을 줄일 수 있으며, 높은 등급의 정보가 낮은 등급의 객체로 흐르는 것을 막아주므로 기존의 방식보다 좀 더 안전한 접근제어 메커니즘을 제공한다. 또한, 서버에서 XML로 접근제어 레벨을 정의해주므로 여러 플랫폼에서 사용 가능한 이점을 지닌다.

1. 서론

현재 웹을 통한 전자상거래에서 활발한 거래가 이루어지고 있으며, 또한 안전한 상거래를 위해서는 서로 알지 못하는 사람간의 인증이 반드시 필요하게 되었다. 서로간의 인증을 위해 최근에는 공개키 기반구조인 X.509를 현재 많이 사용하고 있지만 인증서의 구조가 너무 복잡하여 인트라넷 환경이나 그룹웨어 등에서 적합하지 못한 면이 있다. 그래서 X.509보다는 필드들이 단순하고 인트라넷 환경에서 좀 더 효율적인 SPKI 권한 인증서를 이용하여, 사용자들을 분산시킴으로써 비용을 줄일 수 있는 권한 인증서를 사용한다[1]. 이에 본 논문에서는 권한을 가진 사용자만이 데이터에 접근할 수 있도록 하며 비 권한 사용자로부터 데이터의 변경과 유출을 막을 수 있도록 사용자에게 등급을 부여한다. 사용자는 자신의 등급보다 낮은 보안레벨의 사용자에게 객체에 대한 권한의 추가, 삭제를 원할 경우 인증서의 <authorization>필드를 통해 임시적으로 접근권한을 명시 할 수 있다. 이는 강제적 모델에 유연성을 제공해 주고 자주 변경되는 접근권한을 서버에서 일일이 하지 않아도 되므로 서버의 부담을 줄일 수 있다. 또한, 서버에서 각 사용자에게 접근 모드를 정의해 줄 때 인증서가 여러 플랫폼에 적용 가능하도록 XML을 이용하여 schema를 설계하였다. 본 논문의 구성은 다음과 같다. 2장에서 SPKI 권한 인증서와 관련하여 인증서 구조를 살펴보고, 기존 방식의 문제점에 대해 살펴본다. 3장에서는 SPKI 권한 인증서에 강제적 접근제어 방식을 이용한 접근제어 방안을 제안하고, 서버에서 정의한 접근제어 모드를 XML-schema로 설계한다. 마지막으로 4장에서 결론을 맺는다.

2. 관련연구

2.1. SPKI 권한 인증서 구조

SPKI 권한 인증서가 다른 인증서와 다른 가장 큰

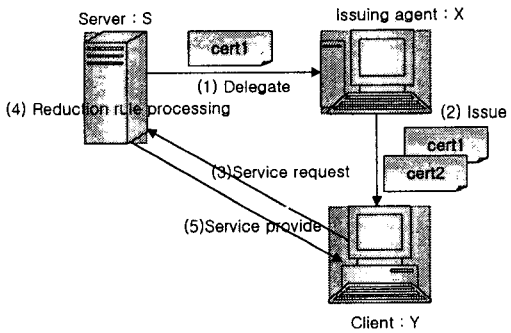
차이점은 <authorization>, <delegation>필드가 존재하여 다른 사람에게 권한을 위임할 수 있고, 자원에 대한 접근여부를 명시할 수 있다는 것이다. 이는 <delegation>필드로 인해 인증서를 발행하는데 있어 사용자들을 분산시킴으로써 비용을 절감할 수 있는 이점을 가진다[1][2].

다음은 SPKI 권한 인증서의 필드 구조이다[3].

- Issuer(발행자) : 인증서의 발행자. 공개키 또는 키의 해쉬값
- Subject(주체자) : 인증서와 함께 권리를 받는 주체 공개키이거나 또는 공개키의 해쉬값
- Delegation : Boolean형. 만약 값이 TRUE라면, 발행자가 주체자에게 다른 사람에게 권한을 위임할 수 있다는 것을 의미
- Authorization : 발행자가 주체자에게 인증서를 발행해 줄 때, 주체자가 객체에 어떠한 권한을 가지는지에 대한 권한을 명시하는 필드
- Validity dates : 인증서의 유효기간을 명시. not-before, not-after 날짜를 명시

2.2 SPKI 인증서 시스템 구성도

[그림1]은 인증서 생성과정과 서비스 제공 과정을 표현한 것이다[4].

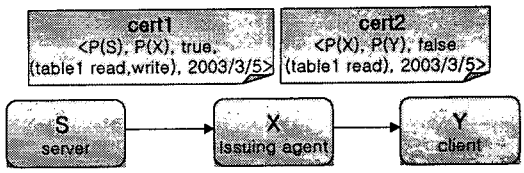


[그림 1] SPKI 시스템 구성도

(1)Delegate : 서버 S의 자원 table1에 대해 read/write의 접근권한을 부여하고, 다른 사람에게 위임할 수 있는 <delegation>필드가 true인 값을 가지는 인증서 <cert1>을 X에게 발급

(2)Issue : 발행 에이전트 X가 서버 S에 대한 접근권한이 명시된 인증서 <cert2>를 클라이언트 Y에게 발급

(3)Service request : 클라이언트 Y가 서버 S에게 서비스 요청



[그림 2] SPKI 권한 인증서 체인

(4)Reduction rule processing : 서버의 공개키 P(S)와 클라이언트 Y가 서비스를 요청하면서 넘겨준 인증서 <cert1>의 공개키를 검증하고, P(S)에 의해 서명되어진 인증서인지를 검사한다. Reduction rule은 <delegation>필드로 인해 인증서 체인이 길어질 우려가 있으므로 각 주체자에게 부여된 권한을 계산하기 위해서 서버에서 실행하는 것이다. 이는 서버에서 인증서 체인을 줄이기 위한 방안으로 사용되고 있다. Reduction rule은 다음과 같다[4].

<P(S), P(X), true, (table1 read/write), 2003/3/5>
+ <P(X), P(Y), false, (table1 read), 2003/3/5> =
<P(S), P(Y), false, AIntersect((table1 read/write), (table1 read)), VIntersect(2003/3/5, 2003/3/5)>

Intersect는 공통권한을 가진 부분을 의미하고, Y는 X보다 더 큰 권한이나 유효기간을 가질 수 없다.

(5)Service provide : Reduction rule을 통해 인증서의 유효성이 검증되고 유효한 값을 가지게 되면 클라이언트 Y는 서버의 자원에 접근할 수 있거나 서비스를 제공받을 수 있다.

임의적인 접근권한 부여는 권한의 남용과 더불어 임의적으로 인증서를 발행하므로 상위객체에 접근권한이 불가능한 데이터에도 접근권한을 줄 가능성이 있어 중요한 문서에 대한 보안이 완전하지 못하다. 또한, 인증서 체인이 너무 길어지게 되면 서버에서 reduction rule을 수행하는데 많은 시간을 소요하게 되므로 효율적이지 못하게 된다.

따라서 본 논문에서는 <authorization>필드를 설정할 때 임의적 접근 제어를 사용하지 않고 Bell-LaPadula[5]모델을 기반으로 한 강제적 접근제어 모델을 적용시켜 중요 데이터나 자원에 대해 높은 등급의 정보가 낮은 등급의 객체로 흐르는 것을 막을 수 있는 SPKI 권한 인증서를 이용한 접근 제어 모델을 제안한다.

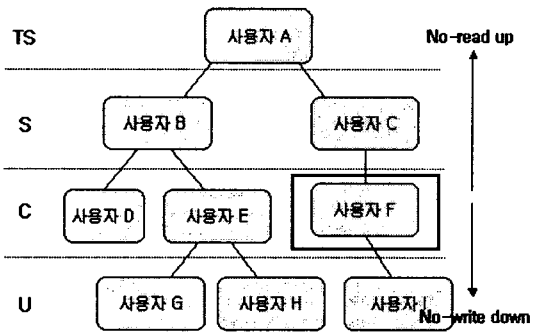
3. SPKI 권한 인증서를 이용한 접근제어 방안

강제적 접근제어는 비밀등급 비교에 의한 객체 접근

통제방법으로 대표적인 모델로 BLP-LaPadula모델을 들 수 있다[5]. 이 모델은 객체, 주체, 객체에 할당된 등급, 주체에 할당된 등급인 접근허가로 설명 할 수 있다. 객체와 주체간의 보안등급은 TS(Top-Secret), S(Secret), C(Classified), U(Unclassified)의 단계별로 정의되어 있으며, 객체에 할당된 보안등급은 TS > S > C > U 와 같이 순서화된다. 또한, BLP모델은 다음과 같은 두 가지 성질을 갖는다[6][7].

- *No-write down* : $L(S) \le L(O)$이면, 주체자 S는 객체 O에게 <write>권한만 가능하다.
- *No-read up* : $L(S) \ge L(O)$이면, 주체자 S는 객체 O에게 <read>권한만 가진다.

*No-write down*은 상위등급을 가진 객체가 자신의 등급보다 낮은 등급을 가진 객체에 <write>할 수 없도록 하는 규칙으로 만약 하위등급을 가진 주체가 상위등급에 <write>할 수 없다면, 하위등급은 상위등급에 자신의 등급으로 접근할 수 없는 정보가 있다는 것을 알 수 있으므로 하위등급으로 정보의 유출이 발생하게 된다. *No-read up*은 하위등급을 가진 주체자는 자신의 등급보다 높은 상위등급의 객체를 <read>할 수 없도록 하는 규칙이다. [그림3]은 사용자에 따른 보안레벨과 계층적인 구조를 보여주고 있다. [그림3]과 같이 사용자 F를 기준으로 자신보다 하위등급의 객체를 <read>할 수는 있지만 <write>는 불가능하다는 것을 의미한다.



[그림 3] 사용자에 따른 보안 레벨

[표1]은 각 사용자에게 서버에서 등급과 접근모드를 부여한 예를 보여주고 있다. 서버에서 사용자에 대한 접근모드와 레벨을 책정해 줌으로써 기밀성을 요하는 문서에 보안을 강화할 수 있다.

[표1]에서 Object는 사용자가 접근하고자 하는 객체 즉 자원을 의미하고, 속성값에는 <secret_level>과 <action>이 명시되고 있다. <secret_level>값은 TS, S, C, U 네 가지 속성값을 가질 수 있고, <action>은 사용자가 자원에 대해 수행할 수 있는 권한으로써 read, write, execute 세 가지를 가진다.

User(name)	Object(<secret_level>, <action>)
사용자(A)	T1(<TS>,<read>), T2(<TS>,<read/write>)
사용자(B)	T3(<S>,<write>), T4(<S>,<read>)
사용자(C)	T5(<S>,<read>/<write>)
사용자(D)	T6(<C>,<read>/<write>)
사용자(E)	T7(<C>,<read>), T8(<C>,<write>)
사용자(F)	T9(<C>,<read>)
사용자(G)	T10(<U>,<read>)
사용자(H)	T11(<U>,<read>/<write>)
사용자(I)	T12(<U>,<read>/<write>)

[표 1] 각 사용자에게 할당된 보안모드

[표2]는 서버에서 결정하는 보안레벨에 따른 접근모드를 XML schema로 설계한 것이다[8][9]. 이는 플랫폼 독립적인 언어인 XML로 schema를 설계함으로써 객체들에 명확한 의미를 부여할 수 있고 다른 시스템에서도 스키마를 쉽게 적용 할 수 있도록 해준다[10].

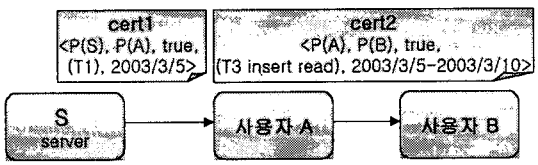
```
<xsd:element name="authorization">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="object" type="xsd:string">
    </xsd:sequence>
  </xsd:complexType>
  <xsd:attribute name="action" type="xsd:string">
    <xsd:simpleType>
      <xsd:restriction base="xsd:string">
        <xsd:enumeration value="Read"/>
        <xsd:enumeration value="Write"/>
        <xsd:enumeration value="Execute"/>
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:attribute>
  <xsd:attribute name="secret_level" use="required">
    <xsd:simpleType>
      <xsd:restriction base="xsd:string">
        <xsd:enumeration value="Top_secret"/>
        <xsd:enumeration value="Secret"/>
        <xsd:enumeration value="Classified"/>
        <xsd:enumeration value="Unclassified"/>
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:attribute>
</xsd:element>
```

[표 2] 보안레벨에 따른 접근제어 스키마 구조

[표1]에서 사용자 A는 TS등급으로써 객체 T1에 대한 <read>권한과 T2에 대해 <read>,<write>권한을 가짐을 알 수 있다. 사용자 A가 사용자 B에게 자원 T3에 대해 <read>권한을 주어야 할 경우가 생긴다면

인증서의 <authorization>필드에 사용자 B가 접근할 수 있는 권한을 명시한다. 사용자 B는 S등급이므로 BLP-LaPadula모델에 근거하여 T1, T2에 대해서는 <write>권한만 가질 수 있다.

가령, 사용자 A가 사용자 B에게 <validity>필드에 명시된 기간동안 임시적으로 T3에 대해 <read>권한을 가지는 인증서를 발급한다. 권한의 삭제는 (T3 delete read)로 명시한다. [그림4]는 사용자 A가 사용자 B에게 T3에 대해 2003/3/5~2003/3/10까지 <read>권한을 가지도록 권한 인증서를 발행한 인증서 체인의 형태를 보여주고 있다.



[그림 4] 강제적 모델이 적용된 인증서 체인

기존 방식에서는 <delegation>필드로 인해 인증서의 체인이 길어지면 서버에 부담을 많이 가지므로, 이러한 reduction rule 처리과정을 없애기 위해 강제적 접근제어 모델을 적용시켰다. 강제적 접근제어는 서버에서 미리 정의해 놓은 권한만을 수행할 수 있기 때문에 서비스 제공자들이 보안에 대해 고수준의 인증을 하며, 인가되지 않은 사람에게 임의로 접근할 수 없도록 한다. 또한, 인증서 내의 <authorization>필드의 insert, delete로 인해 임시적으로 권한을 추가하거나 삭제할 수 있으므로 이는 서버에서의 역할을 줄이고 강제적 모델에 유연성을 제공한다.

4. 결론 및 향후 연구

인터넷이 발전하면서 어플리케이션에 대한 정보능력이 많이 증가했고 공개된 정보에 접속하기도 쉬워졌다. 어플리케이션이나 웹을 선택된 방법으로 접속해야만 하는 곳은 웹에 의한 공유와 분산이라는 보안통제의 정의와 규약이 필요하고, 오직 허가된 객체로의 접근을 허용할 수 있는 인증을 거치는 것이야말로 자원을 안전하게 할 것이다. 본 논문에서 제안한 방안은 다음과 같은 세 가지 장점을 제공한다. SPKI 권한 인증서의 필드를 임의적인 접근제어를 수행하지 않고 서버에서 사용자에 대한 접근권한과 보안레벨을 부여함으로써 높은 등급의 정보가 낮은 등급의 객체로 흐르는 것을 방지할 수 있다. 둘째, 서버에서 정해놓은 권한레벨을 가지므로 사용자가 임의로 권한을 정할 수 없으므로 권한의 남용을 막을 수 있고 기밀 데이터에 대한 보안이 용이하다. 또한, 서버에서 권한레벨을 정의해 줄 때 XML로 schema를 설계함으로써 다른 시스템에서도 스키마를 쉽게 적용 할 수 있도록 해준다. 셋째, 권한 인증서 기반의 접근제어를 하게 되므로 ID/Password보다 좀 더 안전한 보안을 제공한다.

현재 SPKI 권한 인증서가 좀 더 넓은 범위에서 안전한 접근제어 메커니즘을 제공하기 위해서는 사용자 인증 접근제어 및 XML을 이용한 SPKI 구축 방안에 대한 지속적인 연구가 필요할 것으로 판단된다.

[참고문헌]

[1]Yulian Wang, "SPKI : Simple Public Key Infrastructure", Network Security 1998

[2]RFC2692, SPKI Requirements. C. Ellison. (Status: EXPERIMENTAL), 1999.9.

[3]Takamichi SAITO, Kentaro UMESAWA, Hiroshi G. OKUNO, "Privacy enchanced access control by SPKI", 1999, IEEE

[4]RFC2693, SPKI Certificate Theory. C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, T. Ylonen. (Status: EXPERIMENTAL) , 1999.9.

[5]D.E. Bell and L.J. Ra Padula, Secure computer system:Unfied Exposition & Multics Uinterpretation. Technical report, Technical Repory MTIS AD-A023588, MITRE Corporatioon, 1975

[6]심갑식, "데이터베이스 보안", 다성출판사, 2001. 4.

[7]박기홍, 김웅모, "강제적 접근방식과 역할기반 접근제어 그래프를 기반으로 한 보안모델 설계", 2001. 한국정보처리학회

[8]Internet DRAFT
<draft-orri-spki-xml-structure-00.txt
SPKI-XML certificate structure, 2001.11.

[9]Roger L. Costello, XML schema technologies course, http://www.w3.org/TR/xmlschema-0/ (Primer)

[10]Blake, XML Security , Mc Graw Hill, 2002