TSP가 제공된 XML 서명기법

이원진° 김현성
경북대학교 컴퓨터공학과°
경일대학교 컴퓨터공학부
{wjlee°, kim}@kiu.ac.kr

XML Signature Scheme with Time Stamping Protocol

Wonjin Lee°, Hyunsung Kim
Dept. of Computer Engineering Kyungpook Nat'l University
School of Computer Engineering Kyungil University

요 약

2003년 UN이 공식 표준 언어로 XML(eXtensblle Markup Language)을 승인함으로써 전자거래를 위한 정보검색과 데이터 전송에 XML의 활용도가 증가하고 있으며, 전자거래의 표준으로 그 중요성이 높아지고 있다. 이처럼 XML이 광범위하게 이용됨에 따라 XML 보안과 관련된 여러 정책들이 활발하게 연구되고 있다. 본 논문에서는 XML 보안 정책들 중에서 XML 서명 기법들에 대해서 살펴보고, 이러한 XML 서명 기법에 TSP(Time Stamping Protocol)를 제공할 수 있는 효율적인 기법을 제시한다. 본 논문에서 제안한 TSP가 제공된 XML 서명기법에서는 사용자의 서명이 추가된 기법으로 기존의 XML 서명 기법과 비교하여 효율적인 특성을 가진다.

1. 서 론

오늘날 인터넷 기술의 발전으로 인하여 e-commerce의 규모가 커지고 있다. XML은 e-commerce와 데이터를 전송하고 검색하는데 광범위하게 이용되고 있다. 이러한 이유로 XML 문서에 대한 보안 문제가 발생하게 되었고, 다양한 XML 보안의 정책들과 기법들이 개발되고 있다. XML 보안에 관련된 정책들은 XML 암호화, XML 서명, XKMS, SAML, XACML 보안등이 있다. 본 논문에서는 이러한 보안정책 중에서 XML 서명에 대하여 살펴보고, XML 서명기법에 TSP를 제공하기 위한 새로운 기법을 제시한다. Aprville등은 XML 서명기법에 TSP(Time Stamping Protocol)가 제공하는 새로운 기법을 제안하였으나, TSA가 위조된 TSP를 제공할 수 있는 문제점이 존재한다. 본 논문에서는 그러한 문제점을 해결하기 위해서 사용자의 시간 정보가 추가되고, 이것을 사용자가 서명한 형태를 이용한다.

2. 관련연구

본 장에서는 먼저 XML 서명에 대해서 살펴보고, 기존의 XML 서명에 관한 연구에 대해서 살펴본다.

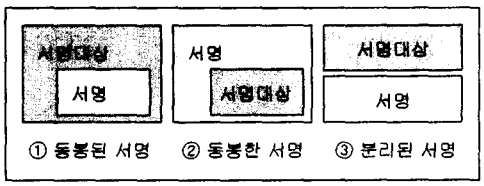
2.1 XML 서명의 유형

XML 서명의 유형에는 동봉된(enveloped), 동봉한(enveloping), 분리된(detached) 서명이 있다.

① 동봉된(enveloped) 서명
서명될 서명대상 안에 서명이 포함되어 있는 기법이다.

② 동봉한(enveloping) 서명
서명될 서명대상이 서명에 포함되어 있는 기법이다.

③ 분리된(detached) 서명
서명될 서명대상과 서명이 분리되어 있는 기법이다.



(a) 서명의 종류

```
<!- -동봉된(enveloped) 서명 - ->
<singing_dataObject>
    <Signature>... </Signature>
</singing_dataObject>

<!- -동봉한(enveloping) 서명 - ->
<Signature>
  <singing_dataObject>
  </singing_dataObject>
</Signature>

<!- -분리된(detached) 서명 - ->
 <Signature>... </Signature>
```

(b) XML 기술

그림 1. XML 서명 유형

2.2 XML 서명에 관한 연구들

XML 서명을 위한 기존의 연구로는 ASN.1구조를 이용한 XER(XML Encoding Rules),시간스템프(Time Stamp)를 이용한 XML서명, 진보된 XML서명 드래프트(XML Advanced Electronic Signatures Draft)등의 연구가 있

다. 그러나 이러한 기법들은 서명은 제공하지만 제대로 된 TSP(Time Stamping Protocol)는 제공하지 못하였다. 이러한 문제를 해결하기 위해서 Aprville등은 XML에 기반하여 TSP를 제공하는 서명 기법을 제안하였다.

Aprville등이 제시한 TSP를 제공한 XML 서명기법은 기본적인 요청(Request), 응답(Response) 메시지 구조를 XML Scheme로 표현 정의하였다. 제안한 서명기법의 전체적인 처리과정은 요청을 위해 클라이언트는 XML스키마로 정의한 해쉬된 문서를 TSA에게 요청한다.

요청 메시지를 받은 TSA는 클라이언트가 보낸 해쉬된 문서의 정당성을 확인 후, 자신의 타임스템프 정보를 함께 추가하고 서명한 후 클라이언트에게 응답 메시지로 보낸다. 하지만 Aprville등이 제안한 서명기법은 다음과 같은 문제점을 가진다.

클라이언트는 인증된 제 3자(TSA, Trusted Security Authority)의 신뢰성에 의존적이기 때문에,TSA가 위조된 타임스템프를 서명하여 전송하였을 때, 위조된 타임스템프를 탐지 할 수 있는 방법이 존재하지 않는다. 다음 장에서는 이러한 문제점을 해결하기 위하여 좀 더 효율적인 XML 서명기법을 제시한다.

3. 사용자의 서명이 추가된 XML 서명 기법

본 장에서는 기존의 TSP를 제공하는 XML 서명 기법들이 가지는 문제점을 해결하기 위해서 새로운 XML 서명 기법을 제안한다.

Aprville등의 프로토콜에서 요청 메시지를 보내는 클라이언트가 단지 문서의 해쉬값을 보내면, TSA는 응답 메시지를 생성하기 위해서 클라이언트로부터 받은 해쉬값의 정당성 여부를 확인한 후 자신의 타임 스템프를 추가하여 받은 문서의 해쉬값에 서명을 하는 방식을 사용한다. 그러므로 서명된 정보에 포함한 시간정보의 정확성은 TSA의 신뢰성을 의존하게 된다.

본 장에서는 이러한 신뢰성 문제를 해결하기 위해 사용자의 서명이 추가된 XML 서명 기법을 제시한다.

이러한 서명 기법은 클라이언트가 TSA에 서명을 요청할 때 클라이언트 먼저 시간 정보가 추가된 해쉬문서를 서명해서 보내고, TSA는 사용자의 서명에 다시 서명을 제공하는 방법을 사용한다.

전체적인 처리과정은 그림 2와 같다.

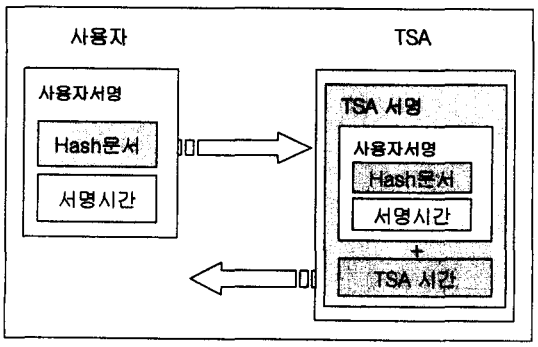


그림 2. 사용자의 서명이 추가된 기법

```
-<element name="TimeStampReq" type="tsp:TimeStampReqType">
 -<complexType name="tsp:TimeStampReqType">
  -<sequence>
    <element name="UserSignatureDoc" type="ds:Signature"/>
   </sequence>
  </complexType>
</element>
```

(a) Request 정의

```
-<UserSignedDoc>
 -<SignedInfo>
   <CanonicalizationMethod Algorithm="..."/>
   <SignatureMethod Algorithm="..."/>
  -<Reference URL="#TimeStampReqInfo"
   Type="http://www.w3.org/2000/09/xmldsig#SignatureProperties">
    <DigestMethod Algorithm="..."/>
    <Digestvalue>...</DigestValue>
   </Reference>
 -</SignedInfo>
  </SignatureValue>...</SignatureValue>
  <KeyInfo>...</KeyInfo>
 -<Object>
  -<SignatureProperties>
   -<SignatureProperty Id="TimeStampReqInfo" Target="ReqInfo">
    -<ReqInfo>
      <!-- the type of this element is TimeStampReqType ..-->
       ...
     </ReqInfo>
    </SignatureProperty>
   </SignatureProperties>
 </Object>
</UserSignedDoc>
```

(b) UserSignedDoc

```
- <element name="TimeStampReq" type="tsp:TimeStampReqInfoType">
 -<complexType name ="tsp:TimeStampReqInfoType">
  -<sequence>
    <element name="MsgImprint" type="tsp:MsgImprintType"/>
    <elemetn name="ReqTime" type="tsp:TimeType"/>
    <element name="ReqPolicy" type="tsp:TSAPolicyType"
     minOccurs="0"/>
    <element name="Nonce" type="long" minOccurs="0"/>
   </sequence>
  </complexType>
  <attribute name="Version" type="positiveInteger"/>
  <attribute name="CertReq" type="boolean" default="false"/>
 </element>
-<complexType name="tsp:MsgImprintType">
 -<sequence>
   <element name ="HashedMsg" type="ds:DigestValueType"/>
  </seguence>
  <attribute name="Algorithm" type="ds:DigestMethodType"
   use="required"/>
  </complexType>
-<simpleType name="TSPTimeType">
 -<restriction base="dataTime">
   <patterm value="\d{4}-\d{2}-\d{2}T\d{2}:\d{2}:d{2}.\d{3}Z"/>
   <patterm value="\d{4}-\d{2}-\d{2}T\d{2}:\d{2}:d{2}.\d{3}+
    \d{2}:\d{2}"/>
   <patterm value="\d{4}-\d{2}-\d{2}T\d{2}:\d{2}:d{2}.\d{3}-\d
    {2}:\d{2}"/>
  </restriction>
 </simpleType>
-<complexType name="TSAPolicyType">
 -<sequence>
   <any namespace ="##other" minOccurs="0" maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Policy" Type="anyURL"/>
 </complexType>
```

(c) Request Info 정의

그림3. Request 메시지 구조

3.1 요청구조

그림 3는 사용자의 서명이 추가된 XML 서명기법의 요청메시지 구조를 XML 스키마로 표현한 형태이다.

요청메시지 구조에서는 그림(a) Request 정의가 TSA에게 전송되고, "UserSingedDoc" 엘리먼트는 XML 서명의 형태로 규정한다.

그림(b)의 UserSingedDoc"의 형태는 XML서명의 형태로 서명되고, 실제 서명이 되는 항목으로는 그림(c)의 내용들이다. 즉 사용자는 TSA에게 요청을 할 때, 자신의 타임스템프의 정보가 포함된(그림 c) 메시지 구조를 자신이 서명을 하여(그림 b) TSA에게 요청를 한다(그림 a).

3.2 응답구조

그림 4는 응답메시지 구조 중에서 주요한 TSA의 타임스템프의 정보를 XML 스키마로 표현한 형태이다.

```
-<complexType name="tsp:TimeStampInfoType">
 -<sequence>
   <element name="TSAPolicy" type="tsp:TSAPolicyType"/>
   <element name="MsgImprint" type="ds:DigestValue"/>
   <elemnet name="UserSignatureDoc" type="ds:signature"/>
   <element name="ResTime" type="tsp:TSPTimeType"/>
   <element name="Time" type="tsp:TSPTimeType"/>
   <element name="Nonce" type="long" minOccurs="0"/>
   <element name="Accuracy type="AccuracyType" minOccurs="0"/>
   <element name="X509Qualifiers" type="ds:X509Data"/>
  </sequence>
  <attribute name="Version" type="positiveInteger"/>
  <attribute name="SerialNumber" type="Integer"/>
  <attribute name="Ordering" type="boolean" default="false"/>
 </complexType>
-<simpleType name="TSPTimeType">
 -<restriction base="dataTime">
   <patterm value="\d{4}-\d{2}-\d{2}T\d{2}:\d{2}:d{2}.\d{3}Z"/>
   <patterm value="\d{4}-\d{2}-\d{2}T\d{2}:\d{2}:d{2}.\d{3}+
    \d{2}:\d{2}"/>
   <patterm value="\d{4}-\d{2}-\d{2}T\d{2}:\d{2}:d{2}.\d{3}-\d
    {2}:\d{2}"/>
  </restriction>
 </simpleType>
```

그림 4. Response 정의

사용자가 자신의 타임스템프 정보를 추가하여 서명 한 요청을 보내면, TSA는 정당성을 확인 후, 자신의 타임스템프 정보를 추가하여 서명한 후, 다시 사용자에게 응답 메시지를 보낸다. 그림 4에서 "ResTime" 엘리먼트는 TSA의 타임스템프 정보이며, "dataTime"의 제한을 규정한다. "UserSignatureDoc"은 서명의 형태로 포함되고, TSA는 "TimeStampInfo"의 모든 내용을 서명될 항목으로 규정하고, 서명하여 사용자에게 응답한다.

4. 분석

본 장에서는 본 논문에서 제안한 기법과 기존의 XML 서명 기법들 간의 특성을 비교 분석한다. 특성을 비교할 때, TSP 제공, 가독성과 쉬운 조작성, XML 서명과 호환성, 시간스템프의 위조 가능 평가 항목을 분석된다.

표 1. XML 서명기법에 대한 비교

서명기법 / 평가항목	XML signatures	XML Advanced Signatures	XML signature by Apvrille	Our proposal: XML Time stamp
TSP제공	제공안됨	제공안됨	제공	제공
가독성·조작성	쉽다	쉽다	쉽다	쉽다
XML서명과 호환성	제공	제공	제공	제공
시간스템프의 위조 가능	제공안됨	제공안됨	위조가능	위조불가

표 1에서 보여준 바와 같이 본 논문에서 제안한 TSP가 제공된 XML 서명기법이 다른 기법보다 우수함을 확인 할 수 있다.

5. 결론

본 논문에서는 기존의 XML 서명 기법의 문제점을 해결하기 위하여 TSP가 제공된 XML 서명 기법을 제안하였다. 제안된 기법은 표1에서 보여준 바와 같이 다른 기법보다 우수한 속성을 가짐을 확인 하였다.

이러한 서명 기법을 통하여 보다 효율적인 XML 보안을 제공 할 수 있을 것으로 기대된다.

[참고문헌]

[1] 류정욱, 류성열, *XML Security*, 인포북, 2002.

[2] ITU-T Recommendation X.693, Information technology - *ASN.1 encoding rules: XML encoding rules(XER)*, OSI networking and system aspects - Abstact Syntax Notation One(ASN.1), Series X : Data networks and open system commmunications, Prepublished version at http://www.itu.int/ITUY/studygroups/com17/languages/X.693 0901.pdf, Dec. 2001.

[3] ITU-T Recommendation X.690,*Information technology-ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), OSI networking and system aspects* - Abstract Syntax Notation One (ASN.1), Series X: Data networks and open system communications, Dec. 1997.

[4] D. Eastlake, J. Reagle, D. Solo, *(Extensible Markup Language) XML-Signature Syntax and Processing*, Network Working Group, RFC 3275, March 2002.W. Diffie, M. Hellman, "New Directions in Cryptography", IEEE Trans. on Information Theory, IT-22, pp.644-654, 1976.

[5] ETSI Technical Committee Security (SEC), *XML Advanced Electronic Signatures (XAdES)*, Technical Specification 101 903 v1.1.1, February 2002.Y. Zheng, "Digital Signcryption or How to Achieve Cost(Signature & Encryption) << Cost(Signature)+Cost(Encry -ption)", LNCS 1294, pp.165-179, 1997.

[6] A.Aprville and V.Girier, "XML Security Time Stamping Protocol", *Proceedings of the Information Security Solutions Europe Confrence* (ISSE 2002) Oct. 2002.