XML Web Services 보안을 위한 XML-Signcryption 설계

한명진*0 이경현**
*부경대학교 전자계산학과
**부경대학교 전자컴퓨터정보통신공학부
{sparkeye*0, khrhee**}@pknu.ac.kr

Design of a XML-Signcryption for XML Web Services Security

Myung-Jin Han*0 Kyung-Hyune Rhee**
*Dept. of Computer Science, PuKyong National University
**Division of Electronic, Computer & Telecommunication Engineering, PuKyong National University

요 약

Web Services가 차세대 e-Business를 주도할 것으로 많은 주목을 받으면서 XML(eXtensible Markup Language)을 기반으로 하여 폭넓게 성장해 가고 있다. 하지만 안전한 서비스의 측면에서 Web Services는 폐쇄환경에서는 존재하지 않았던 새로운 보안 고려사항들을 부각시키고 있다. 이에 대한 해결을 위해 본 논문에서는 XML을 기반으로 하는 Web Services의 특성에 맞추어, 플랫폼 독립적이며 언어 중립적인 특징을 유지한 XML-Signcryption을 제안하는데, 이것은 논리적으로 한번에 전자 서명과 암호화를 함께 수행하도록 하여 기존의 서명 후 암호화에서 요구되는 계산 비용보다 더 적은 비용을 가지고 있는 Zheng의 Signcryption 기법을 XML 보안에 응용한 것이다. 본 논문에서 처음으로 XML 구문 형식을 따라 XML-Signcryption이란 명칭으로 설계하여 제안하는 XML-Signcryption은 암호화와 전자서명을 따로 구현한 W3C(World Wide Web Consortium)의 XML-Encryption이나 XML-Signature 스펙과 비교해, 전자서명과 암호화의 두 가지 보안 메커니즘을 위한 각각의 구현을 따로 할 필요 없이 한번에 할 수 있다는 면에서 개발자들에게 편리성을 제공할 뿐만 아니라 계산 비용 측면에서도 효율적인 장점을 제공한다.

1. 서 론

분산 환경에서 플랫폼이나 프로그램언어에 독립적인 구현과 애플리케이션간의 통신을 할 수 있는 Web Services는 프로그래밍 업계에서 최근 가장 주목받는 분야로 플랫폼과 언어에 중립적인 표준 프로토콜인 HTTP나 XML을 사용함으로써 클라이언트에게 전체 시스템 구현을 숨길 수 있어 기존 기술과 차별화 된 서비스를 웹 상에서 가능하게 한다. 하지만 웹 서비스는 아직 기술적으로 성장기에 있는 기술이므로 수행성능, 확장성, 신뢰성, 보안 등 보완 되어야할 부분들이 아직 존재한다. 그 중에서도 개발자들이 가장 염려하고 있는 것 중의 하나가 Web Services 시스템 상에서 발생할 수 있는 비 인가된 권한사용, 서비스 거부, 데이터 노출/변경, 송수신 부인 등의 보안과 관련된 문제들이다. 보안은 독립적인 애플리케이션을 구현할 때에도 중요한 부분이었으나 애플리케이션이 여러 네트워크에 분산되면서, 동적이고 개방된 웹 환경에서 서비스를 찾아내고 실행할 수 있는 새로운 모델이 가미되어 그 중요성이 더욱 더 강조되고 있다. 본 논문에서는 XML을 기반으로 하는 Web Services의 특성에 맞추어, 플랫폼 독립적이며 언어 중립적인 특징을 유지한 채, 메시지 인증과 데이터 무결성, 기밀성, 송신 부인봉쇄 등의 보안 서비스를 애플리케이션 계층에서 제공할 수 있는 XML-Signcryption을 제안한다. 제안 방안은 논리적으로 한번에 서명과 암호화를 수행하여 기존의 서명 후 암호화에서 요구되는 계산 비용보다 더 적은 비용을 가진다. 이는 암호화와 전자서명을 따로 구현한 W3C의 XML-Signature 스펙[1]이나 XML-Encryption 스펙[2]과 비교해, 전자서명과 암호화의 두 가지 보안 메커니즘을 위한 각각의 구현을 따로 할 필요 없이, 한번에 처리 할 수 있도록 하여 XML Web Services 보안 담당 개발자에게 편리성을 제공할 뿐만 아니라 암호학적인 계산 비용 측면에서도 효율적인 장점을 제공한다. 2장에서 XML Web Services에 적용 가능한 W3C의 XML 보안 메커니즘들을 살펴보고, 3장에서 기존에 Zheng이 제안한 암호학적 Signcryption[4][5]과 이를 변형한 F.Bao의 Signcryption 기법[7]을 비교 한 후, XML Web Services 환경에 적합한 암호학적 Signcryption이 무엇인지 살펴본다. 4장에서 기존의 암호학적 Signcryption을 XML 구문 형식을 따라 XML-Signcryption이란 이름으로 설계하여 Web Services 보안을 위해 활용할 수 있는 새로운 XML 보안 매커니즘으로 제안한다.

2. 관련연구

2.1 XML Web Services의 보안

Web Services의 보안은 전달 계층과 애플리케이션 계층으로 나누어 서비스를 제공할 수 있는데, 네트워크 계층에서는 채널 자체를 안전하게 하는 방법으로 IPSec(IP Security)을 이용할 수 있으며, 전송계층에는 SSL(Secure Socket Layer) 프로토콜을 통해서 보안 서비스를 할 수 있다. 그러나 이러한 전달 계층들에서의 보안은 주고받는 모든 정보에 대해 암호화와 복호화를 수행해야 하기 때문에 보안이 필요치 않은 데이터를 선별하여 제외할 수 없으므로 웹 서버의 성능에 미치는 overhead의 부담이 커서 Web Services에서 사용되기에는 효율적 측면에서 적합하지 못한 면이 있다. 또한 SOAP 모델에 있어서 중요한 개체인 종점간의 메시지를 재전송 해주는 중간 계층에서의 신뢰성이 완전히 보장되기 힘들기 때문에 종점간의 안전한 통신 또한 보장할 수 없으며, 통신 링크 중 어느 하나라도 안전하지 않을 경우, 종점간의 보안성이 깨어지게 되는 문제점도 발생한다. 이런 면에서 오히려 보안이 필요한 정보에만 종단간에 보안 서비스를 해주는 애플리케이션 계층의 보안 방법이 애플리케이션간 프로세서가 연결되어 상호 작용하는 Web Services와는 더 잘 어울리는 면이 있다. 즉 XML Web Services의 애플리케이션 계층의 호출을 책임지는 SOAP 메시지에 암호화와 전자서명을 해주어 기밀성, 메시지 인증, 무결성, 부인봉쇄 등의 보안 서비스를 해주는 것이다. SOAP 1.1에서부터 지원되는 SOAP 보안 확장 모듈[3]은 SOAP Envelope

에 W3C의 XML-Signature와 XML-Encryption을 포함해서 보안 서비스를 해 줄 수 있도록 SOAP Header 엔트리의 문법과 처리 규칙을 다루고 있다.

2.2 W3C의 XML 보안 기술

1) XML 전자서명(XML Digital Signature)[1]

W3C는 IETF(Internet Engineering Task Force)와 공동으로 XML 트랜잭션에서 이용할 수 있도록 디자인된 디지털 서명을 정의하여 XML-Signature로 표준화했다. 이 규격에서는 디지털 서명 오퍼레이션의 결과를 가져올 수 있는 스키마를 정의하고 메시지 인증과 무결성, 서명된 데이터에 대한 부인 봉쇄 등을 지원하기 위한 내용이 포함되어 있다. 이는 2002년 2월 12일 Recommendation 상태로 표준화가 완료된 상태이다

2) XML 암호화(XML-Encryption)[2]

XML 문서에 기밀성을 제공할 수 있는 XML-Encryption은 W3C에서 지금도 표준화가 진행되고 있는 주제로서, XML 기반 데이터의 기밀성을 보장하기 위해, 암호화와 복호화 및 결과 표시를 위한 처리를 명시하고 있다. 이는 현재 2002년 8월 2일 날짜로 Candidate Recommendation의 상태에 있다. [그림1]은 XML-Signature와 XML-Encryption 각각의 기본 구조를 나타낸 것이다.

```
<Signature ID?>
  <SignedInfo>
    <CanonicalizationMethod/>
    <SignatureMethod/>
    (<Reference URI? >
      (<Transforms>)?
      <DigestMethod>
      <DigestValue>
    </Reference>)+
  </SignedInfo>
    <SignatureValue>
  (<KeyInfo>)?
  (<Object ID?>)*
</Signature>
```

```
<EncryptedData>
  <EncryptionMethod/>?
  <ds:KeyInfo>
    <EncryptedKey>?
    <AgreementMethod>?
    <ds:KeyName>?
    <ds:RetrievalMethod>?
    <ds:*>?
  </ds:KeyInfo>?
  <CipherData>
    <CipherValue>?
    <CipherReference URI?>
  </CipherData>
    <EncryptionProperties>?
</EncryptedData>
```

[그림 1] XML Signature(좌), Encryption(우) 기본구조

3. Web Services 보안에 적합한 Signcryption 연구

3.1 Zheng의 Signcryption[4][5]

이 기법은 Zheng이 제안한 것으로, SDSS(Shortened Digital Signature Standard)와 대칭키 암호를 결합시킨 형태이다. 기존의 DSS(Digital Signature Standard)서명-Elgamal 암호 기법[6]을 기반으로 한 서명 후 암호화 기법에서는 송신자의 서명 과정과 암호화 과정에서 3번, 수신자의 서명 확인 과정과 복호화 과정에서 3번의 모듈로 지수 연산을 요구하나, Signcryption기법에서는 전체적으로 3번의 모듈로 지수 연산을 요구하여 계산상 더 효율적인 장점이 있다. 송신자 A는 [표 1]와 같은 Signcryption과정을 통해 문서 m을 signcrypt된 문서로 변환하여 수신자 B에게 보내고, 수신자 B는 unsigncrypt 과정을 통하여 문서 m을 복구한다. 하지만 Zheng이 제안한 Signcryption기법은 송신부인이 발생하여 제3자에게 송신 부인에 대한 검증을 위탁해야 할 경우에 수신자의 비밀키를 제3자에게 공개하지 않으면 제3자가 검증을 할 수 없는 문제점을 가지고 있다.

[표 1] Zheng의 Signcryption

$x \in_R [1,2,\cdots,q-1]$	p : 큰 소수
$k = hash(y_b^x \bmod p)$	q : $p-1$을 나누는 큰 소수
$k_1 \parallel k_2 = k$	g : 위수가 q인 Z_p^*의 원소
$c = E_{k_1}(m)$	$hash$: 해쉬함수
$r = KH_{k_2}(m)$	KH : keyed 해쉬함수
$s = x/(r+x_a) \bmod q$	(E, D): 대칭(암호화, 복호화)
(c, r, s)를 B에게 전송	
$k = hash((y_a g^r)^{s \cdot x_b} \bmod p)$	A의 개인키: $x_a \in_R Z_q^*$
$k_1 \parallel k_2 = k$	A의 공개키: $y_a = g^{x_a} \bmod p$
$m = D_{k_1}(c)$	B의 개인키: $x_b \in_R Z_q^*$
accept m only if $KH_{k_2}(m) = r$	B의 공개키: $y_b = g^{x_b} \bmod p$

이러한 문제는 Web Services와 같이 서로 빈번한 상호 작용을 하는 분산 애플리케이션들 간에 노출된 키를 복구하기 위한 overhead를 증가시키는 문제를 야기하게 된다. 그러나 이것은 F.Bao 등이 제안한 변형 Signcryption 기법을 이용하여 해결할 수 있다.

3.2 F. Bao의 변형 Signcryption 기법[7]

[표 2] 변형 Signcryption

$x \in_R [1,2,\cdots,q-1]$	[표 2]는 F. Bao 변형 기법을 나타낸 것이다. A가 송신 부인을 하였을 경우에, B는 signcrypt된 메시지가 A에 의해 서명되었다는 것을 증명하기 위해 (m, r, s)를 제 3자에게 전송하게 되고, 제 3자는 다음의 절차를 수행함으로서 B의 비밀키를 누출시키지 않고서도 누구에게나 송신 부인에 대한 검증을 부탁할 수 있다.
$k_1 = hash(y_b^x \bmod p)$	
$k_2 = hash(g^x \bmod p)$	
$c = E_{k_1}(m)$	
$r = KH_{k_2}(m)$	
$s = x/(r+x_a) \bmod q$	
(c, r, s)를 B에게 전송	
$t_1 = (y_a g^r)^s \bmod p$	$k_2 = hash((y_a \cdot g^r)^s \bmod p)$
$t_2 = t_1^{x_b} \bmod p$	$r = KH_{k_2}(m)$ 인지 검증
$k_1 = hash(t_2)$	
$k_2 = hash(t_1)$	
$m = D_{k_1}(c)$	
accept m only if $KH_{k_2}(m) = r$	

계산 효율 면에서는 기존 Zheng의 기법에 비해 한번의 모듈로 지수 연산이 더 추가되지만 기존의 서명 후 암호화보다는 더 효율적이며 키를 노출시키는 일없이 송신부인을 막을 수 있다는 면에서 더 나은 기능성을 Web Service 환경에서 제공할 수 있다.

4. 제안하는 XML-Signcryption의 구조와 스키마

기존에 W3C에서 정의하여 명세한 "XML-Signature Syntax and Processing"[1]과 "XML Encryption Syntax and Processing"[2] 명세서에는 각각 XML 트랜잭션에 전자서명과 암호화를 사용할 수 있는 방법을 기술하고 있다. 이는 전자서

명과 암호화를 따로 정의하고 있어, XML-Signature와 XML-Encryption 각각에 다른 분석과 처리를 위한 모듈 개발을 이중으로 해야만 하므로 전자서명과 암호화를 동시에 적용하고자 하는 개발자의 입장에서는 두 가지의 보안 서비스를 효율적으로 동시에 처리할 수 있는 새로운 XML 보안 메커니즘의 필요성이 제기 된다. 이에 본 논문에서는 XML Web Services 시스템 보안에 활용할 수 있는 XML 보안 메커니즘으로 전자서명과 암호화를 동시에 효율적으로 처리할 수 있는 XML-Signcryption을 제안하고, 이를 위한 스키마를 설계하여 개발자들이 공통적으로 XML-Signcryption을 사용할 수 있도록 문서의 의미구조를 정의했다.

[그림2]는 XML-Signcryption의 기본 구조이다. 전체를 감싸고 있는 루트 엘리먼트는 <XML_Signcryption>이다. 이것은 그 하부에 Sincryption의 생성과 검증, 복호 기능에 필요한 정보를 담고 있는 <SigncryptionInfo>와 XML-Signcryption의 실제 데이터 값을 포함하고 있는 <SigncryptionData>를 포함하고 있다. <SigncryptionData>는 다시 <SigncryptionVale>를 자식 노드로 가지고 있으며, Key 정보를 가지고 있는 <KeyInfo>가 선택적 요소로 함께 구성되어 있다. Signcryption의 실제 파라메터 값들인 keyed 해쉬값 $r = KH_{k_2}(m)$은 <SigncryptionDigestValue>에 포함되고, $c = E_{k_1}(m)$는 <SigncryptionCipherValue> 값으로 저장된다, 또한 Signcryption 서명 $s = x/(r+x_a) \bmod q$는 <SigncryptionSign>에 바인딩 되어 XML Data의 비밀성, 메시지 인증, 무결성, 부인봉쇄 등의 서비스를 위해 사용된다. XML-Signcryption은 루트 엘리먼트에 다수의 에트리뷰트를 포함하고 있는데, 그 중 Mode를 이용해, 순수 Signcryption 뿐만 아니라, 암호화와 전자서명 각각을 단독으로 구현할 수 있는 선택을 XML-Signcryption 스펙 안에서 가능하도록 하였다. 또한 Type을 통해서 문서 전체나 엘리먼트 혹은 Value만을 선택해서 각각을 선별적으로 signcrypt 할 수 있다.

```
<XML_Signcryption  Id?  MimeType?
                Mode="Enc|Sig|Signcryption"?
                Type="Document|Element|Content"?
                Encoding?>
    <SigncryptionInfo>
        <SigncryptionMethod/>
        <EncryptedMethod/>
        <SignatureMethod/>?
        <KeyedDigestMethod/>
        <CanonicalizationMethod/>
        (<Transforms>)?
    </SigncryptionInfo>
    <SigncryptionData>
        <SigncryptionValue>
          <SigncryptionDigestValue>
          <SigncryptionCipherValue>
          <SigncryptionSign>
        </SigncryptionValue>
    </SigncryptionData>
    <KeyInfo>?
</XML_Signcryption>
```

[그림 2] 제안하는 XML-Signcryption 기본 구조

[그림 3]은 이러한 XML-Signcryption의 의미를 정의하는 스키마의 일부로써 루트 엘리먼트인 <XML-Signcryption>의 구조적 의미를 표현한 것이다.

```
<element name="XML_Signcryption" type="SigncryptionType"/>
<complexType name="SigncryptionType">
   <sequence>
      <element ref="SigncryptionInfo"/>
      <element ref="SigncryptionValue"/>
      <element ref="KeyInfo" minOccurs="0"/>
   </sequence>
   <attribute name="Id" type="ID" use="optional"/>
   <attribute name="MimeType" type="MIME" use="optional"/>
   <attribute name="Mode"  type="MODE"  use="required"/>
   <attribute name="Type"  type="TYPE"  use="required"/>
   <attribute name="Encoding" type="CODING" use="optional"/>
</complexType>
```

[그림 3] 루트 엘리먼트인 XML_Signcryption의 스키마

5. 결론 및 활용 방안

본 논문에서는 암호화와 전자서명을 따로 구현한 W3C의 XML-Encryption이나 XML-Signature와는 달리, 전자서명과 암호화의 두 가지 보안 메커니즘을 위한 각각의 구현을 한번에 할 수 있는 XML-Signcryption을 제안하였다. 이는 개발자에게 편리성을 제공할 뿐만 아니라 계산 비용 측면에서도 효율적인 장점을 제공하므로, XML Web Services의 보안뿐 만 아니라 전자문서의 안전한 교환 및 유통 서비스 그리고 B2B, B2C 등의 전자상거래에서의 안전한 주문서 교환과 ebXML 기반의 전자상거래 보안 서비스, 또는 EDI 서비스에서의 전자 문서 보호에도 활용 가능할 것이다.

6. 참고문헌

[1] W3C, XML-Signature Syntax and Processing, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/, 2002.

[2] W3C, XML Encryption Syntax and Processing, http://www.w3.org/TR/2002/CR-xmlenc-core-20020802/, 2002.

[3] W3C, SOAP Security Extensions: Digital Signature, http://www.w3.org/TR/2001/NOTE-SOAP-dsig-20010206/, 2001

[4] Y. Zheng, "Digital signcryption or how to achieve cost(signature and encryption) << cost(signature) + cost(encryption)", Advances in Cryptology, Proceedings of CRYPTO'97, LNCS Vol. 1294, Springer-Verlag, pp. 165-179, 1997

[5] Y. Zheng, "Signcryption and its application in efficient public key solutions", Proc. of Information Security Workshop(ISW'97), LNCS Vol. 1396, Springer-Verlag, pp. 291-312, 1998

[6] Proposed Federal Information Proceeding Standard for Digital Signature Standard(DSS), Federal Register, Vol. 56, No.169 30, 1991.

[7] F. Bao and H. Deng, "A signcryption scheme with signature directly verifiable by public key", Proceeding of Public Key Cryptography(PKC'98), LNCS Vol.1431, pp.55-59, 1998

[8] A. J. Menezes P. C. van Oorschot and S. A. Vanstone "Handbook of Applied Cryptography" 1997

[9] Patrick, Professional XML Web Services, Wrox, 2001

[10] Ben, Professional Java Web Services, Wrox, 2002