XML 암호화 제품을 위한 표준 적합성 시험 방법론 연구

채한나°, 이광수
숙명여자대학교 컴퓨터과학과
e-mail : {hannac°, rhee}@sookmyung.ac.kr

A Study on Conformance Testing Methodology for XML Encryption Products

Hanna Chae°, Gwangsoo Rhee
Dept. of Computer Science, Sookmyung Women's University

요 약

국내의 한 인터넷 경매업체는 "대한민국 국민 5명 중 한명은 이미 자신들의 경매를 경험해 보았다."라고 광고할 정도로 웹 기반의 전자상거래는 이미 우리의 일상생활에 깊이 파고든 상태이며, 이제는 단순한 웹상의 전자상거래 뿐이 아닌 웹 서비스 개념의 시대가 현실화 되고 있는 시점이다. 이러한 흐름 속에서 XML은 데이터만을 따로 표현할 수 있다는 특성에 의하여 업계의 표준으로 떠올랐으며, 자연스럽게 이와 더불어 XML의 보안기능은 주목을 받고 있다. XML 전자서명, XML 암호화, XML 키 관리 명세는 주요한 XML 보안기술로서 표준화가 진행되어 많은 부분 완료되었다. 이에 따라 표준을 구현한 제품들이 출시되어 상용화되고 있다. 이러한 제품들은 표준에 적합하도록 개발되어야만 제품의 목적인 안정성과 각 제품들 간의 상호운용성에 있어서의 신뢰도를 검증받을 수 있다. 이에 본 논문에서는 XML 암호화에 대한 표준 적합성 시험 방법을 제시하고 시험도구를 구현하였다.

1. 서 론

2000년부터 W3C에서 제안하여 표준화를 진행해 온 XML 전자서명과 암호화 기술은 이미 표준화가 완료 되었으며, XML 기반 키 관리 기술(XKMS), 보안정보 교환 기술, XML기반 접근 제어 기술 등은 working draft가 나오는 등 XML기반의 보안기술에 대한 표준화 작업들은 활발히 진행되고 있는 상태이다. 이에 따라 XML 전자서명 및 암호화, XKMS 등의 XML 보안기술이 적용된 제품들은 이미 국내외에서 출시되고 있다. IBM, MS, RSA, Phaos, Baltimore, Verisign 등은 이미 상용제품을 개발 완료 하였으며, 국내에서도 역시 ETRI에서 개발된 ESES 패키지를 비롯하여 STI security, 비씨큐어, 아이에이시큐리티 등의 업체에서 XML 보안관련 기술을 적용시킨 상용제품을 출시하였다.[1] 이렇게 XML 보안관련 기술이 적용된 제품들이 국내외에서 활발히 출시되는 환경 속에서 각 제품들이 얼마나 표준에 맞춰 구현되어 있는가 하는 정도는 제품 간 상호운용성을 뒷받침하기 위한 필수조건이 되었다.

또한 웹 서비스의 표준으로 자리 잡아 가고 있는 ebXML 역시 XML기술을 근간으로 하는 것으로서 XML에서 제공하고 있는 전자서명 및 암호화 기술을 채택하고 있는 등 XML 보안기술의 적용범위는 점차 넓어지고 있다.

이러한 추세에 발맞추어 본 논문에서는 XML 암호화 기술의 표준에 대하여 알아보고, 기술 구현 제품들에 적용할 표준항목들을 도출하여, 그에 대한 표준 적합성 시험 방법을 제시하고자 한다.

2. 관련 연구

2.1. XML 암호화 표준화 기구 및 기술 동향

XML 암호화 기술은 W3C 주도 하에 XML 암호화 작업반에서 표준화가 진행되었으며 2002년 12월에 발표된 표준이 현재까지 최종버전으로 명시되어있다.

XML 암호화는 XML 문서의 내용을 의도된 사용자에게만 식별 가능하게 하고, 그 외의 사람들은 알아볼 수 없도록 XML 문서를 암호화 하는 방법을 기술하고 있다. XML 보안 기술은 기존에 의존해왔던 HTTP기반 웹 상거래에서의 전송 프로토콜 수준의 보안과는 다른 부분을 지원하고 있는데, XML 암호화는 전송되는 정보뿐 아니라 저장된 정보의 기밀성까지 제공할 수 있다는 측면에서 기존의 SSL이나 TLS, VPN 등과 구분할 수 있다. XML 암호화는 문서 자체를 이진 데이터로 파악하고 암호화하는 것은 물론, XML 문서의 일부분만을 암호화 할 수 있기 때문에 암호화가 필요한 데이터만 효율적으로 처리할 수 있다.

지위	문서 제목
W3C NOTE	XML Encryption Requirements
W3C REC	XML Encryption Syntax and Processing
	Decryption Transform for XML Signature
IETF I-D	Additional XML Security URIs (Informational):
	application/xenc+xml Media Type Registration

[표 1] W3C에서 발표된 XML 암호화 표준 문서

[표 1]의 다섯 문서 중 앞의 세 W3C가 주요한 내용을 포함

하고 있다. 첫 번째 문서인 XML 암호화 요구사항[2]은 설계 원리와 적용범위, 목적, XML 암호화 처리의 과정, 사용되는 알고리즘과 기대할 수 있는 효과에 관해 기술 하고 있다. 두 번째, XML 암호화 구문과 처리 표준 문서[3]에는 암호화 및 복호화의 방법론적 핵심사항들이 기술되어있다. 세 번째의 XML 서명을 위한 복호화 변환 문서[4]는 XML 전자서명을 암호화 이전 또는 이후에 함께 지원하는 상황에서의 데이터 복호화 처리에 관하여 기술하고 있다.

2.2. XML 암호화 기본구조와 단계별 암호화

XML 암호화의 기본 구조는 다음 (그림 1)과 같다.

```
<EncryptedData Id? Type? MimeType? Encoding?>
  <EncryptionMethod/>?
  <ds:KeyInfo>
    <EncryptedKey>?
    <AgreementMethod>?
    <ds:KeyName>?
    <ds:RetrievalMethod>?
    <ds:*>?
  </ds:KeyInfo>?
  <CipherData>
    <CipherValue>?
    <CipherReference URI?>?
  </CipherData>
  <EncryptionProperties>?      ? : zero or one more occurrence
</EncryptedData>               * : zero or more occurrence
```

(그림 1) XML 암호화 기본 구조

XML 암호화는 가장 핵심이 되는 <EncryptedData> 엘리먼트로 구성된다. 암호화에 어떤 알고리즘이 사용되었는지를 기술하는 <EncryptionMethod> 엘리먼트는 암호화된 XML문서 안에 나타나지 않거나 한 번 이상 나타날 수 있다. XML 암호화는 어느 정도 XML 전자서명으로부터 파생된 부분이 있기 때문에 키의 정보를 나타내는 <ds:KeyInfo> 엘리먼트는 전자서명부분의 정의를 사용하므로 앞에 <ds:....>라는 접두어가 붙는다. 암호화된 데이터가 표시되는 <CipherData> 안에는 실제 암호화된 내용인 <CipherValue>와 <CipherReferenceURI> 엘리먼트를 포함한다.[5]

XML 암호화화는 문서의 일부분만 암호화 하는 것도 가능한데, 그 단계는 5가지로 나눈다.

① XML 엘리먼트 암호화
② XML 엘리먼트 컨텐트 암호화(엘리먼트)
③ XML 엘리먼트 컨텐트 암호화(문자 데이터)
④ XML 문서 또는 임의의 데이터 암호화
⑤ EncryptedData 암호화

```
<?xml version='1.0'?>
<PaymentInfo xmlns='http://example.org/paymentv2'>
  <Name>John Smith</Name>
  <CreditCard Limit='5,000' Currency='USD'>
    <Number>4019 2445 0277 5567</Number>
    <Issuer>Example Bank</Issuer>
    <Expiration>04/02</Expiration>
  </CreditCard>
</PaymentInfo>
```

(그림 1) 원본 문서

```
<?xml version='1.0'?>
<PaymentInfo xmlns='http://example.org/paymentv2'>
  <Name>John Smith</Name>
  <EncryptedData Type='http://www.w3.org/2001/04/xmlenc#Element'
    xmlns='http://www.w3.org/2001/04/xmlenc#'>
    <CipherData>
      <CipherValue>A23B45C56</CipherValue>
    </CipherData>
  </EncryptedData>
</PaymentInfo>
```

(그림 2) XML 엘리먼트 암호화

(그림 1)과 (그림 2)를 비교해 보면, (그림 1)에서 <CreditCard> 엘리먼트가 (그림 2)에서는 <EncryptedData>로 대체되어 암호화가 수행된 결과를 확인할 수 있다. 이러한 방식으로 엘리먼트 컨텐트 암호화(엘리먼트)는 XML의 하나의 엘리먼트 안의 중첩된 엘리먼트에 대하여 암호화를 수행하며, 엘리먼트 컨텐트 암호화(문자 데이터)는 엘리먼트 안의 순수 데이터만을 암호화 할 수 있도록 지원한다.[6]

3. 표준 적합성 시험

3.1 표준 적합성 시험 요소

XML 암호화 구문과 처리 표준에 근거하여 표준 적합성 시험 요소를 선정해 보면 [표 2]와 같다.

분 류	시 험 요 소	요구 사항	해당 항목
EncryptedType 구성	EncryptedData	필수	3.4
	EncryptedKey	필수	3.5.1
암호문의 위치	동봉(CipherValue)	필수	3.3
	참조(CipherRefernce)	필수	3.3.1
해독키 정보	ds:KeyInfo	필수	3.5
	enc:DHKeyValue	선택	3.5
	ds:KeyName	권고	3.5
	ds:RetrievalMethod	필수	3.5.2
	RefrenceList	선택	3.5
	EncryptionProperties	선택	3.7
	AgreementMethod	권고	5.5
암호 처리 규칙	암호화(Encryption)	필수	4.1
	복호화(Decryption)	필수	4.2
블록암호 알고리즘	TRIPLE-DES	필수	5.2.1
	AES-123,256	필수	5.2.2
	AES-192	선택	5.2.2
키 전송 알고리즘	RSA-v1.5	필수	5.4.1
	RSA-OAEP	필수	5.4.2
키 동의 알고리즘	Diffie-Hellman	선택	5.5.1, 5.5.2
대칭키 포장 알고리즘	TRIPLE-DES	필수	5.6.2
	AES-128, 256	필수	5.6.3
	AES-192	선택	5.6.3
메시지 축약 알고리즘	SHA1	필수	5.7.1
	SHA256	권고	5.7.2
	SHA512, RIPEMD160	선택	5.7.3(4)
정규화 알고리즘	주석 포함 정규화	선택	5.9.1
	주석 제거 정규화	선택	5.9.1
	배타적 정규화	선택	5.9.2
인코딩	base64	필수	5.1

[표 2] XML 암호화 표준 적합성 시험 요소

도출된 위의 시험 요소를 바탕으로 구현제품들이 내놓는 결과

물이 제시하고 있는 필수 엘리먼트와 알고리즘, 해독키 정보 등의 요소들을 얼마나 적합하게 구현 하였는지 시험한다.

3.2 표준 적합성 시험 방법론 제안

본 논문에서는 표준 적합성 시험을 진행하기 위하여 시험도구를 구현하였으며, 이 시험도구를 통하여 시험결과를 개별적 또는 일괄적으로 보고하도록 하였다.

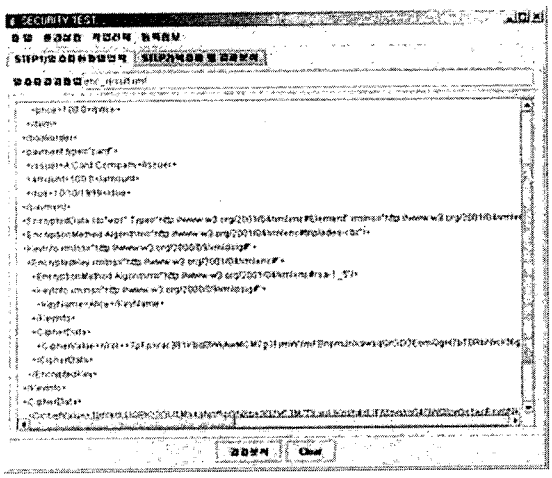
종 류	버 전	파일명	기 능
IBM XSS	20040729	xss4j.jar	XML 암/복호화
IBM JCE	1.3	ibmjceprovider.jar	암호화 알고리즘
Apache Xerces	2.2.0	xercesimpl.jar	XSLT 파서
Apache Xalan	2.6.0	xalan.jar	XML 파서
ICU4j	2.4	icu4j.jar	유니코드 변환

[표 3] 시험 도구 구현 환경

시험 도구 구현환경은 [표 3]에 있는 파일들을 java 홈 디렉토리₩jre₩lib₩ext안에 설치하여 xml 파일 파싱 및 암호화 알고리즘을 지원 할 수 있도록 하였다.

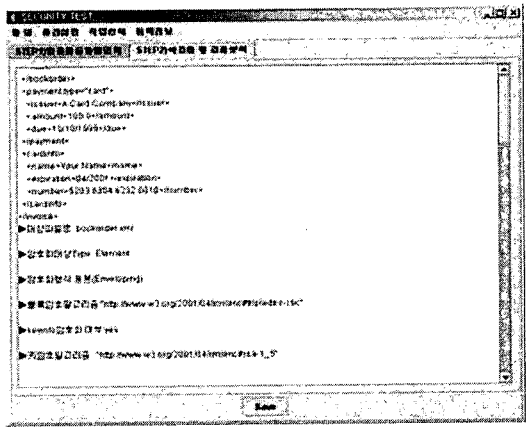
시험 도구는 크게 암호화 기능, 복호화 기능, 결과 보고 기능으로 구성되어 있다. 시험도구에서의 복호화 기능은 암호화 표준 적합성을 시험하는데 이용하며, 시험도구의 암호화 기능은 복호화 표준 적합성을 시험하는데 이용한다.

결과 보고 기능 중, 개별 보고 기능에서는 대상이 되는 문서 하나씩 암호화 또는 복호화에 대한 시험을 하고난 뒤 각 결과에 따라 표준 항목들이 얼마나 적합하게 구현되었는지 보고한다. 보고 된 내용은 저장하여 이 후에도 열람할 수 있도록 한다. 일괄 보고에서는 원하는 수의 테스트 벡터를 임의로 생성하거나, 또는 시험 대상이 되는 제품들로부터 테스트 벡터를 적절한 수만큼 추출하여 암호화 또는 복호화 기능을 시험한다. 시험 도구를 통과하여 얻어진 각 테스트 벡터별 결과에 대하여 위의 [표 2]에 도출된 시험 요소들의 구현 정도 및 테스트 벡터 전체적인 시험 요소 구현 정도를 일괄적으로 정리하여 보고한다. 시험도구의 실행 과정 예로서 복호화



(그림 3) 복호화 시험 과정 첫 번째 단계

과정을 살펴보면 (그림 3)은 복호화 시험과정의 첫 단계로서 시험대상이 되는 제품에서 생성한 암호화된 문서를 시험도구에서 불러들여 보여준다. 결과분석으로 넘어가면 (그림 4)와 같이 원본 문서대로 복호화를 진행한 뒤 암호화대상 단계, 암호화형식, 블록암호화알고리즘의 종류, 키정보 암호화 여부, 키암호화알고리즘의 종류 등 적용된 표준 적합성 시험요소를 보고하고, 보고한 결과를 저장할 수 있도록 지원한다.



(그림 4) 복호화 시험 과정 두 번째 단계, 개별 보고

4. 결 론

본 논문에서 주목하고 있는 표준 적합성 시험 요소가 올바르게 구현된 제품은 XML 암호화 표준안을 잘 따라 만들어진 제품으로 상호운용성의 측면에 잘 부합하는 제품이라 할 수 있다. 표준을 잘 구현하여 상호운용성이 검증된 제품은 경쟁력 측면에서 유리하게 되므로 앞으로의 시장 확장의 기틀을 마련한 것으로 볼 수 있다.

XML 암호화 기술은 단독으로 쓰이기보다는 XML 전자서명 기술 및 키 관리 기술과 연계하여 쓰일 때 그 효과가 증대 되므로 두 기술 이상이 함께 구현된 제품들에 대한 전반적인 검증이 더욱 연구되어야 한다.

참고문헌

[1] 김주한, 김수형, 박남제, 이주영, 이재승, 문기영, 장종수, 손승원, "Standardization and Market Trends for Web Service Security Technologies", 전자통신동향분석 제20권 1호 pp.43-53, 2005

[2] XML Encryption WG, "XML Encryption Requirements", W3C, Apr. 2002

[3] XML Encryption WG, "XML Encryption Syntax and Processing", W3C, Dec, 2002

[4] XML Encryption WG, "Decryption Transform for XML Signature", W3C, Dec, 2002

[5] Blake Dournaee, "XML Security" McGraw Hill, 2002

[6] Donald E. Eastlake III, Kitty Niles, "SECURE XML The New Syntax for Signature and Encryption", Addison Wesley, 2002