XML 암호화 제품을 위한 표준적합성 시험도구 구현

채 한 나[†] · 이 광 수[††]

요 약

XML 암호화는 주로 웹 콘텐츠를 위한 기밀성 서비스 제공에 사용되는데, 물론 응용 영역이 반드시 웹 콘텐츠로만 제한되는 것은 아니다. XML 암호화는 데이터 파일 단위로 적용될 수도 있지만, 주로 XML 문서에 부분적으로 적용되면서 다양한 암호화 범위를 지원한다. 이러한 특성으로 인해 XML 암호화는 여러 웹 애플리케이션에서 SSL/TLS, IPsec, PGP, S/MIME 등의 여타 기밀성 프로토콜보다 효율적인 수단이 될 수 있다.

XML 암호화의 성공적 정착을 위해서는 구현 제품들 사이의 상호운용성이 필수적인데, 이를 위해서는 제품들이 XML 암호화 표준을 정확히 구현해야 한다. 표준적합성 시험에서는 제품들이 관련 표준을 정확히 구현하였는지를 시험한다.

본 논문에서는 XML 암호화 제품을 위한 표준적합성 시험 방법을 제시하고 구현한다. 이를 위해 먼저 W3C에서 개발된 XML 암호화 표준을 먼저 살펴보고, 적합성 시험을 위한 항목들을 도출한다. 그런 다음 시험 방법을 제안하는데, 여기에서는 암호화 기능과 복호화 기능을 분리하여 시험하는 방식을 취한다. 또한 제안된 방법을 GUI 기반의 시험 도구로 구현하여 시험 결과를 제시한다.

키워드 : XML 암호화, 표준적합성 시험

Conformance Testing Tool Implementation for XML Encryption Products

Hanna Chae[†] · Gwangsoo Rhee[††]

ABSTRACT

XML encryption is to provide confidentiality service, though not limited to, for web contents. XML encryption can be applied to entire data files as opaque objects, or more frequently to various parts of XML documents, supporting various encryption granularity. It is this characteristic that makes XML encryption a more efficient alternative for data confidentiality in various web applications than is possible with SSL/TLS, IPsec, PGP, or S/MIME.

It is essential for successful deployment of XML encryption to achieve interoperability among the products implementing this technology, which requires the products to implement the XML encryption standards correctly. Conformance testing is to test if products implement the relevant standard correctly.

In this paper we present a conformance testing method for XML encryption products and implement it. We will first look at XML encryption standards developed by W3C, and extract test criteria. Then we propose a testing method in which the encryption capability and the decryption capability of a product are tested separately. The proposed methody is actually implemented as a GUI-based testing tool and some test results are presented.

Key Words : XML Encryption, Conformance Testing

1. 서 론

이기종 시스템의 집합으로 이루어지는 웹 서비스 환경에서 발생하는 응용 프로그램 사이에서 전송되는 메시지가 갖고 있는 복합적 구조의 표현에 대한 적합성으로 인해 XML은 웹 서비스의 필수 기반 기술로 자리잡아가고 있다. 웹 환경에서 발생하는 메시지들 중에는 기밀성을 요하는 경우가 있으며, 이를 위해 IPsec이나 SSL/TLS 등과 같은 전송 보안 프로토콜을 이용할 수도 있고, PGP나 S/MIME 등과 같은 응용 보안 프로토콜을 사용할 수도 있다. 그러나 IPsec이나 SSL/TLS 등에서는 전송이 이루어지는 동안에만 기밀성을 제공할 수 있으며, PGP나 S/MIME 등의 경우는 메시지 송수신 및 저장 중에도 기밀성이 제공될 수 있으나, 두 경우 모두 전송 정보 전체에 대해서 암호화가 수행된다는 특성을 갖는다.

W3C에서 개발된 XML 암호화는 XML 문서 또는 XML 문서의 형태가 아닌 이진데이터를 암호화하여 XML 형태의 문서로 표현하는 것으로 전송되는 동안과 저장된 문서에 모

※ 본 연구는 숙명여자대학교 2005년도 교내연구비 지원에 의해 수행되었음.
† 준 회 원 : 숙명여자대학교 정보과학부 석사
†† 종신회원 : 숙명여자대학교 정보과학부 교수(교신저자)
논문접수 : 2005년 12월 30일, 심사완료 : 2006년 5월 18일

두 기밀성을 제공한다. 또한 XML 문서의 경우 문서 전체가 아니라 암호화가 필요한 부분들만에 대한 암호화 기능을 제공함으로써 효율성을 제공하면서 중간에 경유하는 제3자에게 특정 정보를 노출시키지 않고 최종 수신자에게 전달할 수 있다.

웹 환경은 이기종 시스템들의 집합이며, 유사한 기능을 갖춘 다양한 제품들이 존재한다. 그렇기 때문에 웹 기반의 응용 프로그램이나 서비스 사이의 상호운용성이 대단히 중요하며, 이를 위해 제품들이 준수해야할 표준을 정하고 있다. 표준적합성은 특정 표준을 구현한 제품을 만들 때 그 표준을 정확히 준수하였음을 보장하는 것으로 해당 응용 프로그램이나 서비스들 사이의 호환성, 즉, 상호운용성 측정에 있어서 기초가 되는 사항이다. 본 논문에서는 XML 암호화 제품들의 상호운용성 검증의 기반으로서, 개별 제품이 XML 암호화 표준에 적합하게 구현되었는지를 시험하는 표준적합성 시험 방법을 제시하고자 한다.

본 논문의 2장에서는 XML 암호화 표준에 대하여 알아보고 3장에서 XML 암호화 표준적합성 시험항목들을 도출한다. 4장에서는 3장에서 도출된 시험항목을 바탕으로 표준적합성 시험 도구를 구현하고 그 실행 결과를 통해 표준적합성 검증 보고 결과물 형태를 제시한다. 마지막으로 5장에서 결론 및 향후 연구 방향을 제시한다.

2. 배경지식

2.1 XML 암호화 표준현황

XML 암호화 기술은 주로 W3C 주도 하에 XML 암호화 작업반에서 표준화가 진행되었으며, IETF에서도 일부 관련 문서들이 제정된 바 있다. W3C와 IETF에서 발표한 XML 암호화 표준화 관련 문서들[1-4]을 살펴보면 <표 1>과 같다.

〈표 1〉 XML 암호화 표준 문서

지 위	문 서 제 목
W3C 비망록	XML Encryption Requirements (XML 암호화 요구사항)
W3C 권고안	XML Encryption Syntax and Processing (XML 암호화 구문과 처리)
	Decryption Transform for XML Signature (XML 전자서명을 위한 복호화 변환)
IETF RFC	Additional XML Security URIs (Informational): (추가적인 XML 보안 URI)

(1) XML 암호화 요구사항

XML 암호화 요구사항[1]은 XML 암호화의 설계 원리와 범위 및 필수요건 등에 대하여 정리한 것으로, 후속 XML 암호화 표준 문서가 다룰 사항들을 규정하고 있다.

(2) XML 암호화 구문과 처리

XML 암호화 구문과 처리[2] 문서는 주어진 자료를 XML 형태의 암호문으로 처리하는 과정과 결과 구문에 관하여 기술한다. 이렇게 암호화된 결과를 복호화하는 과정도 기술하고 있다. 암호화 구문에 사용되는 엘리먼트와 암•복호화 과정에 사용되는 각종 알고리즘 등을 나열하고 있다. 이 문서는 XML 암호화의 핵심적인 문서로서 2002년 12월에 W3C 권고안 형태로 발표되었다.

(3) XML 전자서명을 위한 복호화 변환

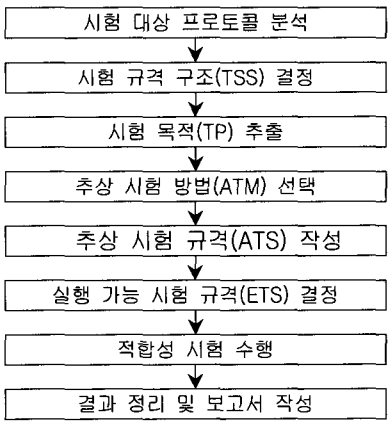
XML 전자서명을 위한 복호화 변환[3] 문서는 XML 전자서명 응용 프로그램에서 먼저 암호화된 데이터에 서명한 경우와 서명한 후 서명과 데이터가 함께 암호화된 경우를 분별하여 복호화함으로써 전자서명의 유효성을 검증할 수 있도록 하는 복호화 처리에 관하여 기술하고 있다.

(4) 추가적인 XML 보안 URI

IETF RFC 정보 문서로 배포된 추가적인 XML 보안 URI[4] 문서는 XML 전자서명과, XML 암호화, 정규화 표준에서 사용하는 추가적인 알고리즘의 URI 식별자 목록을 나타낸 문서이다.

2.2 표준적합성 시험

(그림 1)은 프로토콜 표준적합성 시험의 일반적인 과정을 도식한 것이다. 먼저 시험 대상 프로토콜을 분석한 후 이것을 바탕으로 시험 규격 구조(TSS: Test Suite Structure)와 시험 목적(TP: Test Purpose)을 도출한다. 시험 목적은 결정된 시험 규격 구조에 따라 시험 대상 프로토콜의 특성을 고려하여 프로토콜로부터 세부적으로 추출된다. 또 시험 목적마다 각각의 시험 케이스를 작성한다. 시험 케이스의 작성 과정에서는 선택한 시험 방법상의 제약으로 인하여 시험 케이스로 실현되지 못하는 시험 목적이 포함될 수 있다. 작성된 시험 케이스의 집합이 추상 시험 스위트(ATS: Abstract Test Suite)를 구성하는데, 이러한 ATS로부터 시행 가능 시험 스위트(ETS: Executable Test Suite)를 생성하여 실제 시험에 들어가게 된다. 적합성 시험이 수행된 후에는 이에 대한 결과를 도출하여 작성하는 것으로 적합성 시험 절차를 완료한다.



(그림 1) 적합성 시험 절차

2.3 XML 암호화 상호운용성 시험

상호운용성 시험은 동일한 표준을 참조하여 구현하는 제품들 사이의 접속성, 연동성, 상호 동작 여부를 시험하는 작업이다. XML 암호화의 상호운용성 시험으로 W3C에서 XML 암호화를 구현한 제품사들 사이의 상호운용성 시험 결과를 공개하고 있다. W3C에서 공개하고 있는 상호운용성 시험[5] 결과는 볼티모어, IBM, 파오스, 알렉시사의 XMLSec, NEC, 데이터파워 등 6개사의 XML 암호화 제품을 XML 암호화 구문과 처리[2]에 근거하여 시험한 것이다. 또한 알렉시사의 웹사이트[6]에서는 알렉시사의 암호화 제품 XMLSec과 OpenSSL[7], GnuTLS[8], NSS[9], MSCrypto[10] 등의 암호화 라이브러리들 사이의 상호운용성 결과를 보고하고 있다. XMLSec은 LibXML2[11]에 기반을 둔 C 언어로 구현된 XML 암호화 라이브러리이다.

W3C 상호운용성 시험에 사용된 테스트벡터에는 Merlin Hughes의 merlin-xmlenc-five[12], merlin-decrypt-two[13] 등과 파오스사의 XML 툴킷으로 생성된 phaos-xmlenc-3[14] 패키지 등이 있다.

W3C의 XML 암호화 표준을 위한 상호운용성 시험은 표준의 유효성을 대략적으로 확인하기 위한 것이며, 여기에서 사용된 테스트벡터 모음에서는 데이터가 이미 고정되어 있으며 개수도 많지 않고, 특히 테스트벡터로는 제품의 암호화 기능을 시험할 수 없다는 등의 이유로 인해 XML 암호화 표준[2]에 명세된 다양한 기능과 알고리즘의 조합을 시험하는 표준적합성 시험에 사용하기에는 충분치 않다. 표준적합성 시험에서는 XML 암호화 표준[2]에 명세된 표준 항목들의 다양한 조합을 지원할 수 있는 충분한 수의 테스트벡터가 지원되어야 하므로 본 연구에서는 임의의 시험항목들을 조합하여 테스트벡터를 생성하는 기능을 갖는 시험 도구를 제안한다.

2.4 XML 전자서명 표준적합성 시험

다른 관련 연구로 XML 전자서명 표준적합성[15] 시험이 있다. XML 전자서명[16]은 IETF와 W3C의 공동 작업으로 표준화가 진행되었고 XML 문서 안에서 사용될 수 있도록 설계된 전자서명이다. XML 형식의 데이터뿐만 아니라 하나 이상의 임의 형식 데이터에 대한 전자서명을 지원하고 서명된 데이터에 대해서 데이터 무결성, 송신자 인증, 송신자 부인방지 등의 보안기능을 제공하고 있다. <표 2>는 XML 전자서명 표준문서 현황을 나타낸다.

XML 전자서명 표준 문서 중에서 RFC3275[17]는 XML 전자서명의 구조와 유형을 비롯하여 서명의 생성과 검증에 관한 처리 규칙, 사용되는 알고리즘을 명세한 문서이다. RFC2807[18]은 XML 전자서명 작업반의 작업 범위, 서명 명세서, XML 서명 명세서를 구현한 응용 프로그램의 설계 원리, 범위, 요구사항 등을 나열하고 있다. RFC3076[19]은 논리적으로 동등하지만 물리적 특성의 외형적 표현이 서로 달라 서명 값이 상이한 문제를 해결하기 위해 두 문서가 동일한지 또는 애플리케이션이 XML 1.0과 XML 이름 공간

〈표 2〉 IETF의 XML 전자서명 표준문서 현황

지 위			문 서 제 목
RFC	표준 문서	드래프트표준	RFC3275 XML 서명의 구문과 처리
		제안표준	RFC3075 XML 서명의 구문과 처리
	비표준문서	정보문서	RFC2807 XML 서명 요구사항
			RFC3076 정규 XML 버전 1.0
인터넷 드래프트			제외형 XML 정규화 버전 1.0
			XML 서명 XPath 필터 2.0

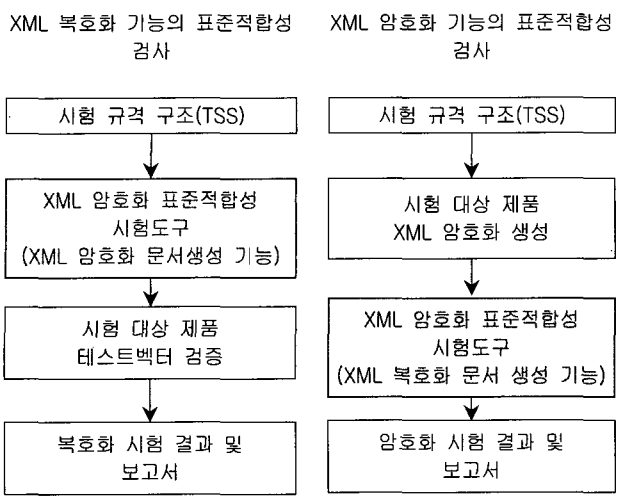
허용하는 변환을 제외하고는 문서를 변경하지 않았다는 것을 결정하기 위한 방법을 제시한다. XML 전자서명 표준적합성 시험에 관한 연구는 <표 2>에 나타난 드래프트표준 'RFC3275 XML 서명의 구문과 처리' 문서와 정보 RFC인 'RFC3076 정규 XML', 'RFC2807 서명 요구사항' 문서에서 명시된 표준 명세를 바탕으로 표준 항목을 도출하고 XML 전자서명 표준 구현 제품들을 시험하였다. 이 시험에서 사용된 시험 도구는 전자서명의 송신자 측면에서의 시험과 수신자 측면에서의 시험을 분리하여 수행하는 방법으로 표준적합성 시험을 하였으며 기본적으로 대상제품들은 개발 완료된 완제품들이므로 블랙박스 시험 방법을 채택하였다.

XML 암호화 제품의 암호화 기능과 복호화 기능에 대한 시험의 분리, 블랙박스 시험의 채택 등은 XML 전자서명 표준적합성 시험에 사용된 방법을 차용한 것이다. 또한 XML 암호화 제품의 표준적합성 시험을 위하여 시험 규격구조에 맞는 임의 조합형 테스트벡터를 생성해 사용하는 방법도 XML 전자서명에 사용된 시험 방법으로부터 차용하였다. 본 연구에서 특히 강화된 시험 기능은 암호화에 대한 검증 시 테스트벡터 모음이 사용될 경우 시험을 통해 검증된 시험항목들을 종합적으로 보고하는 것이다.

3. XML 암호화 표준적합성 시험

3.1 시험 방법

본 절에서는 XML 암호화 구문 및 처리 문서에 근거하여 구현된 암호화 제품의 XML 암호화 또는 복호화 기능에 대한 표준적합성 시험방법을 제시한다. (그림 2)는 XML 암호화 표준적합성을 시험하는 방법을 도식한 것이다. 여기서 시험도구의 역할이 들어가는 부분은 음영 표시된 부분으로 복호화 기능의 표준적합성 검사는 시험도구의 암호화 기능을 이용하고 암호화 기능의 표준적합성 검사는 시험도구의 복호화 기능을 이용하여 암호화 시험 결과를 확인한다. 먼저 XML 암호화 제품의 표준적합성 검사는 (그림 2)의 왼쪽 프로세스와 같이 이루어진다. 왼쪽 프로세스의 XML 암호화 제품의 복호화 기능의 표준적합성 검사 절차를 살펴보면 시험 규격 구조에 의해 시험도구의 적합한 XML 암호화 문서 생성 기능을 이용하여 생성한다. 이렇게 생성된 문서를 시험 대상 프로그램에 적용시켜 사용된 암호화 알고리즘, 암호화 대상, 암호화 형식, 키 정보 등을 바탕으로 복호화를 정확히 수행하는지 평가한다. XML 암호화 기능의 표준적합



(그림 2) XML 암호화 표준적합성 시험 방법

성 검사는 (그림 2)의 오른쪽 프로세스와 같이 이루어진다. 먼저 시험 규격 구조에 맞게 시험 대상 제품이 암호화된 데이터를 생성하면 이를 시험 도구에 입력하여 표준에 적합하게 암호화를 수행하였는지 결과를 보고한다.

3.2 시험항목

XML 암호화 표준적합성 시험항목들은 W3C 상호운용성 시험[5]에서 XML 암호화 구문과 처리 표준[2]에 근거하여 도출한 것으로 <표 3>과 같으며, 각 시험항목들은 XML 암호화 구문과 처리 명세에 근거하여 명세서에 기술되어 있는 순으로 나열하였다.

<EncryptedType> 안에는 <EncryptedData> 엘리먼트 또는 <EncryptedKey> 엘리먼트가 나타날 수 있으며, 이들 모두 나타날 수도 있고, 또 이 엘리먼트들이 여러 개 나타날 수도 있다. 암호문의 위치, 암호문을 해독할 해독키에 대한 정보를 나타내는 엘리먼트, 암호화 및 복호화 등이 XML 암호화 시험항목에서 중요한 처리규칙 표준이다. 암호문 위치에서 동봉은 암호문이 결과 XML 문서 안에 나타나는 것을 의미하며, 참조는 암호문을 별도의 문서에 두고 그 위치만 결과 XML 문서 안에 표시하는 것을 의미한다.

해독키에 대한 정보는 암호화된 데이터 혹은 암호화된 키에 대한 복호화 수행 시에 필요한 키 재료로 XML 전자서명에서 기술한 엘리먼트들을 참조하는 형식이다. 다음은 XML 암호화 생성 시 필요한 알고리즘에 대한 나열로 블록암호화 알고리즘, 키 전송 알고리즘, 키 합의 알고리즘, 대칭키 포장(wrapping) 알고리즘, 메시지 축약 알고리즘, 정규화 알고리즘, 인코딩 방법 등이 있다.

3.3 시험 결과

XML 암호화 표준적합성 시험은 3.1절과 3.2절에서 정의한 표준적합성 시험방법 및 시험항목을 토대로 XML 암호화 제품의 복호화 기능과 암호화 기능의 수행 및 이에 따른 표준적합성 결과 보고를 제시해야 한다. XML 암호화 제품

〈표 3〉 XML 암호화 표준적합성 항목

분 류	시 험 요 소
<EncryptedType> 구성	<EncryptedData>
	<EncryptedKey>
암호문의 위치	동봉(CipherValue)
	참조(CipherRefernce)
해독키 정보	ds:KeyInfo
	enc:DHKeyValue
	ds:KeyName
	ds:RetrievalMethod
	RefrenceList
	EncryptionProperties
	AgreementMethod
암호 처리 규칙	암호화(Encryption)
	복호화(Decryption)
블록암호 알고리즘	TRIPLE-DES
	AES-128, 256
	AES-192
키 전송 알고리즘	RSA-v1.5
	RSA-OAEP
키 합의 알고리즘	Diffie-Hellman
대칭키 포장 알고리즘	TRIPLE-DES
	AES-128, 256
	AES-192
메시지 축약 알고리즘	SHA1
	SHA256
	SHA512, RIPEMD160
정규화 알고리즘	주석 포함 정규화
	주석 제거 정규화
	배타적 정규화
인코딩	base-64

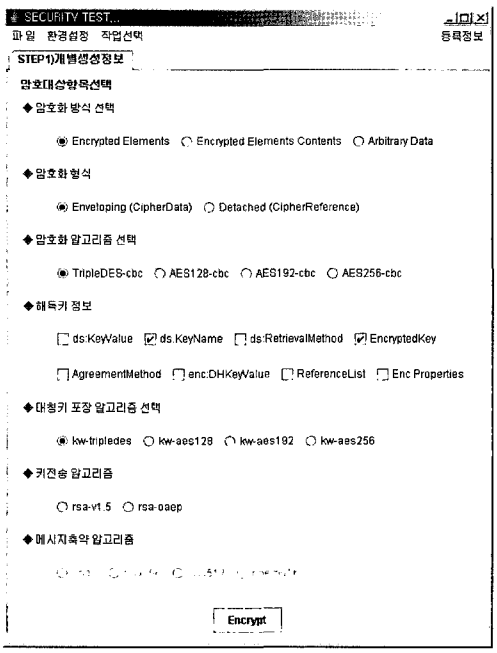
의 암호화 기능 시험의 결과 보고서는 XML 암호화 문서에서 암호화된 유형을 찾아내고 해독할 키에 대한 정보와 알고리즘을 적용하여 최종적으로 본래의 평문을 복호화 하는 결과를 도출해야 한다. XML 암호화 제품의 암호화 데이터 안에 포함되어야 할 필수 엘리먼트들과 암호화된 데이터를 해독할 키에 대한 정보나 속성들이 적합하게 구현되었는지를 시험하여 결과를 도출한다.

4. XML 암호화 시험도구 구현

<표 3>의 XML 암호화 표준적합성 시험항목들에 대한 GUI 기반의 시험 도구를 구현하여 표준적합성 시험 처리과정과 결과 보고 기능을 제시한다. XML 암호화 표준적합성 시험을 위한 프로그램은 현재 W3C에서 정의하고 XML 암호화 구문 및 처리[2]의 참조구현인 IBM XML 시큐리티 스위트(이하 XSS)[20]를 참조하여 자바 언어 기반의 XML 암호화 표준적합성 시험도구를 구현하였다.

4.1 복호화 검증 지원 기능

시험도구에서는 두 가지의 테스트벡터 생성 기능을 지원하고 있다. 하나는 암호화 개별 생성이며 다른 하나는 일괄 생성 기능이다. 개별 생성 기능은 시험 도구 화면에서 선택된 시험항목을 모두 포함하는 한 개의 완전히 유효한 테스



(그림 3) 개별 암호화 생성 화면

트벡터 한 개를 생성해 내는 기능이다. (그림 3)은 시험 도구의 개별 암호화 생성 화면이다.

개별 암호화 생성에서 먼저 시험항목은 암호화 방식은 엘리먼트, 콘텐트, 일반데이터 타입 중 한 가지를 먼저 선택한다. 암호화 형식으로 동봉형인지 참조형인지 둘 중에 한 가지 선택된 항목을 적용시키고, 암호화 알고리즘을 한 가지만 선택한다. 그리고 해독키에 대한 정보는 포함시킬 항목을 복수 또는 하나만 선택하고 대칭키 포장 알고리즘 또는 키 전송 알고리즘 중에 하나만 선택하여 시험항목을 포함시킬 수 있다. 이런 식으로 선택된 시험항목을 모두 포함하는 테스트 벡터 하나를 생성한다.

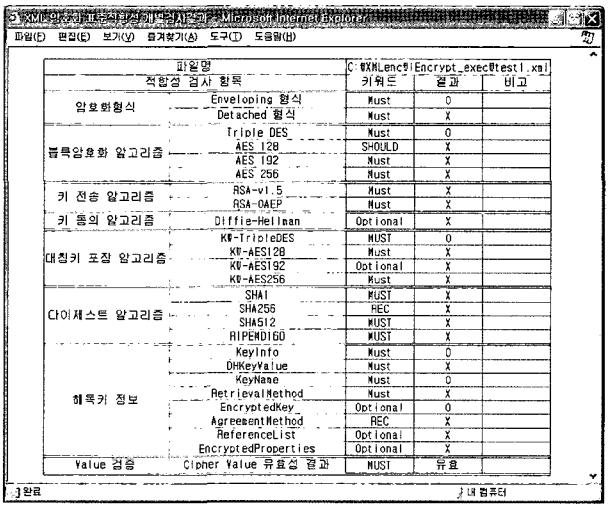
XML 암호화 제품의 복호화 모듈의 다양한 기능을 시험하고자 할 경우 시험항목들이 다양하게 조합된 테스트벡터들을 확보하는 것이 필요한데, 이를 개별 생성 기능을 이용할 경우 많은 시간을 요하게 될 것이다. 일괄 생성 기능에서는 도구 사용자가 먼저 시험하고자 하는 모든 시험항목들을 선택하고, 생성할 테스트벡터 개수를 입력한다. 그러면 시험도구는 선택된 항목들을 무작위로 조합하여 입력된 개수만큼의 테스트벡터를 생성한다. 일괄 생성 기능을 통하여 다양한 알고리즘과 시험항목을 조합한 테스트벡터를 편리하게 그리고 원하는 개수만큼 얻을 수 있다. 시험항목들의 선택이 필요한 이유는 제품에 따라서 표준에서 기술하고 있는 모든 기능들을 구현하고 있지는 않기 때문이며, 또한 집중적으로 시험하고자 하는 시험항목들이 제한되어 있는 경우도 있기 때문이다. 일괄 암호화 생성 화면은 테스트벡터 개수 입력을 위한 대화상자 외에는 기본적으로 개별 생성의 경우와 같으며, 다만 시험항목 카테고리별로 복수 개의 시험항목의 선택을 허용한다는 차이가 있다.

4.2 암호화 검증 지원 기능

암호화 검증을 위한 시험도구의 기능인 복호화 및 결과 보고기능 역시 두 가지의 기능을 지원한다. 하나는 개별 복호화 지원 기능이고 다른 하나는 일괄 복호화 지원 기능이다.

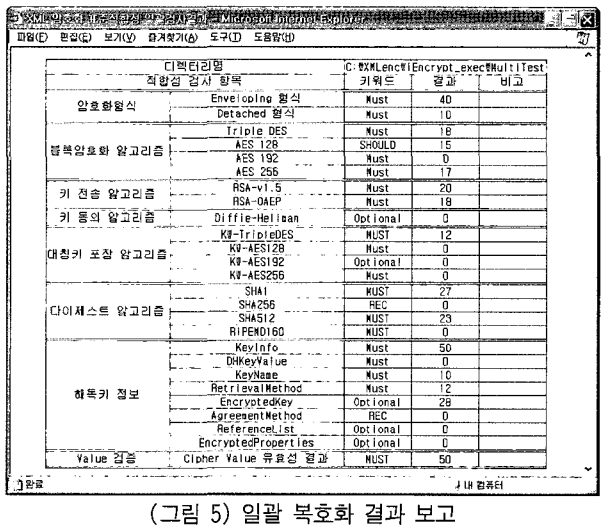
개별 복호화 작업을 통해서는 선택한 하나의 테스트벡터를 복호화하고 그 결과를 보고한다. 복호화 진행 중에 테스트벡터에 포함되어 있는 시험항목들을 분석하여 (그림 4)와 같이 웹 브라우저로 결과를 확인할 수 있는 보고서를 작성한다. (그림 4)의 결과 열에서 'O'는 테스트벡터에 포함된 시험항목으로 성공적으로 검증되었음을 나타내며, 'X'는 테스트벡터에 포함된 시험항목이 아님을 나타낸다.

일괄 복호화에서는 테스트벡터 모음이 들어있는 디렉터리를 선택하여 그 안에 들어있는 모든 파일들을 한꺼번에 복호화하고 그 결과를 (그림 5)와 같이 보고한다. 결과 열에서는 해당 시험항목을 포함하고 있는 테스트벡터의 개수가 표시되며, 마지막 행에서는 성공적으로 검증된 테스트벡터의 개수가 표시된다.



파일명		C:₩XMLenc₩Encrypt_exec₩test1.xml		
적합성 검사 항목		키워드	결과	비고
암호화형식	Enveloping 형식	Must	O	
	Detached 형식	Must	X	
블록암호화 알고리즘	Triple DES	Must	O	
	AES 128	SHOULD	X	
	AES 192	Must	X	
	AES 256	Must	X	
키 전송 알고리즘	RSA-v1.5	Must	X	
	RSA-OAEP	Must	X	
키 동의 알고리즘	Diffie-Hellman	Optional	X	
대칭키 포장 알고리즘	KW-TripleDES	MUST	O	
	KW-AES128	Must	X	
	KW-AES192	Optional	X	
	KW-AES256	Must	X	
다이제스트 알고리즘	SHA1	MUST	X	
	SHA256	REC	X	
	SHA512	MUST	X	
	RIPEMD160	MUST	X	
해독키 정보	KeyInfo	Must	O	
	DHKeyValue	Must	X	
	KeyName	Must	O	
	RetrievalMethod	Must	X	
	EncryptedKey	Optional	O	
	AgreementMethod	REC	X	
	ReferenceList	Optional	X	
	EncryptedProperties	Optional	X	
Value 검증	Cipher Value 유효성 결과	MUST	유효	

(그림 4) 개별 복호화 결과 보고



디렉터리명		C:₩XMLenc₩Encrypt_exec₩MultiTest		
적합성 검사 항목		키워드	결과	비고
암호화형식	Enveloping 형식	Must	40	
	Detached 형식	Must	10	
블록암호화 알고리즘	Triple DES	Must	18	
	AES 128	SHOULD	15	
	AES 192	Must	0	
	AES 256	Must	17	
키 전송 알고리즘	RSA-v1.5	Must	20	
	RSA-OAEP	Must	18	
키 동의 알고리즘	Diffie-Hellman	Optional	0	
대칭키 포장 알고리즘	KW-TripleDES	MUST	12	
	KW-AES128	Must	0	
	KW-AES192	Optional	0	
	KW-AES256	Must	0	
다이제스트 알고리즘	SHA1	MUST	27	
	SHA256	REC	0	
	SHA512	MUST	23	
	RIPEMD160	MUST	0	
해독키 정보	KeyInfo	Must	50	
	DHKeyValue	Must	0	
	KeyName	Must	10	
	RetrievalMethod	Must	12	
	EncryptedKey	Optional	28	
	AgreementMethod	REC	0	
	ReferenceList	Optional	0	
	EncryptedProperties	Optional	0	
Value 검증	Cipher Value 유효성 결과	MUST	50	

(그림 5) 일괄 복호화 결과 보고

5. 결 론

본 논문에서는 XML 암호화 제품들 간의 표준적합성을 시험하기 위하여 먼저 XML 암호화 표준[2]을 분석하여 시험항목을 도출하고 이를 시험하기 위한 시험 도구를 개발하였다. 또한 시험도구의 암호화 복호화 기능을 이용하여 다양한 테스트벡터를 생성하고 결과를 보고하였다.

시험도구의 암호화 기능은 간단하게는 시험항목을 하나하나 선택하여 그에 적합한 하나의 테스트벡터를 생성하는 기능과 이를 발전시켜 여러 가지 항목을 한 번에 선택하고 암호화 방식에서부터 사용되는 암호화 알고리즘 및 기타 정보에 이르기까지 무작위 조합할 수 있는 기능을 제공한다. 이러한 기능을 통해 다양한 테스트벡터를 확보할 수 있으며 다양한 테스트벡터의 확보는 시험대상 제품의 표준적합성 및 상호운용성 정도의 측정에서 보다 신뢰성 있는 기반을 마련할 수 있을 것으로 기대한다.

또한 대상 제품의 암호화 기능을 시험할 수 있는 시험 도구의 복호화 부분에서도 일괄 복호화 기능을 제공한다. 또한 여러 테스트벡터의 분석 결과를 표 형태로 제공함으로써 한 번에 알아보기 쉽도록 구성하였다.

이러한 결과 보고 및 암호화 테스트벡터의 적용에 의한 시험으로 표준적합성 및 상호운용성이 검증된 제품이 시장 경쟁력을 높이는 부분에 기여할 수 있을 것으로 기대한다.

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 할 것이다.

참 고 문 헌

[1] XML Encryption WG, "XML Encryption Requirements," W3C, Apr., 2002. http://www.w3.org/TR/xml-encryption-req

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

[3] Decryption Transform for XML Signature, http://www.w3.org/TR/xmlenc-decrypt

[4] D. Eastlake 3rd, "Additional XML Security Uniform Resource Identifiers (URIs)," IETF RFC4051. http://www.ietf.org/rfc/rfc4051.txt

[5] W3C XML 암호화 상호운용성 시험, http://www.w3.org/Encryption/2002/02-xenc-interop.html

[6] 알렉시사에서 제공하는 XML 암호화 상호운용성 시험, http://www.aleksey.com/xmlsec/xmlenc.html

[7] OpenSSL, http://www.openssl.org/

[8] GnuTLS, http://www.gnu.org/software/gnutls/

[9] NSS, http://www.mozilla.org/projects/security/pki/nss/

[10] MSCrypto, http://msdn.microsoft.com/security/

[11] LibXML, http://xmlsoft.org

[12] merlin-xmlenc-five.tar.gzhttp://lists.w3.org/Archives/Public/xml-encryption/2002Mar/0008.html

[13] merlin-decrypt-two.tar.gz http://lists.w3.org/Archives/Public/xml-encryption/2002Aug/att-0000/01-merlin-decrypt-two.tar.gz

[14] phaos-xmlenc-3.zip http://lists.w3.org/Archives/Public/xml-encryption/2002Mar/att-0052/01-phaos-xmlenc-3.zip

[15] 김지현, 이광수, "XML 전자서명 제품의 표준적합성 시험 방법 및 구현", 정보보호학회논문지, 14(4):3-12, 2004.

[16] IETF/W3C XML-DSig Working Group, http://www.w3.org/Signature/

[17] D. Eastlake, J. Reagle, D.Sole, "XML-Signature Syntax and Processing," IETF RFC3275

[18] J. Reagle, "XML Signature Requirements," IETF RFC2807

[19] J. Boyer, "Canonical XML Version 1.0," IETF RFC3076

[20] IBM XML Security Suite, http://www.alphaworks.ibm.com/tech/xmlsecuritysuite

채 한 나

e-mail : hannac@naver.com

2004년 숙명여자대학교 전산학과(학사)

2006년 숙명여자대학교 대학원 컴퓨터과학과(이학석사)

관심분야 : 네트워크 보안

이 광 수

e-mail : rhee@sookmyung.ac.kr

1981년 서울대학교 계산통계학과(학사)

1986년 Washington University 대학원 컴퓨터과학과(이학석사)

1990년 Washington University 대학원 컴퓨터과학과(이학박사)

1990년~현재 숙명여대 정보과학부 교수

관심분야 : 알고리즘, 네트워크 보안