2000년 한국정보처리학회 추계 학술발표논문집 제7권 제2호

XML Signature를 이용한 기업간(B2B) 보안모듈 설계

박정환, 지석진, 임두욱, 장우영, 신동규, 신동일
세종대학교 컴퓨터공학과

B2B Security Design of XML Siganture

Jung-Hwan Park, Seok-Jin Jee, woooyoung Jang, DooWook Im,
DongKyoo Shin, Dongil Shin
Dept. of Computer Engineering, Sejong UniversityJ

요 약

XML은 단순함과 융통성이라는 특징을 가지고 있기 때문에 Internet B2B(Business to Business) 메세지 송수신을 용이하게 한다. Internet B2B에서 메세지 송수신을 하는 데 있어서 보안이 점차 중요하게 대두되고 있다. 인터넷은 공용 네트워크이므로 도청과 위조와 같은 공격에 어떠한 보호 장치도 있지 않기 때문에 메시지가 송수신 되는 동안 자신의 중요한 정보가 다른곳으로 유출되거나 손실될 경우 B2B 메시지 송수신에 있어서 크나큰 손실을 가져올 수 있다. SSL(Secure Socket Layer)은 transport-level 보안 프로토콜이 제공하는 인증, 무결성, 기밀성을 제공하고 있다. 하지만 부인방지를 제공하고 있지 못하고 있는 실정이다. 하지만 XML-Signature를 이용하면 이러한 문제점을 해결할 수 있고 프로토콜 차원이 아닌 어플리케이션 차원에서 보안 시스템을 설계하므로 B2B 간 메시지 송수신 하는데 있어서 서버와 클라이언트에 각각 XML-Signature 사용하여 안전하게 통신 할 수 있도록 해주는 보안모듈 설계를 소개한다.

1. 서 론

전자상거래는 상업적인 거래의 당사자간에 정보기술을 활용하여 거래를 보다 효율적이며 효과적으로 수행하기 위한 제반 행동으로 정의 할 수 있다. 전자상거래 참여 대상에 따라 나눈다면 크게 두 가지로 구분할 수 있는데 B2C(business to Customer)와 B2B(Business to Business)형태가 된다. 대부분의 업체들이 내세우는 전략의 공통점은 B2C 보다는 B2B에 중점을 두고 있다. 이러한 B2B 시장에 XML(eXtensible Markup Language)[1]이라는 웹상에서 구조화된 문서를 전송 가능하도록 한 마크업 언어를 이용한 솔루션을 제공하는 업체들이 증가하고 있는 추세이다. 또한 XML 기술을 이용함으로써 기업간의 비즈니스 문서형식과 메시지를 형태에 상관없이 서로 교환을 할 수 있게 되고, 기업의 기존 legacy 어플리케이션과 쉽게 연동 가능하게 해준다. 기존의 EDI가 가진 고비용, 고정된 구조와 유연성 결여들의 문제들을 해결하기 위해 등장한 것이 XML/EDI(Extensible Markup Language/Electronic Data Interchange)이다. XML은 문서의 구조와 형식이 분리되어 있기 때문에 다양한 형태의 지능적인 검색이 가능하게 하므로 B2B, 전자상거래 시장을 조장하고 있는 추세이다. 전자상거래 B2B시장 규모가 증가함에 따라 가장 민감한 문제점인 보안성 문제가 제기 되었다. 이러한 보안성 문제가 제기되자 W3C에서 2000년2월에 XML-Signature[1][2]를 제안하기 시작했고 그 뒤로 5월, 6월, 7월 계속해서 업데이트되고 있는 상태이다. 웹의 폭발적인 사용과 함께 공개적으로 사용되던 웹을 제한된 집단이나 상업적인 용도로 이용하고자 하는 움직임이 활발해지게 되었고, 또한 웹이 단순한 정보 검색만이 아닌 신용카드 정보와 같이 타인에게 노출되어서는 안될 중요한 정보의 전송 등 다양한 용도로 사용됨에 따라서 다음과 같은 주요 웹 보안 요구사항이 중요시되고 있다.

2. 요구사항

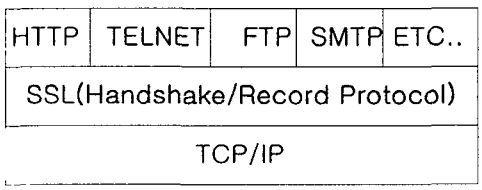
첫째, 특정 그룹 구성원 사이에서만 민감한 정보를 공유하고자 하는 응용 형태가 있다. 이 경우에는 서버의 정보에 접근하는 클라이언트를 제어하기 위해 클

라이언트에 대한 인증(Authentication)이 요구된다. 중요한 정보를 신뢰성 있게 교환하고자 하는 응용 형태가 있다. 예를들면 구매 주문이나 중요한 공문서를 발행하고자 하는 경우 클라이언트 뿐만 아니라 서버 역시 정당한 서버인지를 인증할 수 있어야 하며, 교환되는 메시지 또는 문서 자체에 대한 인증도 요구된다. 둘째, 웹을 이용하여 교환되는 정보 자체가 타인에 노출되지 않기를 바라는 통신의 비밀보장 서비스가 요구될 수 있다. 셋째, 웹을 이용하는 상거래 응용의 경우에는 웹 상에서 전자 지불 기능을 요구하게 되며, 이 경우 판매자의 정당성 인증과 구매자의 지불이 안전하게 이루어 질 수 있도록 하는 보호기능이 요구된다. 위의 보안 요구사항을 정리해보면 클라이언트와 서버간의 상호인증, 교환되는 메시지 또는 문서 자체에 대한 무결성, 웹을 통해서 교환되는 정보가 타인에게 노출되지 않게 하는 기밀성이 요구된다.[2]

2. 관련연구

2.1 채널기반 웹 보안방식

넷스케이프사에서 개발한 대표적인 채널 보안 방식인 SSL은 상호인증(Mutual Authentication), 무결성을 위한 메시지 인증 코드(MAC : Message Authentication Code), 기밀성을 위한 암호화 등을 제공함으로써 클라이언트와 서버 사이에 안전한 데이터 통신을 제공한다.



[그림 1] SSL의 계층 모델

SSL의 동작은 크게 두 가지로 분류 할 수 있는데 먼저 핸드쉐이크 프로토콜에 의해 통신하고자 하는 어플리케이션 간에 공개키 암호화 기술을 이용하여 안전한 통신 채널을 설정하고 상호인증과정과 세션키 교환을 수행하고, 그 후에 레코드 프로토콜에 의해 안전한 통신 채널로 어플리케이션 간에 공유된 세션 키를 이용하여 응용 실체 사이의 대칭 키 방식의 암호 통신을 하게한다.[6]

2.2 내용기반 웹 보안방식

내용기반 웹 보안방식 중의 한 방법으로 서버와 브라우저의 외부에서 수행되는 프로그램을 따라 설치하는 방법이다. 독립적으로 암호 기능을 수행하는 외부 프로그램이 서버와 클라이언트에 연결되어 있으며, 이 외부 프로그램은 HTTP 요청 및 응답 메시지의 암/복호화에 이된다. 즉 메시지가 서버와 브라우저을 떠나 전송되기 직전에 각 외부 프로그램에 보내지고, 암호화된 메시지들은 서버와 브라우저로 보내져서 인터넷을 통해 전송되게 된다. 이와 같은 외부 프로그램은 기존의 CGI 프로그래밍 기법을 사용하여 서버와 연결되며, 클라이언트는 브라우저에 따라 여러 가지 방법이 이용된다. 넷스케이프인 경우, 플러그 인 또는 외부 표시기 기법을 이용하고, 모자익의 경우는 NCSA에서 제공하는 CCI 라이브러리를 이용한다, Microsoft Internet Explore는 SSPI를 이용할 수 있다. 이 방법의 가장 큰 장점은 기존의 웹 시스템에 아무런 수정을 요구하지 않는다는 것이다.[4][5]

3. XML-Signature 구문과 전체 시스템 구성

XML의 장점인 문서 자체에 구조적 정보를 가지고 있기 때문에 Signature 일부 혹은 문서전체에 적용이 용이하고 Manifest를 이용하여 서명시 각각의 다른키로 아주 많은 문서를 암호화 시키는데 용이하다. 또 하나의 장점은 XML문서 에 NameSpace를 사용할 수 있다는 점이다. XML Signature은 완전성, 메시지확인(Message
Authentication) 및 서명자 확인 서비스 제공한다.

3.1 XML-Signature Syntax 구조 및 태그별 기능

```
(1) <Signature>
(2)     <Signedinfo>
(3)     (canonicalizationMethod)?)
(4)     (SignatureMethod)
(5)     <Reference (URI=)?>
(6)       (Transforms)
(7)       (DigestMethod)
(8)       (DigestValue)
(9)     (</Reference>)+
(10)    </SignedInfo>
(11)    (SignatureValue)
(12)    (KeyInfo)?
(13)    (Object)*
(14) </Signature>
```

[그림 2] XML Signature Syntax 구조

(1-14) Signature 엘리먼트는 루트엘리먼트이고 다음과 같은 구조을 따른다.

" ? " : zero or one occurrence
" + " : one or more occurrence
" * " : zero or more occurrence

(2-10) Signedinfo 엘리먼트는 사실상 서명된 정보이고 Core validation of SignedInfo는 두 가지 의무적인 프로세스로 구성된다.

1. Validation of the signature over SignedInfo
2. Validation of each Reference digest within SignedInfo

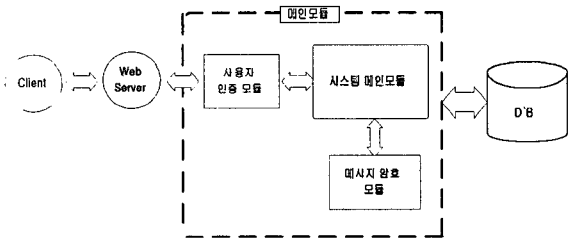
(3) CanonicalizationMethod Signedinfo가 서명의 일부로써 Digest되기전에 Signedinfo 엘리먼트를 Canonicalize 하는데 사용된다.

(4) SignatureMethod은 Canonicalized Signedinfo 를 SigntureValue로 바꾸기 위해 사용된 알고리즘이다. 이것은 digest algorithm과 키의 독립적인 알고리즘의 조합 그리고 다른 padding과 같은 알고리즘과도 조합되는 것이 가능하다. (그예로 RSA-SHA1이 있다.)

(5-9) 각각의 레퍼런스 엘리먼트는 데이터 객체에 정의된 것 위에 digest method 그리고 결과 digest 값으로 계산된 것을 포함한다. 그것은 또한 digest 하기위한 입력을 만들어 낼수 있는 전송(Transforms)을 포함한다.
(6) Transform 엘리먼트는 어떻게 서명자가 digested된 데이터 객체를 얻는지를 묘사하고 각각의 Transform의 출력은 다음 Transform 엘리먼트의 입력값이 된다.
(10) Keyinfo는 서명을 검증하는데 필요한 정보를 가지고 있다. 즉 식별하기 위한 가능한 폼의 자격여부, 키 이름, 키 등의 알고리즘등과 같은 정보를 포함하고 있다.
(11) SignatureValue 엘리먼트는 디지털 서명의 실제 값을 가지고 있고 SignatureMethod에 정의된 것에 따라 인코드 되어 진다.
(12) KeyInfo 엘리먼트 Keys, Certificates, 공개키 관리정보를 포함한다.
(13) Object 엘리먼트는 MIME 타입, ID, Encoding 속성을 포함한다.

3.2 전체 시스템 구조도 및 작동

XML/EDI 시스템의 전체 구조는 시스템 사용자 인증 모듈, 시스템 메인모듈(문서 생성 모듈, 문서 저장 모듈, 문서 검색 모듈, 문서 관리 모듈, Template 문서 관리 모듈, E-mail 전송 모듈, 메시지 암호 모듈), DB부분으로 구성되어 있다.

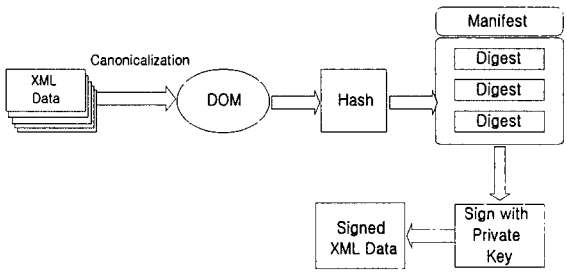


[그림3] XML/EDI 시스템 전체 구조도

본 시스템의 전체 구조도는 [그림3]과 같고 이 시스템은 Microsoft Internet Explore를 사용하여 사용자가 메시지를 암호화하여 다른 사용자에게 메시지를 보내는 것인데 이것은 반드시 이 시스템에 사용자 등록절차를 마친 사용자들끼리만 서로 메시지를 주고받을 수 있도록 설계되어 있다. 즉 어떤 사용자가 메시지를 암호화하여 보내고자 할 때 항상 이 시스템의 모듈을 거쳐 보내지고 또한 수신자 역시 이 시스템를 통해 복호화 하여 메시지를 읽을 수 있다.

3.3 메시지 서명모듈 구조도

XML Signature가 DOM, SAX Processing을 사용하는 시스템에서 검증하거나 인증된다면 Caninical Method는 SAX event 순서나 DOM Tree의 관계된 부분을 직렬화 할 필요가 있는데 본 시스템을 XML-C14N과 같은 XML Canonicalization 스펙에 정의를 따르므로 직렬화 문제를 해결한다.[7]



[그림4] 전자서명 구조도

전자서명 구조도는 [그림4]와 같고 XML 문서는 DOM Parser를 이용해 직렬화 하기 위해 Canonicalization를 거친다음 DOM Parser를 이용해 파싱 하고 Hash를 거친다음 Manifest를 사용하여 Hash를 거친 메시지를 Digest하고 Digest를 거친 메세지를 개인키를 사용해 전자서명된 XML Data을 생성한다.

3.4 알고리즘 정의 및 구현 요구사항

XML 디지털 서명(digital Signature)표준에 사용되는 알고리즘을 상술하면 다음과 같다.

1) Digest Algorithm - SHA-1(Required)
Algorithm URI : http://www.w3.org/2000/07/xmldsig#sha1

2) Encoding Algorithm - base 64(Required)
Algorithm URI
http://www.w3.org/2000/07/xmldsig#base64

3) MAC Algorithm - HMAC-SHA1(Required)
Algorithm URI - http://www.w3.org/2000/07/xmldsig#hmac-sha1

4) Signature Algorithm - DSAwithSHA-1(Required)
RSAwithSHA1(Recommended)
Algorithm URI - http://www.w3.org/2000/07/xmldsig#dsa-sha1
http://www.w3.org/2000/07/xmldsig#rsa-sha1

5) Canonicalization Algorithm - minimal(Recommended)
Canonical XML(Required)
Algorithm URI
http://www.w3.org/2000/07/xmldsig#minimal

http://www.w3.org/TR/2000/WD-xml-c14n-20000710

6) Transform - XSLT(Optional)
XPath(Recommended)
Enveloped Signature(Required)
AlgorithmURI- http://www.w3.org/TR/1999/REC-xslt-19991116

http://www.w3.org/TR/1999/REC-xpath-19991116

http://www.w3.org/2000/07/xmldsig#enveloped-signature

알고리즘들은 알고리즘기능(DigestMethod,Transform, SignatureMethod, CanonicalizationMethod)]을 하는 엘리먼트에 대한 애트리뷰트의 식별자인 URI에 의해 식별된다.

4. 결론 및 향후연구 방향

본 논문에서는 인터넷 상에서 XML/EDI 시스템을 거쳐 XML-Signature를 이용하여 메시지를 서명하므로써 송수신이 이루어지므로 메세지를 안전하게 통신할 수 있게 하기 위한 모듈을 설계하였다. 향후 연구는 인터넷의 급속한 보급 및 활용으로 전자상거래 및 B2B 시장에 보안 기능을 요구하는 서비스가 웹 보안의 중요성이 더욱 강조되고 있으므로 향후 PKI(Public Key Infrastructure)시스템 기술의 도입으로 네트워크상에 연결된 각 사용자 및 메시지에 대한 인증기능을 부여하므로 강력한 보안 체계를 구축할 수 있도록 연구 할 것이다.

5. 참고문헌

[1] W3C, "XML-Signature Requirements" http://www.w3.org/TR/xmldsig-requirements
[2] W3C, "XML-Signature Syntax and Processing" http://www.w3.org/TR/2000/WD-xmldsig-core-20000711/
[3] W3C, "Extensible Markup Language(XML)Activity http://www.w3.org/XML
[4] G. Bossert, et al., Considerations for Web Transaction Security, RFC 2048, 1997.1.
[5] J. Weeks, etc, CCI-Based Web Security : A Design Using PGP, WWW Journal 95, 1995
[6] A. Freier, P. Karlton, and P. Kocher, The SSL Protocol, Version 3.0, http://www.netscape.com/eng/ssl3/3-spec.ps, 1996.3.
[7] W3C, "Canonical XML Version 1.0" http://www.w3.org/TR/xml-c14n