B2B 기반의 XML 문서 설계 및 보안에 관한 연구

김승중*, 조현훈**, 류성열***
*숭실대학교 컴퓨터학과
{seaice, hhcho}@selab.soongsil.ac.kr syrhew@computing.soongsil.ac.kr

A Study on the B2B based XML Document Design and Security

Seung-Joong Kim*, Hyun-Hoon Cho**, Sung-Yul Rhew***
*School of Computing, Soongsil University

요 약

"B2B 에서의 XML 보안"에 관해서 현재 많은 연구가 활발히 진행되고 있다. 인터넷상에서 뛰어난 확장성을 가지고 있고, 풍부한 자료구조, 국제적 문자에 대한 탁월한 처리를 가진 XML 을 많은 기업들이 B2B(Business to Business)에서 많이 사용하고 있다. 또한 EDI(Electronic data Interchange)에서도 XML 을 사용한 문서 교환이 활발하게 이용되고 있다. 하지만 XML 에서는 보안에 관한 많은 취약점을 가지고 있는 것이 사실이다. 본 논문은 XML 의 보안상의 취약점, XML 의 보안에 대한 기술, 그리고 인터넷에서 XML 디지털 인증에 관해 구현하였다.

1. 서론

HTML은 초기 출판을 목적으로 탄생된 마크업(Markup) 표준으로, 어떤 내용을 어떻게 화면에 표시할 것인지를 정의할 수 있었다. 많은 수의 상품이나 기타 문서들을 받아서 비교, 분석하거나 문서를 전달 받아 자동으로 정보시스템에 저장할 때, HTML 형태로 전달된 데이터를 자동으로 이해하는 데에는 많은 한계가 있다.

어떠한 하나의 웹 사이트로부터 생성된 HTML문서를 분석하여, 원하는 정보를 추출하는 방법은 너무 비효율적이며, 추출한 정보의 가공도 어렵다. 따라서 이러한 문제점들을 해결하기 위한 새로운 표준 즉, 새로운 형태의 언어가 필요하게 된 것이다.

XML은 해당 분야에서 필요한 마크업(Markup)을 정의하여, 그 분야에서 필요한 의미를 표현할 수 있도록 허용하는 메타 언어(Meta Language)이다. XML문서의 내용과 구조를 검증하는 데에는 DTD(Documents Type Definition)와 XML Schema가 사용된다. [2][4][6]

2장에서는 본 논문과 관련된 EDI, XML&EDI, XML에서의 문서 교환, SSL을 통한 문서 교환 등에 대하여 기술한다. 3장에서는 B2B에서의 XML 문서를 설계하여 EDI와의 차이점을 기술하고 4장에서는 XML 문의 디지털 서명에 관해서 기술한다. 5장에서는 본 논문의 결론과 향후 연구과제에 관해서 기술한다.

2. 관련 연구

2.1 EDI (Electronic Data Interchange)

EDI는 기업과 기업간에 교환되는 공식적인 문서를 전자문서 형태로 변환하여 네트워크 상에서 전달함으로써 시간과 비용을 절감하기 위한 것이다. 임의의 기업과 기업 사이에 전자문서 교환을 가능하게 하기 위해서 산업별, 지역별 표준화가 진행되었고, UN/EDIFACT 국제 표준이 제정되어 현재 사용되고 있다. EDI의 문제점으로는 문서의 내용을 추가하거나 삭제 수정할 수 없다는 점이다. 예를 들어 기업의 접촉 창구에 대한 회사명, 이름, 제목, 주소 등으로 구성되었을 때 개별 회사의 입장에서는 필드들을 추가하거나 삭제할 수 없다. 따라서 이러한 문제점을 해결하기 위해서는 결국 회사간에 동일한 솔루션을 설치해야 한다. [7][8]

2.2 XML & EDI

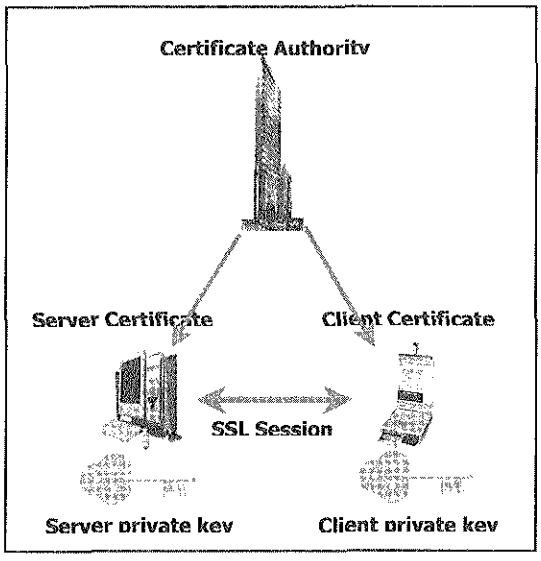
XML과 EDI의 차이점은 XML의 경우에는 구성된 요소를 보고 그 문서의 내용을 알 수 있다는 점이다. EDI의 경우에는 UN/EDIFACT에 익숙하지 않은 사람인 경우에는 EDIFACT 스펙(Specification)이 필요하다. 예를 들면 EDI의 NAD 코드 대신에 XML의 name, address라는 의미가 있는 구성요소를 사용하여 의미를 전달할 수 있다. 이러한 메시지는 프로그램에 의해 처리되지만, 프로그램을 개발하고 유지, 보수하는 일은 프로그래머가 하게 된다. 따라서 프로그램의 판독성은 중요한 것이다. [7][8][12]

2.3 B2B에서의 문서 교환의 보안

일반적으로 B2B에서의 안전한 메시지 교환은 여러 가지 고려 사항이 있다. 첫째로, 문서 내용이 인증 받지 않은 실체에 의해 감시되거나 복사될 수 없다. 둘째로, 문서 내용이 인증 받지 않은 실체에 의해 변경될 수 없다. 셋째로, 문서는 반드시 CA에 의하여 인증되어야 한다. 넷째로, 문서 송신자가 문서 송신 사실과 문서의 내용을 부인할 수 없다. 본 논문에서는 인증기관에 의해 인증이 되어야 하지만, 인증기관의 인증을 사용하지 않고 key 생성에 의해 구현하였다. [7][12][13]

2.4 SSL을 통한 문서 교환

인터넷 상에서 가장 중요한 요소는 바로 보안이다. 마찬가지로 B2B에서의 문서 교환은 보안이 바로 핵심 사항이다. 문서가 감시되거나 변경된다면 사업 파트너와의 신뢰관계를 형성하기는 어렵다. 암호를 필요로 하는 웹 사이트는 문서 암호화를 위하여 SSL(Secure Socket Layer)을 사용한다. SSL은 HTTP 연결을 안전하도록 만들려고 넷스케이프에 의해 정의되었다. 브라우저안에서 SSL을 구현하였으므로 SSL은 안전한 HTTP 연결의 표준이 되었으며, 현재는 모든 브라우저들과 HTTP 서버들은 SSL을 지원한다. SSL은 세션 계층에 있으며, 현재의 버전은 SSL v3이다. SSL의 인증을 위해 X.509 인증서를 사용한다. [1][2][5][6]



[그림1] SSL Session

[그림 1]은 서버 인증을 위하여 SSL이 동작하는 과정을 나타내고 있다. SSL을 사용하기 위하여, 웹사이트는 디지털 인증서를 발급하는 인증기관(CA)으로부터 디지털 인증서를 받아야 한다. SSL에서 사용하는 디지털 인증서 포맷은 X.509로서 이는 ITU-T에 의하여 정의되었다. [1][5][8]

3. XML 문서의 설계

3.1 XML 문서 설계

XML 기반으로 B2B 문서 교환에 적합한 문서 포맷에 대한 설계를 하기 위해서는 여러 가지 고려해야 할 사항이 있다. 문서는 하나의 어플리케이션에서 발생하여 전송된 다음, 다른 어플리케이션에서 소모된다. 이러한 어플리케이션은 B2B에서 사용되며, 일단 고정되면 고치는 것은 어렵다. 본 논문에서는 DTD설계에 있어서 다루어야 할 확장성, 호환성, 일반화 등에 대하여 여러 가지 방법을 제시하겠다.

3.2 XML 문서 설계시 고려 사항

DTD간의 호환성을 기술할 수 있는 정해진 방법은 없다. DTD가 고정되어 사용되고 있다면 수정하기가 어렵다. 좋은 DTD는 오랜 기간 동안 갱신 없이 사용될 수 있어야 한다.

첫째로, DTD를 읽기 쉬우면서도 유지하기 쉽도록 하기 위한 한가지 방법은 엔티티를 광범위하게 사용하는 것이다. 즉, 공통의 내용을 각각정의하기 보다는 하나의 엔티티 안에 사용하는 것이 좋다. [그림2]는 DTD를 설계함에 있어 엔티티를 사용하는 방법에 대한 예제이다. (1)보다는 (2)를 사용해서 확장성을 높일 필요가 있다. [3][4][6]

(1).

```
<! ELEMENT order (customer, shop, itemlist)><! ELEMENT
customer (name, address)>
<! ELEMENT shop (name, address)><! ELEMENT name
(#PCDATA)>
<! ELEMENT address (#PCDATA)>
```

(2).

```
<!ELEMENT % format "name, address">
<!ELEMENT order (customer, shop, itemlist)><!ELEMENT
customer (% format;)>
<!ELEMENT shop (% format;)>
<!ELEMENT name (#PCDATA)>
<!ELEMENT address (#PCDATA)>
<!ELEMENT itemlist (#PCDATA)>
```

[그림 2] DTD 설계

둘째로, DTD가 읽기 쉽고 유지하기 쉽다고 해도, DTD를 수정할 때에는 여러 가지 사항을 고려하여야 한다. 허용된 구성요소들의 개수에 관한 조건을 완화시키는 것이 중요하다.[3][4][6][8]

4. XML 문서의 디지털 서명

4.1 XML 문서의 서명

XML 문서에 필요한 서명을 하는 방법으로 본 논문에서는 해시 값을 사용하도록 하겠다. XML 문서를 하나의 문자열로 간주하여 그 해시 값을 계산하는 것이 가능하다.

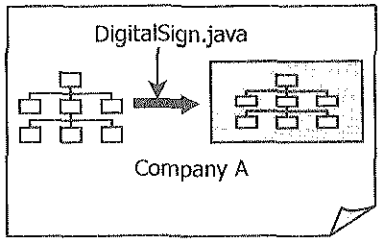
기업과 기업간에 서로 서명한 XML 프로세서에 대한 구현이 다르게 이루어졌다면, 논리적인 내용에 변화가 없음에도 불구하고 처리하는 동안 표면적인 문자열이 바뀔 것이며 따라서 무효한 서명으로 끝나게 될 것이다.

4.2 XML 문서의 처리

첫째, 여백문자 처리는 속성들 사이의 여백 문자들의 개수는 XML에 있어서 중요하지 않으므로 XML 프로세서는 빈칸의 개수를 유지할 필요가 없다. 둘째, 속성들의 기본값은 고정되어 선언된 속성들은 선택적으로 존재할 수 있다. 예를 들어 <creator status="closed">와 <order/>는 동등한 것이다. 셋째, <creator/>와 같이 사용하거나, <creator> </creator>과 같이 사용하여 표현할 수 있다. 넷째, 속성들의 순서를 중요하지 않다. [4][8][9]

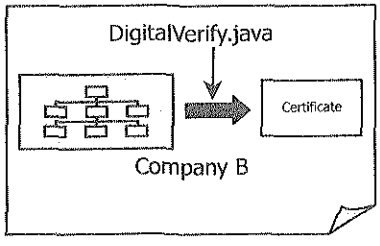
4.3 XML 문서의 디지털 서명

XML 디지털 서명은 두개의 Java프로그램과 두개의 XML 문서로 이루어 진다. XML 문서에 디지털 서명을 하는 프로그램(DigitalSign.java), 검증을 하는 프로그램(DigitalVerify.java), XML 문서(Send.xml), 디지털 서명을 저장하는 XML 문서(Save.xml)으로 구성된다.



[그림3] 디지털 서명

[그림3]에서 보듯이 전송하는 XML문서를 DigitalSign.java을 이용하여 디지털 서명을 하게 된다. 이때 DOMHash를 사용한다. 서명을 하여 보낸 XML 문서를 DigitalVerify.java를 구조를 분석하고, 실제로 서명된 서명인지의 여부를 검증한다. [3][5][6][9][10][11]



[그림4] 검증

[그림4]는 Company A에서 Company B로 전송된 XML문서의 검증 과정을 나타낸 것이다. [그림5]는 전송되는 XML 문서의 내용이다. [6][10][11][12]

```
<?xml version="1.0">
<root>
    <order>
      <item id="K4" date="2001.03.08">5768-KKK</item>
          <quantity>5</quantity>
          <name>Soongsil Company</name>
    </order>
</root>
```

[그림5] XML 문서

5. 결론 및 향후 연구과제

본 논문에서는 B2B에서의 XML 문서 설계에 대한 방법을 제시하였고, B2B에서의 XML 문서 교환시 디지털 서명에 관해서 구현하였다. 초기 XML이 발표되었을 때에 많은 기업들이 환영하였지만, 현재 B2B에서는 너무 많은 XML 문서들이 어떠한 표준 없이 교환되어지고 있다. 따라서 XML이 많은 효율성을 가져왔지만, 반대로 많은 표준을 양산함으로써 오히려 기업과 기업사이에 혼란을 야기시켰다. 이러한 문제점을 해결하기 위해서는 RDF 같은 것이 빨리 정착되어야 한다. 또한 B2B에서 XML 문서의 교환에서 현재의 보안으로서는 너무 미약하므로 더 많은 연구와 개발이 있어야 할 것이다.

6. 참고문헌

[1] 이정하, 이규철, "XML 프로토콜," 정보과학회지, 19 권 제 1 호, pp 31-37, 2001
[2] 이강찬, 손홍, 박기식, "XML 표준화 동향," 정보과학회지 19 권 제 1 호, pp 6-14, 2001
[3] David Hunter, Curt Cagle, Dave Gibbons, Nikola Ozu, Jon Pinnock, Paul Sepencer, Beginning XML, Wrox press, 2000
[4] Neil Bradley, The XML companion, ADDISON-WESLEY, 2000
[5] Calisle Adams, Stefe Lloyd, UNDERSTANDING PUBLIC-KEY INFRASTRUCTURE, MTP, 2000
[6] Alexander Nakhimovsky, Tom Myers, Professional Java XML Programming, 정보문화사, 2000
[7] 김형도, B2B 전자상거래 @XML, 배움터, 2000
[8] W3C(World Wide Web Consortium), Extensible Markup Language(XML)1.0, Available at http://www.w3.org/XML/
[9] W3C, Extensible Stylesheet Language(XSL), Available at http://www.w3.org/Style/XSL/
[10] W3C, Documents Object Model(DOM), Available at http://www.w3.org/DOM/
[11] W3C, XML Signature WG, Available at http://www.w3.org/Signature/
[12] W3C, XSL Transformation(XSLT), Available at http://www.w3.org/TR/xslt
[13] 한국전자인증, 전자서명, Available at http://www.crosscert.com/