XML 보안 기술을 이용한 SOAP 기반 XML 전자상거래 시스템의 설계 및 구현

진성근° 이재동 박진표
경남대학교 정보통신공학부
donquis°@hanmail.net {jdlee, jppark}@eros.kyungnam.ac.kr

Design and Implementation of XML E-commerce System based on SOAP using XML Security Technology

Sungkeun Jin° Jaedong Lee Jinpyo Park
Dept. of Information and Communication Engineering, Kyungnam University

요 약

정보통신 기술의 비약적인 발전으로 인해 인터넷을 이용한 전자상거래가 일반적인 거래형태의 하나로 자리 잡아 나가고 있다. 그러나 보안상의 문제로 전자상거래 활성화에 걸림돌로 작용하고 있다. 이에 본 논문에서는 전자상거래 서비스의 보안성 문제를 해결하는 방안으로 XML 서명과 XML 암호화 표준에 입각한 SOAP 기반의 전자상거래 시스템을 설계 및 구현하였다.

1. 서 론

오늘날 정보통신 기술의 발달 및 WWW의 출현으로 인터넷의 이용이 급격히 증가함에 따라 상거래 분야에 있어서도 시간적 공간적인 제약을 뛰어넘는 전자상거래가 일반적인 거래형태의 하나로 자리 잡아 나가고 있다. 그러나 전자상거래가 가져다 주는 편리함과 효율성에도 불구하고 비대면적이라는 특성에서 오는 신뢰성 및 안전성에 대한 문제가 전자상거래를 활성화하는데 큰 걸림돌로 작용하고 있다.

사용자를 대상으로 한 여러 가지 여론조사에 따르면 전자상거래의 가장 큰 장애요인은 전자상거래에 대한 신뢰성 결여에서 야기되는 보안문제로 지적하고 있다.

전자상거래 서비스의 안전성 문제의 해결 방안은 크게 두가지로 외부의 불법적인 침입을 방어하거나, 통신 내용을 보호하는 기능이다. 이 두부분을 구체적으로 보면 사용자 인증, 데이터 무결성 보장, 송수신 부인봉쇄 및 키 관리 및 접근제어 등 다양하고 복잡하다.

최근, XML 기술의 유용함이 인식되기 시작하면서, 여러 분야에서 기존의 보안기술 표준을 XML로 재구성하고자 하는 노력이 일고 있다. 많은 전자상거래 업체들의 자사의 서비스 플랫폼을 XML 기반의 분산시스템으로 바꾸고 있는 실정이다.

이런 변화에 발맞추어 XML 기술을 적용한 XML 보안 기술의 중요성이 크게 부각되고 있다. 이는 전자상거래 및 글로벌 비즈니스의 활성화를 위해 반드시 필요한 기술이며, 이에 대한 연구 및 지원이 지속적으로 이루어져야 할 것이다.

현재 XML 보안 기술 분야로는 디지털 서명,암호화, 키 관리, 접근제어 등에 관한 것이 있으며, 분산시스템 기술 분야로는 SOAP에 기반한 웹서비스가 있다. IETF와 W3C에서 XML-Signature, XML-Encryption 등에 대한 표준화를 진행중에 있다[1,2,3].

이에 본 논문에서는 기업 간 문서교환을 위한 SOAP 기반 XML 전자상거래 시스템을 구축하고, 보안상의 요구를 충족하기 위하여 W3C의 XML 전자서명과 XML 암호화 표준에 입각한 보안을 위한 시스템을 설계 및 구현하였다.

2. 관련 연구

XML 기술의 급속한 성장으로 기존의 범용적인 네트워크 보안 기술과 함께 XML 기반의 보안기술 또한 중요하게 여겨지고 있다. 현재 XML 보안 기술은 아래 그림 1과 같이 W3C에서 표준화가 계속 진행되고 있다.

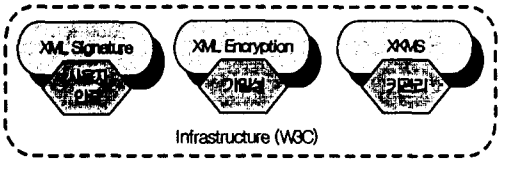

그림 1. 계층별 XML 보안기술

그리고 분산 시스템 구축 기술로 많이 사용되고 있는 SOAP 기술에 대해 알아본다.

2.1 XML 서명 (XML Signature)과 원시 전자서명

전자서명은 전자문서의 메시지 내용이 수정 및 변조되지 않았음을 보장하는 데이터 무결성과 메시지의 주체인 사용자의 신원을 받는 사람에게 확인할 수 있게끔 하는 인증 기능을 한다.

전자서명의 생성 절차는 다음과 같다. 전자서명을 해야 할 데이터를 가지고 있다고 하자. 서명자는 데이터를 해쉬 함수를 사용해 넓은 범위의 데이터를 작은 범위의 데이터로 바꿔준다. 그 데이터를 다이제스트라 한다. 다이제스트를 서명자의 비밀키로 암호화한다. 암호화된 값인 서명값을 원본 데이터와 함께 보낸다. 원시 전자서명은 그림 2와 같다[4].

```
MA0GCSqGSIb3DQEBBQUA
kvQjL0pmMhUWZ3NYvAYvnVpTWQa7ed+bb3pfFjq3jxbTwNLoPFqH9wwtl6Rgg
ApcraGCrbKPlAYMlVGaVdtqA==
I authorize a payment of $2 from my checking account to the paperboy.
L. Mever
```

그림 2 원시 전자서명

첫 번째 줄에는 알고리즘 식별자에 대한 정보가 담기며, 다음 두 번째 줄에는 서명값이 담기고, 나머지는 원본 문서가 된다. XML 서명은 그림 3과 같다[4].

```
<Signature>
  <SignedInfo>
    <SignatureMethod
      Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <Reference="file:///C:\check.txt">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>MA0GCSqGSIb3DQEBBQUA=</DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue>
    kvQjL0pmMhUWZ3NYvAYvnVpTWQa7ed+bb3pfFjq3j
    xbTwNLoPFqH9wwtl6RggApcraGCrbKPlAYMlVGaVdtqA==
  </SignatureValue>
</Signature>
```

그림 3 XML 서명

<SignatureMethod>는 서명 알고리즘을 식별하고 <Reference>는 실제 파일을 가리키기 위해서 쓰인다.

원시 포맷은 서명의 조각들을 구별할 구조가 없다는 게 문제가 된다. 그래서 이런 서명의 수취인은 이 포맷에 대해 미리 알고 있어야 한다. XML 서명은 쉽게 데이터의 구조를 알 수 있고 플랫폼에 독립적이라는 장점이 있다.

2.2 XML 암호화 (XML Encryption)

XML 문서의 일부분 즉, 보호해야 할 중요한 데이터만을 암호화할 수 있는 보안기술로서 기밀성을 강화할 수 있다.

2.3 SOAP (Simple Object Access Protocol)

SOAP은 텍스트 기반 XML 프로토콜이다. 이 점 덕분에 이종 플랫폼에 종속되지 않는다. 다른 분산 시스템과는 달리 HTTP, XML과 개방형 표준안을 근간으로 만들어 졌다.

3. 구 현

3.1 개발 환경

전체 시스템 개발환경은 아래와 같다.

① SUN J2SE 1.4.x : 자바 개발툴
② IBM XML Security Suite(XSS4J) : XML 서명과 XML 암호화 API 제공[5]
③ Apache Xerces-J 2.2.1 : XML 파서
④ Apache SOAP 2.3.x : SOAP RPC API 제공[6]
⑤ Apache Tomcat 4.1.x : 웹 애플리케이션 서버

3.2 전체 시스템 구성도

현재 구현된 시스템은 그림 4와 같이 내부적으로 구성되어 있다.

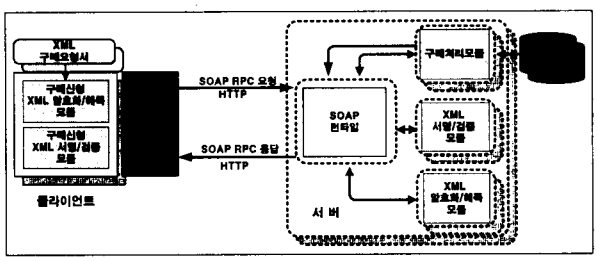

그림 4 전체 시스템 구성도

3.3 처리 과정

전체 시스템 처리 과정은 아래와 같다

① 클라이언트는 구매신청서를 XML 암호화 시킨다.
② 암호화된 문서를 XML 서명한다.
③ 서버측 SOAP-RPC 메소드를 호출한다.
④ 서버는 먼저 서명을 확인한다.
⑤ 서명 검증이 성공하면 해독하여 주문내역을 DB에 저장하고 구매 확인 메시지를 생성한다.
⑥ 서명 검증이 실패하면 서명 실패 메시지를 생성한다.
⑦ ⑤와 ⑥에 생성된 각각의 메시지는 다시 서명하여 클라이언트측에 전송한다.
⑧ 클라이언트는 서명된 문서를 확인하고 최종 구매 확인서를 받게 된다.

3.4 시스템 모듈

전체 시스템은 3개의 모듈로 구성되어 있다.

① XML 암호화/해독 모듈
- XSS4J를 사용하여 입력으로 구매신청서(XML문서)를 받아 중요하다고 생각되는 부분을 암호화한다. 그림 5는 신용카드 정보를 암호화 하였다. 또한 암호화된 구매신청서를 원본 문서로 해독한다.

② XML 서명/검증 모듈
- XSS4J를 사용하여 구매신청서를 서명하는 모듈이다. 그림 6에 나타난다. 또한 서명된 구매신청서를 검증한다.

그림 5 암호화된 구매신청서

그림 6 서명된 구매신청서

③ 구매 처리 모듈

- XML 파서를 이용하여 구매확인서를 생성한다. XML 서명이 성공했을 때와 실패했을 때에 따라 다른 메시지가 생성된다.

4. 결 론

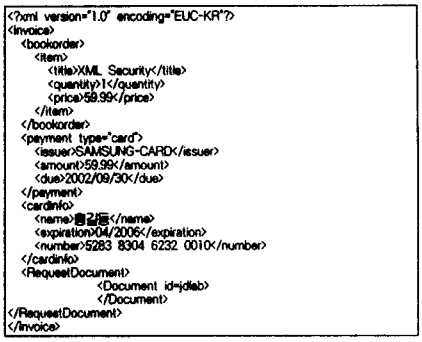

그림 7. 구매 신청서

본 논문에서는 전자상거래 서비스의 보안성 문제를 해결하여 전자상거래에 활성화를 가져오도록 XML 서명과 XML 암호화 표준에 입각한 SOAP 기반의 전자상거래 시스템을 구현하였다.

최근 W3C에서는 여기에서 사용한 XML 보안기술보다 나은 기능을 포함하는 기술들이 계속 연구되고 있으며 그에 대한 프로그램들도 개발되고 있다. 그래서 좀 더 나은 플랫폼을 구성하여 시스템을 업그레이드 시킬 수 있을 것이며 많이 활용될 수 있을 것이다.

키관리 분야의 기술인 XKMS(XML Key Management)가 W3C에 표준화된 상태지만 여기에서는 구현하지 않았다. XKMS는 한층 더 전자상거래 서비스의 보안성 문제를 해결해 줄 기술이다[7].

향후 본 시스템과 연동하여 차세대 PKI 기술인 XKMS를 사용하여 사용자의 편의성과 보안성을 동시에 만족시키는 응용 시스템을 개발할 예정이다.

여러 보안 분야에 대한 XML 표준들이 계속 연구되고 있으므로 앞으로 더욱 더 발전된 전자상거래의 활성화를 가져 올 것이다.

5. 참고 문헌

[1] W3C, "SOAP Version 1.2 Part 2: Adjuncts", Candidate Recommendation 19 December 2002, http://www.w3.org/TR/2002/CR-soap12-part2-20021219

[2] W3C, "XML-Signature Syntax and Processing", Recommendation 12 February 2002, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212.

[3] W3C, "XML Encryption Syntax and Processing", Recommendation 10 December 2002, http://www.w3.org/TR/2002/REC-xmlenc-core-20021210.

[4] Blake Dournaee, "XML Security", McGraw-Hill, 2002.

[5] IBM, "XML Security Suite", 2002, http://www.alphaworks.ibm.com/tech/xmlsecuritysuite.

[6] Apache, "Apache SOAP v2.3.x Documentation", 2002, http://ws.apache.org/soap/docs/index.html.

[7] W3C, "XML Key Management", W3C Working Draft 18 March 2002, http://www.w3.org/TR/2002/WD-xkms2-20020318.