전자상거래 환경에서의 안전한 메시지 전송을 위한 웹 서비스 시스템 설계 및 구현

박종훈* · 김철원**

Design and Implementation of Web Service System for secure Message Transmission in Electronic Commerce

Jong-Hoon Park* · Chul-Won Kim**

요 약

본 논문은 웹 서비스 표준을 이용하여 안전한 메시지 전송을 위한 웹서비스 시스템을 구현하였다. 본 시스템은 싱글사인온 모듈과 SSL(Secure Socket Layer) 모듈과 안전한 메시지 모듈로 구성되어 있다. 이들 모듈들을 적용하기 위해 가격비교사이트를 대상모델로 하여 설계하였다. 싱글사인온 모듈은 SAML(Security Assertion Markup Language) 표준을 사용하였으며, 또한 권한부여와 인증을 제공한다. SSL 모듈은 종단간에 메시지 암호화를 처리하기 때문에, 시스템의 메시지를 안전하게 전송한다. 또한 안전한 메시지 모듈은 웹 서비스 보안 표준을 따르는 XML 암호화와 서명을 적용하였다.

ABSTRACT

This paper describes construction of web services system for secure message transmission appling web services standards. This system composes single sign on module, SSL module and secure message module. We applied these modules to price comparison site. Single sign on module used SAML standards. This module was designed, in order to provide authentication and authorization. As SSL module processes message encryption among end to end, messages of this system are secure. Secure message module is designed according to WS-Security standards and processes authentication, XML signature and XML encryption.

키워드

웹 서비스, 싱글 사인 온, SSL, XML 암호화

Key word

Web Service, Single sign on, SSL, XML encryption

* 중부대학교 컴퓨터학과 (주저자)

** 호남대학교 컴퓨터공학과 (교신저자, cwkim@honam.ac.kr)

접수일자 : 2010. 05. 12

심사완료일자 : 2010. 06. 07

Ⅰ. 서 론

기업환경에서 웹 서비스를 적용하는데 있어서 가장 큰 장애물은 보안 문제이다. 웹 서비스는 방화벽을 통해 외부와도 트랜잭션이 가능한 형태로 변해가고 있다. 결과적으로 웹 서비스는 현재 보안의 새로운 불안요소로 떠오르고 있다. 웹 서비스는 기존 기술보다 더 많은 보안 및 개인정보 유지와 관련된 문제를 야기하고 있다. 따라서 이러한 보안의 취약성을 보완하기 위해 사용자의 신뢰성을 보장하기 위한 인증 및 권한 부여를 제공하는 SAML(Security Assertion Markup Language) 기술과 XML 메시지의 보호를 위해 XML 서명 표준과 XML 암호화 표준들이 필요하다. 또한 서비스 지점간의 메시지 보호를 위해 SSL 기술을 이용할 수 있다. 이러한 다양한 기술을 혼합함으로서 어느 정도 전송 메시지의 보안을 보장할 수 있다.

본 논문에서는 안전한 메시지 전송을 위한 웹 서비스 적용 기술 분야로 전자상거래 분야 중에서 현재 가장 인기 있는 가격비교 사이트에 대한 적용 가능성을 분석하고, 이에 대한 가격비교 시스템을 대상 모델로 선정하여 안전한 메시지 전송을 위한 웹 서비스 시스템을 설계하였다.

먼저 싱글 사인온을 위한 시스템을 구현하기 위해 SAML 환경을 구성하는 서비스 집합을 구성한 후 관련 사이트에 접속할 경우 인증 및 권한부여를 제공하도록 설계하였다. 또한 안전한 메시지 전송을 위해 크게 두가지 방법으로 메시지를 전송하도록 구현하였다. 첫 번째는 SSL를 이용한 메시지 방식을 선택하여 종점간에 메시지를 암호화하여 중간에서 메시지 노출을 보호하는 방식을 선택하였다. 두 번째 방식은 WS-Security 표준 중에서 SOAP 메시지 내에서 인증과 전자서명과 암호화 표준을 이용하여 메시지를 보호하는 방식을 선택하였다. 이들 보안 표준들을 다양하게 적용함으로서 안전한 웹 서비스 구현을 하고자 하였다.

Ⅱ. 웹 서비스 보안 관련 기술

2.1 XML 서명

W3C의 XML 서명 표준은 디지털 서명을 대체하기 위한 XML 기반의 표준을 정의하고 있다. XML 서명은 XML 서명 작업 그룹이 개발하였으며, W3C와 IETF간의 공식적인 연합 프로젝트이다. 이 표준은 인증, 메시지 무결성 및 부인 봉쇄 등을 제공한다. 이 표준이 사용하고 있는 알고리즘에는 디지털 서명 표준 공개키 알고리즘과 보안 해시 인증 알고리즘을 포함하고 있다. 개발자들은 자신들의 알고리즘과 보안 모델을 지원하도록 XML 서명을 확장할 수 있다. XML 서명은 단지 XML 문서만이 아니라 어떠한 타입의 파일이든 서명이 가능하다. 이러한 데이터 객체는 암호화되어 서명되고, 메시지 다이제스트를 생성하는데 사용되게 한다. URI를 통해서 서명 받은 데이터 객체와 연결됨으로서 서명이 이루어진다. XML 서명은 디지털 서명을 통해서 인증을 수행하는 XKMS, SAML 및 그 밖의 다른 XML 기술의 기반이 된다[1,2]. XML 서명 형식은 Enveloped 서명, Enveloping 서명과 Detached 서명으로 3가지 형식이 있다.

2.2. XML 암호화

XML 암호화 표준은 현재 W3C에서 개발된 상태이다. 이 표준은 웹 서비스 보안의 기반을 형성하고 있으며, 디지털 컨텐츠를 암호화하고 해독하는 과정을 정의하는 것을 목표로 하고 있다. XML 암호화는 수신자가 암호화된 내용을 해독할 수 있도록 하는 정보를 표현하고 있고, 또한 암호화된 내용을 표현하기 위해 XML 문법을 사용한다[3,4].

XML 암호화는 보안을 위해서, XML 서명을 사용한 문서의 암호화 및 해독을 처리한다. XML 암호화는 XML 엘리먼트 및 그 내용을 비롯한 어떠한 형태의 데이터이든 보호가 가능하다. XML 암호화는 XML 문서에서 엘리먼트 별로 암호화가 가능하다. 암호화할 데이터는 XML 문서의 EncryptedData 엘리먼트로 대체된다. EncryptedData 요소의 Type 속성은 요소, 컨텐츠 또는 임의의 데이터 중 어떤 것이 암호화되었는지를 나타낸다[5,6,7].

2.3.SAML(Security Assertion Markup Language)

SAML은 인터넷에서 인증, 권한부여 및 승인정보교환을 위해 만든 표준이다. OASIS의 보안 서비스 기술 위원회에서 B2B 및 B2C 통신을 위한 XML 표준으로 SAML을 개발하였다. SAML 프로토콜은 시큐란트 테크놀러지의 AuthXML과 내테그러티의 보안 서비스 마크업 언어(S2ML:Security Services Markup Language)의 2가

지 XML 보안 표준을 결합하여 개발한 것이다. SAML은 서로 다른 조직사이에서 정보를 공유하는 방향으로 추세가 증가함으로 인해 파생된 기술이다. 비록 웹 서비스 기술들이 내부 조직의 분산 컴퓨팅을 발전시킨다 할지라도 조직의 보안 도메인에서 관련 정보를 공유할 표준 방법이 필요하다. 사용자의 증명서 또는 정책 정보와 같은 보안관련 정보를 공유할 수 있는 방법이 필요하며, 이러한 보안 정보를 공유하는 교차 도메인을 지원하는 것이 바로 SAML 표준이다. SAML은 서로 다른 보안 시스템 사이에서 정보를 교환 가능하게 하는 통합 시스템을 지원한다[8,9,10].

Ⅲ. 안전한 메시지 전송을 위한 웹 서비스 시스템 설계 및 구현

3.1 시스템 개발도구 및 개발 환경

본 시스템에서의 개발환경으로 운영체제는 MS 윈도우 2000, 자바환경은 JDK6.0이며, 싱글사인온 통합 서비스를 구현하기 위해 네티그러티사의 jSAML 툴킷을 사용한다. XML 키 관리 스펙과 XML 서명과 XML 암호화를 위해 베리사인사의 TSIK(Trust Service Integration Kit)를 사용하며, 이것은 WS-Security 규격을 지원하는 인터페이스이다.

본 시스템의 백엔드 서비스를 제공하기 위해 EJB환경을 지원하는 BEA SYSTEM사의 Weblogic 서버를 사용하고, 데이터베이스 도구로는 MySQL을 이용하였으며, 웹 서비스 개발 도구로는 Sun사에서 배포하는 JWSDP(Java Web Services Developer Pack)을 이용하여 웹 서비스를 개발한다.

3.2 전체 시스템 설계 구성 모델

먼저 본 논문에서는 기존의 웹 서비스 표준 기술을 적용하여 안전한 메시지를 전송하기 위한 웹 서비스 시스템을 구현하였다. 그림 1의 시나리오 모델에서 맨 먼저 싱글 사인온을 위한 시스템을 구현하기 위해 SAML 환경을 구성하는 서비스 집합을 구성한 후 각각의 백엔드 서비스들은 자기들의 웹 서비스 정보들을 UDDI 레지스트리에 등록한다(1). 이후 프런트 엔드 서비스들은 자기가 서비스요청을 하고자 하는 백엔드 서비스 정보들을 UDDI 레지스트리에서 검색한다. 이때 원하는 정보를 가지고 서비스 바인딩을 준비한다(2). 클라이언트는 자기가 원하는 서비스 지점에 접속하기 위해 해당 SAML 서비스 엔진에 서비스 요청을 한다(3). 요청 받은 SAML 서비스 엔진은 사용자 인증과 권한부여를 수행하고 정당한 사용자일 경우 해당 서비스 사이트로 접속을 허용한다(4). 이때 사용자와 서비스 사이트들과의 실제적인 접속이 이루어지며, 상호간에 메시지 전송은 안전한 메시지를 이용하여 데이터가 전달된다. 이때 전송 방법에는 HTTPS-SSL을 이용한 전송 방식(5)과 WS-Security의 XML 서명과 암호화를 적용한 전송방식(6)을 적용하여 SOAP 메시지를 전송한다.

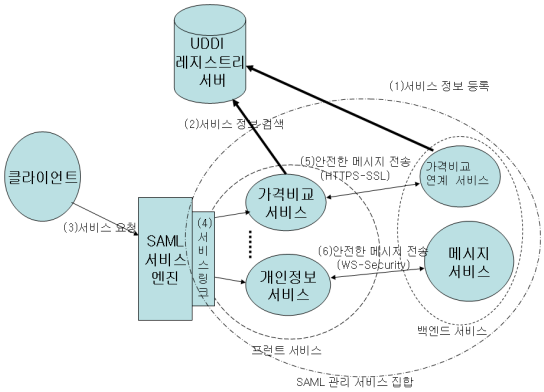

그림 1. 상위수준의 전체 설계 시나리오 모델
Fig. 1 Design senario model of high level

3.3. SAML 시스템 시나리오 및 구현

처음 사용자가 로그인 한 후 이에 대한 인증과 권한부여를 처리하여 원하는 서비스에 로그인 하는 시나리오를 보여주고 있다. 그리고 중간에 SAML 규격을 통하여 인증 및 권한 부여를 하고 있는 SAML 메시지를 보여주고 있다. 다음순서로 시나리오를 실행한다.

(1) 싱글사인온 로그인 시에 세션 아이디를 생성한다. 접근제어 목록과 사용자 인증정보를 인증한다(그림 2).
(2) 가격비교 사이트 접근시 SAML 메시지 프로토콜을 사용하여 보안 접근 요청을 위한 메시지를 출력을 한 후 서버가 클라이언트의 권한을 가지고 있는지 검증한다 (그림 3). 클라이언트의 권한 검증 후 가격비교 사이트에 접속한다.

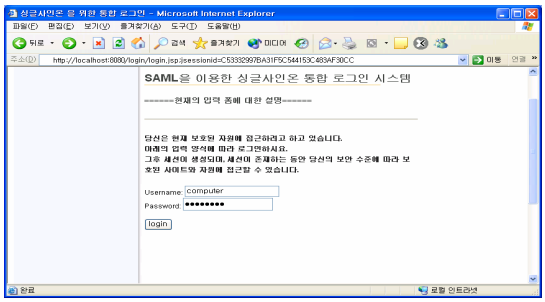

그림 2. 싱글사인온 로그인 화면
Fig. 2 Login screen of single sign on

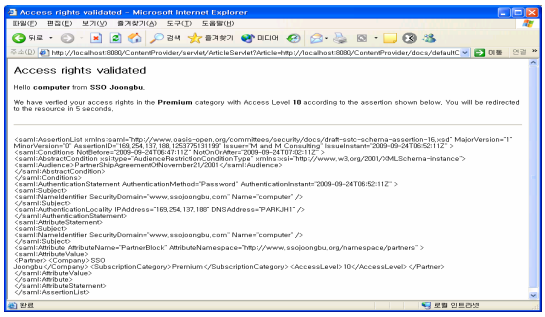

그림 3. SAML 메시지 출력화면
Fig. 3 Output screen of SAML message

3.4. 안전한 메시지 전송을 위한 시스템 구현

3.4.1. 설계 모델

안전한 웹 서비스 시스템 구성을 하기 위해 다음 그림 4와 같이 구성하였다. 이때 클라이언트와 서버 서비스 사이에는 HTTPS-SSL 프로토콜을 이용하여 점대점 암호화를 이용하여 보안을 제공한다. 메시지 서비스 서버 모듈은 클라이언트와 WS-Security의 보안 표준인 인증, XML 서명과 XML 암호화를 이용하여 메시지를 안전하게 전송한다.

이와 같은 안전한 메시지 웹 서비스 시스템을 구현하기 위해 본 논문에서는 그림 5와 같은 시나리오를 구성하였다. 웹 서비스 클라이언트 모듈은 가격비교 사이트로 가정하며, 웹 서비스 서버 모듈은 가격비교 사이트에서 관리하는 연계된 업체들로 가정한다. 클라이언트가 관련 업체들에게 가격을 요청하면, 업체들로부터 가격을 전송받으며, 이때 HTTPS-SSL 방식을 이용하여 메시지를 암호화 한다. 메시지 클라이언트 모듈과 메시지 서비스 서버는 개인 사생활 정보를 송수신 한다고 가정하여 메시지 정보를 암호화하여야 한다. 본 논문에서는 메시지 클라이언트가 개인정보에 대한 질의를 메시지 서비스 서버 모듈에게 하면 이에 대한 응답을 하도록 하였으며, 메시지 내용은 WS-Security의 보안 표준을 이용하여 메시지를 보호한다.

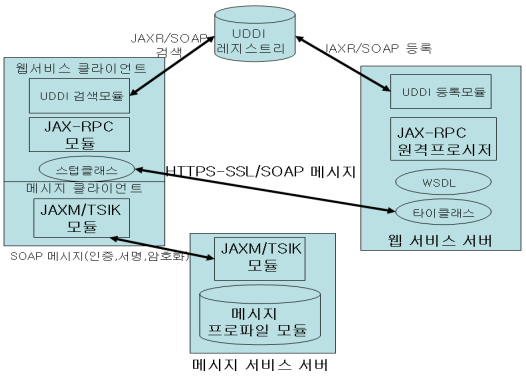

그림 4. 안전한 메시지 전송 시스템 모델
Fig. 4 System model for secure message transmission

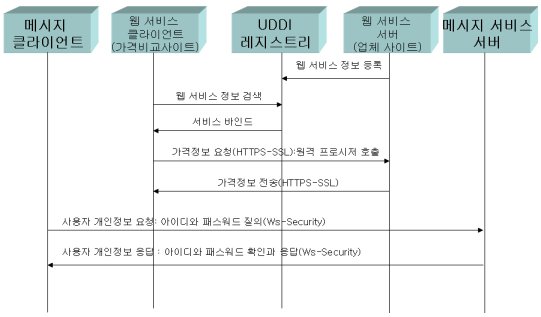

그림 5. 안전한 메시지 전송 시나리오
Fig. 5 Senario for secure message transmission

3.4.2. HTTPS-SSL을 이용한 시스템 구현

구현된 시나리오는 다음과 같다.

가격비교 사이트와 상호 분산 연결된 백엔드 시스템인 shop1, shop2, shop3사이트와 SSL 접속을 하여 필요한 가격정보를 가져오기 위해 준비하고 있다.

다음 그림 6은 shop1 사이트와 SSL 접속을 진행하면서 보안 인증을 요구하고 있다. 이때 클라이언트의 전자서명과 서버의 공개키를 요구한다. 보안 경고 대화창에서 예를 클릭한다.

다음 그림 7은 SHOP1 서버가 클라이언트의 인증서와 개인 서명을 확인한다. 그리고 클라이언트의 아이디와 패스워드를 입력한 후 클라이언트의 인증과 권한 부여를 결정한다.

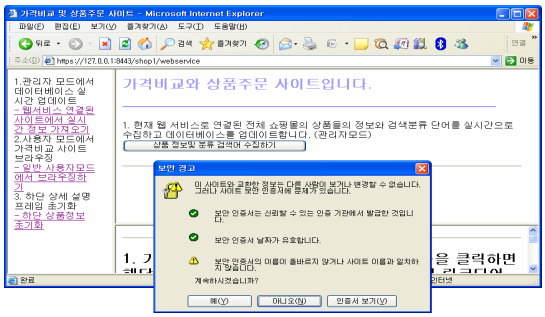

그림 6. 백 엔드 웹 서비스 시스템에 SSL 접속 화면
Fig. 6 SSL connection screen to backend system

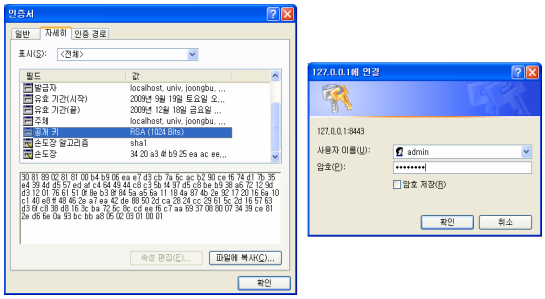

그림 7. 인증서, 사용자 아이디와 패스워드 확인
Fig. 7 Confirmation of user id, password and authentication

3.4.3. WS-security의 보안을 이용한 시스템 구현

본 시스템의 구현 시나리오는 다음과 같다.

먼저 메시지 전송 방식인 XML 서명 또는 XML 암호화를 선택한다. 이러한 메시지 전송 방식에 따라 WS-Security 규격으로 메시지를 변환한다. 요청하고자 하는 정보를 선택한다. 여기서는 개인정보들인 ID, Password, 여권 번호, 카드번호와 같은 중요한 정보를 요청한다. 이들 요청 메시지를 서명하고 암호화하여 전송한다. 이를 메시지 서버가 수신하여 메시지의 인증과 복호화를 한다. 그리고 요청한 내용을 선택하여 그에 맞는 데이터를 데이터베이스에서 가져온다. 메시지 서버에서 이들 내용을 서명하고 암호화하여 메시지를 생성한다. 그리고 이러한 안전한 메시지를 다시 메시지 클라이언트에게 전송한다. 이들 전송시 메시지와 수신시의 메시지를 다음 그림에 보여준다.

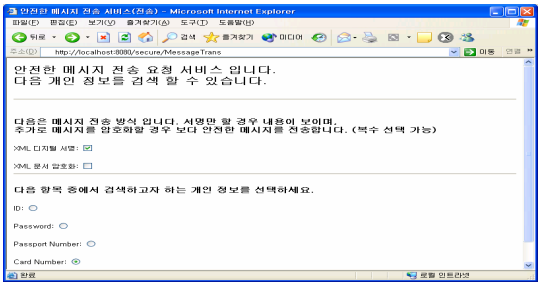

그림 8. 메시지 전송을 위한 카드번호 선택
Fig. 8 Card number selection for message

위 그림 8은 메시지 전송시 사용자가 보안 방식을 선택할 수 있으며, 이에 따라 메시지가 전송된다. 또한 개인 정보를 선택하여 응답 받고자 하는 항목을 선택할 수 있다.

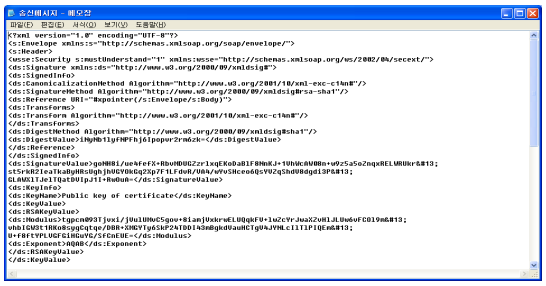

그림 9. 서명된 송신메시지
Fig. 9 Signed transmission message

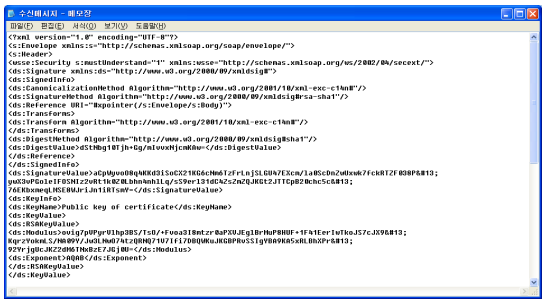

그림 10. 서명된 수신메시지
Fig. 10 Signed reception message

그림 9와 그림 10은 인증과 서명된 송신 XML 메시지와 수신 메시지이다. 메시지 전송 방식에 따라 WS-Security 규격으로 메시지를 변환한다.

Ⅳ. 결 론

본 논문에서는 웹 서비스 표준환경에서 안전한 메시지 전송을 위한 기본요소들을 설계 및 구현하였다. 이러한 표준 웹 서비스 환경을 적용하기 위해 전자상거래 모델 중에서 가격비교 시스템을 적용하여 구현하였다. 본 시스템은 싱글사인온 기술을 적용하기 위해 SAML 표준 기술을 이용하여 사용자 인증 및 권한 허가를 위한 시스템을 구성하였다. 또한 안전한 메시지 전송을 위해 SSL 방식과 함께 WS-security에서 정의된 SOAP 메시지 보안을 이용하여 웹 서비스를 기반으로 한 안전한 웹 서비스 시스템을 설계하고 구현하였다.

본 시스템의 설계 기본 방향은 다음과 같다.

WS-Security규격을 따르는 안전한 메시지를 주고 받을 수 있는 웹 서비스 표준 환경을 구현하는 것이다. 또한 통합 연계 사이트를 운영하여 사용자 인증을 통합하여 로그인 절차를 단순화하는 것이다.

안전한 메시지 전송을 위한 웹 서비스 시스템 구축시 고려사항으로는 이러한 시스템 구축시에 다양한 응용분야에 따라 보안에 대한 여러가지 조합을 필요로 한다. 따라서 시스템 보안 등급에 따라 시스템 성능과 신뢰성 등 다양한 고려를 해야 할 것으로 본다.

참고문헌

[1] E. Simon,, P. Madsen and C. Adams, "An Introduction to XML Digital Signature", www.xml.com, Aug. 2001.

[2] "XML-Signature Syntax and Processing", community.roxen.com, March 2001

[3] 홍기융외 3인, "웹 서비스 보안 기술 표준화 동향", 정보보호학회지 제14권 제4호, 2004.8

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

[5] 강민구, "SOAP 기반의 ebXML 암호화 설계 및 성능 분석", 한국 콘텐츠 학회 논문지 제6권 11호, 2006년

[6] M. Mactaggart, " Enabling XML Security : An Introduction to XML Encryption and XML Signature", www-106.ibm.com, Sep. 2001.

[7] T.Imamura, B. Dillaway, and E. Simom, XML Encryption Syntax and Processing, 2002

[8] Chris McLaren, ed. "Security and Privacy Considerations for OASIS Security Assertion Markup Language." OASIS, April 19, 2002.

[9] Harvey M. Deitel and et al., Java Web Services for Experienced Programmers, Prentice Hall, 2003.

[10] E. DeJesus, "SAML Brings Security to XML", XML Magazine Feb. 2002. XACML

저자소개

박종훈(Jong Hoon Park)

1995년 광운대학교 전자계산기 공학과(공학박사)
1995년 ~ 1998년 한국전산원 선임연구원
1999년 ~ 현재 중부대학교 컴퓨터학과 교수
※관심분야: XML 웹서비스, XML 검색, 시맨틱 웹, XML 보안

김철원(Chul Won Kim)

1997년 광운대학교 전자계산기 공학과(공학박사)
1988년 ~ 현재 호남대학교 컴퓨터공학과 교수
※관심분야: XML 웹 서비스, 이미지 처리 및 검색