XML 정보보호 기술을 이용한 웹 서비스 어플리케이션 보안 모델

전형득, 송유진

동국대학교

Security model of web service application using XML information security

Hyung-deuk jeon, You-jin Song

Dongguk University

요 약

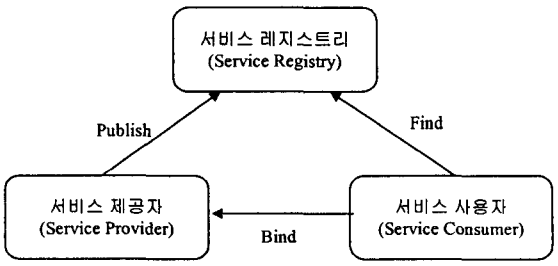
최근 인터넷의 급속한 발전과 함께 웹 어플리케이션 형태로 서비스를 제공하였던 것이 다양하고 개별적인 웹 어플리케이션들을 효율적으로 통합하는 웹 서비스 방식으로 진화하고 있다. 이에 따라, 차세대 플랫폼의 대안으로 웹 서비스(Web Service)가 급부상하고 있다. 이러한 환경에서 서비스의 보안은 필수적인 요소이며, 웹 서비스 보안에 대한 연구개발이 필요하다. 본 논문에서는 웹 서비스에 대한 전반적인 사항을 분석하여 문제점을 도출하고 XML 정보보호기술을 기반으로 웹 서비스의 보호 방안을 제시한다. 그리고, XML-Web Service 보안 모델을 검토하고, 기반구조 및 기능을 살펴본다. 최종적으로 제안된 모델은 차세대 웹 서비스 플랫폼의 기반 기술이 될 것으로 기대된다.

I. 서론

최근 인터넷의 급속한 발전과 함께 웹 어플리케이션 형태로 서비스를 제공하였던 것이 이제는 다양하고 개별적인 웹 어플리케이션들을 효율적으로 통합하는 웹 서비스 방식으로 진화하고 있다. 이에 따라, 차세대 플랫폼의 대안으로 웹 서비스(Web Service)가 급부상하고 있다. 이러한 환경에서 서비스의 보안은 필수적인 사안이며, 웹 서비스 보안에 대한 연구개발이 필요하다. 본 논문에서는 웹 서비스에 대한 전반적인 사항을 분석하여 문제점을 도출하고 이를 보호할 수 있는 방안을 XML 정보보호기술을 기반으로 제시한다. 이에, XML-Web Service 보안을 위한 모델을 설명하고, 기반 구조 및 기능을 살펴본다. 최종적으로 제안된 모델은 차세대 웹 서비스 플랫폼의 기반 기술이 될 것으로 기대된다. 본 논문의 구성은 1장에서 웹서비스 보안 연구의 필요성에 대해 언급하고, 2장에서는 웹서비스의 개요, 3장에서는 웹서비스의 보안 요구사항, 4장에서는 현재 제안되고 있는 웹서비스의 보안기술을 정리하였다. 마지막으로 웹 어플리케이션을 위한 보안모델을 제시하고 결론을 내린다.

II. 웹 서비스 개요

웹 서비스는 네트워크상에서 접근 가능한 소프트웨어 기능 단위로 플랫폼, 프로그래밍 언어 및 컴포넌트 모델에 독립적인 기술로 만들어진 소프트웨어를 말한다. 웹 서비스는 일반적으로 다음 [그림 1] 과 같은 구조로 구성된다.



[그림 1] 웹 서비스 구조

서비스를 개발한 제공자는 레지스트리에 자신의 서비스를 등록하여 사용자가 이용할 수 있도록 하고, 서비스를 이용하려는 이는 검색 기능을 통해 레지스트리 서버를 검색하여 원하는 서비스를 찾

고 선택하여 이용한다. 사용자가 일단 서비스를 등록하면 그 이후의 과정은 서비스와 사용자간의 RPC(Remote Procedure Call)로 이루어진다. 웹 서비스 구조의 3가지 요소는 모두 독립적으로 존재하며 이들간의 통신과정도 모두 XML로 표준화되어 있기 때문에 구조적으로 매우 유연하며, 레지스트리라는 일종의 네이밍 서버가 있기 때문에 서비스와 사용자가 자유롭게 분산될 수 있는 구조임을 알 수 있다.

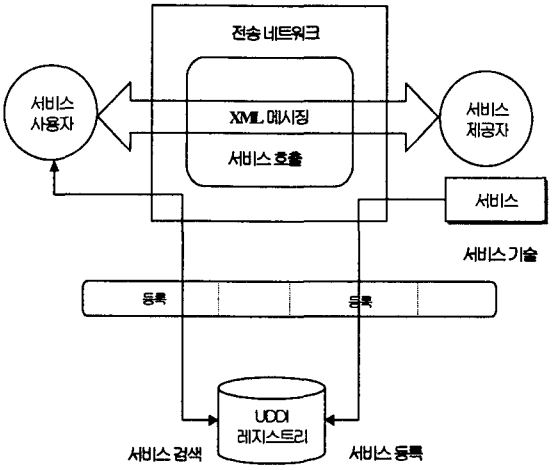
위의 웹 서비스 구조 모델은 추상적인 모델이고, 이를 구체화된 것이 상호 운용 가능한 웹 서비스 스택으로, IBM과 마이크로소프트 등의 회사에 의해 정의되었다. 웹 서비스 스택은 find, bind, publish 등과 같은 기능을 구현하는 기술을 정의한다. 웹 서비스 스택은 특정 플랫폼이나 제조사에 의존하지 않는 표준을 채용하여 상호 운용성을 가능하게 한다. 웹 서비스 스택은 다음 [그림 2]와 같은 네가지 기술로 구현된다.

서비스 등록과 검색	UDDI
서비스 기술	WDSL
XML 메시징	SOAP
전송 네트워크	HTTP, TCP/IP

[그림 2] 웹 서비스 스택과 관련기술

최하위 계층은 전송 계층으로 종단점간의 통신을 담당하고 널리 알려진 표준 프로토콜만을 지원한다. XML 메시징 부분은 웹 서비스 사용자와 서비스간 호출과 결과에 대한 전송 방법을 정의하는 부분으로 SOAP인 XML로 기술된 표준방식을 사용한다. 서비스 제공자는 WDSL(Web Service Description Lanaguage)을 사용하여 웹 서비스 인터페이스를 표준 방식으로 기술한다, 최상위 계층은 서비스의 등록과 검색에 대한 계층으로 UDDI(Universal Description and Discovery Interface)로 구현되어 있다.

지금까지 분석한 웹 서비스의 구조 및 스택 내용을 바탕으로 일반적인 웹 서비스 구조를 살펴보면 다음과 [그림 3]과 같다.



[그림 3] 일반적인 웹 서비스 구조

이러한 웹 서비스의 특징을 살펴보면 다음과 같다.

1) 서비스의 이용도 (Availability)
기존 인터넷 관련 기술들을 이용해 웹 서비스를 사용하고 배포할 수 있다.
2) 서비스 이용 용이성 (Transparency)
사용자는 언제 어디서나 HTTP를 이용할 수 있는 곳이면 웹 서비스를 사용할 수 있다.
3) 플랫폼 독립성 (Platform Independent)
특정 플랫폼에 속하지 않는 오픈형이며, 웹 서비스 내부 구성이 플랫폼에 관계없이 사용가능한다.
4) 표준 기반(Standard Based)
웹 서비스에는 다양한 표준이 존재하며 이 표준들이 대부분의 웹 서비스를 기술하고 있다.
5) 상호 호환성(Interoperability)
표준에 근거하여 플랫폼 독립적이고 개방형으로 구현된 웹 서비스는 서비스의 상호 호환성을 위한 초석으로 기반된다.
6) 지원 용이성 (Support)
웹 서비스의 모든 표준 사항 및 구현내용은 대부분 업계 선두와 표준 단체에 의해 표준화가 진행된다

Ⅲ. 웹 서비스를 위한 보안 서비스 요구사항

웹 서비스의 기반이 되는 표준인 XML은 데이터에 대한 의미적 접근과 확장성을 제공하는 표준으로서 언어적 미들웨어의 역할을 수행하는 반면, 중요 정보에 대한 표현이 구조적으로 드러나게 되어 있어, XML 문서상에 나타나는 많은 정보들이 외부에 무방비 상태로 노출되는 것이 사실이다. 웹 서비스 환경에서 일반적으로 적용되어지는 OSI 7 계층별 보안기술과 안전한 웹 서비스를 위해 제공되어야 할 보안 서비스를 분석하면 다음 [표 1][표 2]와 같다.

[표 1] OSI 7 계층에서의 보안기술

계층번호	계층명	웹 서비스 환경
Layer 7	Application	HTTP, SMTP, SOAP etc
Layer 6	Presentation	Encryption data, Compressed data
Layer 5	Session	POP/25, SSL
Layer 4	Transport	TCP, UDP
Layer 3	Network	IP Packets
Layer 2	Data Link	PPP, 802.11, etc
Layer 1	Physical	ADSL, ATM, etc

· 기밀성(Confidentiality)
교환되는 전자정보에 대한 보호를 보장하는 서비스로, 통신로 상의 데이터를 기존의 암호 알고리즘을 적용하여 보안 서비스를 제공한다.

· 무결성 (Intergrity)
정보의 변경에 대한 보장을 제공해주는 보안 서비스로서 일방향 해쉬 함수가 사용된다.

· 인증(Authentication)
송수신자에 대한 신원의 정확성을 보장해 주는 보안 서비스로서 전자서명을 통해 제공된다.

· 부인봉쇄(Non-repudiation)
송신측의 송신 사실을 부인할 수 없도록 보장해주는 서비스를 제공한다.

[표 2] 안전한 웹서비스 보안기술

보안 서비스	위협 요소	적용 보안 기술
기밀성	메시지 도청	- XML Encryption - SSL/TLS, S/MIME,
무결성	메시지 변조	- XML Signature - SHA-1, SSL/TLS, IPSec
인증	메시지 위조	- ID/PWD, Kerberos - TLS, IPSec, PKI, XKMS
부인방지	메시지 송신 및 수신 부인	- XML Signature - XKMS
접근제어	불법적 서비스 및 정보이용	- XACML, PMI, SAML

Ⅳ. 웹 애플리케이션을 위한 보안 기술

1. W3C 보안기술

1) XML 전자서명 기술

XML 문서에 대해 XML 형태의 전자서명을 생성하고 검증할 수 있는 XML 기반의 전자서명 기법이며, 전자문서에 대해 인증, 무결성, 부인봉쇄 등의 정보보호 서비스를 제공한다.

2) XML 암호화 기술

XML 암호화 기술은 XML 문서의 부분적 요소에 대한 암,복호화를 지원하는 기술로 기밀성 서비스를 제공한다.

3) XML 키 관리 기술

XML 키 관리 기술은 XML 기반의 공개키 관리를 위한 프로토콜로 공개키의 효율적인 공유 기능을 제공한다.

2. OASIS 보안기술

1) SAML

SAML은 인증과 인가 정보를 안전하게 교환할 수 있게 하는 표준으로 인증(Authentication)과 인가(Authorization) 서비스를 제공하는 다양한 서비스 플랫폼간의 상호운영성을 지원한다.

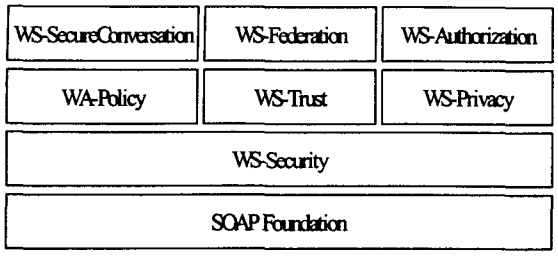
2) XACML

XML 기반 접근 제어는 인가에 대한 규칙을 표현하기 위한 XML 어휘로 구성된다. 접근 제어 규칙을 정의한 XML 어휘를 이용하여 보안이 요구되는 자원에 대해 미세한 접근 제어 서비스를 제공한다.

3) WS-Security

2002년 7월 IBM, 마이크로소프트, 베이사인은 WS-Security 명세안을 제안하고 OASIS 통해 표준화를 진행하고 있다. WS-Security는 웹 서비스 보안 명세의 일부분으로서 현재 계속 추가적인 작

업이 이뤄지고 있다. 웹 서비스 보안의 전체 구성을 살펴보면 다음 [그림 4]와 같다.



[그림 4] 웹 서비스 보안 명세 구성

웹 서비스 보안 명세 중 첫 번째 단계은 신뢰된 도메인간의 웹 서비스 보안에 필요한 스펙을 포함한다. 정보 인증의 여부와 정보 공유에 대한 내용을 담당한다.

- WS-Policy : 보안 수준에 대한 요구사항, 제약조건, 정책 등을 규정한다.
- WS-Trust : 보안 도메인간 상호작용을 가능하게 하는 보안 Trust 모델을 정의한다.
- WS-Privacy : 개인정보에 대한 비밀성의 보안에 대해 정의한다.

두 번째 단계는 보다 진보된 요구사항을 만족하는 스펙들을 포함하는 것으로 WS-SecureConversation, WS-Federation, WS-Authorization으로 구성된다.

- WS-SecureConversation : 신뢰된 도메인간의 키 교환을 통합 신뢰를 동적으로 형성하는 방법을 정의한다. 웹 서비스가 요청자의 메시지의 신원을 어떻게 확인하고 요청자가 서비스의 신원을 어떻게 확인하며, 상호 신원이 확인된 보안 상태를 어떻게 구축하는지를 설명한다.
- WS-Federation : WS-Security, WS-Policy, WS-Trust 및 WS-SecureConversation을 연합된 시스템간의 관계와 기타 정보 관리 방법을 정의한다.
- WS-Authorization : 웹 서비스 환경에서의 권한 부여 데이터와 정책 관리 방법을 정의한다.

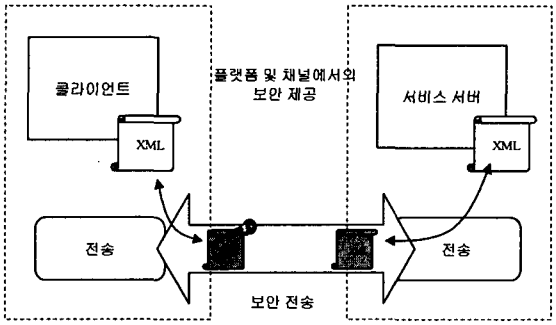
WS-Security는 무결성과 기밀성을 제공하기 위해 SOAP을 어떻게 확장하고, 메시지 내부에 보안 토큰을 어떻게 포함하는지를 정의한다. 이는 X.509 인증서를 포함한 바이너리 포맷 데이터를 어떻게 인코딩하는가에 대한 정의도 포함된다. 따라서 웹 서비스 보안 스펙의 주요 내용은 E2E 무결성 및 기밀성을 포함한 다중 보안 토큰, 신뢰 도메인, 암호화 기술을 지원하기 위한 명시 조건 등에 대한 기술이다.

V. 웹 어플리케이션을 위한 보안 모델

웹 서비스 환경의 웹 어플리케이션을 위한 보안 모델은 다음의 3가지로 분류될 수 있다.

1. 플랫폼 기반의 보안 모델

웹 서비스 클라이언트와 서비스 서버 사이의 전송 채널에 해당되는 보안 모델 구성은 다음 [그림 5]와 같다.



[그림 5] 플랫폼 기반의 보안 모델

플랫폼 보안 모델을 사용하는 경우 다음과 같은 특징이 있다.

- 서버의 인증 방법으로는 디이제스트, 통합 인증서 인증 등이 있다.
- 인증 및 권한 부여기능을 상속한 기능이 제공 가능하다.
- 메시지 무결성, 기밀성을 제공하기 위해 SSL 및 IPSec을 사용할 수 있다.

2. 응용 어플리케이션 기반의 보안 모델

응용 어플리케이션 수준의 보안을 적용하려면 응용 어플리케이션에서 보안을 담당하며 사용자 지정 보안 기능을 사용한다. SSL을 사용해 기밀성과 무결성을 지원하고, 응용 어플리케이션은 웹 서비스의 요청에 따라 사용자를 인증하기 위해 사용자 지정 SOAP 헤더를 사용하여 사용자 증명을 전달할 수 있다. 이 모델은 다음과 같은 경우에 적용이 가능하다.

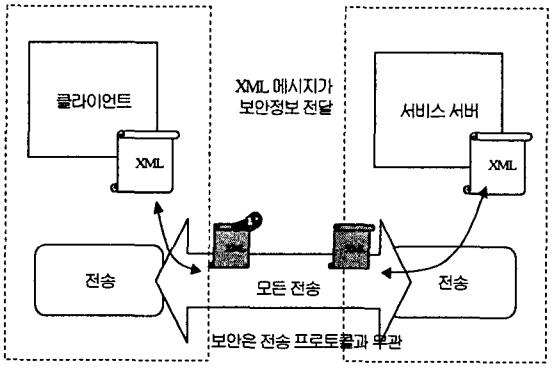
- 기존의 응용 어플리케이션에서 사용된 기존의 사용자 및 역할 DB 스키마를 이용하려는 경우
- 전체 데이터 스트림이 아니라 메시지 일부를

암호화하려는 경우

3. 메시지 기반의 보안 모델

메시지 수준의 보안 모델은 매우 유연한 방법으로 WS-Security를 근간으로 한다. WS-Security는 메시지 무결성, 기밀성, 단일 메시지 인증을 제공하는 강화된 SOAP 메시징 기능을 지원한다. 이 모델은 이 기종 웹 서비스 환경에서 보안 메시지 교환을 위한 프레임워크를 구축하는데 사용될 수 있다. 메시지 수준의 보안은 다음과 같은 특징을 지닌다.

1) 기본적인 전송 메커니즘으로부터 독립적이다.
2) 이기종 보안 구조에 사용할 수 있다.
3) 종단간 보안을 제공한다.
4) 여러 암호화 기술을 지원하며, 부인방지 기능을 제공한다.

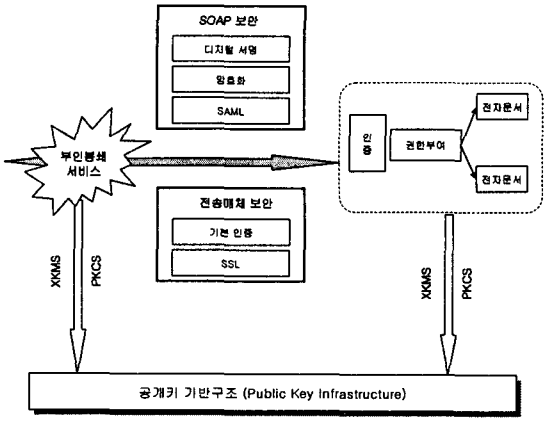


[그림 6] 메시지 기반의 보안 모델

4. 웹 서비스 어플리케이션 보안 모델 구성

3가지 기본 모델을 기반으로 본 논문에서는 2가지의 구성 모델을 제시한다.

1) 구성 모델 1



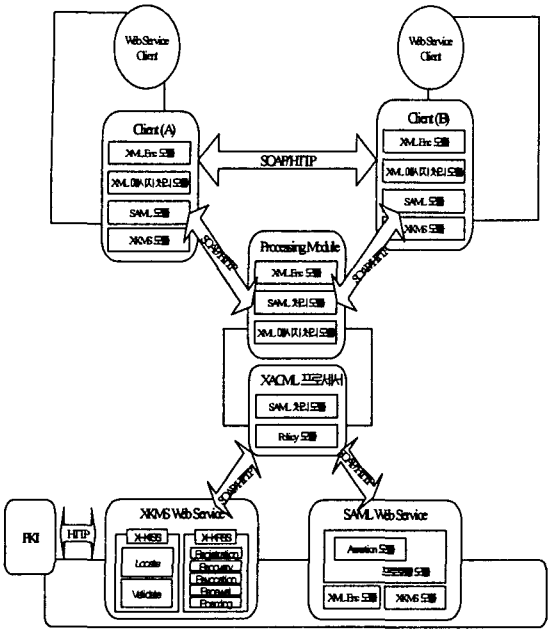
[그림 7] 보안 모델 1

HTTPS가 일반적으로 보급되어 있으므로 전송계층으로서 HTTP에 초점을 맞추어 설명하고 SOAP 및 SOAP-DSIG는 HTTP 이외의 전송계층에서도 이용할 수 있다.

SOAP-DSIG는 XML 전자서명을 사용해서 SOAP 메시지에 MAC이나 전자서명을 부가하기 위한 포맷을 정의한다. SOAP-DSIG는 단순히 데이터 포맷이고 특정 프로토콜을 규정하고 있는 것이 아니므로 그대로 송수신자 인증을 구현할 수는 없다. 이러한 관점에서 부인방지기능을 구현하기 위해 SOAP-DSIG와 SSL을 동시에 이용하는 것이 좋다. 즉, 전자서명에 의한 메시지 인증을 위해 SOAP-DSIG를 이용하고 송수신자 인증을 위해 SSL 클라이어트/서버 인증을 이용하면 된다.

2) 구성 모델 2

XML 보안기술을 활용한 웹 서비스를 위한 어플리케이션 보안 모델을 세부 모듈 단위로 구성한다.



[그림 8] 보안 모델 2

Ⅵ. 결론

본 논문에서는 웹 서비스의 개요 및 웹 서비스 보안 분석, 웹 서비스 보안 모델을 통해 전반적인 보안 기술 및 내부적인 구조를 분석하였다.

국내 웹 서비스 적용 및 활용분야는 계속 활성화되어 가고 있지만, 웹 서비스 보안에 대한 인식은 저조한 편이다. 앞으로 웹 서비스 보안의 필요성 및 보안 표준간의 상관관계, 웹 서비스 보안에 대한 인식 공유가 빠르게 확산되기를 기대한다.

참고문헌

[1] Web Service Security Specification, http://www.verisign.com/wss/wss.pdf
[2] XML-Signature Syntax and Processing, http://www..w3.org/TR/2002/REC-xmldsig-core20020212/
[3] Liberty Alliance Project, http://www.projectliberty.org
[4] SOAP version1.1(W3C note) http://www.w3.org/TR/SOAP/
[5] UDDI consortium http://www.uddi.org
[6] WSDL Web site http://www.w3.org/TR/wsdl
[7] Verisign http://www.verisign.com
[8] OASIS Web site http://www.oasis-open.org
[9] Internet Engineering Task Force http://ietf.org
[10] Web service Architecture http://www-106.ibm.com/developworks/webservices/library/w-ovr/
[11] http://www.webservice.org
[12] Steve Graham, Simeon Simeonov, Toufic Boubez, Doug Davis, Glen Daniels, Yuichi Nakamura, Ryo Neyama, Bulding Web Service with Java, SAMS, 2002