웹 서비스 보안기술에 관한 연구

김배현* · 권문택**

요 약

웹 서비스로의 진화는 기존에 존재하고 있는 다양한 시스템들을 통합하여 운영해줌으로써 기업의 비즈니스 환경에 변화를 가져올 뿐 아니라 다양한 분야에서 활용될 것이다. 하지만 아직 웹 서비스 표준이 완전히 정립되지 않았고, 업체 간 상호운영성 및 보안 문제 등 웹 서비스가 실제적으로 운영되기 위해서 해결 되어할 문제가 아직 많다. 특히 웹 서비스 보안 문제를 해결하지 않는다면 웹 서비스 기술은 더 이상 활성화되지 않을 것이다. 그러므로 웹 서비스의 특성에 적합한 보안기술 개발이 요구된다. 본 논문은 웹 서비스가 실제적으로 운영되기 위한 몇 가지 문제점들 가운데 보안에 관련된 문제점을 해결하기 위한 웹 서비스 보안 기술의 개발 방향과 발전 방향을 분석하여 제시한다.

A Study on Web Service Security

Baehyun Kim* · Moon Taek Kwon**

ABSTRACT

Web service technology will be used in various business fields and it will affect business paradigms. But, however, there is no standard so far and we have many problems to be solved in order to insure interoperability and security. Especially we have to solve Web service security for effective utilization of the technology and otherwise, the technology will not be used in the business field. We, therefore, need to develope security technology which fits to the Web service characteristics. This document describes a proposed strategy for addressing security within a Web service environment based on the results of analysis on the Web service security problems.

Key words : Web Security, Interoperability, Web Service

* 경희대학교 전자정보대학

** 경희대학교 테크노경영대학원

1. 서 론

웹 서비스는 전자상거래 어플리케이션에 의한 기업 상호간 거래의 흐름에서 사람이 개입하지 않고 자동으로 웹상에서 서비스를 찾아서 요청하고 서비스하기위한 웹 서비스가 차세대 인터넷 표준으로 향후 e-비즈니스를 비롯한 IT 산업의 환경변화에 큰 영향을 미칠 것이다. 그러나 웹 서비스가 실제적으로 운영되기 위해서는 표준 정립, 상호 운용성, 그리고 보안문제 등 여러 가지 해결해야 할 문제점들이 있다. 따라서 본 논문은 웹 서비스가 실제적으로 운영되기 위한 몇 가지 문제점들 가운데 보안에 관련된 문제점을 해결하기 위한 웹 보안 기술을 분석하여 발전방향을 제시한다.

본 논문의 구성은 2장에서 웹 서비스를 이해하기위한 웹 서비스 정의와 특징 그리고 구조를 소개하고, 3장에서는 웹 서비스를 안전하게 하기 위한 웹 서비스 보안모델과 요소기술을 분석한다. 그리고 4장에서는 분석된 웹 서비스 보안모델과 요소기술의 문제점과 방전방향을 제시하고 5장에서 결론을 기술한다.

2. 웹 서비스

2.1 웹 서비스의 정의와 특징

일반적인 웹 서비스를 정의하면 다음과 같다. 웹 서비스는 인터넷과 같이 공개된 네트워크 및 관련 표준을 통해 단일한 기업내부 또는 다수의 기업 간에 기존의 어플리케이션을 OS 및 프로그램 언어에 상관없이 상호운영이 가능하도록 해주는 표준화된 소프트웨어 기술로서 거래기업간의 필요한 서비스를 발견, 제공하여 다양한 비즈니스를 가능케 해 주는 것이다.

웹 서비스 제공을 위한 4가지 개념적인 필수 조건은 다음과 같다.

- 인터넷상에서 서비스된다.

웹 서비스는 ASP처럼 인터넷상에서 제공되지만, ASP와 다른 점은 사용자가 자신이 웹 서비스를 통해 서비스를 사용하고 있는지를 인식하지 못한다는 것이다.

- 인터넷 표준을 지원한다.

웹 서비스는 HTTP, TCP/IP 등의 표준뿐만 아니라, 차세대 인터넷 표준인 XML, SOAP, UDDI, WSDL 등을 지원한다. 이를 통해 플랫폼에 독립적이며, 상호 운용성(Interoperability)이 높은 서비스 제공이 가능하다.

- 비즈니스 로직을 포함하고 있다.

웹 서비스는 기업의 가치사슬(Value Chain)내에서 발생할 수 있는 특정 태스크의 비즈니스 로직을 포함하고 있다. 비즈니스 로직은 특정 기업을 위해 최적화된 것이 아니라 모든 기업이 공통적으로 사용할 수 있는 표준화된 비즈니스 로직이다. 비즈니스 로직을 보유하고 있기 때문에 웹 서비스 관련 요소가 변경되었을 때 프로그래밍이 아닌 단순 조작으로 변화에 대처할 수 있다.

- 객체기술이 기반으로 된 컴포넌트이다.

컴포넌트이므로 산업에 구별 없이 어떤 기업의 비즈니스 시스템에도 적용될 수 있으며, 기존의 패키지 소프트웨어나 자체 개발(Custom-Developed) 시스템뿐만 아니라 다른 웹 서비스와의 커뮤니케이션도 가능하다.

또한 웹 서비스의 대표적인 특징을 정리하면 다음과 같다.[8]

- 분산 컴퓨팅 기술 측면에서 플랫폼 독립적이다.

웹 서비스는 매우 유연한 어플리케이션(loosely coupled application) 구조를 가지고 있다. 따라서 웹 서비스는 유연한 어플리케이션 구조

를 가지고 있기 때문에 서비스 공급자, 수요자가 특별한 기능을 추가하기 위해 새로운 플랫폼을 사용하지 않아도 되며, 플랫폼 선택도 자유롭다.

• 디바이스 및 위치 독립적이다.

웹 서비스를 통해 PC, PDA, 핸드폰 등 다양한 유무선 디바이스를 통해 시간 및 장소에 상관없이 웹 서비스에 접근이 가능하다.

• 동적인 기능(dynamic function)이다.

동적 기능이란 인간이 개입하지 않고 자동으로 어플리케이션이 자신이 필요한 어플리케이션을 찾아서 원하는 기능을 수행하는 것이다.

• 상호운영성을 제공

표준화된 SOAP, WSDL을 사용하여 인터페이스하기 때문에 이기종 환경에서 상호운영성을 제공할 수 있다. 따라서 웹 서비스를 기존 시스템이 적용이 가능하다. 기존에 투자되었던 IT 어플리케이션 및 인프라 등 기존의 시스템에 특별한 웹 서비스 프로세스를 포함시켜 운영할 수 있다.

2.2 웹 서비스의 구조

웹 서비스의 구조는 3가지의 빌딩 블록과 각 빌딩 블록의 기능을 수행하기 위한 요소기술로 이루어진다[7]. 웹 서비스의 주요 빌딩 블록은 Discovery, Description, Invocation의 개념으로 이루어진다. Discovery는 XML 웹 서비스를 사용하기위해, 사용자 어플리케이션 프로그램이 필요한 웹 서비스를 발견하는 것이다. Descripion은 사용자에게 XML 웹 서비스가 어떤 것인지 설명하는 것으로서 XML 웹 서비스의 의미를 나타내거나, XML 웹 서비스를 설명하는 메타 데이터로 생각할 수 있다. Invocation은 사용자가 웹 서비스에 필요한 입력요소를 넘긴 다음, 적절한 결과 데이터를 반환 받을 수 있도록 웹 서비스를 호출(invole)하는 것이다. 이러한 invoke 블록은 확장 형태의 SOAP 프로토콜을 포함하고 있다. invoke 빌딩 블록은 전송 프로토콜(일반적으로 HTTP, SMTP등)로 구성되어 있는 전송계층의 최상위에 위치한다.

〈표 1〉 웹 서비스 구조 및 기술요소

빌딩 블록	기술요소	기술표준
Invocation	• Message Exchange • Security √ Message Encryption √ Digital Signature • Binary Attachment • Reliable Messaging • Transaction • Routing • scalability	SOAP SAML, XKMA, SOAP Security Extions (WS-Security) XML Encryption XML Digtal Signature SOAP with Attachment SOAP 1.2 - BTP - -
Description	• Service Description • process Flow	WSDK, WSCL BPML, WSFL, XLang
Discovery	• Inspection • Discovery	WSIL(WS-Inspection) UDDI

3. 웹 서비스 보안

3.1 웹 서비스 보안 요구 사항

웹 서비스는 각각의 보안 정책을 가지고 있는 서비스 주체(subject)간의 trust, Federation설정을 통한 상호 협력적인 방식으로 서비스가 이루어지기 때문에 웹 서비스 보안 아키텍처 는 보안 기술 측면뿐만 아니라 비즈니스 프로세스 측면의 보안을 효율적이고 안전하게 지원하기 위해 유연성 및 확장성이 있는 구조이어야 한다. 또한 요청자와 웹 서비스 사이에 여러 Intermediary가 존재하는 Multi-Hop Topology이기 때문에 양단간의 End-to-End 보안이 지원되어야 한다.

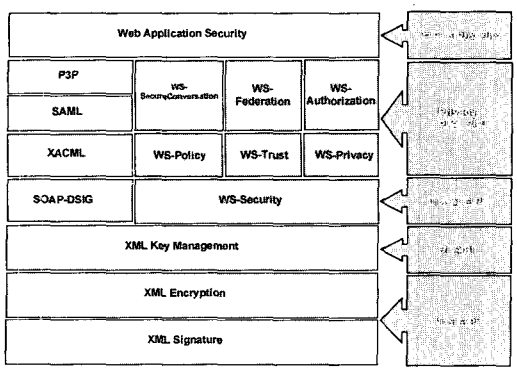
웹 서비스에서 요구하는 보안 서비스를 정리하면 다음과 같다[7, 8].

- 인 증
- 권 한
- 무결성
- 기밀성
- privacy
- 가용성
- 부인봉쇄

이외에도 End-to-End 보안, Challenge/Response 형태의 보안 Context 설정, 키 교환 및 Derived key, Multiple Trust Domains 환경에서의 Trust/Federation의 설정 및 관리 등이 요구된다.

3.2 웹 서비스 보안 기술

(그림 1)는 MS와 IBM에서 제안하고 표준화를 위해서 작업 중인 웹 서비스 보안 Specification의 Road map이다. 현재 WS-Security가 발표되어 OASIS(Organization for the Advancement of Structured Information Standards)에 제출되어 검토되고 있는 상황이며 나머지 Specification에 대한 작업은 진행 중이다. (그림 1)에서 알 수 있듯이 보안에 관련된 Specification은 요구 사항별로 모듈화 되었으며 완성 단계별로 계층화되어 있다[3, 7, 8].



(그림 1) XML 보안기술 유형별 분류

3.2.1 WS-Security

WS-Security는 SOAP 메시지에 대한 무결성, 기밀성, 인증 제공을 통해서 웹 서비스 어플리케이션이 안전하게 SOAP 메시지 교환을 할 수 있게 하는 웹 서비스 보안의 기반이 되는 Specification이다. 즉 SOAP 메시지가 XML을 사용해서 구성되기 때문에 WS-Security Encryption/Signature 등의 보안을 위한 XML의 Specification들을 기반으로 이를 SOAP 메시지에 적용하는 방식을 기술하고 있다. 또한 이 사양은 SOAP 메시지 내에 보안 토큰을 어떻게 첨부하고 포함시킬 것인지를 기술한다. 마지막으로, 이진수로 암호화된 보안 토큰(예 : X.509 인증서)을 지정하기 위한 하나의 메커니즘이 제공된다. 이러한 메커니즘들은 광범위한 보안 모델과 암호화 기술들을 수용하기 위해 독립적으로 혹은 결합되어 사용될 수 있다.

WS-Security에서는 다음과 같이 크게 3가지 주요 메커니즘을 지원한다.

- 보안 토큰 Propagation

요청자 혹은 웹 서비스의 Name, 패스워드, X.509인증서, Kerberos 티켓, 세션 키 등 인증에 관련된 정보를 나타내는 보안 토큰을 SOAP 메시지 헤더에 나타낸다. WS-Security는 어떠한 형태의 인증 정보도 포함시킬 수 있는 유연하고 확장된 형태의 구조를 지원한다. 인증 정보는 세션 키로 암호화되거나 송신자의 개인키로 전자서명 값과 함께 전송된다.

- 메시지 무결성

XML Digital Signature Specification에 따르는 전자서명 방식을 지원한다. Digital 전자서명은 헤더에 위치하며 헤더와 바디에 있는 데이터

의 전부 혹은 일부에 대해서 Digital 전자서명을 생성할 수 있다.

• 메시지 기밀성

XML Encryption Specification의 암호화 방식을 기반으로 한다. SOAP 헤더와 바디의 일부 혹은 전부나 Attachment를 암호화 할 수 있다. 암호화에 관련된 정보는 헤더에 위치하며 암호화되기 전의 SOAP 메시지 부분이나 Attachment는 암호화된 암호문으로 대체된다.

WS-Security는 특정한 보안 기술이나 보안 프로토콜에 의존적이지 않은 추상적인 모델의 유연한 방식을 제안하고 있다.

3.2.2 WS-Policy

WS-Policy에는 다음의 4가지 문서가 포함되어 있다:

- Policy Framework(WS-Policy) 문서 : 웹 서비스 정책을 표현하는 문법 정의.
- Policy Attachment(WS-Policy-Attachment) 문서 : 정책들을 웹 서비스에 어태치하는 방법 정의.
- 일반적인 정책 선언(WS-Policy-Assertions).
- 보안 정책 선언(WS-Security Policy).

Policy 프레임워크는 확장성이 적용될 수 있다. 정책이란 말은 포괄적인 용어이고 보안, 신용, 트랜잭션, 사생활 보호 등이 포함된다. 마찬가지로, 정책을 표현하는 기능 역시 일반적인 정책이나 보안 정책을 표현하는 데에만 한정되어 있지 않다. WS-PolicyAttachment는 웹 서비스로 정책 선언을 광고할 수 있는 여러 가지 방식을 제공한다. 이것은 WSDL과 UDDI 스펙에서 구현되고 확장성도 지원한다. 웹 서비스에 대한 일반적인 정책들과 더불어 특정 정책(예를 들어, 보안 정책)이 만들어질 것이다. WS-Policy Assertions Language는 이러한 유형의 일반적인 정책 표현을 제공한다. 이것은 웹 서비스를 위한 일반적인 정책 선언을 정의한다. 보안은 하나의 도메인이고 보안정책 표현을 설명하기 위해서 개별적인 문서인 WS-Security-Policy는 WS-Security 스펙을 지원하는데 관련된 정책과의 통신에 필요한 정책들을 표현하기 위해서 언어를 제안한다.

3.2.3 WS-Trust

웹 서비스 패러다임에서 서비스 요청자와 서비스 제공자간의 신용(trust)이란, 예견되고 상호 이해된 방식으로 양자간의 정보 교환을 통해 확립된다. WS-Security 스펙은 이미 보안 토큰을 사용하여 메시지들을 안전하게 교환하는 기본 메커니즘을 정의해놓고 있다. WS-Trust 스펙은 이 모델을 기반으로 구현되어 그와 같은 보안 토큰이 어떻게 발행되고 교환되는지를 정의한다. WS-Trust는 보안 토큰 서비스가 보안토큰의 발행, 교환, 유효성검사를 제공하는데 사용되는 인터페이스를 정의하는 것으로 신용 관계 정의 작업을 시작한다. 이것은 다양한 인증 및 권한 메커니즘을 수용하는 여러 개의 보안 토큰 포맷의 생성을 지원하도록 설계되었다. 발행된 보안 토큰 서비스는 인풋 요청과 ID 증명을 받아들여 해당 ID가 요청되었음을 나타내는 토큰으로 응답한다. 보안 공간 내에서 이러한 예견된 작동은 신용 정책(trust policy)으로서 표현될 수 있고 WS-Policy 프레임워크는 그 신용 구문을 표현하고 교환하는 신용 파트너를 지원한다.

3.2.4 WS-Privacy

웹 서비스를 개발, 관리, 사용하는 조직들은 종종 자신들의 프라이버시 정책을 명확하게 표명하고 들어오는 요청들이 발신자에게 이러한 정책을 따르도록 요구하도록 할 필요가 있다. WS-

Policy, WS-Security 및 WS-Trust를 결합하여 사용함으로써 조직들은 프라이버시 정책을 명시하고 이를 따르도록 지시할 수 있다. 이 사양은 프라이버시 용어가 WS-Policy 설명에 어떻게 포함될 수 있는지, 그리고 프라이버시 클레임을 메시지와 연결시키는데 WS-Secrutity을 어떻게 사용할 수 있는지를 설명할 것이다. 마지막으로, 이 사양은 사용자 선호와 조직적인 실행 요구에 대해 이들 프라이버시 클레임을 평가하는데 WS-Trust 메커니즘이 어떻게 사용될 수 있는지를 설명할 것이다.

3.2.5 WS-SecureConversation

WS-SecureConversation은 웹 서비스가 요청자 메시지의 신원을 어떻게 확인하고 요청자가 서비스의 신원을 어떻게 확인하며 상호 신원 확인된 보안 문맥을 어떻게 구축하는지를 설명할 것이다. 이 사양은 세션 키, 파생 키(derived key), 및 메시지당 키를 구축하는 방법을 설명할 것이다. 마지막으로, 이 사양은 서비스가 문맥 (보안 속성과 관련 데이터에 관한 클레임 집합)을 어떻게 안전하게 교환할 수 있는지를 설명할 것이다. 이를 위해 사양은 WS-Security와 WS-Trust에 정의된 보안 토큰 발행 개념과 교환 메커니즘을 설명하고 이를 기반으로 구축될 것이다.

3.2.6 WS-Federation

이 사양은 WS-Security, WS-Policy, WS-Trust 및 WS-SecureConversation 사양을 사용하여 연합된 신임 시나리오를 구축하는 방법을 정의할 것이다. 예를 들어, 이 사양은 Keberos와 PKI 인프라를 연합시키는 방법을 설명할 것이다. 또한, 중개되고 있는 신임의 유형을 가리키고 제한하고 확인하기 위한 신임 정책이 소개될 것이다. 이 사양은 또한 신임 관계를 관리하기 위한 메커니즘을 정의할 것이다.

3.2.7 WS-Authorization

이 사양은 웹 서비스에 대한 접근 정책이 어떻게 지정되고 관리되는지를 설명할 것이다. 특히, 보안 토큰 내에서 클레임이 어떻게 지정되고 이 클레임들이 종단점(End point)에서 어떻게 해석될지를 설명할 것이다. 이 사양은 인증 포맷과 인증 언어 모두에 대해 유연하고 확장성 있도록 설계될 것이다. 그러면 광범위한 시나리오가 가능해지고 보안 프레임워크의 장기적인 생존력이 보증된다.

3.3 웹 서비스 보안 모델

웹 서비스는 크게 전송단계와 어플리케이션 단계에서 보안 문제를 처리하며, 각 단계에서 보안을 처리하는 방식에는 여러 가지가 있다. 웹 서비스를 구현하는 데에 있어서 SMTP 보다 HTTP을 훨씬 많이 사용하지만, 웹 서비스 보안을 위한 대부분의 어플리케이션 프로그램 계층의 접근에서는 HTTP와 SMTP 혹은 그 밖의 다른 전송 프로토콜에 있어서 같은 비중을 차지한다. 각 웹 서비스 보안 방법에는 나름대로의 장단점이 있다. 웹 서비스 보안 방법은 주로 메시지 교환에 관련된 플랫폼 및 아키텍처의 특징에 따라 선택한다.

웹 서비스 보안은 다음과 같이 2가지 단계에 적용할 수 있다[7].

- 전송 단계(point-to-point level) 보안
- 어플리케이션 단계(End-to-end level) 보안

3.3.1 전송단계 보안

네트워크 계층에서 전송 단계 보안을 구현하는 것은 IPSec(Internet Protocol Security), SSL, VPN, 방화벽와 같은 기술을 사용하여 IP 트래픽에 대한 보안을 구현하는 것으로 이루어진다.

- SSL

어플리케이션 계층과 전송 계층 중간에서 서

버와 클라이언트 양단간의 Handshaking을 통한 Line Encryption으로 보안을 지원하는 방식으로 현재 많이 쓰이고 있다. SSL은 검증된 프로토콜이지만 End-to-End 보안이 지원되지 않고 Line Encryption으로 인해 성능 측면에서 큰 영향을 받기 때문에 Credential과 같은 주요 정보를 전송할 때만 사용해야 한다.

• VPN(Virtual Private Network)

VPN은 인터넷과 같은 공중망에서 구성된 가상망을 의미하며 IPsec을 이용해 Network-Level 인증, 데이터 암호화/복호화를 제공한다. 송신자와 수신자 사이에서 형성된 임시 Connection상에서의 패킷 필터링으로 Long-Term Point-to-Point 보안을 지원한다. 요청자의 IP가 미리 고정적으로 알려지는 웹 서비스에 적용 가능하며 Connection이 Long-Term인 관계로 성능 면에서 문제가 있을 수 있다.

• 방화벽

방화벽은 외부 네트워크와 내부 네트워크 사이에서 송신자 IP 주소 혹은 포트 번호를 통한 패킷 필터링 기능으로 내부 네트워크를 보호하는 역할을 한다. 웹 서비스에서 적용될 때는 IP Blocking으로 허용되지 않은 접근을 차단한다. 따라서 요청자가 불특정한 웹 서비스 경우에는 적용이 곤란하다.

전송 단계 보안과 관련한 주요 문제점은 다음과 같다.

보안이 기본 플랫폼, 전송 메커니즘 및 보안 서비스 공급자(예 : NTLM, Kerberos 등)와 밀접하게 연결되어 의존적이다. 중간 어플리케이션 프로그램 노드를 통과하는 다중 홉과 라우팅에 대한 규정이 없어 보안이 지점 간 기준으로 적용된다.

3.3.2 어플리케이션 단계 보안

어플리케이션 단계 보안은 전송단계 보안의 지원 없이 어플리케이션의 메시지 자체에서 내부적으로 보안 메커니즘을 가지고 있는 것이다. 메시지에 단순히 Credential를 넣어서 전송하는 것으로는 보안가 지원되지 않으며 메시지에 암호학적인 여러 기법을 사용하여 인증, 무결성, 기밀성, 부인봉쇄를 제공한다. 어플리케이션 단계 보안에서 중요한 점은 End-to-End 보안을 제공한다는 것이다. 이와 같은 장점 때문에 최근의 웹 서비스 보안의 흐름은 어플리케이션 단계 보안으로 가고 있다. 이에 크게 기여한 것이 W3C의 보안 관련 여러 XML Specification들이다. 웹 서비스는 근본적으로 요청자와 웹 서비스 상호간의 SOAP 메시지 교환이라고 볼 수 있기 때문에 가장 기본적인 웹 서비스 보안은 XML, 즉 SOAP 메시지 보안부터 시작해야 한다.

전송 단계에서의 보안은 SOAP 메시지 자체에 영향을 미치지 않지만, 서버와 클라이언트 소프트웨어의 설정이 필요하고, 클라이언트 소프트웨어를 수정해야할 필요가 있다. 어플리케이션 단계에서는 보안을 적용할 때에는 SOAP 메시지 자체를 수정한다. 이러한 방식으로 수정한 메시지는 어떠한 프로토콜로도 전송할 수 있으며, 서버나 클라이언트 시스템 소프트웨어를 특별히 설정해줄 필요가 없다. 그러나 웹 서비스 메시지를 교환하는 클라이언트와 서버에서 동시에 지원하도록 하기위해 어플리케이션 단계의 특정한 구현이 필요하다. 종단간의 보안은 컴퓨터나 어플리케이션 프로그램과 같은 하나의 점에서 다른 점으로 직접 연결할 필요가 없는 통신에서 구현되는 보안을 말한다.

어플리케이션 단계 보안을 사용하면 어플리케이션 프로그램에서 보안을 담당하며 사용자 지정 보안 기능을 사용한다. 예를 들면 다음과 같다.

• SOAP 메시지에 포함된 인증서

어플리케이션 프로그램은 웹 서비스 요청에 따라 사용자를 인증하기 위해 사용자 지정 SOAP

헤더를 사용하여 사용자 자격 증명을 전달할 수 있다. 일반적으로, SOAP 헤더에서 티켓(사용자 이름이나 라이센스)을 전달하는 방법을 사용한다.

- 커버로스와 티켓 기반 인증

티켓 기반 인증은 어플리케이션 단계이며, 이것은 어떠한 전송 프로토콜에서도 사용할 수 있음을 의미한다. 일반적으로 티켓 기반인증은 전자서명, 전자인증, 대칭키 혹은 비대칭키 암호화 기술을 사용한다. 어플리케이션 프로그램에서 인증을 위한 코드를 포함하고, 내용을 암호화하며, 전송하는 메시지에 전자서명을 하거나, 받은 메시지의 전자 서명을 유효화한다. 따라서 티켓 기반 인증을 수행하기 위해서는 더 많은 작업이 동반되지만, 더 많은 융통성을 제공한다. 비록 티켓 기반 암호화 지원이 제한적이기는 하지만, 새로운 버전의 웹 서비스 툴킷과 웹 서비스 구현 프레임워크에서는 증가할 것으로 확신한다.

- XML 보안 관련 스펙

웹 서비스의 보안 중, 특히 XML 문서에 보안을 적용하고 SOAP 메시지를 확장하는 문제에 대하여 여러 업체에서 제안한 보안 관련 스펙을 W3C에서 개발하고 있다. 보안을 표준적인 방식으로 처리하는 것은 선택한 프로토콜에 의존하지 않고, SOAP 매개물을 포함한 매개물 간에 동작하는 구현을 가능하게 한다. XML 프로토콜 워킹 그룹은 XML 보안 관련기술이 SOAP 메시지에 표준 헤더를 추가한다.

어플리케이션 단계 보안의 특징은 다음과 같다.

- 기존 전송으로부터 독립적일 수 있다.
- 이기종 보안 아키텍처를 사용할 수 있다.
- 종단 간 보안을 제공하여 중간 어플리케이션 프로그램 노드를 통해 메시지 라우팅을 조절한다.
- 여러 암호화 기술을 지원한다.
- 부인방지를 지원한다.

4. 웹 서비스 보안기술 발전 방향

웹 서비스 보안을 효율적이고 안전하게 지원하기 위해서는 유연성 및 확장성이 있는 구조이어야 하며 양단간의 End-to-End 보안이 지원되어야 한다. 그리고 웹 서비스 보안을 위해 기존의 보안기술을 그대로 적용할 경우, 기존 보안기술에서 일부 문제점이 지적되고 있는 상황이며, 웹 서비스 특성에 맞는 보안요구사항을 만족할 수 없다.

웹 서비스 보안 접근 방법은 전송단계 보안과 어플리케이션 단계 보안으로 구분할 수 있다. 전송단계 보안에서는 Point-to-Point 보안으로 기존의 네트워크 보안 기술인 IPsec, SSL, VPN, S/MIME 등을 사용하여 무결성과 기밀성을 제공한다. 어플리케이션 단계 보안은 End-to-End 보안으로 어플리케이션의 메시지 자체에 보안 메커니즘을 가지고 있는 것이다. 어플리케이션 단계 보안을 위해서는 XML 명세들을 사용하는데, 대표적인 것으로 WS-Security을 사용하여 무결성, 기밀성, 인증을 제공한다.

우선 전송단계 보안의 경우, 웹 서비스에서는 전송단계에서 일반적으로 HTTP를 사용한다. HTTP는 인증 위주의 보안기술을 주로 적용한다. HTTP의 Basic 인증은 ID/패스워드만으로 인증을 하는 가장 간단한 형태의 보안 방식이다. 그러나 이 방식은 사용자의 패스워크가 평문 형태로 전송되기 때문에 공격자에게 노출될 위험성이 크다. 다른 방법으로는 패스워드에 대한 Digest를 생성하여 이를 전송하는 방식이 있지만 이것 역시 Digest가 평문 형태로 전송되기 때문에 안전하지 못하다. 이를 해결하기 위해서 검증된 가장 널리 쓰이는 방식이 SSL을 사용하여 Line 암호화를 하는 방식이다. 그러나 전송되는 모든 데이터가 전송 노드사이에서 암호화/복호화 되기 때문에 Multi-Hop 토플로지에서 End-to-End 보안을 지원하지 못한다. 또한 SSL은 웹 서비스에

서 성능에 부담을 준다. 따라서 SSL은 중요한 웹 서비스에 강력히 권고되지만, 보안 수준이 낮은 상황이나, 인트라넷과 같은 네트워크를 쉽게 통제할 수 있는 상황에서는 다른 인증 방식이 더 좋은 성능을 발휘한다. 또한 SSL은 암호화 통신 시 타이밍 기반 공격(Timing-based Attacks)에 의한 비밀키 노출, Klima-Pokorny-Rosa 공격, SSL/TLS상의 CBC 암호시 타이밍기반 공격, 암호화 라이브러리 및 어플리케이션 프로그램에 대한 타이밍 공격 등 취약성을 가지고 있다. 다음으로 VPN과 방화벽을 사용하는 경우, VPN은 요청자의 IP가 미리 고정적으로 알려지는 웹 서비스에 적용 가능하며 Connection이 Long-Term인 관계로 성능면에서 문제가 있을 수 있다. 방화벽은 웹 서비스에서 적용될 때는 IP Blocking으로 허용되지 않은 접근을 차단한다. 방화벽은 외부에 주로 서버를 운용하는 웹 사이트와는 달리 웹 서비스는 기업 내 어플리케이션과 다른 기업 내 어플리케이션간의 통신이 필요하기 때문에 방화벽을 통과하면서 보안을 지원해야 하기 때문에 웹 서비스에는 적용이 곤란하다.

어플리케이션 단계 보안은 WS-Security에서 PKI, Kerberos, 전자서명 등을 사용할 수 있다. 그러나 PKI는 사용자 쪽의 부담 때문에 웹 사이트의 인증 방식으로 널리 쓰이지는 않으며, Kerberos는 상호 호환성이 없기 때문에 Cross-Platform 환경에 적용하기는 힘들고 패스워드 사전 공격에 취약성을 가지고 있다. 전자서명은 이미 사용된 서명 값을 재사용하는 Replay공격에 대한 취약점이 있다.

따라서 기존 보안기술을 SOAP 메시지에 적용할 때도 역시 발생할 수 잇기 때문에 이에 대한 해결책이 고려되어야 한다. 서명과 함께 난수값, Timestamp, 순서번호, Expirations, 메시지 Correlation등의 정보를 같이 전송하는 방안을 고려해야 한다. 웹 서비스 보안 모델의 방향이 어플리케이션 단계 보안 모델 쪽으로 방향을 잡아가는 흐름 속에서 웹 서비스 보안의 요구 사항을 만족시켜 줄 수 있는 웹 서비스 보안 아키텍처의 모델을 기반으로 보안 요구 사항을 충족시켜 주는 표준 Specification의 필요성이 확산되었다. 표준 Specification 없이 기업들이 나름대로의 웹 서비스 보안 솔루션을 적용한다면, 상호 운영성이 떨어지게 되고 이를 맞추기 위해서 또 추가적인 작업이 소요되는 경우가 발생하게 된다. 이러한 상황을 인식하고 MS와 IBM은 위에서 언급한 웹 서비스 보안 요구 사항을 반영한 웹 서비스 보안 아키텍처를 제안하였다.

5. 결 론

웹 서비스는 인터넷 표준 프로토콜을 이용하여 원격지에 있는 웹 객체를 XML 기반으로 접근, 이용, 재사용을 할 수 있는 웹 분산 환경의 분산 컴포넌트 모델이다. 따라서 웹 서비스는 전자상거래, 에이전트 시스템 등 다양한 어플리케이션에서 널리 사용될 수 있다. 웹 서비스는 Cross-Platform 환경에서의 기업 내 또는 기업간의 어플리케이션을 원하는 방식으로 서로간의 기능을 공유하는 것이 필수적이다. 그러나 이러한 기능을 제공하기 위해서는 보안문제가 필수적으로 대두된다. 웹 서비스 보안을 효율적이고 안전하게 지원하기 위해서는 유연성 및 확장성이 있는 구조이어야 하며 양단간의 End-to-End 보안이 지원되어야 한다. 따라서 웹 서비스에서 요구하는 보안 서비스는 인증, 권한, 기밀성, 무결성, 가용성, 부인방지, End-to-End 보안 등 이다. 웹 서비스 보안 접근 방법은 전송단계보안과 어플리케이션 단계 보안으로 구분할 수 있다.이 두가지 방법 모두 장단점이 있으나 웹 서비스의 특성상 전송단계 보안 보다는 어플리케이션 단계의 보안으로 가는 추세이다. 그러나 기존의 인터넷 보안 기술 등을 단순하게 적용하는 것으로

웹 서비스 보안 요구사항을 만족할 수 없다. 따라서 웹 서비스의 특성에 맞는 보안기술이 따로 개발되어야 한다. 또한 웹 서비스의 상호운영성을 위해 표준화가 필요하다.

참 고 문 헌

[1] Martin Naedele, "Standards for XML and Web Services Security", computer, pp.96-98, April 2003.

[2] Yuichi Nakamur, Satoshi Hada and Ryo Neyama, "Towards the Integration ofWeb Services Security on Enterprise Environments", SAINT, 2002.

[3] Francisco Curbera, Matthew Duftler, Rania Khalaf,William Nagy, Nirmal Mukhi, and Sanjiva Weerawarana, "Unraveling the Web Services Web", IEEE INTERNET COMPUTING, March, April 2002.

[4] J.D. Meier, Alex Mackman, Michael Dunner, and Srinath Vasireddy, "웹 서비스 보안", http://www.microsoft.com/korea/msdn/library/dnnetsec/html/SecNetch10.asp.

[5] Giovanni Della-Libera, Brendan Dixon, "WS-SecureConversation," http://www.microsoft.com/korea/msdn/library/dnglobspec/html/ws-secureconversation.asp, 2002.

[6] Giovanni Della-Libera, Phillip Hallam-Baker, "WS-SecurityPolicy", http://www.microsoft.com/korea/msdn/library/dnglobspec/html/ws-securitypolicy.asp, 2002.

[7] SOAP Version 1.2 Part 0 : Primer, W3C Recommendation 24 June 2003, http://www.w3.org/TR/2003/REC-soap12-part0-20030624/.

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

[8] Patric Cauldwell, Rejesh Chawla, Vivek Chopra, "Professional XML Web Services", Wrox Press, September 2001.

[9] 이해규, 이상수, 김문규, "웹 서비스 보안", 정보처리학회지, 제9권, 제4호, pp.36-45, 2002.

김 배 현

1995년 호원대학교 전자계산학과 (이학사)

1997년 수원대학교 전자계산학과 (이학석사)

2003년 경희대학교 컴퓨터공학과 (박사수료)

현재 경희대학교 강사, 한신대학교 강사

권 문 택

1970년 육군사관학교(이학사)

1981년 미국 University of Iowa 대학(공학석사)

1987년 미국 University of Wisconsin 대학(경영정보학 박사)

경희대학교 테크노경영대학원 종신교수

경희대학교 정보처리처장

경희사이버 대학교 학장