제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

웹 서비스 보안에 관한 연구

김 배 현*, 나 원 식*, 권 문 택**
* 경희대학교 전자정보대학, ** 경희대학교 테크노경영대학원

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 제시하고자 한다.

A Study on Web service security

Baehyun Kim*, Won Shik Na*, 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.

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.

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

웹 서비스는 개방된 네트워크와 관련 표준을 통해 하나의 기업 내부 또는 다수의 기업 간에 기존의 전자상거래 어플리케이션을 OS 및 프로그램 언어에 관계없이 상호운영이 가능하도록 해주는 표준화된 소프트웨어 기술로서 거래기업간의 필요한 서비스를 발견하고 제공하는 다양한 비즈니스를 가능케 해 주는 것이다.

웹 서비스 제공을 위한 4가지 개념적인 필수조건은 다음과 같다.

- 인터넷상에서 서비스된다.
- 인터넷 표준을 지원한다.
- 비즈니스 로직을 포함하고 있다.
- 객체기술이 기반으로 된 컴포넌트이다.

또한 웹 서비스의 대표적인 특징을 정리하면 다음과 같다.[8]

- 분산 컴퓨팅 기술 측면에서 플랫폼 독립적이다.
- 디바이스 및 위치 독립적이다.
- 동적인 기능(dynamic function)이다.
- 상호운영성을 제공한다.

2.2 웹 서비스의 구조

〈표 1〉 웹 서비스 구조 및 기술요소

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

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.

Description는 사용자에게 XML 웹 서비스가 어떤 것인지 설명하는 것이다. Description 빌딩 블록은 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.

3. 웹 서비스 보안

3.1 웹 서비스 보안 요구 사항

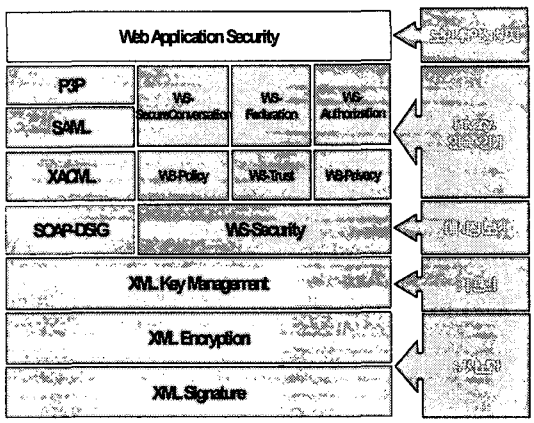
웹 서비스에서 요구하는 보안 서비스를 정리하면 다음과 같다.[7][8]

- 인증
- 권한
- 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 Roadmap이다. 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

WS-Security는 SOAP 메시지 무결성과 기밀성을 통해 보안 품질을 제공하기 위하여 MS와 IBM이 Verisign과 함께 만든 웹 서비스 보안의 기반이 되는 Specification이다. WS-Security는 SOAP 메시지에 대한 어플리케이션 단계 보안에 대한 내용을 기술하고 있다.

WS-Policy에는 다음의 네 가지 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)

WS-Trust는 보안 토큰 서비스가 보안토큰의 발행, 교환, 유효성검사를 제공하는데 사용되는 인터페이스를 정의하는 것으로 신용 관계 정의 작

업을 시작한다. 이것은 다양한 인증 및 권한 메커니즘을 수용하는 여러 개의 보안 토큰 포맷의 생성을 지원하도록 설계되었다.

웹 서비스를 개발, 관리, 사용하는 조직들은 종종 자신들의 프라이버시 정책을 명확하게 표명하고, 들어오는 요청들이 발신자에게 이러한 정책을 따르도록 요구하도록 할 필요가 있다. 따라서 WS-Policy, WS-Security 및 WS-Trust를 결합하여 사용함으로써 조직들은 프라이버시 정책을 명시하고 이를 따르도록 지시할 수 있다. WS-Privacy는 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 설명한다.

WS-SecureConversation은 웹 서비스가 요청자 메시지의 신원을 어떻게 확인하고 요청자가 서비스의 신원을 어떻게 확인하며 상호 신원 확인된 보안 문맥을 어떻게 구축하는지를 설명한다.

WS-Federation은 WS-Security, WS-Policy, WS-Trust 및 WS-SecureConversation 사양을 사용하여 연합된 신임 시나리오를 구축하는 방법을 정의한다.

WS-Authorization은 웹 서비스에 대한 접근 정책이 어떻게 지정되고 관리되는지를 설명한다.

3.3 웹 서비스 보안 모델

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

전송 단계 보안은 특정 웹 서비스가 사용하고 있는 전송 또는 네트워크 계층 프로토콜에 이미 구축된 보안 특성을 사용하는 것으로 이루어진다. 전송 단계 보안은 웹 서비스와 관련해서는 점대점 보안 (point-to-point security)이다. 점대점 보안은 컴퓨터나 어플리케이션 프로그램과 같은 하나의 점(Point)으로부터 다른 점으로 직접 안전하게 통신하는 것을 의미한다. 이것은 둘 사이에 다른 SOAP 매개물이 존재하지 않고 직접 접속된다는 것을 내포하고 있다. 전송 단계 보안 모델은 간단하고 이해하기 쉬우며 주로 인트라넷 기반의 여러 시나리오에 적합하다. 네트워크 계층에서 전송 단계 보안을 구현하는 것은 IPSec(Internet Protocol Security), SSL, VPN, 방화벽와 같은 기술을 사용하여 IP 트래픽에 대한 보안을 구현하는 것으로 이루어진다.

어플리케이션 단계 보안은 전송단계 보안의 지원 없이 어플리케이션의 메시지 자체에서 내부적으로 보안 메커니즘을 가지고 있는 것이다. 어플리케이션 단계 보안에서 중요한 점은 종단간(End-to-End) 보안을 제공한다는 것이다. 이와 같은 장점 때문에 최근의 웹 서비스 보안의 흐름은 어플리케이션 단계 보안으로 가고 있다. 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. 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.

4. 웹 서비스 보안 기술 발전 방향

웹 서비스 보안을 위해 기존의 보안기술을 적용할 수 있다. 그러나 기존의 보안기술을 그대로 적용할 경우, 기존 보안기술에서 지적되고 있는 일부 문제점이 웹 서비스에서도 발생할 수 있다. 또한 기존 보안기술을 그대로 웹 서비스에 적용

하기 때문에 웹 서비스 특성에 맞는 보안요구사항을 만족할 수 없다. 따라서 이에 대한 해결책이 고려되어야 한다.

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 서비스에서 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 암호 시 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 성능 면에서 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 Replay 공격에 대한 취약점이 있다. 따라서 기존 보안기술을 SOAP 메시지에 적용할 때도 역시 발생할 수 잇기 때문에 이에 대한 해결책이 고려되어야 한다. 서명과 함께 난수 값, 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, 상호운영성이 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 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 두 가지 방법

모두 장단점이 있으나 웹 서비스의 특성상 전송 단계 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.

참고문헌

[1] Martin Naedele, "Standards for XML and Web Services Security" computer April 2003 p 96~98

[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

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

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

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

[6] 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

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

[8] 이해규, 이상수, 김문규, "웹 서비스 보안" 정보처리학회지 2002년 제9권 4호, pp.36-45

김 배 현

1995년 호원대학교 전자계산학과(이학사)
1997년 수원대학교 전자계산학과(이학석사)
2003년 경희대학교 컴퓨터공학과(박사수료)
현재 경희대학교 강사, 한신대학교 강사

나 원 식

2004년 경희대학교 컴퓨터공학과(박사수료)

권 문 택

1970년 육군사관학교(이학사)
1981년 미국 University of Iowa 대학(공학석사)
1987년 미국 University of Wisconsin 대학(경영정보학 박사)
경희대 테크노 경영대학원 종신교수
경희대 정보처리처장
경희사이버 대학교 학장
한국 정보기술응용학회 회장
한국 사이버테러정보전 학회 부회장