웹서비스 보안을 위한 XML 기반 정보 보호 기술 연구

박병철[O], 성백호, 차무홍, 신동일, 신동규
세종대학교 컴퓨터공학과
e-mail:{leon, guardia, bidon}@gce.sejong.ac.kr,{dshin, shindk}@sejong.ac.kr

A Study about Information Security Technology on XML for Web Service Security

Byung-chul Park[O], Baek-ho Sung, Moo-hong Cha, Dong-il Shin, Dong-kyoo Shin
Dept. of Computer Engineering, Sejong University

요 약

웹서비스는 최근 들어 e-business에서 가장 주목받고 있는 신기술이다. 웹서비스는 기존 웹 기반의 디스플레이에 그쳤던 단순정보 교환을 애플리케이션 차원에서 데이터를 통신할 수 있어 개발 가능성이 무한한 프레임워크로 각광받고 있다. 그러나 보안에 취약성을 가지고 있어 웹서비스의 도입과 활성화가 되지 못하고 있는 실정이다. 따라서 본 논문에서는 웹서비스에서 통신에 있어 반드시 지켜져야 할 메시지 무결성, 기밀성, 부인 방지 등의 신뢰성 보장 기법이 어떻게 적용될 수 있는지를 살펴보고, XML 기반의 보안 기술 및 적용 분야 분석을 통해 웹서비스에서의 확장성 및 상호운용성을 보장하는 보안 취약성 해결책을 제시한다.

1. 서론

인터넷을 통한 e-business의 시장이 그 규모와 영역에 있어서 매년 기하급수적으로 성장하고 있다. 이러한 추세 속에서 최근 가장 주목 받고 있는 신기술은 바로 '웹서비스(Web Service)'이다.

웹서비스는 기존 인터넷 프로토콜을 사용할 수 있어 기본 제반비용이 작아지고 XML 기반의 SOAP 인터페이스를 사용해 접근할 수 있는 어플리케이션으로 확장성과 유연성이 뛰어나다. 하지만, 효율적 자원 관리와 자원 사용의 권한 설정이 명확히 정의되지 않고 보안에 취약성을 가지고 있어 범용적으로 e-business에 적용되지 못하고 있다. 이에 본 논문에서는 W3C와 OASIS의 주도하에 된 XML 기반 정보 보호 기술을 적용하여 웹서비스 보안 강화에 대한 방안 연구를 하였다.

2. 관련 연구

2.1 Web Services

2.1.1 Web Services의 개요

지금까지 제공되어온 일반적인 웹서비스와는 달리 Web Services는 표준 RPC를 통해 프로토콜에 의존적이지 않도록 배치되어 바인딩 될 수 있는 비즈니스 분산 객체이다. 표준 인터넷 프로토콜인 SOAP을 사용하여 기존의 HTTP와 같은 인터넷 프로토콜을 그대로 사용하므로 제반 비용이 적어지고 XML을 기반으로 하기 때문에 확장성과 유연성이 있다. 캡슐화된 어플리케이션으로 웹에 존재하는 컴포넌트의 재조립으로 새로운 웹서비스로의 구성이 가능하다. 웹서비스의 기본 구성요소는 서비스 요청자, 제공자, 레지스트리로 나눌 수 있는데 서비스 제공자는 레지스트리에 제공하는 웹 애플리케이션 객체를 등록하고 요청자는 레지스트리에서 서비스를 검색하여 원하는 서비스를 찾을 수 있고 WSDL을 사용하여 서비스와 통신하기 위한 모듈을 생성하여 제공자와 직접 통신할 수 있게 된다 [1].

2.2 Web Services의 핵심 기술

- SOAP(Simple Object Access Protocol)

XML기반 프로토콜로 복잡한 객체 데이터 타입도 쉽게 모델링 할 수 있게 해주며 RPC프로토콜을 지원한다. HTTP뿐 아니라 FTP, SMTP, POP3등 기존의 프로토콜 상에서 동작하므로 부가적인 비용이 발생하지 않으며 특정 벤더에 종속되지 않은 공개프로토콜로 웹서비스에서 사용되는 모든 메시지는 SOAP을 사용하여 통신한다 [2].

- WSDL(Web Service Description Language)

XML기반의 웹서비스 기술 스크립트 언어로 웹서비스에 접촉하고 이용하기 위한 메시지 스키마를 정의하고 있다. 웹서비스 제공자의 endpoint가 어떤 메서드, 속성, 인수, 리턴 값을 가지는지 알려주어 클라이언트에서의 모듈 생성을 가능하게 한다. 이는 자동으로 이루어질 수 있으며 서비스 구현에 따라 생성 방법은 다양할 수 있다 [3].

- UDDI(Universal Description, Discovery and Integration)

일종의 디렉토리 서비스로서 웹서비스의 제공자는 자신의 서비스의 기능을 기술하고 UDDI에 WSDL을 등록하게 된다. 서비스 요청자는 UDDI를 통해 등록된 웹서비스를 간단히 검색할 수 있으며 WSDL에 의한 클라이언트 생성으로 서비스 제공자와 통신할 수 있다 [4].

2.2. XML 보안 기술

2.2.1 XML 전자서명(XML Digital Signature)

XML 전자서명[5] 명세는 W3C와 IETF가 공동으로 표준화를 추진한 XML 기반의 전자서명 기술이다. 현재 XML 전자서명은 2002년 2월 12일부로 W3C에서 표준화가 완료된 상태이며 Recommendation 상태인 표준안이다 [2].

기존의 전자서명의 경우, 수신자 측에서는 송신자가 보낸 데이터를 메시지와 서명으로 분리한 후 각각의 다이제스트 값을 생성하여 비교하였다. 따라서 수신자 측에서 다이제스트를 계산해야 하는 단점이 있다. 하지만 XML의 경우 문서에 수신자가 생성한 다이제스트와 서명 값이 포함되어 있기 때문에, 수신자 측에서 송신자가 보낸 데이터를 메시지와 서명으로 분리하여 다이제스트 값을 계산할 필요가 없다는 장점을 갖고 있다.

2.2.2 XML 암호화(XML Encryption)

현재 인터넷상으로 어떠한 데이터를 전송 할 때 IPSec나 SSL만으로도 충분한 데이터에 대한 기밀성을 보장 할 수 있으며 PGP(Pretty Good Privacy)나 S/MIME을 사용하면 송수신 및 저장 시 암호화를 수행 할 수 있다. 하지만, 이러한 방법은 데이터 전체에 대한 암호화를 수행함으로써 데이터의 일부만 암호화가 필요한 경우에는 부적절할 방법이 된다. 이에 따라 데이터 중 일부분만을 암호화해 중간에 경유하게 되는 제 3자에게 특정 정보를 노출시키지 않으면서 최종 수신자에게 전달 할 수 있는 방법으로 현재 XML 암호화는 2002년 12월 10일부로 W3C에서 Recommendation 상태로 승격시킴으로써 표준화가 완료된 상태이다 [6].

2.2.3 XKMS(XML Key Management Specification)

XKMS[7]는 마이크로소프트와 베리사인, 웹메소드 사가 2001년 4월 W3C에 제안한 XML 기반의 공개 키 관리 명세이다. XKMS명세의 최초 설계 목적은 XML 전자서명과의 연동시 기존 PKI(Public Key Infrastructure) 시스템에 대한 복잡성을 클라이언트에게 숨겨 키 관리 부담을 트러스트 서비스(trust service)에 위임해 그 구현을 용이하게 하기 위함이다. XKMS는 X-KISS(XML Key Information Service Specification)과 X-KRSS(XML Key Registration Service Specification)의 두 부분으로 구성된다.

X-KISS는 티어 서비스 모델(tiered service model)로 구성되며, 각 티어의 주요 역할은 다음과 같다.

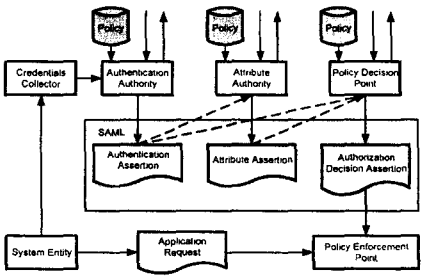
- Tier 0: <ds:KeyInfo>내의 <ds:RetrivalMethod>를 처리. 트러스트 서비스 이용 하지 않음.
- Tier 1(Location Service): <ds:KeyInfo>요소 처리를 트러스트 서비스에 위임하고 공개키 정보 획득. 키에 대한 유효성 확인은 하지 않음.
- Tier 2(Validation Service): Tier 1 서비스 및 키에 대한 유효성 검증 결과 제공

공개 키 쌍에 대한 관리는 X-KRSS가 담당하며 주요 기능은 키 등록(key registration), 키 폐지(key revocation), 키 복구(key recovery) 등이다.

2.2.4 SAML(Security Assertion Markup Language)

SAML[8]은 OASIS의 STTC(Security Services Technical Committee)가 제안한 XML 기반의 인증(authentication) 및 승인(authorization) 정보를 안전하게 교환하기 위한 프레임워크이다.

[그림 1]은 SAML을 이용하여 시스템 엔터티가 접근 제한된 자원에 접근하는 유즈케이스(use-case)의 흐름을 나타낸 것이다. 우선, 보증 정보(credential information)를 모아 credential assertion을 구성한다. 다음으로는 수집된 보증 정보를 이용해 사용자를 인증하게 된다. 인증 시 authentication assertion을 전달하기 위해 외부 PKI 서비스를 이용할 수도 있다. 추가적인 요구에 따라 session assertion 또는 authorization decision assertion 단계로 진행된다.



[그림 1] SAML 아키텍처

2.2.5 XACML(XML Access Control Markup Language)

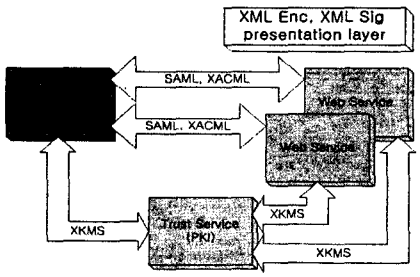
XACML[9]은 2003년 7월 24일 W3C에서 제안한 접근제어 리스트(access control list)를 통해 보안이 요구되는 자원에 대해 미세한 접근 제어 서비스를 제공할 수 있는 XML 기반의 언어이다. XACML은 SAML PDP(Policy Decision Point)의 일부로서 역할을 수행 할 수 있다. XACML의 정의에 따라 각각의 사용자 별 XML 문서 접근 정책을 수립하고 적용 할 수 있다.

XACML은 크게 object, subject, action의 3가지 요소로 구성되는데 subject는 사용자의 ID나 그룹, 또는 역할 등을 나타낼 수 있으며, object 요소는 subject가 접근할 데이터를 의미하며 그 데이터 참조로서 단일 XML 문서에서 개별 요소 수준까지 지정 할 수 있다. action은 4가지 수행 가능 동작으로 구성되며 각각은 읽기, 쓰기, 생성, 삭제 작업이다.

3. 웹서비스의 보안 구조

[그림 2]는 웹서비스 보안 아키텍처를 보여주고 있다. 여기서, 서비스 요청자와 제공자 사이의 통신은 SOAP을 이용하며, XML 전자서명과 암호화를 통하여 통신 메시지의 기밀성, 무결성, 부인방지가 이루어진다. 이 때, 서명과 암호화에 사용되는 키의 관리는 XKMS를 통해 수행된다.

자원 관리와 권한 설정을 위해 SAML, XACML이 적용된다. SAML을 통해 요청자는 ID, 속성, 권한 정보 등 인증 전반의 정보를 서비스 제공자에게 보내고 XACML이 이를 가지고 각 서비스 정책에 따라 권한을 결정, 요청자에게 부여한다.



[그림 2] 웹서비스 보안 아키텍처

4. 웹서비스 보안 요소 분석 및 보안 기술의 적용

4.1. 웹서비스 보안 요소 분석

UN/CEFACT와 OASIS에서 2001년 제안한 ebXML Technical Architecture Risk Assessment v1.0 기술 보고서에서는 e-business에서의 보안 위해 요소(Risk)를 크게 5가지 범주로 나누어 기술하고 있다. 아래는 5가지 보안 위해 요소를 간략히 설명한 것이다.

① 비 인가된 거래 및 사기 - ebXML은 개방된 네트워크인 인터넷을 이용하기 때문에 거래 메시지에 있어 무결성 검증과 거래 당사자의 인증 없이는 신뢰 할 수 있는 거래를 수행 할 수 없다.

② 기밀성 - 인터넷상에서는 기밀성이 요구되는 메시지에 대해 각별한 주의를 필요로 한다.

③ 에러 감지 - 거래 메시지 처리 시 오류가 발생한다면 잘못된 메시지를 전송할 수 있기 때문에 거래 활동에 있어 지속성을 해칠 수 있다.

④ 관리 및 회계에 있어서의 잠재적 손실 - 거래 시 발생하는 각종 데이터에 대한 부주의한 처리는 추후 중요한 법적인 증거물로서의 역할을 수행 할 수 있다는 점에서 거래 증거물과 암호화 키 관리의 중요성을 인식해야한다.

⑤ 잠재적인 법적 책임 - ebXML에서의 기본적인 보안 위해 요소라고 할 수는 없지만, 전자적 거래에 있어서 법적인 제도가 뒷받침이 되지 않는다면, 거래에 대한 근본적인 신뢰성에 문제가 될 수 있다.

4.2 웹서비스 보안 기술 적용

앞서 거론된 웹서비스 보안 기술로 위의 보안 위해 요소를 해결 방안은 다음과 같다.

4.2.1 인증

현재까지의 사용자 인증은 주로 HTTP 사용자 인증 방식을 사용해왔다. 즉, 서비스 제공자는 userid와 password를 발급하고 사용자는 이를 통해 인증을 받아왔으나 웹서비스 사용자가 증가함에 따라 그 정보의 관리에 있어서 매우 비효율적이었다.

그러나 SAML은 서비스간의 인증 상호운용성을 제공하고 Single Sign-On을 실현할 수 있으며 접근 권한에 대한 정보를 제공한다. 가장 중요한 목표는 보안서비스를 요구하는 다른 시스템간의 표준 인증방식으로 상호운용성을 도모하는 것이라 할 수 있다.

SAML은 인증(Authentication), 속성(Attribute), 권한(Authorization)에 관한 내용을 SAML system에 요청하고 이에 대한 응답으로 Assertion을 받게 된다. 인증은 요청 주체에 대한 고유 ID와 같은 인증 정보를 일컫는 것이고, 속성은 요청 주체에 대한 속성에 대한 정보를 제공한다. 즉 e-mail 주소, 시스템이나 조직에서의 역할 등이 될 수 있다. 권한은 시스템의 리소스에 접근할 수 있는지 여부에 대한 요청이며, 이 요청은 시스템 Policy에 따라 접근 여부를 허가 또는 거부하게 된다. 요청과 응답에 대한 메시지는 SOAP을 통하여 이루어지게 된다.

4.2.2 기밀성

메시지의 기밀성 유지를 위해 기존에는 S/MIME이나 PGP를 사용해왔다. 이러한 기존의 기술로도 암호화에는 지장이 없으나 이러한 기술들은 메시지 전체를 암호화하는 방식이다. 따라서 메시지 중에서 중요한 일부분만을 암호화하는 방식에 비해 효율성이 떨어진다. XML 암호화를 이용하면 필요에 따라 메시지 전체 또는 일부분만을 암호화함으로써 메시지의 기밀성을 보다 효율적으로 유지할 수 있다.

4.3.3 부인봉쇄

기존의 전자서명의 경우 단일 홉(Single-hop) 메시지 전송에 적합한 메시지 인증 기능을 제공하지만 XML 전자서명의 경우 단일 XML 문서에 대한 다수의 전자서명을 포함할 수 있어 다중 홉(Multi-hop) 메시지 전송 모델 적합한 기술이다. 이러한 특징은 전자상거래 관련 메시지가 최종 목적지에 도달하기 전 여러 중간 경유지의 메시지 인증이 필요한 경우 매우 유용하다. 또한 XML 문서 전체에 대한 전자서명 뿐 아니라 개별적인 요소 또는 요소의 내용 자체에 세부적으로 전자서명을 수행 할 수 있다. 서명 생성을 위한 자원의 제한 역시 없으며 이진 데이터형식이면 무엇이든 전자서명 생성이 가능하다.

4.3.4 키 관리

암호화나 전자 서명을 사용하기 위해서는 필연적으로 암호학적인 키를 교환하고 사용하여야 한다. 이 때 사용하는 키의 관리에 관한 제반 사항들은 현재까지 일반적인 통일된 적용 기술이 없이 CA(Certification Authority)의 정책에 따라 수행되어왔다. XKMS을 통해 키의 관리를 수행하면 복잡한 공개키 확인 연산을 서버 측에서 전담할 수 있도록 하는 기능을 제공함으로써 개발자의 부담과 클라이언트의 부담을 줄여줄 수 있다.

5. 결론 및 향후 연구방향

웹서비스의 채택 및 지원은 현재 빠른 속도로 증가하고 있으며, 국내에서도 향후 2~3년 내에 가장 유망한 e-business 프레임워크로 전망되고 있다 [10]. 하지만, 전자상거래에 있어 보안 취약점을 가지고 있고 이를 극복하지 못하면, 아예 business 자체가 성립될 수 없음으로 보안 취약점에 대한 효과적인 대응책이 그 무엇보다 중요하다고 할 수 있다.

이에 본 논문에서는 웹서비스의 보안 강화를 위해 XML 보안 기술을 현재 적용 가능하거나 향후 개발 및 적용될 XML 기반의 보안 기술을 살펴봄으로써 웹서비스 프레임워크에서 제안하는 신뢰성 있는 사업 지원 방안을 논의하였다.

향후 연구로는 분석된 요구 사항을 만족하는 실제 웹서비스 시스템의 설계 및 구현을 통해 제안된 기법을 검증함으로써 추가적인 보안 취약 요소의 식별 및 대책에 대한 연구가 요구된다.

6. 참고 문헌

[1] WebService,
http://www.w3c.org/2002/ws/
[2] Simple Object Access Protocol (SOAP),
http://www.w3.org/TR/SOAP/
[3] WSDL,
http://www.w3.org/TR/wsdl/
[4] UDDI,
http://www.oasis-open.org/committees/uddi-spec/
[5] XML Signature Press Release
http://www.w3.org/2002/02/xmlsignature-pressrelease.html.en
[6] XML Encryption
http://www.w3.org/Encryption/2001/
[7] XML Key Management Specification
http://www.w3.org/2001/XKMS/
[8] Security Assertion Markup Language
http://www.oasis-open.org/committees/security/
[9] XML Access Control Markup Language
http://www.oasis-open.org/committees/xacml/index.shtml
[10] SOAP Security Extensions: Digital Signature
http://www.w3.org/TR/SOAP-dsig/