情 報 保 護 學 會 誌
第 14 券 第 4 號, 2004. 8

안전한 웹 서비스를 위한 SOAP 메시지 보안기술 연구

박 배 효*, 이 재 일*

요 약

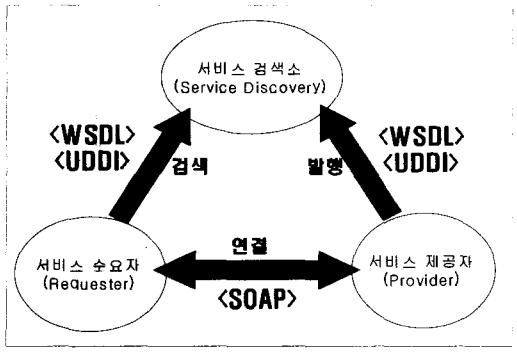
상호운영성, 유연성, P2P(피어투피어), 역동성, 확장성 등 웹 서비스가 지닌 다양한 특성으로 인하여 웹 서비스 보안은 안전한 웹 서비스 운영을 위한 핵심요소라 할 수 있다. 웹 서비스의 기본 구성은 서비스 수요자와 제공자, 검색소로 구성되며 WSDL(Web Service Definition Language), UDDI (Universal Discovery and Integration of Business for Web), SOAP(Smple Object Access Protocol) 등 세 개의 표준으로 서비스는 이루어진다. 이 중에서 특히 메시지 교환을 담당하는 통신 프로토콜인 SOAP는 웹 서비스 보안의 중심에 있으며, 웹 서비스 보안은 SOAP 메시지의 사용자 인증과 무결성, 기밀성을 보장하는 것으로 정의할 수 있다. SOAP는 HTTP를 통해 일반적으로 전송되므로 HTTP 상의 모든 위협을 가지게 되며 전송계층에 기반을 둔 보안을 생각할 수 있지만, 사실상 웹 서비스는 다수의 중간 중개자를 가질 수 있는 구조이기 때문에 단대단 보안(메시지 레벨의 보안)이 반드시 필요하다. 또한, 웹 서비스 상에서 단대단 보안을 보장하기 위해서는 각 객체와 키와의 연결이 중요하며 특정 객체에게 발행한 보안토큰의 신뢰성 확보를 위한 메카니즘을 필요로 한다. 본 논문에서는 이러한 보안 요구사항을 만족하기 위하여 XML 메시지 보안을 위한 전자서명 및 암호화 표준과 SOAP을 위한 W3C, OASIS의 통합표준을 중심으로 SOAP 메시지 보안기술을 분석하고자 한다.

Ⅰ. 서 론

1. 웹 서비스 개요

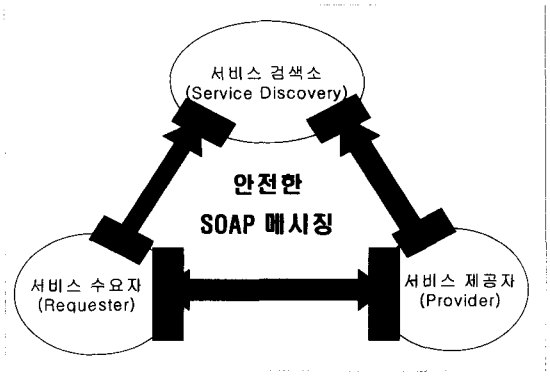
최근 IT 기술 진화의 한 획을 차지하고 있는 웹 서비스는 플랫폼 독립적으로 인터넷과 같은 네트워크를 통해 시스템간 연계, 통합과 자원 공유를 가능하게 하는 표준화된 인터넷 확장성표기언어(이하 XML) 기반 웹 기술이다. 이러한 웹 서비스 아키텍처[1]는 크게 나누어 서비스를 제공하는 서비스 제공자(Provider)와 서비스를 필요로 하는 서비스 수요자(Requester), 이들 사이를 중개하는 서비스 검색소(Discovery Service)로 구성된다. 그리고 이들 사이에서는 서비스를 발행(publish)하고, 이를 검색(find)하고 나서 제공자와 수요자 사이의 서비스에 대한 연결(interact)이라는 기본적인 세 가지 기능을 갖게 된다.

[그림 1]과 같이 웹 서비스는 기본적으로 WSDL (Web Service Definition Language)[2], UDDI (Universal Discovery and Integration of Business for Web)[3], SOAP[4] 등 세 개의 표준으로 구성된다. WSDL은 웹 서비스 호출에 대한 인터페이스, 의미론(Semantics) 등을 기술하고 있는 XML 문서이고, UDDI는 서비스 탐색 및 게시를 위한 공개된 디렉토리이며, SOAP는 HTTP, SMTP 등과 같은 저수준 프로토콜을 통해 웹 서비스 상의 각 객체간 통신 프로토콜을 총칭한다.



[그림 1] 웹 서비스 개요도

* 한국정보보호진흥원 전자거래보호단 ({parkbh, jilee}@kisa.or.kr)



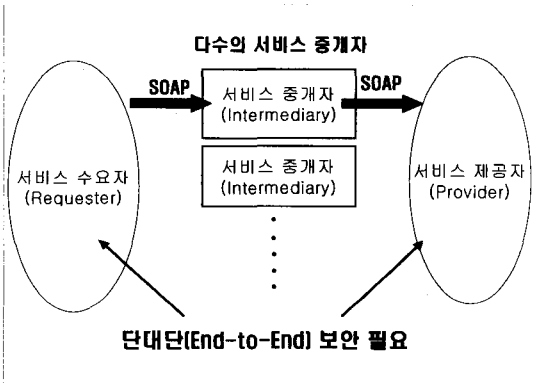
〔그림 2〕 SOAP 메시지 보안

2. 웹 서비스 보안 = SOAP 메시지 보안

웹 서비스 특성상 서비스 구성원이 여러 네트워크에 분산되고 외부에서 접근이 쉽기 때문에 보안은 단순한 중요성 이상의 의미가 있다. 상호운영성, 유연성, P2P(피어투피어), 역동성, 확장성 등 웹 서비스가 지닌 다양한 특성을 제대로 구현하기 위해서는 보다 엄격한 보안이 필요하다.

〔그림 2〕와 같이 웹 서비스는 서비스 수요자, 제공자, 검색소가 공유하는 정보에 대한 보안으로 단순화시킬 수 있다. 이들 객체간에는 어떤 환경에 있든지 간에 서로 데이터를 자유롭게 주고 받을 수 있으며 어떤 애플리케이션이라 하더라도 서로 호출하여 사용할 수 있도록 되어 있기 때문에, 데이터 교환을 담당하는 통신 프로토콜인 SOAP의 보안은 무엇보다 중요하다고 할 수 있다. 따라서, 웹 서비스 보안이란 SOAP 메시지의 사용자 인증과 무결성, 기밀성을 보장하는 것으로 정의할 수 있다.

SOAP는 HTTP를 통해 일반적으로 전송되므로 HTTP 상의 모든 위협을 가지게 되며 전송계층에 기반을 둔 보안을 생각할 수 있다. 하지만, 〔그림 3〕과 같이 웹 서비스는 서버 클라이언트(C/S)의 구조가 아닌, 다수의 중간 중개자를 가질 수 있는 구조이기 때문에 SSL/TLS와 같은 점대점(Point-to -Point) 보안이 아니라, 단대단 보안(End-to-End,메시지 레벨의 보안)이 반드시 필요하다. 추가적으로, 웹 서비스 상에서 단대단 보안을 보장하기 위해서는 각 객체와 키와의 연결이 중요하다. 어떤 기관이 특정 객체에게 보안토큰을 발행했는지에 따라 신뢰가 결정되므로 이를 다룰 수 있는 메카니즘을 필요로 한다.〔1〕



〔그림 3〕 단대단 보안

본 논문에서는 SOAP 보안 요구사항 및 관련 표준을 중심으로 SOAP 메시지 보안을 위한 기술을 분석하기로 한다.

3. SOAP 관련 보안 표준

SOAP 메시지를 보호하기 위해서는 크게 XML 전자서명과 암호화 등 기반요소 표준과 SOAP-SEC, WS-Security 등 통합 표준으로 〔표 1〕과 같이 분류할 수 있다. 〔표 1〕에 나타난 표준 및 관련 기술에 대해서는 〔Ⅲ~Ⅳ절〕에 걸쳐 다루기로 한다.

〔표 1〕 SOAP 관련 보안 표준

구분	표 준 명	기 구
기반요소 표 준 (Ⅲ장)	XML Signature〔5〕	W3C
	XML Encryption〔6〕〔7〕	W3C
	XKMS 2.0〔8〕	W3C
통합표준 (Ⅳ장)	SOAP-SEC〔9〕*	W3C
	SOAP Message Security 1.0〔10〕	OASIS
	SAML token profile 1.0**〔11〕	
	SAML 2.0〔12〕, XACML 1.0〔13〕	

* 2001년 이후 표준화 진행 없음
** 현재(2004.7) Working Draft 상태임

Ⅱ. 웹 서비스 위협요소 및 보안 요구사항

1. SOAP 메시지 위협요소

〔그림 3〕과 같이 일반적으로 웹 서비스는 SOAP 메시지 기반으로 다양한 중간 중개자를 통하여 통신이 이루어진다. 즉, 전통적인 네트워크 레벨의 보안과 달리 웹 서비스는 다양한 경로를 통한 메시지 라우팅을 포함할 수 있도록 메시지 기반의 단대단 보안이 필요하다. 이에 따른 웹 서비스에서의 SOAP 메시지 위협요소는 아래와 같다.

- **메시지 변조** : 공격자가 메시지나 첨부물의 전체나 일부를 수정하기 위하여 SOAP 헤더나 몸체 부분을 공격하는 것
- **기밀성** : 인증되지 않는 객체에게 SOAP 메시지 전체나 일부의 정보에 대한 접근을 허용하는 것
- **Man-in-the-middle** : SOAP 메시지의 중간 중개자를 공격하여 웹 서비스 수요자와 제공자 사이의 메시지를 수집하는 것.
- **스푸핑** : 공격자가 신뢰된 객체의 Identity로 가지고 목표 객체에 접근하는 것
- **Denial of Service(DoS)** : 정상적인 네트워크의 사용이나 관리를 방해하여 웹 서비스 사용자들로 하여금 서비스를 사용하지 못하도록 막는 것
- **재생 공격** : 공격자가 이전에 특정 서비스 수요자와 제공자간에 행해졌던 통신을 도청하여 보관하고 있다가 나중에 다시 재생하여 전송하는 공격하는 것

2. 보안 요구사항

안전한 웹 서비스를 위해서는 각 객체간의 단대단 보안을 고려하여 중간 중개자와 서비스 수요자, 제공자와 통신시 보안 설정이 필요하다. 웹 서비스 위협요소로부터 SOAP 메시지에 대한 보안을 유지하기 위해서 요구되는 보안 요구사항은 인증, 권한부여, 기밀성, 무결성, 부인봉쇄 등이 있다.

- **인증** : 인증은 서비스 수요자와 제공자의 신원을 검증하기 위해서 필요한 것으로 보통 패스워드나 PIN (Personal Identification Number), 스마트 카드와 같은 보안토큰을 이용해 인증한다. 웹 서비스에서 인증은 SOAP와 보안토큰간의 바인딩(Binding)으로 이루어지며, 토큰으로는 X.509 인증서, 커버러스 티켓, SAML 등을 이용할 수 있다.
- **권한부여** : 권한부여는 특정 자원에 대한 접근을 통제하기 위해서 필요하다. 웹 서비스에서는 일단 인증된 객체에 대하여 접근권한을 통해 해당 자원에 접근을 허용하고 이를 접근제어(access control)라고 한다. 웹 서비스에서는 SOAP에 SAML을 바인딩 함으로써 권한부여를 가질 수 있는 기술을 제공한다.
- **기밀성 및 무결성** : 전송되는 SOAP 메시지에 대한 보안 유지는 항상 고려해야 한다. 다수의 중간 중개자가 있음에도 불구하고 단대단간 메시지에 대한 기밀성과 무결성이 보장되어야 한다. 데이터에 대한 암호화를 통해 중간에 데이터를 가로채더라도 이를 읽을 수 없도록 하고, 전자서명을 통해 무결성을 확보한다.
- **부인봉쇄** : 부인봉쇄(Non-repudiation)는 실제 거래가 부인될 수 없도록 하는 것으로 인증이나 감사, 로그 등의 보안 기술이 요구된다. 전자서명을 통한 SOAP 메시지 전송으로 부인봉쇄를 만족시킬 수 있다.

Ⅲ. XML 메시지 보안

웹 서비스에서 사용되는 SOAP 메시지는 XML메시지로 구성되어 있음에 따라, SOAP 메시지 보안을 위해서는 기존의 XML 보안을 수용해야 한다. 이를 위하여, 본 장에서는 W3C을 중심으로 표준화가 진행되는 XML 전자서명 [5], 암호화 기술[6][7]과 XKMS(XML Key Management Specification) [8]을 통한 키 관리 기술에 대하여 분석하고자 한다.

1. XML 전자서명

XML 전자서명은 W3C와 IETF가 공동으로 표준화를 추진한 XML 기반의 전자서명 기술로서 2000년 7월에 XML Signature Requirements (RFC 2807)[14]를 채택한 이래로 많은 논의가 진행되었다. 2002년 2월에 XML 서명 문법과 처리에 대한 W3C 권고안(XML-Signature Syntax and Processing W3C Recommendation)을 RFC로 채택하였다. 현재 XML 전자서명 워킹그룹에는 IBM, 베리사인, 볼티모어, 마이크로소프트, 선, 코르섹 시큐리티(Corsec Security), 시그니오(Signio), 모토로라 등 해외 유수 기업들이 참여하고 있다. 이 표준에서는 전자서명 오퍼레이션의 결과를 가져올 수 있는 스키마를 정의하고 인증과 데이터 무결성, 서명된 데이터에 대한 부인봉쇄 등을 지원하기 위한 내용이 포함되어 있다. XML 전자서명의 특징은 선택된 부분 일부에 관한 전자서명 기능과 여러 객체가 참여할 수 있는 다중 전자서명 기능으로 인증 기술에 많은 확장성을 줄 수 있다. 이러한 특징은 기존의 PKI 서명과 분명한 차이점을 보인다. [15]

1.1 PKI 전자서명 vs XML 전자서명

일반적으로 XML 전자서명은 PKI 전자서명을 비교하면 아래 [표 2]와 같이 정리할 수 있다.

1.2 XML 전자서명 생성 및 검증[5]

XML 전자서명은 기존의 PKI 전자서명과 유사한 방식으로 생성된다. 먼저, 전자서명할 문서를 선택하고, 각 문

〔표 2〕 PKI 전자서명과 XML 전자서명 비교

항목	PKI 전자서명	XML 전자서명
암호화 방식	공개키 암호화 개인키 및 공개키 부여	공개키 암호화 개인키 및 공개키 부여
서명 방식	문서 전체 서명 문서 해쉬값 동일	문서 부분 서명 가능 동일한 문서 해쉬값을 위해 Canonicalization 필요
서명 파일	원본 및 해쉬값 파일 함께 전송	서명 정보를 세분화 가능

서의 해쉬값을 계산한 뒤 문서에 대한 레퍼런스를 모은다. 이후 해쉬값에 대해 전자서명을 실행하고 키 정보를 추가한 뒤 전자서명을 마치면 된다. 이렇게 생성된 XML 전자서명을 검증하는 방법은 〈SignedInfo〉 엘리먼트에 있는 서명을 검증하면 된다. 이를 위해 먼저 지정된 해쉬 알고리즘을 이용하여 〈SignedInfo〉 엘리먼트의 해쉬값을 계산한 후 키 정보에 있는 공개키를 이용해 해독한 값과 동일한지를 검토하면 된다. 그 다음에는 각각의 레퍼런스에 대한 해쉬값을 검증할 수 있는데, 각각의 〈Reference〉 엘리먼트에 대한 해쉬값을 계산하고 이를 〈DigestValue〉 엘리먼트 값과 동일한지 검토하면 제대로 서명됐는지, 그리고 중간에 문제가 없었는지 알아볼 수 있다.

또한, XML 전자서명은 XKMS를 이용하여 효율적으로 검증할 수 있다. XKMS에서 XML 전자서명의 검증 방식은 XKMS에서 자체적으로 검증 서버를 이용하여 검증하거나, PKI의 검증서버(SCVP, OCSP)들과 연동하여 XML 전자서명을 검증하는 두 가지의 방식이 있다. OASIS 등의 표준화 단체에서는 아직 구체적인 연동 방안은 제시하고 있지 않으며, 전자서명 검증에 XKMS를 사용할 것인가 PKI와 연동할 것인가는 구현 환경에 따라 달라질 수 있다. XKMS에 대한 추가적인 내용은 〔Ⅳ절〕에서 설명하도록 하겠다.

2. XML 암호화

현재 인터넷 상으로 어떠한 데이터를 전송할 때 IPSec이나 SSL으로 데이터에 대한 기밀성을 보장할 수 있고, PGP(Pretty Good Privacy)나 S/MIME을 사용하면 송수신 및 저장시 암호화를 수행할 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 방법이 XML 암호화이다. W3C는 2002년 10월에 XML 암호화와 관련된 새로운 표준 2개를 승인했다. 암호규격은 'XML 암호구성 및 처리과정(XML Encryption Syntax and Processing)'과 'XML용 해독 전환 서명(Decryption Transform for XML Signature)'등으로 두 규격 모두 웹사이트 등의 XML 응용분야를 위한 보안 개선 목적을 갖고 있다.

2.1 XML 암호화와 SSL/TLS 의 차이

〔표 3〕는 XML 암호화와 SSL/TLS를 비교한 것이다. XML 암호화는 암호화의 범위도 지정할 수 있도록 하고 있다. 엘리먼트 이름만 암호화될 수도 있고, 그 내부에 포함된 데이터를 같이 암호화할 수도 있으며, 데이터만 암호화할 수도 있다. 또한 부분 암호화를 통하여 해당 키에 정보를 아는 사람만이 특정 부분을 볼 수 있도록 하는 접근권한의 역할을 수행할 수도 있다.

〔표 3〕 SSL/TLS와 XML 암호화 비교

	SSL/TLS	XML 암호화
특징	· 점대점 보안 · 전체 암호화만 가능 · 하나의 키로 암호화	· 단대단 보안 · 부분 암호화 가능 · 한 문서에 다중 키로 부분 암호화 가능

2.2 XML 암호화 생성 및 검증〔6〕〔7〕

XML 암호화를 생성하기 위해서는 가장 먼저 암호화할 문서를 선택하고 전체 문서의 암호화인지 특정 엘리먼트의 암호화인지를 결정한다. 이후 암호화 알고리즘을 선택하고 암호화를 실행한다. 암호화된 문서를 받을 경우 이를 검증하기 위하여 가장 먼저 알고리즘을 결정하는 엘리먼트를 처리한다. 여기서는 키 정보 에리먼트의 사용 여부를 확인하고 키 정보 엘리먼트에 따른 데이터 암호화키를 찾는다. 만일 키가 암호화되어 있다면 그것을 복구한 뒤 문서 복호화 준비를 한다. 그 후 〈CipherData〉 엘리먼트에 포함되어 있는 데이터를 복호화한다. 이때 엘리먼트 타입과 엘리먼트 내용 타입인지 알아내어 복호화 과정을 처리한다.

3. XKMS 키 관리 기술

3.1 XKMS 개요〔8〕

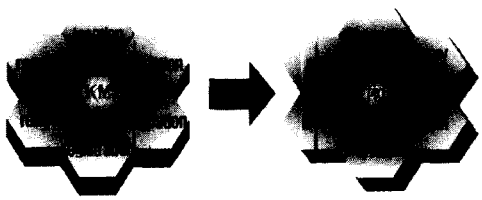
XML 메시지를 안전하게 관리하기 위해서는 XML 전자서명과 암호화 기술이 필수적으로 요구된다. 그러나 XML 전자서명과 암호화는 통상적으로 전통적인 PKI의

도움을 기반으로 하고 있다. 예를 들어, XML 서명을 검증하려는 해당 어플리케이션은 서명 메시지를 받아들이기 전에 서명자의 신원을 확인해야 하며 수신자와 암호화된 통신을 하려면 적절한 암호화키를 검색해야 한다. 이러한 이슈들은 XML을 기반으로 한 서비스뿐만 아니라 기존의 시스템과의 상호연동을 위해서도 위해서는 꼭 필요하다. 이에 따라 제안된 표준이 XKMS(XML Key Management Specification)이다. W3C에서는 2004년 4월에 XKMS 2.0을 권고 후보(Candidate)로 발표하였다. XKMS는 공개키를 분배하고 등록하기 위한 관리 프로토콜을 정의하고 있으며 복잡한 PKI 프로토콜들을 웹 서비스에서 사용하여 서명검증, 유효성 검증 및 사용자의 공개키를 관리하는 방법을 제공하다.

XKMS의 목표는 다음과 같다. 첫째, XKMS는 PKI와는 달리 XML 문서를 기반으로 한다. 따라서 XKMS는 이러한 XML의 단순함을 이용하여 기존의 PKI의 사용자 어플리케이션의 복잡성을 배제하고 PKI의 복잡함을 서버 측으로 돌리는 것이다. 둘째, 기존의 인프라와의 상호연동을 하는 것이다. 이를 통하여 데이터베이스와 PKI 인프라 및 데이터베이스의 이중화된 구조를 극복하고 하나의 데이터베이스에서 이를 처리할 수 있다.

3.2 PKI vs XKMS[15]

기존의 PKI와 XKMS의 각 구성요소와의 관계를 대비하면 [그림 4]와 같다. 그림에서 알 수 있듯이 기존 PKI 기능을 XKMS에 통합함으로 클라이언트 측에 부담을 줄여주어 XML 전자서명 및 암호화 보안 응용 개발이 용이



[그림 4] XKMS와 PKI의 구성요소 대응관계

[표 4] XKMS 장점

구 분	XKMS 장점
구 현	XML의 단순성 이용 신뢰처리를 서버측 전담
표 준	개방형, 산업적 표준
접 근	장치의 접근 용이 (모바일 포함)
확 장	기능 확장 용이

해진다. 기존 PKI에 비해 XKMS의 장점을 나타내면 [표 4]와 같다.

3.3 XKMS 시스템 구성[8]

XKMS는 X-KISS(XML Key Information Service Specification)과 X-KRSS(XML Key Registration Service Specification)의 두 부분으로 구성되어 있다. X-KISS 명세는 XML 전자서명내에 포함된 공개키 정보를 해석하는 Trust 서비스에 대한 프로토콜을 정의한다.X-KISS 프로토콜은 키 정보 요소를 처리하기 위해 요구된 작업을 처리하기 위한 서비스 등을 클라이언트에게 제공한다. 프로토콜 설계의 핵심적인 목표는 기본적인 PKI에서의 구문과 복잡성을 극복하고, 응용 구현의 복잡함을 최소로 하기 위한 것이다. 기본적인 PKI는 X.509/PKIX, SPKI 및 PGP와 같은 다른 명세에 기초를 두고 있다. X-KRSS 명세는 공개 키 정보의 등록을 받아들이는 웹 서비스에 대한 프로토콜을 정의한다.공개키는 등록된 즉시 X-KISS를 포함하는 다른 웹 서비스와의 결합으로 사용되어질 수 있다. 두 프로토콜은 XML 스키마, WSDL(Web Services Definition Language)에 의해 정의된 메시지 사이의 관계와 SOAP을 채택하는 프로토콜 내에서 표현된 구조로 정의된다. 다른 부합되는 객체 인코딩 구조에서의 XKMS의 표현 또한 가능하다.

3.4 XKMS 2.0 보안이슈

XKMS 2.0은 기존 1.0 버전에 메시지 정의 및 프로토콜상의 보안 요구사항 등이 추가되었다. XKMS 2.0에 관한 OASIS WG에서 다루는 주요 보안 이슈는 다음과 같다. 대부분 기존의 PKI와 유사한 문제점들이 도출되었다. [15][16]

- **모호한 바인딩(Binding)** : 서로 다른 도메인에서 Key name의 중복으로 인하여 바인딩 문제 발생 가능함
- **인증정책** : 인증서 정책검증 및 정책매핑에 대한 규정 없음
- **서비스 위치정보** : XKMS 서비스의 위치정보를 획득하는 방법이 명확하지 않음
- **검증정책** : 인증서 검증시 사용자가 초기 검증정책을 설정할 수 없음
- **키 사용용도** : 암호화, 전자서명, 키교환의 용도만을 제공함
- **유효성 정책** : 유효, 폐기, 미결의 세가지 상태만을 제공함

- **키 복구 서비스** : 개인키의 저장, 권한설정, 전송방법 등이 설정되어 있지 않음
- **대칭키 관리** : 대칭키 서비스 지원 논의 중임
- **서비스 리퍼럴(Referral) 및 루프(Loop) 위험** : XKMS 서비스가 다른 XKMS에게 서비스 요청을 할 때 루프 형성 가능함
- **신뢰관계 형성** : Bridge나 Cross Certification 등 신뢰관계 형성에 관한 규정 없음
- **신뢰된 시간 생성기** : 인증서 검증을 위한 신뢰된 시간 생성기 없음
- **속성 인증서** : PKI에서 사용되는 속성 인증서에 대한 언급 없음
- **익명 요청자** : 익명 요청자에 알맞은 인증정책 확립 및 서비스 제공 필요함
- **접근권한** : 접근권한 설정에 대한 언급이 없음
- **개인정보 정책** : 개인정보 정책에 대한 명확한 언급 없음

Ⅳ. SOAP 메시지 보안을 위한 통합표준

웹 서비스에서는 확장성을 제공하는 언어인 XML 메시지를 SOAP을 이용하여 기존의 인터넷 통신 프로토콜(HTTP, SMTP, or FTP)들을 통해 이질적인 어플리케이션들간의 직접적인 연동을 가능하게 하였다. SOAP 메시지는 프로그래밍 언어, 미들웨어, 플랫폼에 상관없이 상호운용성을 쉽게 극대화시킬 수 있도록 하지만 다양한 보안 요구사항을 필요로 한다. [그림 2]과 같이 웹 서비스에서는 각 객체간의 거래를 중심으로 크게 세 가지의 보안이 필요하다. 가장 먼저, 실제 운영상태에서 서비스 수요자(Requester)와 제공자가 공유하는 메시지에 대한 보안이 필수적이다. 사실상 메시지 보안 이전에 배포되는 네트워크에 대한 보안이 선결과제이지만, 이에 대한 논의는 하지 않기로 한다. 두 번째는 서비스 수요자와 UDDI 사이의 안전한 거래이다. 서비스 수요자가 UDDI에서 필요한 서비스를 찾는(Discovery) 과정을 나타내는 특정 프로토콜은 없으며, 특정 보안 정책에 의해서 관리가 가능하다. 셋째, 서비스 수요자와 제공자 사이의 안전한 거래이다. 본 절에서는 이러한 보안을 해결하기 위하여 개발되어온 SOAP 메시지 보안표준에 대한 논의를 다루기로 한다.

4.1 SOAP-SEC[9]

2000년 5월에 W3C 표준으로 발표된 SOAP 1.1에는 XML 전자서명이 포함되어 있지 않아서 보안 취약성이 지적되었다. 이를 위하여 2001년 2월에 IBM과 마이크로소프트가 W3C에 제출한 규격으로 SOAP 1.1 메시지에 XML 전자서명을 사용하는 표준화된 방법을 제공하는 SOAP-SEC이 있다. 전자서명을 통하여 전송자 인증, 자료의 무결성 보장, 부인방지 등의 문제해결이 가능하게 되었다.

[Ⅲ절]에서 살펴보았듯이 XML 전자서명과 암호화 표준은 XML 문서에 대해 동시에 적용되어 해당 문서가 서명되고 암호화되도록 할 수 있다. SOAP 메시지에 SOAP-SEC를 이용해 서명하고 여기에 암호화한 문서를 첨부하고 전달할 수 있다. 데이터의 서명을 검사하기 위해 먼저 암호화한 첨부 문서를 해독해야 가능하도록 할 수도 있다. SOAP-SEC 표준에서는 〈SOAP-SEC : Signature〉라는 헤더 엔트리를 추가하는 방식으로 전자서명을 지원하고 있으며, actor와 mustUnderstand라는 기존 헤더 아이템을 이용하여 헤더 엘리먼트 수신자와 XML 서명에 대해 검증 여부를 지정하고 있다. SOAP 메시지는 XML 문서로 구성되어 있기 때문에 SOAP 메시지에 대한 전자서명은 W3C의 XML 전자서명 표준을 동일하게 이용한다.

4.2 SOAP 보안을 위한 웹 서비스 통합 표준 : SOAP MessageSecurity 1.0(WS-Security 2004)[10]

2004년 3월 15일에 OASIS는 SOAP 보안에 대한 규격으로 WS-Security 2004라는 표준을 발표했다. 이 표준은 SOAP 확장성 모델을 이용하여 풍부한 메시징 환경을 제공할 수 있고, 보안 토큰, 디지털 서명, 암호화에 이르는 기본적인 보안 이슈를 모두 다루고 있다. 따라서, 이는 SOAP-SEC에 비해 자세하면서도 한층 진보한 표준으로 알려지고 있다.

WS-Security 2004는 웹 서비스 상에서 안전한 SOAP 메시지 교환을 구축할 수 있도록 하는 것으로 메시지 인증, 메시지 기밀성 및 무결성을 제공하기 위하여 SOAP 메시징을 개선하였다. 또한, 보안 토큰과 메시지를 연결시키는 범용 메카니즘을 제공하며, 바이너리 보안 토큰을 인코딩하는 방법을 설명하고 있다. WS-Security 2004는 기본적으로 XML 서명과 XML 암호화 표준을 기반으로 작성되었다. SOAP를 확장하기 위해 WS-Security 2004는 SOAP 헤더를 이용하며 여기에 X.509 인증서, 커버러스 티켓 등 보안토큰과 전자서명, 암호화와 관련된 각종 요소가 자리를 잡는다.

4.2.1 보안토큰을 이용한 인증

인증에 대한 문제를 해결하기 위해 WS-Security

2004는 보안토큰을 교환하는 방법을 정의한다. 여기에서 보안토큰은 보안토큰의 소유주를 식별할 수 있는 유일한 것이면 어떤 것이든 이용할 수 있다. 예를 들어, ID/PW, X.509 인증서나 커버로스 티켓 등을 모두 이용할 수 있다. 보안토큰의 교환 및 인증과 관련한 WS-Security 2004에서는 〈wsse:Security〉 헤더를 정의하여 보안정보를 전달하는 방법을 제공한다. 이 헤더를 확장시켜 SOAP 헤더 속에 보안토큰을 직접적으로 넣을 수 있도록 하고 있다. 또한 〈wsse:Security Token Reference〉를 통하여 보안토큰을 참조하기 위한 확장 가능한 메카니즘을 제공한다.

4.2.2 SOAP 메시지 무결성

WS-Security 2004는 메시지 무결성을 위하여 전체 SOAP 메시지나 일부 메시지에 XML 전자서명을 이용한다. 이를 통하여 메시지 발신자는 메시지 수신자로 하여금 메시지가 전송 중에 변경되었는지를 감지할 수 있으며, 메시지 서명자의 보안 토큰의 검증을 통하여 특정 소유자를 확인할 수 있도록 한다. XML 전자서명을 위해 〈Security Token Reference〉를 이용할 때, 메시지 서명자의 보안 토큰이 이에 연결되고, 해당 보안 토큰의 요구(Claim)와 메시지간의 매핑이 애플리케이션에 의해 이루어진다. 일부 SOAP 헤더의 가변성 때문에 XML 전자서명에 정의된 Enveloping Signature Transform을 사용해서는 안 되며, 대신 메시지가 원하는 엘리먼트가 서명되도록 명확하게 포함시켜야 한다. WS-Security 2004에서는 한 메시지에 여러 개의 서명이 첨부될 수 있도록 하고 각각의 서명이 메시지를 참조할 수 있도록 하였다. 이러한 과정은 여러 처리 단계를 거쳐야 하는 수많은 분산 애플리케이션에서 전자서명을 위해 아주 중요한 사항이다.

4.2.3 SOAP 메시지 기밀성

전자서명이 된 메시지는 메시지 무결성을 보장하지만 기밀성을 보장하는 것은 아니다. SOAP 메시지 자체는 텍스트 문자열로 전송되기 때문에 기밀성을 제공하기 위해서는 메시지 암호화에 대한 고려가 있어야 한다. WS-Security 2004에서는 메시지 본문, 헤더, 하위 구조에 속한 모든 것, 또한 첨부 문서들이 어떻게 결합되든 간에 메시지 발신자와 수신자가 공유하는 공통 대칭키를 사용하거나 암호화된 형식으로 메시지와 함께 전달되는 키를 사용해 모두 암호화할 수 있다. 암호화가 필요한 데이터는 SOAP 메시지 내에 〈xenc:EncryptedData〉 엘리먼트에 포함되도록 하면 된다. 암호화된 SOAP 메시지를 만들기 위한 방법은 XML 암호화 표준을 따른다.

4.3 SAML in SOAP[11]

OASIS의 WS-Security에서 개발중인 SAML (Security Assertion Markup Language)[12] 토큰 프로파일은 OASIS 표준인 SAML을 SOAP에 보안토큰으로 내장하여 객체에 대한 인증, 권한부여, 그리고 속성 등의 XML 포맷을 지정함으로써 SOAP 보안을 지원할 수 있도록 하고 있다.

XML에 기반한 SAML은 인증 및 권한 정보를 교환하기 위한 표준으로 접근 제어 기술로는 접근제어 리스트(access control list)를 통해 보안이 요구되는위치정보에 대해 미세한 접근 제어 서비스를 제공할 수 있는 XML 기반의 XACML(XML Access Control Markup Language)[13]을 활용한다.

4.3.1 인증 및 권한 정보 교환을 위한 SAML[12]

SAML는 OASIS가 제안한 것으로 인터넷상의 서로 다른 도메인간에 XML에 기반한 인증 및 권한 정보(토큰)를 교환하기 위한 표준이다. SAML은 XML로 인코딩된 보안 어서션(assertion)과 XML로 인코딩된 요청/응답 프로토콜, 그리고 기존의 표준 통신채널 및 메시지 프로토콜을 응용하여 SAML 메시지를 주고받는 기술을 정의한 바인딩 등으로 구성된다. 사용자의 보안 정보는 어서션으로 표현되는데 어서션의 종류는 크게 세 가지이다. 사용자에 따른 인증정보를 표현하는 인증 어서션, 사용자에 따른 여러 특별한 정보(개인 주소, 전화번호, 이메일 주소, 신용한도, 신용등급 등)를 표현하는 속성 어서션, 그리고 특정 리소스에 대한 접근 권한을 정의하는 인가 어서션이다.

이러한 어서션은 XML로 인코딩 되어서 추후에 변경, 추가, 삭제가 용이하다. 또한 SAML이 제공하는 인증토큰 교환에 따른 싱글사인온(SSO)을 활용하여, 사용자는 단 한번의 로그온 과정으로 여러 전자거래 서비스를 자유롭게 이용할 수 있게 된다. Policy Enforcement Point (PEP)는 사용자의 인증 및 권한정보를 다른 전자거래 서비스에게 제공하기 전에 Policy Decision Point(PDP)에 SAML 요청을 통하여 권한검증을 수행한다. SAML은 토큰을 암호화하기 위해 XML 암호화를, 토큰인증을 위해 XML 전자서명을 활용한다.

4.3.2 접근제어를 위한 XACML[13]

XACML 역시 OASIS에 의해 주도되는 표준으로 SAML에 부족한 접근제어 정책을 XML로 표현한 것이다. XACML은 접근제어 리스트(access control list)를 통해 보안이 요구되는 자원에 대해 미세한 접근 제어 서비스를 제공하며, SAML PDP의 일부로서 역할을 수행

할 수 있다. XACML의 정의에 따라 각각의 사용자별 XML 문서 접근 정책을 수립하고 적용 할 수 있다.

V. 결 론

지금까지 웹 서비스 보안을 위하여 XML 전자서명 및 암호화 표준과 W3C 및 OASIS의 통합표준을 중심으로 SOAP 메시지 보안 기술을 분석하였다. 이러한 보안기술 분석의 출발은 SOAP 메시지가 웹 서비스에서 차지하는 중요성에서 기인한다. 웹 서비스는 서비스 수요자, 제공자, 검색소간의 데이터 교환으로 정의할 수 있으며 이러한 데이터 교환을 담당하는 통신 프로토콜이 바로 SOAP이기 때문이다. 이에 따라, SOAP 메시지의 사용자 인증, 무결성, 기밀성을 보장하기 위한 SOAP 메시지 보안기술 개발 및 표준화 움직임은 웹 서비스의 핵심 요소기술로 자리잡고 있으며 신뢰성 있는 서비스 프레임워크 구축에 핵심 기능을 수행할 것으로 보인다. 다만, 현재 웹 서비스의 표준이 외국 기업 주도로 이루어지고 있어 국내기술의 종속화가 염려된다. 웹 서비스의 상호운용의 특성상 국제 표준의 장악력이 절대적임을 고려해 볼 때, 국내 기업의 보다 활발한 기술개발과 표준화 활동이 필요할 때임을 강조하고 싶다.

참 고 문 헌

[1] W3C, Web Services Architecture - working group note, http://www.w3.org/2002/ws/arch/February 2004

[2] OASIS, Web Services Description Language (WSDL) 1.1, http://www.w3.org/TR/wsdl, March 2001

[3] UDDI consortium, http://www.uddi.org

[4] W3C, SOAP Version 1.2 - Recommendations, http://www.w3.org/TR/soap, June 2003

[5] W3C, XML-Signature Syntax and Processing, http://www.w3.org/TR/xmldsig- core, February 2002

[6] W3C, XML Encryption Syntax and Processing, http://www.w3.org/TR/xmlenccore, December 2002

[7] W3C, Decryption Transform for XML Signature, http://www.w3.org/TR/xmlenc-decrypt, December 2002

[8] W3C, XML Key Management Specification (XKMS) Ver 2.0-Candidate Recommendation, http://www.w3.org/TR/xkms2, April 2004

[9] W3C, SOAP Security Extensions: Digital Signature, http://www.w3.org/TR/2001/NOTE-SOAP-dsig-20010206, February 2001

[10] OASIS, Web Services Security: SOAP Message Security 1.0(WS-Security 2004), http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf, March 2004

[11] OASIS, Web Services Security: SAML Token Profile - working drafts, http://www.oasis-open.org/committees/download.php/7837/WSS-SAML-15.pdf, July 2004

[12] OASIS, Security Assertion Markup Language(SAML), http://www.oasis-open.org /committees /security, July 2004

[13] OASIS, eXtensible Access Control Markup Language(XACML) Version 1.0 - Standards, February 2003

[14] J. Reagle, IETF RFC2807 XML Signature Requiremets, July 2000

[15] 중앙대학교, *위치기반 서비스에 적합한 전자서명 인증기술 연구*, December 2003

[16] W3C, XML Key Management(XKMS 2.0) Requirements, http://www.w3.org/TR/xkms2-req, May 2003

〈著 者 紹 介〉

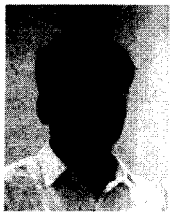
박 배 효(Park, BaeHyo)

1997년 2월 : 한국과학기술원 전기 및 전자공학과 학사

2002년 8월 : 광주과학기술원 기전공학과 석사

2002년 7월~현재 : 한국정보보호진흥원 연구원

〈관심분야〉 유비쿼터스 정보보호, 암호프로토콜



이 재 일(Lee, Jae-il)
종신회원

1986년 2월 : 서울대학교 계산통계학과 학사
1988년 2월 : 서울대학교 계산통계학과 석사
1991년 1월~1996년 6월 : 한국 IBM
1996년 7월~현재 : 한국정보보호진흥원 전자거래보호단장
〈관심분야〉 정보보호, 유·무선PKI, 유비쿼터스 보안