情 報 保 護 學 會 誌
第 14 券 第 4 號, 2004. 8

웹 서비스 보안기술 표준화 동향

홍 기 융*, 홍 기 완*, 박 종 운*, 이 규 호*

요 약

웹 서비스는 인터넷 기술을 이용한 표준화된 오픈 네트워크를 통해 조직 내 및 조직간 모든 컴퓨터 시스템을 결합시키는 새로운 컴퓨팅 패러다임으로 자리 잡으면서, 기술과 서비스의 융합(Convergence), 표준화(Standardization)가 급속도로 진행되고 있다. 이러한 현상은 정보 및 서비스의 공유를 필수적으로 수반하므로, 프라이버시, 기밀성, 무결성, 인증, 및 접근제어 등과 같은 보안과 신뢰성에 대한 중요성을 부각시킨다. 현재 웹 서비스 보안기술은 W3C, OASIS, WS-I의 세 표준화 단체를 중심으로 표준화가 진행되고 있다. 본 논문에서는 각 표준화 단체에서 추진하고 있는 웹 서비스 보안기술의 최근 동향을 분석한다.

Ⅰ. 서 론

인터넷을 통한 웹의 발전은 웹 서비스라는 새로운 컴퓨팅 분야를 산업 전반에서 많은 주목을 받게 하고 있다. 웹 서비스는 정의 주체별로 약간씩 다르게 정의되고 있지만 일반적으로 다음과 같은 개념을 포함한다. 웹 서비스는 인터넷을 통한 네트워크 상에, 단일 또는 다수의 비즈니스간 기존 시스템을 표준화된 기술로 결합시켜주는, 즉, 매우 유연하고 이질적인 운영시스템, 프로그램 언어간의 커뮤니케이션 차이를 극복해 주는 연결고리이다. 다시 말하면, 웹 서비스는 내용 중심의 인터넷 환경을 기능 중심으로 바꾸는 새로운 변화를 일컫는다. 이는 다양한 플랫폼에서 운영되던 기존 시스템들 간의 표준화된 인터페이스를 통한 통합 시도를 통해 실체화 되고 있다.

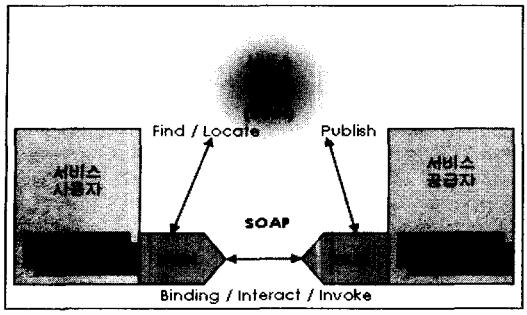
대표적인 웹 서비스 관련 표준화는 인터넷을 통해 웹 서비스가 통신할 수 있도록 해주는 SOAP(Simple Object Access Protocol), 특정 조직이 자신의 웹 서비스를 온라인 디렉터리에 등록, 광고하거나 외부에서 웹 서비스를 검색하는데 사용되는 UDDI (Universal Description, Discovery, and Integration), 웹 서비스를 정의하는 언어로서 특정 조직이 웹 서비스를 기술할 때 사용되는 WSDL(Web Service Description Language), 그리고 플랫폼 독립적으로 데이터 형태를 표현할 수 있는 XML(eXtensible Markup Language) 분야 등을 통해 진행되고 있다.

그러나 웹 서비스의 광범위한 적용을 방해하는 요소들도 함께 공존하고 있는데, 그 중 대표적인 것이 바로 보안 문제이다. 상호 의사소통에서의 뛰어난 웹 서비스의 장점은 더 많은 통합과 커뮤니케이션을 지원하지만, 이렇게 많은 부분들이 연결됨에 따라 자연스럽게 보안의 중요성이 부각되고 있다. 이로 인해 W3C, OASIS 등의 표준화 단체는 서둘러 웹 서비스 보안기술 관련 표준안을 제정하고, 각 소프트웨어 업체들도 이를 지원해 나가고 있다. 본 논문에서는 웹 서비스의 전반적인 개념과 이를 통해 제기되는 보안 이슈들을 설명하고, 현재까지 개발된 웹 서비스 보안기술 관련 표준화 동향을 분석한다.

Ⅱ. 웹 서비스 보안

웹 기술의 진화는 W3(World Wide Web)의 개발 이후 오늘날까지 급속도로 이루어지고 있다. CGI를 통한 동적인 기술로의 진화, 스크립트 기술을 통한 e-비즈니스로의 진입, XML을 통한 현재의 웹 서비스의 등장, 이 모든 변화는 유비쿼터스 환경의 진입을 바라보는 시점에서 필연적인 결과라 할 수 있다. 이러한 시점에서 개인의 프라이버시와 기업의 자산을 지키기 위한 보안기술에 대한 관심은 시대적 요구사항을 반영한 것이라 볼 수 있다.

* (주)시큐브/정보보호기술연구소({ceo, kwhong, hizcool, perry}@secuve.com)



〔그림 1〕 웹 서비스 아키텍처

1. 웹 서비스 개요

웹 서비스는 인터넷상의 비즈니스를 위한 메시징 프로토콜과 프로그래밍 표준으로 구분할 수 있다. 여기에는 단순 및 복합의 두 가지 유형이 존재한다. 단순 유형은 기본적인 "요청/응답" 기능을 제공하며, SOAP, UDDI, WSDL 이라고 하는 세 가지 XML 기반의 공개 표준을 바탕으로 하고 있다. 복합 유형은 비즈니스간의 협업과 비즈니스 프로세스 관리 등과 같이 여러 업체들간의 장기간 비즈니스 "대화" 기능을 총체적으로 일컫는다.

아래 〔그림 1〕은 이러한 웹 서비스를 가능하게 하는 기반 컴포넌트 사이의 동작 관계를 표현하는 아키텍처 [4][5]를 나타낸다.

서비스 제공자, 요청자, 중개자의 관계로 구성되는 웹 서비스의 아키텍처를 흔히 SOA(Service Oriented Architecture)라 말하며, 이는 서비스를 기반으로 응용 프로그램을 구축하거나 서비스 자체를 구축하도록 제공되는 아키텍처 또는 설계방법을 의미한다.

현재 W3C에서 추진하고 있는 웹 서비스 표준 규약에서 웹 서비스 아키텍처를 구성하는 기본 컴포넌트를 좀 더 자세히 설명하면 다음과 같다.

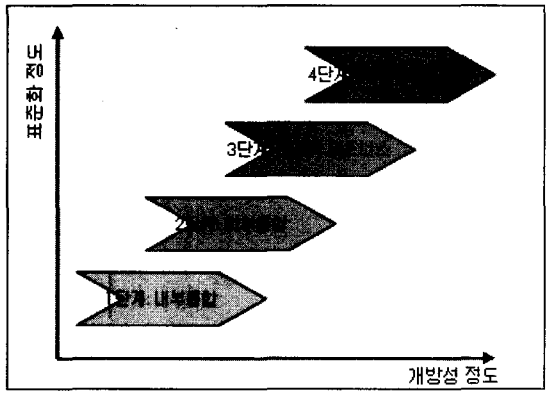
〔표 1〕 웹 서비스 구성 컴포넌트

XML	웹 서비스의 근간으로 빌딩 블록의 역할을 하며 웹 서비스의 데이터를 정의하고, 이 데이터가 어떻게 프로세싱 되어야 하는지를 정의하는 언어 제공
SOAP	웹 서비스 통신 프로토콜로 인터넷상에서 XML 데이터를 교환하는데 사용되는 메시징 프레임워크를 정의
WSDL	XML의 하나로 프로그래밍 단계의 자동적 통합에 요구되는 모든 기술적 세부항목을 구성하는 언어에 대한 사전 역할 수행
UDDI	글로벌 전자적 옐로 페이지 역할과 검색 역할 수행

2. 웹 서비스 보안 문제

웹 서비스들 사이에 연결이 가능하다는 웹 서비스의 특징은 보안에 대한 보다 심도 깊은 고려를 요구한다. 이를 위해 본 논문에서는 웹 서비스 발전 단계별 비즈니스 모델[3]에 따라 필요한 보안 고려사항을 분석한다.

웹 서비스 발전 단계에 따른 비즈니스 모델은 아래 〔그림 2〕와 같이 4단계로 나뉜다.



〔그림 2〕 발전 단계별 웹 서비스 모델

먼저 1단계인 내부 통합 모델은 조직 내에 존재하는 기존의 응용 프로그램들을 일대일 형태로 통합하여 단일 프레임워크를 운영하고자 하는 것으로, 사용자 및 각 엔터티를 식별하는 인증 그리고 특정 권한을 통한 접근을 제어하는 권한부여 보안 요구사항을 반드시 고려해야 한다.

2단계인 외부 통합 모델은 조직 외부의 개체와 계약을 통해 비즈니스 프로세스를 공유하는 것으로, 통신 데이터의 암호화 및 위·변조 방지를 위한 무결성, 그리고 다수의 조직들 사이의 통합 관리를 위한 SSO(Single Sign On) 등의 보안 요구사항을 고려한다.

3단계인 소극적 비즈니스 모델은 2단계의 비즈니스 모델이 성숙해지면서 보다 유연한 통합을 추구한다. 따라서 부인방지 및 End-to-End 암호화의 새로운 보안 요구사항을 고려할 수 있다.

마지막으로 4단계인 적극적 비즈니스 모델은 개방성, 신뢰성을 추구한다. 따라서 여기에서는 신뢰 관리, 보안 관련 법 및 제도의 정비와 같은 새로운 요구사항을 고려할 수 있다.

이러한 비즈니스 발전에 따른 보안에 대한 문제는 표준화 기구와 웹 서비스 기술을 주도하는 산업체에 의해 보안기술 표준화에 가속을 붙이고 있다.

Ⅲ. 웹 서비스 보안기술 표준화 동향

현재 웹 서비스 보안 기술들은 여러 업체들이 참여하여 W3C, OASIS 등의 표준화 기구에서 많은 표준화 작업이 진행되고 있다. 본 장에서는 웹 서비스에서 사용되는 보안 기술을 웹 서비스가 이용하는 프로토콜의 전송계층에 대한 보안과 메시지에 대한 보안 그리고, 서비스 수준에서의 보안으로 구분하여 이와 관련된 보안 기술 동향을 분석하였고, W3C에서 담당하고 있는 XML 관련 보안 기술들인 XML 서명, XML 암호화, XML 키 관리 명세와 OASIS에서 추진 중인 웹 서비스 보안 기술들인 SAML, XACML, WS-Security에 관한 표준화 동향을 기술하였다.

1. W3C 표준화 동향[6]

가. XML 서명(Signature)

온라인상에서 이루어지는 개인과 개인, 개인과 기업의 소규모 거래에서 기업간의 대규모 거래에서는 거래에 필요한 중요한 데이터가 외부로 유출되지 않도록 보안해 줄 기술이 필요에 따라 전자서명 기술이 출현하게 되었다.

(1) 전자서명의 특징과 웹 서비스에의 응용

한 사람만이 사용할 수 있는 개인키를 사용해 서명을 보내면 수신자는 공용키를 이용해 송신자의 메시지를 해독하는 기술이다. 이 때 공용키는 제 3자에 의해 위조될 가능성이 있기 때문에 공인된 인증기관이 전자서명자에 관한 신원정보가 담긴 인증서를 수신자에게 발급하게 된다. 전자서명은 이미 우리나라에서도 인터넷을 통한 전자문서 교환 시 일반 문서에서 쓰이는 도장이나 인장과 똑같은 효력을 지니게 되는 것으로 규정하고 정의하고 있다. 이러한 전자서명의 특징은 아래와 같다.

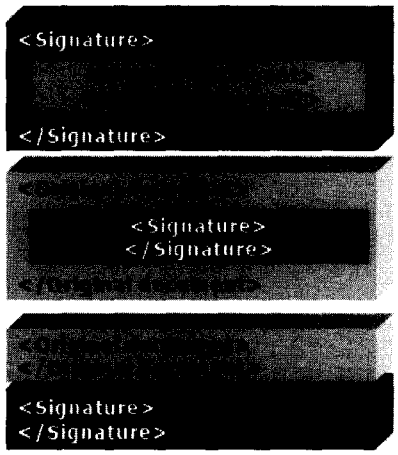
- 인증 : 문서나 메시지를 보낸 사람의 신원이 진짜임을 증명한다.
- 무결성 : 전달된 메시지나 문서의 내용이 변조되지 않았음을 보증한다.
- 부인방지 : 서명자가 서명한 메시지에 대해 쉽게 부인하는 것이 불가능하다.

최근 웹 서비스에서 이러한 보안이슈를 만족하기 위해서 기존의 전자서명의 장점을 그대로 도입하면서도 XML 문서에 이용할 수 있게 표준화 작업이 이루어지고 있으며, 기존의 전자서명과 다른 점은 XML 문법을 그대로 이용하여 서명을 한다는 것이다.

(2) XML 서명의 유형과 표준화 동향

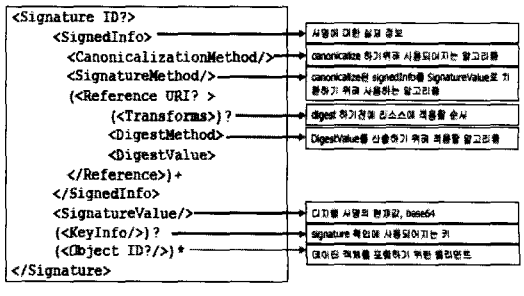
XML 서명의 유형에는 아래와 같은 세 가지가 있다.

- 데이터를 동봉한 서명 (Enveloping Signature)
- 데이터에 동봉된 서명(Enveloped Signature)
- 분리된 서명(Detached Signature)



[그림 3] XML 서명 유형

XML 서명기술과 관련된 표준화 동향으로는 IETF와 W3C가 공동으로 XML 서명 워킹 그룹을 구성하여 표준화 작업을 수행하고 있다. 현재 나와 있는 표준 명세들은 다음과 같다. 서명 문법과 절차(signature Syntax and Processing) 명세, 정규화 XML(Canonical XML) 명세, 배타적 정규화 XML(Exclusive Canonical XML) 명세, XPath 필터(XPath Filter) 명세, XML 서명 요구사항(XML Signature Requirements) 명세가 있다.



[그림 4] XML 서명 기본 구조

나. XML 암호화(Encryption)

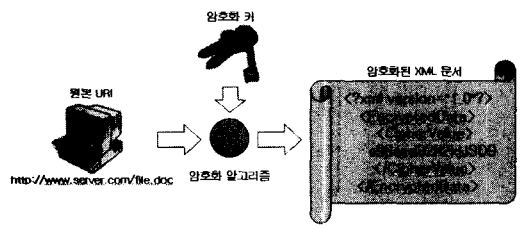
(1) 암호화의 특징과 웹 서비스에의 응용

암호화(Encryption)는 정해진 수신자 외에는 해당 데이터를 알아볼 수 없도록 기밀화 하는 것을 말한다. 수많은 민감한 정보들이 인터넷을 통하여 서로 교환되고 있는 시점에서 이러한 암호화 기능은 매우 중요하며, 이를 가능케 하는 기술들이 이미 많이 존재한다.

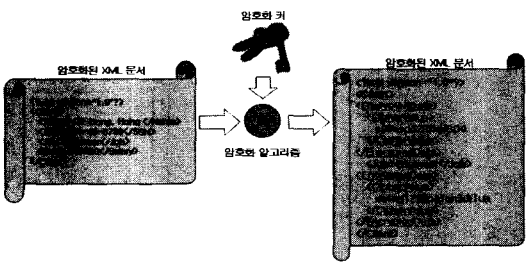
XML 문서도 암호화 표준들을 이용하여 암호화가 가능하며 XML 문서는 다른 부분들은 그대로 사용하면서, 문서의 일부분만 암호화할 필요가 있다. XML 암호화는 암호화한 데이터를 XML 문법을 사용해서 표현하는 일련의 과정이라고 정의 할 수 있다. XML 암호화는 완전히 새로운 아이디어라기보다는 기존의 기술들을 묶어놓은 것이며 실제 XML 암호화 표준은 XML 서명에 많은 부분을 의존하고 있다. 또한 XML 암호화의 가장 큰 장점은, 암호화된 결과물이 XML 형태의 암호화된 데이터라는 점이다. 이는 XML이 가진 장점을 그대로 가지면서 암호화 기능을 사용할 수 있도록 한다.

(2) XML 암호화의 유형과 표준화 동향

XML 암호화는 크게 이진데이터를 암호화하는 연산과 XML 데이터를 암호화하는 연산으로 나눌 수 있다. 이진데이터를 암호화하는 연산을 살펴보면, URI(Uniform Resource Identifier)가 가리키고 있는 실제 자료를 가져와서 암호화된 XML 형식의 데이터를 만드는 암호화 알고리즘을 적용한다. XML 데이터를 암호화하는 연산은 평문 XML에서 XML 마크업을 경계로 보호해야 할 데이터와 그냥 보내도 되는 데이터를 타로 떼어낼 수 있으며 보호해야 할 데이터를 암호화하여 XML 문서에 치환하는 형태로 이루어진다.



〔그림 5〕 임의의 이진 데이터 암호화



〔그림 6〕 엘리먼트 단위의 암호화

XML 암호화(XML Encryption)는 W3C에서 표준화를 담당하고 있다. W3C는 크게 도메인, 엑티비티, 작업그룹들로 조직이 구성되어 있는데, XML 암호화는 Technology and Society 도메인의 XML Encryption Activity, XML Encryption 작업그룹에 속한다. 이 작업그룹에서는 2002년 3월에 XMl Encryption Requirements를 W3C Note로 발표했으며, 12월에는 XMl Encryption Syntax and Processing과 Decryption Transform for XML Signature를 Recommendation으로 발표하였다. 현재 모든 작업들은 완료되었으며 XML Encryption 작업그룹도 2002년 12월 31일로 종료된 상태이다.

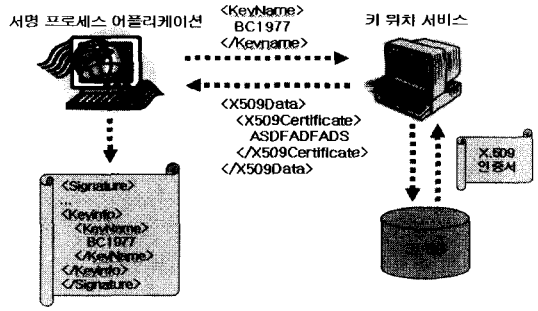
XML 암호화는 여러 가지 보안 이슈들 중 암호화(Encryption) 부분을 커버하며, 이는 문서의 기밀성을 제공하는데 있어서 매우 중요한 역할을 한다. XML 암호화 사양에는 다중 수취인 지원과, 기존 보안 구조 활용 등이 필요한데, W3C의 XML 암호화는 이러한 요구사항들을 만족시키고 있다.

다. XML 키 관리 명세(Key Management Specification)와 표준화 동향

(1) XML 키 관리 명세와 XKMS(XML Key Management Specification) 서비스

XML 키 관리 명세는 XML 문서를 교환하는 환경에서 보안을 위한 핵심 요소 중 하나인 암호화키의 안전한 관리를 위해서 나왔다. 기본적으로 암호화에 보호되는 XML 문서 보안은 키에 달려있다. 인터넷 비즈니스 거래에서 XMl 키 관리에 대한 요소는 필수적이다. 이러한 XML을 이용하는 애플리케이션에서의 키 관리에 대한 문제에 PKI(Pulic Key infrastructure) 기술을 적용하는데 세계 최대의 보안 인증회사인 VeriSign이 주도가 되어 XKMS (XML Key Management Specification)이 등장하였다.

VeriSign, Microsoft 및 WebMethods에서는 현재 사용되고 있는 PKI 및 공개키 인증서와 XML 애플리케이션의 통합이 용이하도록 개방형 XKMS을 작성하였다. XML 키 관리 명세는 공개키 관리를 위한 프로토콜을 정의한다. 이러한 공개키 기술은 XML 서명과 XML 암호화, 기타 여러 보안 응용분야에 필수적으로 사용된다.



〔그림 7〕 키 위치 정보 서비스 과정

XKMS (XML Key Management Specification) 서비스는 암호화 기능이 있는 XML 애플리케이션에 신뢰성을 추가하기 위해 포괄적이고 개방적이며 표준에 기반을 둔 접근방식에 기반하고 있다. 또한 구조는 XML 전자서명과 XML 암호화 워킹그룹내의 W3C 표준화 활동과 호환성이 있도록 설계된다. XKMS는 X-KISS와 X-KRSS의 두 영역으로 구성된다.

X-KISS는 XML을 기반으로 하는 애플리케이션에서 신뢰할 수 있는 곳에서 XML 서명, XML 암호화 데이터 또는 기타 공개키 사용과 관련된 키 정보를 지원하는 프로토콜을 정의한다. 주요 기능은 주어진 식별자 정보에 필요한 공개키의 위치를 부여하고 공개키를 연결하는 것이다. 이 서비스의 목표는 PKI에서의 복잡성을 극복하고, 애플리케이션 구현의 복잡성을 최소화하기 위한 것이다.

X-KRSS는 키 쌍에 대한 관리를 지원하는 프로토콜로 서비스의 요청과 응답의 메시지 교환으로 구성된다. XML 인증기반의 XML 인터페이스 프로토콜은 특정 PKI를 필요로 하지 않지만 X.509v3, XPKI(Simple PKI) 및 PGP(Pretty Good Privacy)와 같은 전통적인 표준을 포함한 기반과 상호 호환성이 있도록 설계되었다.

XML 기반의 키 관리 서비스인 XKMS는 W3C에 의해 표준화가 진행 단계에 있으며, 2001년 3월 XKMS 1.0이 발표된 이후 2003년 3월 XKMS 2.0이 워킹 드래프트(Working Draft) 상태에 있다. XKMS 2.0에서는기존 내용을 XKMS 워킹그룹에서 논의하여 메시지 정의 및 프로토콜 상의 보안 요구사항 등을 추가로 정의하고 있다. 이와 같이 XML 키 관리 기술은 표준화가 진행중이며 이를 완전히 구현한 제품은 아직 없다.

2. OASIS 표준화 동향[7]

가. SAML과 XACML

e-비지니스 환경에서 기업들이 서로 다른 기업간에 웹을 통해 제휴를 맺는 경우가 늘어나면서 새로운 파트너 관계를 맺고자 할 때, 기존의 시스템을 수정하거나 새롭게 설정해야 하는 부담을 가져왔다. 또한 어떻게 보안 정보를 교환하는가에 대한 문제도 발생한다. XML 기반의 공개 표준인 SAML은 이러한 문제에 대한 해결책이 되었으며, 보안 정책을 표현하는 XACML과 함께 사용되어 인터넷상에서 인증, 권한 부여 및 승인 정보 교환 서비스를 가능하게 해 주는 방법으로 등장하였다.

SAML은 XML 기반으로 XML에서 제공하는 장점들을 사용할 수 있다는 점과, 누구나 사용할 수 있는 공개 표준이라는 점, 다른 플랫폼과 사이트 사이에서도 한번 인증 정보를 입력하면 다른 다양한 영역에서도 인증을 받을 수 있도록 제공해 주는 싱글 사인 온 기능을 가능하게 한다는 점 그리고, SOAP이나 ebXML 등의 프로토콜과 함께 사용이 가능하다는 점 등을 들을 수 있다. 특히 웹 서비스의 경우 여러 서비스들로 이뤄진 하나의 통합 서비스가 가능한데 이러한 통합 서비스를 하나의 인증을 가지고 사용할 수가 있다.

XACML은 SAML과 함께 주로 사용되며, assertion control 정보의 통합된 묘사와 이동성 방법을 제공한다. XACML은 XMl 기반으로 되어있어 다양한 시스템들 사이에서 security control 정보의 교환을 가능하게 하며, 한번에 여러 자원들의 관리가 가능하고 non-IT 자원들도 자신의 정책을 만들어 낼 수 있어, 확장성과 유연성의 장점을 가진다.

SAML과 XACML은 OASIS에서 표준화를 담당하고 있다. SAML은 OASIS의 Security Services Technical Committee에, XACML은 eXtensible Access Control Markup Language Technical Committee에 각각 속해있다. SAML V1.1은 2003년 9월 7일에 표준이 완성되었으며, 현재 SAMl V2.0을 진행 중이다. SACML V1.1 역시 2003년 7월 24일에 표준이 완성되었고, 현재 XACML V2.0이 진행 중이다.

나. WS-Security

이 명세는 최초 2001년 10월 23일에 Microsoft에서 웹 서비스 보안에 대한 규격으로 발표하였다. 그 이후에 IBM, VeriSign이 공동으로 작업에 참여하여 2004년 4월 IBM, Microsoft 그리고 VeriSign이 공동으로 WS-Security V1.0을 발표하였으며, IBM은 2002년 4월 10일에 발표된 WSTK 3.1에 WS-Security를 포함하게 되었다. 다른 많은 웹 서비스 보안 명세와 마찬가지로, WS-Security는 유연할 뿐만 아니라, 커버로스

(Kerberos), PKI, SSL과 같은 다른 많은 보안 수단을 제공하고 있으며, 기본적으로 XML 서명과 XMl 암호화를 사용하여 안전한 웹 서비스를 구축할 때 사용되는 무결성(Integrity)과 기밀성(Confidentiality)을 구현하기 위한 SOAP 확장의 표준 세트를 제공하고 있다. 이 명세가 제공하는 주요 메커니즘은 보안 토큰 확산(Security Token Propagation), 메시지 무결성, 메시지 기밀성 들이 있다.

최초의 IBM, Microsoft, VeriSign의 WS-Security를 시작으로 현재 34개의 업체가 OASIS Web Sercives Security Technical Committee에 참여하여 SOAP 메시지 보안에 관한 표준화에 힘쓰고 있으며, 이 명세들은 XML의 확장성을 잘 살이고 있어 기존의 XML 관련 보안 표준들을 수용할 뿐 아니라 여러 보안 기술을 수용하기 위한 모델들을 제공하고 있다.

다. AVDL(Application Vulnerability Description Language)

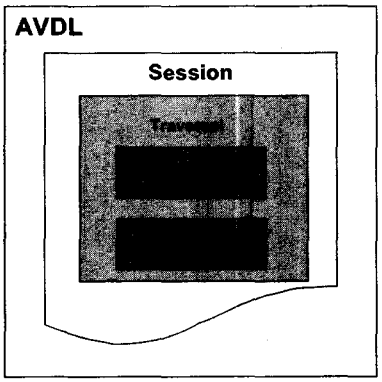
AVDL은 네트워크에 알려진 응용 프로그램 취약성 서술을 일반화하기 위해 표준화가 진행 중인 언어이다. XML을 기반으로 효과적이고 다양한 XML 스키마들을 정의하고 있으며, 취약성 진단/분석 도구, 방화벽/IDS, 취약성 해결방안 제시도구(Remediation Tool), 상호 연관관계 분석도구(Correlation Tool)에서 취약성에 대한 일반화된 언어를 사용하여 상호 정보를 정확히 교환하는 것을 가능하게 하는 것을 목적으로 한다.

(1) AVDL 구조

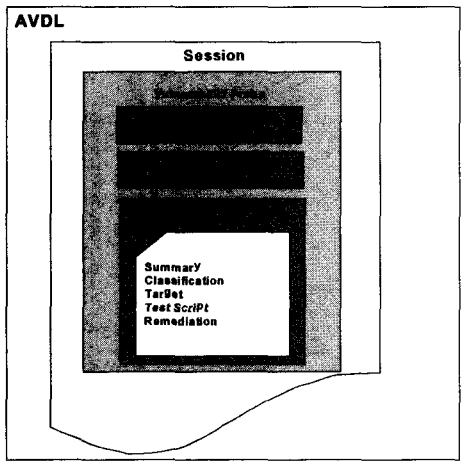
AVDL은 XML을 기반으로 하고 있으며, XML 메시지의 형식은 AVDL 스키마에 정의되어 있다.

AVDL 결과물은 Traversal과 Vulnerability probe의 두 부분으로 구성되어 있다. Traversal은 해당 웹 사이트의 기본 구조를 반영한다. 서버와 브라우저 사이의 각 Request와 그에 따른 Response를 담고 있다.

Traversal의 구조는 위 그림과 같다. root node인 AVDL은 session 헤더를 가지고 있다. 세션 안에는 그 세션에서 수행된 Traversal들의 정보가 들어가게 되며, 각 Request/Response 헤더에는 헤더, 쿠키, URL, query, POST data 등 교환된 HTTP byte stream에 대한 상세정보가 들어있다.



〔그림 8〕 AVDL Traversal 구조



〔그림 9〕 AVDL Vulnerability Probe 구조

위 그림은 Vuleranbility Probe의 구조를 보여주고 있다. root node인 AVDL은 마찬가지로 session에 대한 헤더를 가지고 있으며, session 안에는 Vulnerability Probe 헤더를 가지고 있다. Traversal 헤더가 웹 어플리케이션과 그 Request/Response 정보를 가지고 있는 것에 반해, Vulnerability Probe 헤더는 웹 어플리케이션의 취약성 정보를 가지고 있다. 세션 안에는 여러 개의 Vulernability Probe 들이 포함될 수 있으며, 취약성이 발견되었다면 Request, Response 정보와 함께 Vulnerability description 정보도 포함하게 된다. 이 정보는 아래와 같은 5가지 항목에 대한 정보를 가지고 있다.

- Summary : 취약성에 대한 짧은 설명
- Classification : 취약성에 대한 논리적인 그룹
- Target : target에 대한 정확한 설명 (예 : 호스트, OS, 프로토콜, 웹 서버 등)
- Test Script : 취약성을 찾아낸 방법에 대한 상세한 기술

· Remediation : 취약성을 제거하기 위한 방법에 대한 상세한 서술

3. WS-I 표준화 동향[8]

WS-I(Web Services Interoperability Organization)은 2002년 2월에 IBM와 Microsoft를 주축으로 46개 업체가 모여서 웹 서비스의 상호 운영성을 위하여 출범한 단체이다. 이 단체에서는 WS-Basic Profile을 발표하였는데, 이 프로파일은 상호 운영성을 위하여 기본적으로 웹 서비스로 통신하는데 있어 기본이 되는 요소들과 예제 시나리오들을 제공하고 있다. WS-I에서는 신뢰성 있는 메시지를 위하여 웹 서비스의 보안 부분에 가장 중점을 두고 있다. 그러나 아직까지 Ws-Basic Profile에는 HTTPS와 같은 전송 계층의 보안 부분에 대한 간략한 언급만 되어 있다.

WS-I에서는 전송 계층의 보안, SOAP 메시지 보안, Basic Profile 중심의 웹 서비스 보안 고려사항 등을 개발하기 위한 Basic Security Profile Working Group을 결정하였다. 이 Working Group의 헌장에 의하면 Security Scenario와 Basic Security Profile에 대한 문서를 각각 2003년 7월, 2003년 10월까지 출판하기로 하였지만, 아직까지 작업이 늦어지고 있는 상황이다. Basic Security Profile은 HTTPS, SOAP attachment security, OASIS Web Services Security V1.0 등에 명세들에 기반을 두고 있다.

Ⅳ. 결 론

웹 서비스 분야는 향후 유비쿼터스 시대에 필요한 기본적인 인프라로 인식되면서, 국제 표준화 기구뿐만 아니라 MS, IBM, SUN 등 세계 IT 산업을 이끌어 가는 산업체들에 의해 발전되고 있다. 특히 웹 서비스를 이용한 4세대 비즈니스 모델의 출현은 프라이버시, 정보침해 등 보다 많은 보안에 대한 고려를 요구하고 있다. 이러한 보안에 대한 필요성이 증가함에 따라 현재 웹 서비스 보안 기술은 인증(SAML), 접근제어(XACML), 전자서명(XML Signature), 암호화(XML Encryption), 키 관리(XML Key Management), 취약성 진단(AVDL) 등의 분야에서 기술 표준화가 진행되고 있다.

그러나 현재까지의 기술 표준화는 기존의 보안 위협요소만을 고려하고 있어, 차세대 비즈니스 환경에서의 다양한 응용에 대한 고려를 포함하고 있지 않다. 따라서 향후 웹 서비스를 위한 보안기술 표준화는 기존의 보안 위협요소들을 그대로 계승하고, 여기에 차세대 웹 서비스 환경에서 발생할 수 있는 다양성, 편재성, 호환성, 확장성 그리고 유연성을 고려하여 표준화를 진행해야 할 것이다.

참 고 문 헌

[1] 한국전산원, "웹 서비스 보안 기술 분석 및 응용 방안 연구", 연구보고서 , 2003년 12월.

[2] 김주한, 문기영, "XML 기반 접근제어 기술 동향", 정보보호학회지 13(4), 2003년 8월.

[3] KISDI, "웹 서비스의 현황 및 비즈니스 모델의 변화", 정보통신정책 저널 14(15), 2002년 8월.

[4] Microsoft Corporation, "Web Services Security", MSDN Library, January 2004.

[5] Oracle, "Securing Web Services: Today and Tomorrow", Technical Articles 33206, November 2002.

[6] W3C, http://www.w3.org

[7] OASIS, http://www.oasis-open.org

[8] WS-I, http://www.ws-i.org

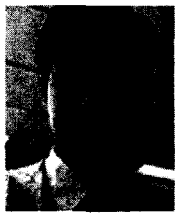
〈著 者 紹 介〉

홍 기 융 (Ki-Yoong Hong)
종신회원

1985년 2월 : 전남대 전자계산학과 졸업(학사)
1990년 2월 : 중앙대 대학원 전자계산학과 졸업(석사)
1996년 2월 : 아주대 대학원 컴퓨터공학과 졸업(박사)
1985년 9월~1995년 10월 : 한국전자통신연구원 선임연구원
1995년 10월~1996년 4월 : 한국전산원 선임연구원
1996년 4월~2000년 2월 : 한국정보보호센터(응용기술팀장, 평가체계팀장, 인증관리팀장)
1998년 3월~2004년 2월 : 동국대학교 국제정보대학원 겸임교수
2000년 3월~현재 : (주)시큐브/(주)케이사인 대표이사
〈관심분야〉 시스템보안, 보안운영체제, 전자서명 인증관리 등

홍 기 완 (Ki-Wan Hong)

1997년 2월 : 전남대 산업공학과 졸업(학사)
2002년 2월 : 동국대 정보보호학과 졸업(석사)
2003년 2월~현재 : 전남대 정보보호학과 박사과정 재학
1997년 7월~2000년 7월 : 한국정보보호센터 연구원
2000년 8월~현재 : (주)시큐브 연구소 연구소장
2001년 6월~현재 : 국제공인정보시스템보안전문가
〈관심분야〉 PKI, 취약성분석, 보안운영체제 등



박 종 운 (Jong-Woon Park) 정회원

1998년 2월 : 아주대 컴퓨터공학과 졸업(학사)
2001년 2월 : 아주대 대학원 컴퓨터공학과 박사과정 수료
2000년 2월~현재 : (주)시큐브 연구소 팀장
2004년 1월~현재 : 국제공인정보시스템보안전문가
〈관심분야〉 접근제어, 침입탐지, 유비쿼터스보안 등

이 규 호 (Kyo-Ho Lee)

1999년 2월 : 아주대 컴퓨터공학과 졸업(학사)
2001년 2월 : 아주대 대학원 컴퓨터공학과 졸업(석사)
2001년 3월~현재 : 경기대 대학원 박사과정 재학
2002년 4월~현재 : (주)시큐브 연구소 팀장
〈관심분야〉 네트워크/서버보안, 침입탐지, 취약성분석 등