情 報 保 護 學 會 誌
第 13 券 第 6 號, 2003. 12

안전한 XML 기반 웹서비스를 위한 웹 애플리케이션 보안 프레임워크

문 기 영*, 박 남 제*, 송 유 진**, 손 승 원*, 박 치 항*

요 약

최근 인터넷의 급속한 발전과 함께 웹 애플리케이션 형태로 서비스를 제공하였던 것이 다양하고 개별적인 웹 애플리케이션들을 효율적으로 통합하는 웹서비스 방식으로 진화하고 있다. 이에 따라, 차세대 플랫폼의 대안으로 웹서비스(Web Services)가 급부상하고 있다. 웹서비스를 통해 인터넷이나 인트라넷상에서 웹 애플리케이션간의 연동 즉, 비즈니스 통합이 가능하게 된 것이다. 이러한 비즈니스 통합 환경에서 웹 애플리케이션 보안은 필수적인 요소이며, 웹서비스 보안에 대한 연구개발이 필요하다. 본 고에서는 웹서비스에 대한 전반적인 사항을 분석하여 문제점을 도출하고 XML-Web Services 보안 모델을 검토하며 그 기반 구조 및 기능을 살펴본다. 그리고, XML 정보보호기술을 기반으로 웹서비스 애플리케이션의 보안 프레임워크를 제시한다. 최종적으로 제안된 모델은 차세대 웹 애플리케이션 보안 프레임워크의 기반 기술이 될 것으로 기대된다.

Ⅰ. 서 론

급변하는 정보기술의 변화는 개인의 입장에서 기업의 입장으로 웹을 통해 모든 애플리케이션을 이용할 수 있도록 변화의 흐름을 주도하고 있다. 이렇듯 기업 사용자가 웹을 통해 모든 업무를 처리할 수 있도록 웹의 범위를 확장한다는 것이 요즘 거론되고 있는 웹서비스이다. 이러한 확장이 가능하게 되기 위해서는 웹서비스 내의 통합을 가능케 하는 표준 기술의 정립이 진행되어야 한다. 현재 대두되고 있는 웹서비스의 표준 기술로서는 SOAP(Simple Object Access Protocol), UDDI(Universal Description, Discovery and Integration), WSDL(Web Services Description Language) 등이 있으며, 이 외에도 여러 가지 표준 기술들이 유기적인 조합의 과정을 거치고 있다.

최근 웹서비스를 둘러싼 업계의 동향이 활발하다. 선마이크로시스템즈는 2001년 9월, XML를 사용한 웹서비스에 의한 인증을 위한 기술표준을 추진하는 기업 연합인 Liberty Alliance를 설립했다[6]. 또한, 마이크로소프트는 닷넷 전략에서의 웹서비스를 강력하게 추진하고 있고, IBM도 독자적으로 웹서비스의 연구개발에 박차를 가하고 있다. 웹서비스는 전통적인 프로그래밍 방식인 컴파일을 통한 정적 바인딩에서 벗어나 실행시에 동적으로 서비스를 검색하는 살아 움직이는 e-비즈니스의 서막을 알린다는 측면에서 그 의미가 깊다. 이러한 상호 협력을 통한 동적인 서비스 제공을 통해 플랫폼이나 프로그램 언어에 중립적인 구현을 할 수 있게 된다. 인터넷의 급속한 발전과 함께 웹 애플리케이션 형태로 서비스를 제공하였던 것이 다양하고 개별적인 웹 애플리케이션들을 효율적으로 통합하는 웹서비스 방식으로 진화하고 있는 것이다. 이에 따라, 차세대 플랫폼의 대안으로 웹서비스가 급부상하고 있다. 웹서비스를 통해 인터넷이나 인트라넷상에서 웹 애플리케이션 간의 연동 즉, 비즈니스 통합이 가능하게 된 것이다. 이러한 웹서비스의 움직임에 공통되는 것은 인증이나 보안에 대한 강화이다. 비즈니스 통합 환경에서 웹 애플리케이션 보안은 필수적인 요소이며, 웹서비스 보안에 대한 연구개발이 필요하다.

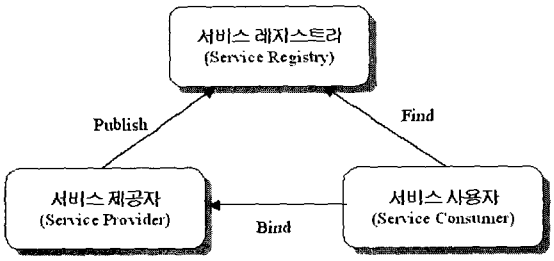
* 한국전자통신연구원 정보보호연구본부 ({kymoon,namjepark,swsohn,chpark}@etri.re.kr)
** 동국대학교 전자상거래대학원 (song@mail.dongguk.ac.kr)

본 고에서는 웹서비스에 대한 전반적인 사항을 분석하여 문제점을 도출하고 XML-Web Services 보안 모델을 검토하여 그 기반 구조 및 기능을 살펴본다. 그리고, XML 정보보호기술을 기반으로 웹서비스 애플리케이션의 보안 프레임워크를 제시한다. 최종적으로 제안된 모델은 차세대 웹 애플리케이션 보안 프레임워크의 기반 기술이 될 것으로 기대된다.

본 논문의 구성은 1장에서 웹서비스 보안 연구의 필요성에 대해 언급하고, 2장에서는 웹서비스의 개요, 3장에서는 웹서비스 보안 기술의 표준화 동향, 4장에서는 웹서비스의 보안 요구사항 분석과 웹 애플리케이션 보안 모델을 살펴본다. 5장에서 기존 보안 모델을 기반으로 웹서비스 애플리케이션 보안 프레임워크를 제시하고 결론을 내린다.

II. 웹서비스 개요

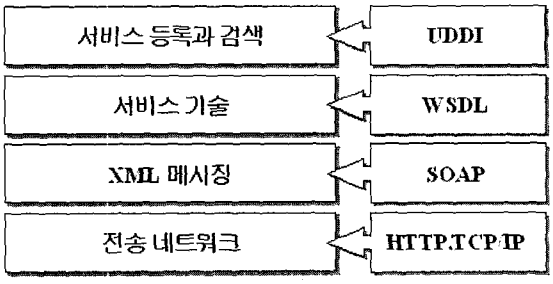
웹서비스는 네트워크상에서 접근 가능한 소프트웨어 기능 단위로 플랫폼, 프로그래밍 언어 및 컴포넌트 모델에 독립적인 기술로 만들어진 소프트웨어를 말한다. 웹서비스의 목적은 인터넷이나 인트라넷상에서 애플리케이션 간의 연동을 가능하게 하는 것이다. 이를 위해 벤더의 독자 기술 규격이 아니라 SOAP나 WSDL라는 XML 기반의 표준 기술 규격을 사용한다. 웹서비스는 일반적으로 다음 [그림 1]과 같은 구조로 구성된다.



[그림 1] 웹서비스 구조

서비스를 개발한 제공자는 레지스트리에 자신의 서비스를 등록하여 사용자가 이용할 수 있도록 하고, 서비스를 이용하려는 이는 검색 기능을 통해 레지스트리 서버를 검색하여 원하는 서비스를 찾고 선택하여 이용한다. 사용자가 일단 서비스를 등록하면 그 이후의 과정은 서비스와 사용자간의 RPC(Remote Procedure Call)로 이루어진다. 웹서비스 구조의 3가지 요소는 모두 독립적으로 존재하며 이들간의 통신과정도 모두 XML로 표준화되어 있기 때문에 구조적으로 매우 유연하며, 레지스트리라는 일종의 네이밍 서버가 있기 때문에 서비스와 사용자가 자유롭게 분산될 수 있는 구조임을 알 수 있다.

위의 웹서비스 구조 모델은 추상적인 모델이고, 이를 구체화된 것이 상호 운용 가능한 웹서비스 스택으로, IBM과 마이크로소프트 등의 회사에 의해 정의되었다. 웹서비스 스택은 Find, Bind, Publish 등과 같은 기능을 구현하는 기술을 정의한다. 웹서비스 스택은 다음 [그림 2]와 같은 4가지 기술로 구현된다.

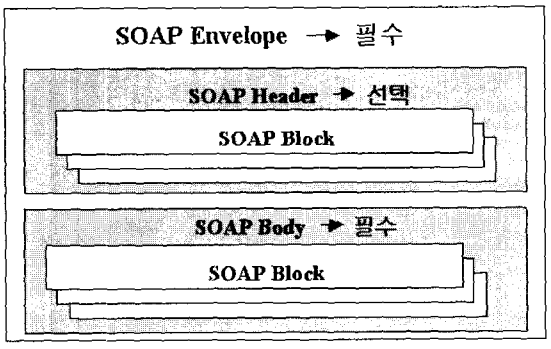


[그림 2] 웹서비스 스택과 관련 기술

2.1 SOAP

최하위 계층은 전송 계층으로 종단점간의 통신을 담당하고 널리 알려진 표준 프로토콜만을 지원한다. XML 메시징 부분은 웹서비스 사용자와 서비스간 호출과 결과에 대한 전송 방법을 정의하는 부분으로 SOAP인 XML로 기술된 표준방식을 사용한다.

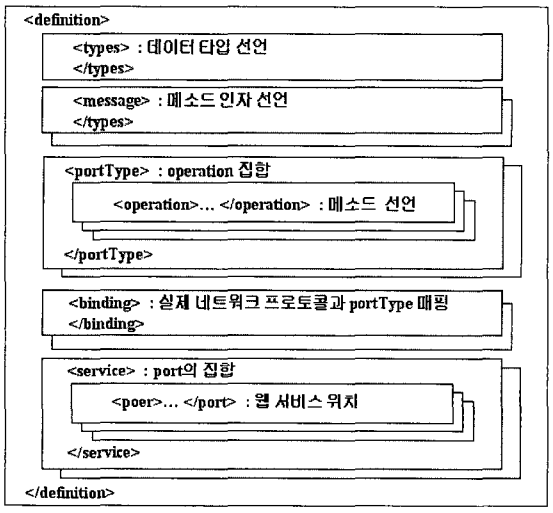
SOAP 메시지는 SOAP Envelope, SOAP Header, SOAP Body 3부분으로 나뉜다. SOAP Envelope는 SOAP Header와 SOAP Body를 포함해야 하는데, SOAP Body는 하나만 가질 수 있다. 반면 SOAP Header는 선택 필드로 필수 사항은 아니다[7].



[그림 3] SOAP 메시지 구성

2.2 WSDL

서비스 제공자는 WDSL을 사용하여 웹서비스 인터페이스를 표준 방식으로 기술한다. WSDL의 목표는 웹서비스를 기술하는 것이다. WDSL은 SOAP와 함께 웹서비스의 근간을 이루는 가장 중요한 기술이며, 웹서비스가 어떤 오퍼레이션을 지원하며, 어디에 어떤 방식으로 접근하면 되는지를 기술해 준다. 비즈니스 애플리케이션은 WSDL 파일을 주고 받음으로써 서로의 서비스를 이해하게 되며, 각 비즈니스가 파트너의 서비스를 일단 알게 되면 SOAP는 해당 서비스에 필요한 객체를 실행할 때 이용한다. WSDL은 웹서비스를 기술하기 위해 다음과 같은 요소들을 사용한다. Message (서비스 호출을 위한 메소드 인자), Operation(서비스 호출을 위한 메소드 용법), PortType(Operation의 집합) 요소는 메소드 호출을 위한 추상적인 정의를 가지는 요소이며, 이러한 추상적인 정보를 가지는 요소는 Binding 요소를 통해 SOAP 프로토콜과 연결된다. 이렇게 연결된 정보는 정보는 Port(웹서비스의 위치)와 Service(Port의 집합) 요소를 통해 실제 웹서비스 위치와 연결된다. 다음 [그림 4]는 WSDL이 가지는 요소가 WSDL 문서 안에서 어떻게 나타나는지 보여준다[9].

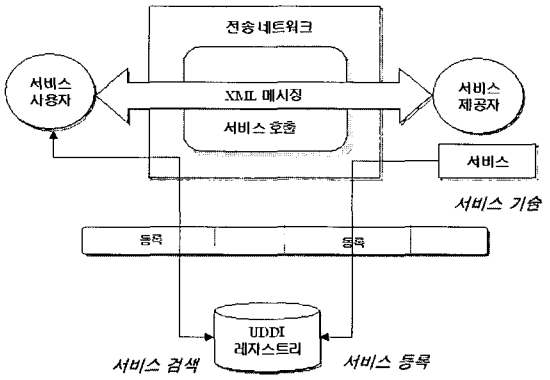


[그림 4] WSDL 구조

2.3 UDDI

최상위 계층은 서비스의 등록과 검색에 대한 계층으로 UDDI로 구현되어 있다. UDDI는 웹서비스에 대한 분산 웹 기반 정보 레지스트리를 위한 규격이다. 이들 레지스트리는 공개적으로 액세스될 수 있으며 현재 소프트웨어 회사, 개인 개발자, 표준 기구에 대한 서비스 타입 등록은 물론 기업이 지원하는 서비스를 기술하고 있는 비즈니스 타입 등록을 지원한다[8].

지금까지 분석한 웹서비스의 구조 및 스택 내용을 바탕으로 일반적인 웹서비스 구조를 살펴보면 다음 [그림 5]와 같다.



[그림 5] 일반적인 웹서비스 구조

이러한 웹서비스의 특징을 살펴보면 서비스의 이용의 편리함(Availability), 서비스 이용의 용이성(Transparency), 플랫폼의 독립성(Platform Independent), 표준 기반의 구조(Standard Based), 상호 호환성(Interoperability), 표준화에 따른 지원 용이성(Support) 등이다.

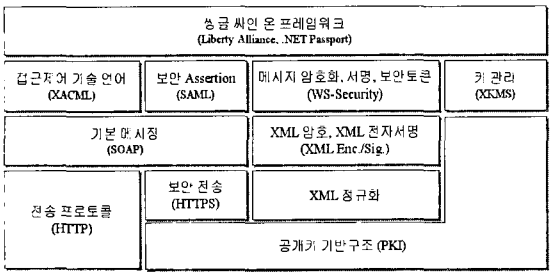
III. 웹서비스 보안 표준 및 기술

공개키 기반의 PKI는 전자상거래, 전자정부의 인증 기반으로서 주목받고 있다. 그럼에도 불구하고 PKI 애플리케이션은 아직 많은 보급이 이루어지고 있지 않다. VPN이나 S/MIME, 웹의 SSL/TLS 인증 등은 PKI 애플리케이션으로서 사용되고 있지만 여러 가지 기업 애플리케이션이나 전자정부에서 전자신청 애플리케이션을 PKI로 활용하는 것은 아직 미흡하다. 이러한 배경에는 PKI 애플리케이션 개발상의 어려움 등 여러 요인이 있다. 예를 들면, PKI 기반 프로토콜의 상당수는 ASN.1으로 정의되기 때문에 ASN.1의 구현상의 제약점이 있다는 것이다. PKI의 공개키 증명서나 키관리 프로토콜, 전자서명이나 암호화 포맷의 표준은 IETF의 PKIX 워킹 그룹, S/MIME 워킹 그룹에 의해 ASN.1 기반으로 구현되어 왔다. 한편, 웹 브라우저상에서 실행되고 있는 인터넷상의 많은 애

플리케이션은 SSL/TLS를 통해 보안이 유지되고 있지만 이것은 웹 브라우저의 세션 인증이나 프라이버시를 지키기 위한 것이며 문서의 전자서명이나 파일의 영속적인 암호화 등에는 사용할 수 없다. 따라서, 웹서비스의 애플리케이션이 PKI 기반의 보안기능을 제공하기 위해 PKI 인터페이스의 복잡함을 완화하고 어려운 ASN.1의 데이터 구조가 아닌 전자서명이나 서명검증 및 암호화, 복호화가 쉬운 PKI 애플리케이션의 API가 구현되어야 할 것이다. 이러한 관점에서 웹서비스 기반의 유연하고 동적인 PKI 애플리케이션을 구현하려는 업계의 움직임이 활발하게 되었다.

3.1 웹서비스 보안 표준

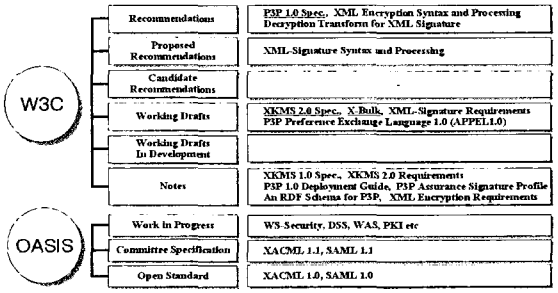
개인정보와 같은 기밀 데이터를 인터넷으로 이용할 때는 보안의 확보가 중요하게 된다. 이러한 보안 서비스를 제공하기 위해 웹서비스 보안 규격이 표준화되고 있다. 웹서비스 보안 표준화 관련 규격의 구성은 PKI를 이용하는 XML 정규화 부분이나 XML 전자서명, 암호화 등에 의해 XML 문서를 서명하고 암호화하는 부분으로 나눌 수 있다. 또한, 액세스 제어나 Assertion, 키 관리 등을 위한 규격으로 구성된다. 웹서비스의 보안 표준은 W3C(World Wide Web Consortium)나 OASIS(Organization for the Advancement of Structured Information Standards)로부터 많은 규격이 구성되어 있고 이러한 규격의 관계를 〔그림 6〕과 같이 나타낸다.



〔그림 6〕 웹서비스 보안 표준화 관련 규격 구성

W3C 표준은 XML을 이용하여 웹서비스를 기술하는 언어인 WSDL, XML 보안의 기반이 되는 XML 전자서명이나 XML 암호화, 또는 XML를 사용한 키 관리 기술인 XKMS(XML Key Management Specification)나 XML 메시징 프로토콜인 SOAP 등이 있다.

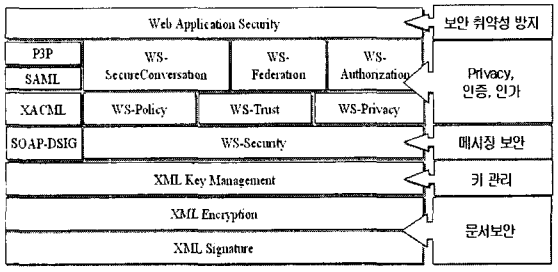
OASIS 표준에는 웹서비스의 상호 운용성을 높이기 위한 활동, W3C의 표준을 사용한 비지니스 메시징 표준의 검토를 주로 내용으로 하고 있으며 이러한 표준에는 인증, 인가 정보를 전달하는 방법인 SAML (Security Assertion Markup Language), 액세스 제어 관리 방법인 XACML(Extensible Access Control Markup Language), SOAP를 사용한 메시징 ebXML(Electronic Business XML) 등이 있다. W3C와 OASIS에서 진행중인 XML 웹서비스 보안기술의 표준화 진행 현황을 살펴보면 다음 〔표 1〕 및 〔그림 7〕과 같다.



〔그림 7〕 XML 웹서비스 보안기술 표준화 진행 현황

3.2 웹서비스 보안 기술

현재 W3C 및 OASIS 등의 국제 표준화 단체에서 진행되어온 XML 웹서비스 유형별 국제 표준 보안기술을 살펴보면 다음 〔그림 8〕과 같다.



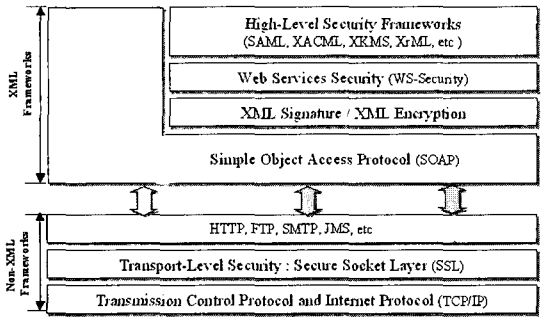
〔그림 8〕 XML 웹서비스 유형별 보안기술 구분

웹서비스 보안은 전송 계층의 보안과 메시지 계층의 보안으로 구분할 수 있다. 전송 계층의 보안은 SSL/TLS로 대표되는 보안 프로토콜을 SOAP의 하위 프로토콜로서 사용하는 방법으로서 HTTPS와 SOAP의 조합으로 구현되고 있다. 이러한 방법으로 메세지 전체의 암호화, 위변조 방지 및 클라이언트/서버 인증 등의 기본적인 보안 기능을 제공할 수 있다. 그러나 전송계층의 보안으로는 기업의 기밀문서를 부분적으로 암호화하고 담당자에 의해 접근할 수 있는 범위를 제

〔표 1〕 XML 웹서비스 보안 관련 국제 표준 문서 목록

구분	표준명세	상태	날짜
XML Signature	Signature Syntax and Processing	W3C Recommendation	2002. 02. 12.
	Canonical XML V1.0	W3C Recommendation	2001. 03. 15.
	Exclusive Canonical XML V1.0	W3C Recommendation	2002. 07. 18.
	XPath Filter V2.0	W3C Recommendation	2002. 11. 08
	XML Signature Requirements	W3C Working Draft	1999. 10. 14.
XML Encryption	XML Encryption Requirements	W3C Note	2002. 03. 04.
	XML Encryption Syntax and Processing	W3C Recommendation	2002. 12. 10.
	Decryption Transform for XML Signature	W3C Recommendation	2002. 12. 10.
	Additional XML Security URIs (Informational)	IETF INTERNET-DRAFT	2003. 02.
	Application/xenc+xml Media Type Registration	IETF INTERNET-DRAFT	2002. 09.
XKMS	XML Key ManagementRequirements V2.0	W3C Note	2003. 05. 05.
	XML Key Management Specification V2.0	W3C Working Draft	2003. 04. 18.
	X-Bulk	W3C Working Draft	2002. 08. 22.
P3P	Platform for Privacy Preferences (P3P V1.0)	W3C Recommendation	2002. 04. 16.
	A P3P Preference Exchange Language V1.0 (APPEL V1.0)	W3C Working Draft	2002. 04. 15.
	The Platform for Privacy Preferences V1.0 Deployment Guide	W3C Note	2002. 02. 11.
	A P3P Assurance Signature Profile	W3C Note	2001. 02. 02.
	An RDF Schema for P3P	W3C Note	2002. 01. 25.
SAML	Bindings and Profiles V1.0	OASIS Standard	2002. 11. 05.
	Conformance Program Specification V1.0	OASIS Standard	2002. 11. 05.
	Assertions and Protocol V1.0	OASIS Standard	2002. 11. 05.
	Glossary V1.0	OASIS Standard	2002. 11. 05.
	Security and Privacy Considerations V1.0	OASIS Standard	2002. 11. 05.
	Bindings and Profiles V1.1	OASIS Committee Specification	2003. 07. 18
	Conformance Program Specification V1.1	OASIS Committee Specification	2003. 07. 18
	Assertions and Protocol V1.1	OASIS Committee Specification	2003. 07. 18
	Glossary V1.1	OASIS Committee Specification	2003. 07. 18
	Security and Privacy Considerations V1.1	OASIS Committee Specification	2003. 07. 18
XACML	XACML Specification Version V1.0	OASIS Standard	2003. 02. 18.
	XACML Specification Version V1.1	OASIS Committee Specification	2003. 06. 11.
	XACML profile for Web-services	OASIS Working Draft	2003. 07. 23.
	XACML RBAC Profile	OASIS Working Draft 01	2003. 06. 05.
	XACML XML DSig Profile	OASIS Working Draft 0.2	2003. 03. 14.
	WSDL and SOAP bindings for WSPL	OASIS Working Draft 01	2003. 06. 11.
	Web-services policy language use-cases and requirements	OASIS Working Draft 04	2003. 04. 18.
Web Service Security	Web Service Security SOAP Message Security	OASIS Working Draft	2003. 06.
	Web Service Security Username Token Profile Draft Web Service Security Kerberos Token Profile Draft Web Service Security SAML Token Profile Draft Web Service Security x509 Token Profile Draft Web Service Security XrML Token Profile Draft Web Service Security XCBF Token Profile Draft		2003. 06
DSS	DSS UseCase Requirement Analysis	OASIS Working Draft 0.9	2003. 07. 22

한하고 싶은 경우, 1개의 품의서에 담당자가 차례로 서명할 경우 적용상의 한계점이 있다. 이를 해결하기 위해 XML 암호화, XML 전자서명, WS-Security, SAML, XACML 등의 메시지 계층 보안이 필요하게 된다.



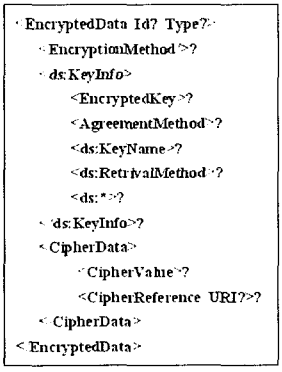
〔그림 9〕 계층별 XML 웹서비스 보안 구분

3.2.1 W3C 보안 기술

1) XML 암호화와 전자서명

XML 암호화 기술은 XML 문서의 부분적 요소에 대한 암,복호화를 지원하는 기술로 기밀성 서비스를 제공한다. XML 암호화를 이용함으로써 문서의 부분적인 암호화가 가능하게 된다. XML 암호화에서는 XML에 한정하지 않고 다양한 정보를 암호화하고 그 결과를 XML 문서에 넣을 수가 있다.

XML 암호기술에서의 암호화 대상은 XML 요소의 암호화, XML 요소의 내용 암호화(요소 및 문자 데이터), 임의의 데이터 및 XML 문서를 암호화, 중복 암호화 등이다. XML 암호화를 위한 구문은 다음과 같은 XML 서문, 정의, 내부 엔터티 등을 포함한 XML-Schema를 통해 정의된다. 다음 〔그림 10〕은 XML 암호 기술에서 사용되는 구문을 간단히 표시한 것이다.



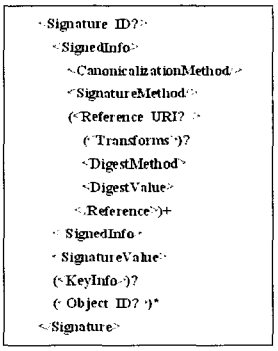
〔그림 10〕 XML 암호화의 구조

XML 암호화의 각 요소들의 내용은 다음과 같다.

- 〈EncryptedData〉와 〈EncryptedKey〉의 추상 타입인 〈EncryptedType〉로부터 유도된 타입들이다.
- 암호화된 데이터를 포함하는 〈CipherValue〉나 〈CipherReference〉를 갖는 〈CipherData〉는 필수 요소이다.
- 〈ReferenceList〉는 이 키를 이용하여 암호화된 데이터 및 키들을 가리키고 있는 임의의 요소이다.

XML 전자서명은 XML 문서에 대해 XML 형태의 서명을 생성하고 검증할 수 있는 서명 기법이며 전자문서에 대해 인증, 무결성, 부인봉쇄 등의 정보보호 서비스를 제공한다. XML 전자서명을 이용하여 문서의 일부분에 서명하거나 어떤 담당자가 서명한 문서에 또 다른 담당자가 서명하는 복잡한 경우에도 적용할 수 있다. XML 암호화와 같이 XML 전자서명에서도 XML에 한정하지 않고 다양한 정보에 서명하여 그 결과를 XML 문서에 넣을 수 있다[5].

XML 전자서명은 〔그림 11〕과 같은 구조를 갖는 Signature 요소로 표현된다. XML 전자서명은 URI를 통해 서명 대상인 리소스와 연관지어진다. XML 문서 내부에서 XML 전자서명은 단편 식별자 (fragment identifier)를 이용해 같은 XML 문서 내에 존재하는 서명 대상인 리소스와 연관지어진다.

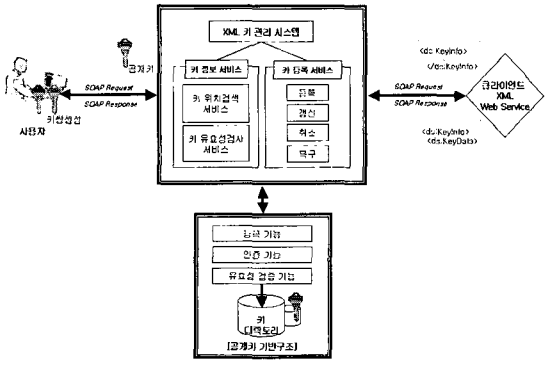


〔그림 11〕 XML 전자서명의 구조
(?: 0 혹은 1번, +: 1번 이상, *: 0번 이상 나타남)

2) XKMS

XKMS는 키의 등록, 키 정보의 해결이나 유효성 검증 등의 서비스 인터페이스와 프로토콜을 정하고 있으며, XML 기반의 공개키 관리를 위한 프로토콜로 공개키의 효율적인 공유 기능을 제공한다. XML 암호화, XML 전자서명, WS-Security, SAML은 많은

부분에서 PKI에 의존하고 있는데 기존의 PKI를 이용하기 위해서는 복잡한 데이터 구조나 API를 구현해야 한다. 이를 웹서비스를 통해 해결하고 이용 가능하게 하는 것이 XKMS의 목적이다. XKMS는 XML 키 정보 서비스(XKISS)와 XML 키 등록 서비스(XKRSS)로 구분된다. 키 정보 서비스는 XML 전자서명에 포함된 공개키 정보(<ds:KeyInfo>요소)의 실제 내용인 인증서 정보, 공개키 매개변수, 인증서 폐지정보, 유효성 상태 정보 등을 전송하는데 사용되며, 키 등록 정보 서비스는 클라이언트가 이러한 공개키 정보를 신뢰할 수 있는 인증 기관에 등록 또는 폐기, 갱신 등을 요청하는데 사용된다[2].

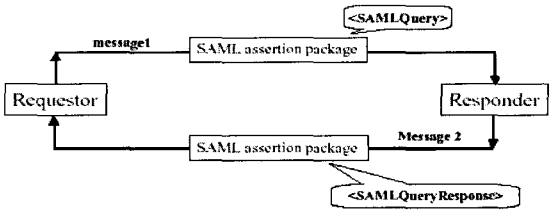


〔그림 12〕 XKMS 서비스 구조

3.2.2 OASIS 보안 기술

1) SAML

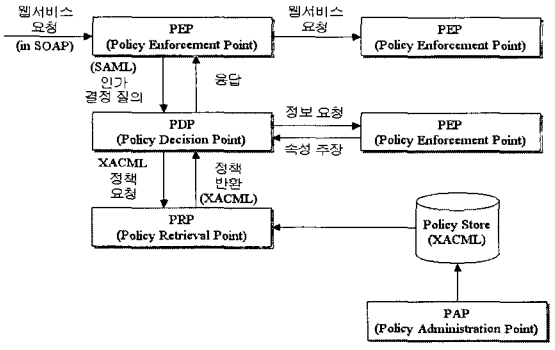
SAML은 인증과 인가 정보를 안전하게 교환할 수 있도록 하는 표준으로 인증(Authentication)과 인가(Authorization) 서비스를 제공하는 다양한 서비스 플랫폼간의 상호운영성을 지원한다. OASIS에서 표준화가 진행되고 있는 SAML은 클라이언트의 인증 정보, 속성 정보, 혹은 인가 정보를 저장하는 Assertion이라고 하는 XML 기반의 증명서에 관한 규격이다. Assertion의 메세지 형식, Assertion 발행처(SAML Authority)의 역할, 그리고 클라이언트와 SAML Authority간의 메세지 규칙인 SAML 프로토콜을 정하고 있다. SAML은 Assertion이나 이를 교환하기 위한 프로토콜을 표준화 하는 것으로 싱글·싸인온(SSO)을 위한 기반을 제공하고 있다. 그러나 SAML에서는 구체적인 인증 방법까지는 규정하고 있지 않기 때문에 SSO를 구현하기 위해서 한층 더 상위의 체제가 필요하게 된다. Liberty Alliance는 SAML 기반의 SSO를 위한 규격의 예이다.



〔그림 13〕 SAML 프로토콜

2) XACML

XACML은 접근제어 정책을 기술하기 위한 XML 기반의 언어와 메세지 형식을 정하는 규격이다. XML 기반 접근제어는 인가에 대한 규칙을 표현하기 위한 XML 어휘로 구성된다. 접근제어 규칙을 정의한 XML 어휘를 이용하여 보안이 요구되는 자원에 대해 미세한 접근제어 서비스를 제공한다. 접근제어 정책이란 누가 어느 자원에 어떠한 조작을 실시할 수 있을까를 정하는 것이다. XACML은 SAML의 인가 Authority 부분을 공유하고 있지만 XACML 규격은 SAML에 의존하지 않고 CORBA나 EJB(Enterprise JAVA Beans) 등 폭넓은 애플리케이션으로부터 이용할 수 있다. XACML은 정책 언어와 요청/응답 언어로 구성되어 있다. 정책 언어는 가장 기본이 되는 규칙(Rule), 여러 규칙들을 포함하는 정책(Policy) 및 정책들의 집합인 정책세트(Policy Set)으로 구성된다. 〔그림 14〕는 XACML 구조적 다이어그램을 나타내는 것으로 SOAP 프로토콜 상에서 PDP(정책 요구 부문)에게 단일의 PEP(정책 결정 부문)가 동작하는 것을 보여준다. 이 모델은 다중의 PEP들이 단일의 PDP와 동작하는 것보다 더 효율적이다.



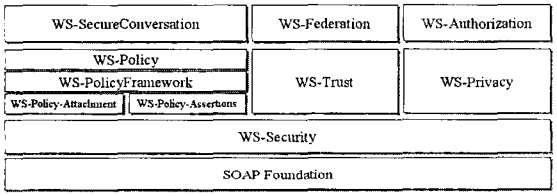
〔그림 14〕 XACML 구조적 다이어그램

3) WS-Security

SOAP 메세지가 되는 XML 문서에 암호화나 서명을 하는 경우 XML 암호화와 XML 전자서명을 사용하지

만 이것만으로는 불충분하다. SOAP 메세지의 Header 또는 Body에 암호화 또는 서명된 XML 요소를 저장하는 방법이 필요하다. OASIS에서 표준화가 진행되고 있는 WS-Security에서는 이러한 방법을 규정하고 있다. 또한, WS-Security는 클라이언트의 인증과 인가를 위해 사용하는 보안 토큰을 SOAP 메세지에 넣는 방법도 규정하고 있다. 보안 토큰이란 클라이언트의 신원을 서버에 신고하기 위한 증명서이다. 사용자명과 패스워드, X.509 증명서, SAML Assertion 등을 보안 토큰으로서 사용할 수 있다[4].

2002년 7월 IBM, 마이크로소프트, 베리사인은 WS-Security 규격안을 제안하고 OASIS 통해 표준화를 진행하고 있다. WS-Security는 웹서비스 보안 규격의 일부분으로서 현재 계속 추가적인 작업이 이뤄지고 있다. 웹서비스 보안의 전체 구성을 살펴보면 다음 [그림 15]와 같다[10].



[그림 15] 웹서비스 보안 규격의 로드맵 구성도

웹서비스 보안 규격 중 첫 번째 단계는 신뢰된 도메인간의 웹서비스 보안에 필요한 규격을 포함하고 정보 인증의 여부와 정보 공유에 대한 내용을 담당한다.

- WS-Policy:송수신자간의 보안 요구사항과 프라이버시, 인코딩 포맷, 지원 알고리즘을 포함하는 여러 가지 기본 서비스 애트리뷰트들을 명시하는 보안 정책 사항과 제약을 표현하기 위한 방법을 정의하고 있다.
- WS-Trust:보안 도메인간 상호작용을 가능하게 하는 보안 Trust 모델을 정의한다.
- WS-Privacy:WS-Security, WS-Policy, WS-Privacy를 함께 사용하여 기업들은 기술된 프라이버시 정책에 대한 적합성을 기술하고 지적할 수 있다.

두 번째 단계는 보다 진보된 요구사항을 만족하는 규격들을 포함하는 것으로 WS-SecureConversation, WS-Federation, WS-Authorization으로 구성된다.

- WS-SecureConversation:신뢰된 도메인간의 키 교환을 통합 신뢰를 동적으로 형성하는 방법을 정의한다. 웹서비스가 요청자의 메시지의 신원을 어떻게 확인하고 요청자가 서비스의 신원을 어떻게 확인하며, 상호 신원이 확인된 보안 상태를 어떻게 구축하는지를 설명한다.
- WS-Federation:WS-Security, WS-Policy, WS-Trust 및 WS-SecureConversation을 연합된 시스템간의 관계와 기타 정보 관리 방법을 정의한다.
- WS-Authorization:웹서비스 환경에서의 권한 부여 데이터와 정책 관리 방법을 정의한다.

WS-Security는 무결성과 기밀성을 제공하기 위해 SOAP을 어떻게 확장하고, 메시지 내부에 보안 토큰을 어떻게 포함하는지를 정의한다. 이는 X.509 인증서를 포함한 바이너리 포맷 데이터를 어떻게 인코딩하는가에 대한 정의도 포함된다. 따라서 웹서비스 보안 규격의 주요 내용은 단대단 보안의 무결성 및 기밀성을 포함한 다중 보안 토큰, 신뢰 도메인, 암호화 기술을 지원하기 위한 명시 조건 등에 대한 기술이다.

Ⅳ. 웹 애플리케이션 보안모델

4.1 웹 서비스를 위한 보안 요구사항

웹서비스의 기반이 되는 표준인 XML은 데이터에 대한 의미적 접근과 확장성을 제공하는 표준으로서 언어적 미들웨어의 역할을 수행하는 반면, 중요 정보에 대한 표현이 구조적으로 드러나게 되어 있어, XML 문서상에 나타나는 많은 정보들이 외부에 무방비 상태로 노출되는 것이 사실이다. 웹서비스 환경에서 일반적으로 적용되어지는 OSI 7 계층별 보안기술과 인터넷 보안 서비스 요구사항인 기밀성(Confidentiality), 무결성(Intergrity), 인증(Authentication), 부인방지(Nonrepudiation) 등의 보안 서비스 해당별 위협 요소에 대한 보안 서비스를 분석하면 다음 [그림 16]과 [표 2]와 같다.

계층번호	계층명	웹서비스 환경
Layer 7	Application	HTTP, SMTP, SOAP etc.
Layer 6	Presentation	Encryption Data, Compressed Data
Layer 5	Session	POP/25, SSL
Layer 4	Transport	TCP, UDP
Layer 3	Network	IP Packets
Layer 2	DataLink	PPP, 802.11, etc
Layer 1	Physical	ADSML, ATM etc.

[그림 16] OSI 7 계층에서의 보안기술

〔표 2〕 웹서비스 기반 위협 요소별 적용 보안기술

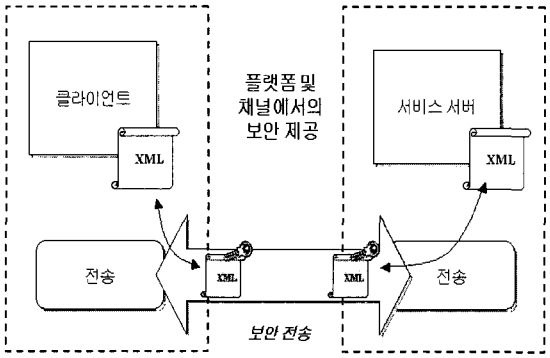
보안 서비스	위협 요소	적용 보안 기술
기밀성	메시지 도청	XML Encryption, SSL/TLS, S/MIME
무결성	메시지 변조	XML Signature, SHA-1, SSL/TLS, IPSec
인증	메시지 위조	ID/PWD, Kerberos, TLS, IPSec, PKI, XKMS
부인방지	메시지 송신 및 수신 부인	XML Signature, XKMS
접근제어	불법적 서비스 및 정보이용	XACML, PMI, SAML

4.2 웹 애플리케이션을 위한 보안 모델

웹서비스 환경의 웹 애플리케이션을 위한 보안 모델은 다음의 3가지로 분류될 수 있다[10,13].

4.2.1 플랫폼 기반의 보안 모델

웹 클라이언트와 서비스 서버 사이의 전송 채널에 해당되는 보안 모델 구성은 다음 〔그림 17〕과 같다.



〔그림 17〕 플랫폼 기반의 보안 모델

플랫폼 보안 모델을 사용하는 경우 다음과 같은 특징이 있다.

- 서버의 인증 방법으로는 다이제스트, 통합 인증서 인증 등이 있다.
- 인증 및 권한 부여기능을 상속한 기능이 제공 가능하다.
- 메시지 무결성, 기밀성을 제공하기 위해 SSL 및 IPSec을 사용할 수 있다.

4.2.2 애플리케이션 기반의 보안 모델

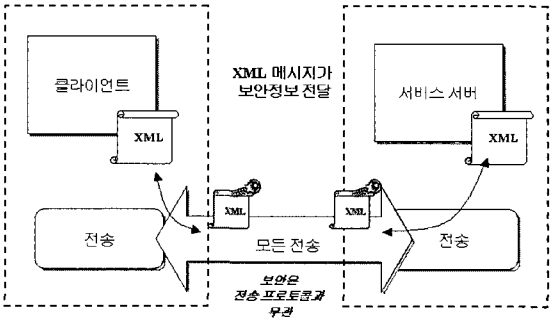
응용 애플리케이션 수준의 보안을 적용하려면 응용 애플리케이션에서 보안을 담당하며 사용자 지정 보안 기능을 사용한다. SSL을 사용해 기밀성과 무결성을 지원하고, 응용 애플리케이션은 웹서비스의 요청에 따라 사용자를 인증하기 위해 사용자 지정 SOAP 헤더를 사용하여 사용자 증명을 전달할 수 있다. 이 모델은 다음과 같은 경우에 적용이 가능하다.

- 기존의 응용 애플리케이션에서 사용된 기존의 사용자 및 역할 DB 스키마를 이용하려는 경우
- 전체 데이터 스트림이 아니라 메시지 일부를 암호화하려는 경우

4.2.3 메시지 기반의 보안 모델

메시지 수준의 보안 모델은 매우 유연한 방법으로 WS-Security를 기본으로 한다. WS-Security는 메시지 무결성, 기밀성, 단일 메시지 인증을 제공하는 강화된 SOAP 메시징 기능을 지원한다. 이 모델은 이기종 웹서비스 환경에서 보안 메시지 교환을 위한 프레임워크를 구축하는데 사용될 수 있다. 메시지 수준의 보안은 다음과 같은 특징을 지닌다.

- 기본적인 전송 메커니즘으로부터 독립적이다.
- 이기종 보안 구조에 사용할 수 있다.
- 종단간 보안을 제공한다.
- 여러 암호화 기술을 지원하며, 부인방지 기능을 제공한다.



〔그림 18〕 메시지 기반의 보안 모델

V. 웹서비스 애플리케이션 보안 프레임워크

4장에서 언급한 웹 애플리케이션의 3가지 기본 보안 모델을 기반으로 본 장에서는 현재 표준화가 진행

되고 있는 WS-Security의 보안 토큰 서비스 모델을 분석하여 이를 기반으로 글로벌 XML 웹서비스를 위한 웹서비스 애플리케이션 보안 프레임워크를 검토하고 보안 모델을 분석한다.

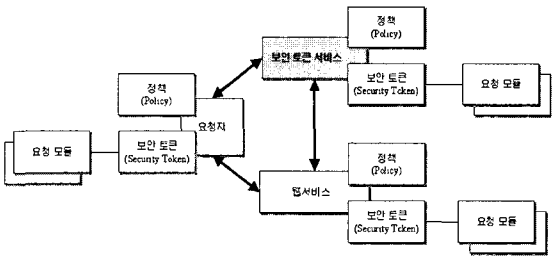
5.1 보안 토큰 서비스 모델

웹서비스 플랫폼의 주요 이점은 통합되고 상호 운용 가능한 솔루션을 제공하는 데 있다. 포괄적인 보안 모델의 적용을 통해 웹서비스의 무결성과 기밀성 및 보안을 보장하는 것은 서비스 사업자와 이용자 모두에게 중요한 문제이다. IBM과 Microsoft는 웹서비스 환경에서 교환되는 메시지를 어떻게 보호할지를 다루는 웹서비스 보안 플랫폼을 개발하기 위해 웹서비스 보안 로드맵을 진행하고 있다. 이는 광범위한 애플리케이션과 비즈니스 토폴로지에 걸쳐 신원 확인, 인증, 프라이버시, 신임(trust), 무결성, 기밀성, 보안 통신 채널, 연합, 위임 및 감사 등을 포함한 보안 기술들을 다루는 폭넓은 플랫폼을 고려한다. 이 사양들은 확장성 있고 유연한 프레임워크를 제공하며, 기존 보안 인프라를 극대화한다. 이 사양들은 이전에 제안되었던 유사한 사양(예, SOAP-Security, WS-Security 및 WS-License)들에서 표현되었던 개념들을 포함하여 확장되고 있다[13].

오늘날의 웹서비스 애플리케이션 토폴로지는 모바일 장치, 게이트웨이, 프록시, 외부 위탁된 데이터 센터 및 전 세계적으로 분산되고 동적인 구성이 가능한 시스템들이 광범위하게 결합되어 있다. 이 모든 시스템들은 메시지 전달을 위해 메시지 처리 중개자의 능력에 의존한다. 데이터가 전송 층을 넘어서 중개자에 의해 수신되고 전송될 때, 데이터의 무결성과 데이터와 함께 전달되는 모든 보안 정보를 잃어버릴 수 있다. 이같은 위험 때문에 모든 상향식 메시지 처리자는 이전의 중개자가 내린 보안 평가에 의존하고, 메시지의 컨텐츠에 대한 그들의 처리를 완전히 신임하게 된다. 광범위한 웹서비스 플랫폼 내에 필요한 것은 단대단 보안 방식을 제공하는 메커니즘이다. 성공적인 웹서비스 보안 솔루션은 포괄적인 보안 기능 세트를 제공하기 위해 전송층과 애플리케이션층 양쪽의 보안 메커니즘을 응용할 수 있다. 이러한 메커니즘들을 기반으로 한 보안 토큰 서비스 모델은 다음과 같은 기능을 수행할 수 있게 한다.

- 웹서비스는 들어오는 메시지가 요청 모듈 (예:이름, 키, 허가, 기능 등)을 입증하도록 요구할 수 있다. 만일 메시지가 필요한 요청없이 도착하게 되면, 서비스는 메시지를 무시하거나 거부할 수 있다. 우리는 요구되는 요청 모듈과 관련 정보를 정책(Policy)이라고 한다.
- 요청자는 메시지와 보안 토큰을 결합시킴으로써 필요한 요청에 대한 증명을 가진 메시지를 보낼 수 있다. 이리하여 메시지들은 특정 행위를 요구하고, 발신자가 그러한 행위를 요구할 수 있는 요청을 가졌음을 입증한다.
- 요청자가 필요한 요청을 가지고 있지 않은 경우, 요청자 혹은 이를 대신한 누군가가 다른 웹서비스와 접촉하여 필요한 요청을 얻으려고 시도할 수 있다. 보안 토큰 서비스라고 부르는 이러한 다른 웹서비스들은 이번엔 그들 자신의 요청 모듈을 요구할 수 있다. 보안 토큰 서비스 브로커는 보안 토큰을 발행함으로써 서로 다른 신임 도메인들 사이를 신뢰한다.

이와 같이 보안 토큰 서비스 모델은 모든 요청자가 서비스가 될 수 있고, 정책을 표현하고 보안 토큰을 요구하는 등 완전한 하나의 웹서비스 보안 모델을 지향하고 있다[13].



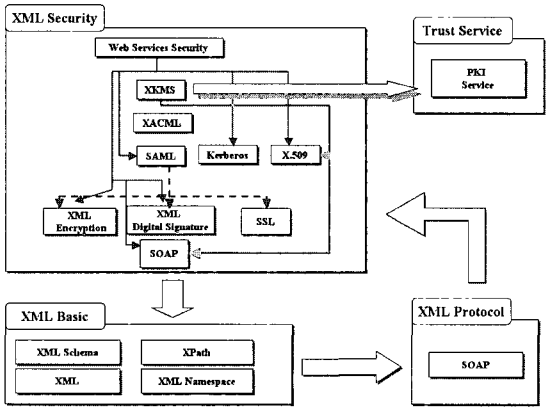
〔그림 19〕 보안 토큰 기반의 XML 웹서비스 신뢰모델

보안 토큰이란 요청의 모음을 나타내는 것으로 서명된 보안 토큰은 특정 인증기관에서 암호화하여 승인된 보안 토큰(예, X.509)을 뜻하고, 소유 증명 토큰은 보내는 쪽이 소유 증명을 보여 주기 위해 사용할 수 있는 데이터가 들어 있는 보안 토큰을 말한다. 보안 토큰 서비스란 보안 토큰을 발행하는 웹서비스를 뜻하는 것이다.

5.2 웹서비스 애플리케이션 보안 프레임워크

XML 웹서비스 보안기술을 구성하고 있는 XML 보안기술들은 인터넷상의 상호 운용성을 위해 국제적

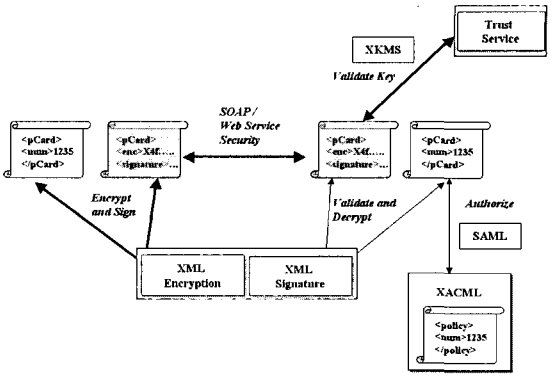
으로 표준화가 진행되고 있으며, 각 단위 시스템으로의 기능에 대한 연구가 지속적으로 이루어지고 있다. 모든 XML 웹서비스 보안기술들은 상호 연계를 가지며 그 기능들이 동작된다. [그림 20]은 이러한 기술들의 상호 연계 현황을 보여준다.



[그림 20] XML 웹서비스 보안기술 상호 연계도

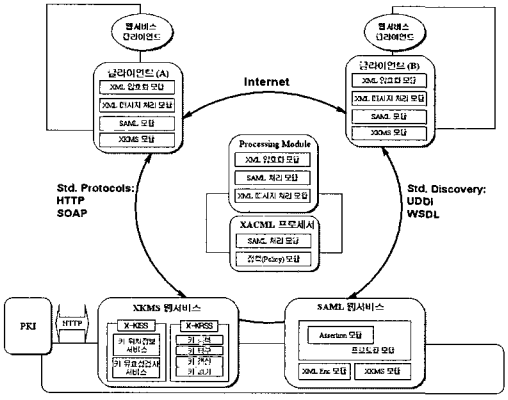
XML 웹서비스는 XML 표준을 기반으로 XML 도구와 XML 프로토콜을 지원하며, 각각의 XML 보안 표준간의 기능을 활용한다. XML 웹서비스 보안기술은 다른 XML 보안 표준과 마찬가지로 XML Schema, XPath, XML, XML Namespace등의 기본 XML 도구를 기반으로 한다. XML 전자서명과 XML 암호화는 전자서명 또는 암호화될 데이터를 XPath로 표현하여 XML 문서의 특정한 일부분만 처리할 수 있도록 해준다. 또한 XML Namespace를 통해 키 정보를 표현하거나 전자서명에서의 기능 확장성을 제공한다. XML 보안기술 부문에서 XKMS는 공개키의 정보를 표현하기 위해 XML 전자서명을 이용하고, 개인키를 암호화하는데 XML 암호화 표준을 근간으로 한다. SAML은 인가 서비스를 위해 XML 전자서명 및 암호화를 통해 무결성, 기밀성의 보안 기능을 지원하고, XACML은 SAML의 처리를 통해 세부적인 접근 통제 규칙의 설정이 가능하다. 이와 같이 XML 웹서비스 보안 기술들은 상호 연계를 기본으로 운용된다. [그림 21]은 이러한 상호 연계 기능을 구체적인 예를 들어 보여주는 상호 운영 기능도를 나타내고 있다.

현재의 XML 웹서비스 기반 애플리케이션의 환경은 서비스 프레임워크 상에서 기본 전제사항이라고 할 수 있는 보안 측면에 대한 연구보다는 실제 비즈니스 컴포넌트와 세부 구현 기술에 집중되어 있다. 또한 기본의 보안 기술을 적용한 서비스 운영을 대부분 사용



[그림 21] XML 웹서비스 보안기술의 상호운영 기능도

하고 있어 최적화된 XML 웹서비스 애플리케이션 보안 모델의 연구가 요구된다. 이에, 앞서 살펴본 XML 웹서비스 기술과 XML 보안기술을 활용한 웹서비스를 위한 애플리케이션 보안 모델을 세부 모듈 단위로 구성하면 [그림 22]와 같다.



[그림 22] 웹서비스 애플리케이션 보안 프레임워크

XML 웹서비스 애플리케이션 보안 프레임워크는 신뢰성 기반의 환경에서 수행할 수 있는 시스템 플랫폼을 목표로 하며, 비즈니스 컴포넌트에 대한 접근 제어 및 메시지 보안 측면을 중심으로 보안 요구사항을 만족한다. 두 웹서비스 애플리케이션 클라이언트의 XML 암호화 및 전자서명 기능은 XKMS 및 SAML 웹 서비스의 MSH(Message Service Handler)에 위치해 송수신되는 메시지에 대한 인증 및 암복호화 과정을 수행한다. 이 과정 수행시 키 정보에 대한 PKI 서비스 기능은 XKMS 웹서비스에서 처리하게 된다. SAML 웹서비스는 작업 요청 시 요구자의 인증 및 승인을 위한 정보를 제공해 자원 접근제어 기능을 수행한다. 이때 실제적인 접근 제어 정보는 XACML

정책 파일에 정의되며 XML 요소에 대한 세부 접근 제한을 가능하게 한다.

Ⅵ. 결 론

본 고에서는 웹서비스의 개요, 웹서비스의 보안분석 및 보안모델을 통해 전반적인 보안 기술 및 내부적인 구조를 분석하였다.

향후 이러한 웹 애플리케이션 보안 프레임워크 구성안을 기반으로 유,무선 통합 환경을 위한 모바일 웹서비스 보안기술에 대한 연구와 통합 보안 환경을 위한 기술개발 연구가 필요하다. 기술적으로 소프트웨어 및 하드웨어 웹서비스의 환경과 작은 단말기를 포함하는 다양한 플랫폼에서 동작하는 소프트웨어 에이전트 환경을 갖게될 것으로 예상된다. 따라서, 웹서비스 기반의 웹 애플리케이션 부문에 대한 보안 취약성을 분석하여 안전성을 제공할 수 있는 WAS(Web Application Security)에 대한 연구가 요구된다.

국내 웹서비스 적용 및 활용분야는 계속 활성화되어 가고 있지만, 웹서비스 보안에 대한 인식은 저조한 편이다. 앞으로 웹서비스 보안의 필요성 및 보안 표준간의 상관 관계, 웹서비스 보안에 대한 인식 공유가 빠르게 확산되기를 기대한다.

참 고 문 헌

[1] 문기영, 손승원, "XML 정보보호 개요", *정보처리학회지*, 제10권 제2호, pp.108-116, 2003.

[2] 박남제, 문기영 외 3명, "안전한 전자거래를 위한 XML 키 관리 기술", *정보보호학회지*, 제13권 제3호, 2003.

[3] 김주한, 문기영, "XML 기반 접근제어 기술동향" *정보보호학회지*, 제13권 제4호, pp.68-73, 2003

[4] Web Service Security Specification, http://www.verisign.com/wss/wss.pdf.

[5] XML-Signature Syntax and Processing, http://www.w3.org/TR/2002/REC-xmldsig-core20020212/.

[6] Liberty Alliance Project, http://www.projectliberty.org.

[7] SOAP version1.1(W3C note), http://www.w3.org/TR/SOAP/.

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

[9] WSDL Web site, http://www.w3.org/TR/wsdl.

[10] Verisign, http://www.verisign.com.

[11] OASIS Web site, http://www.oasis-open.org.

[12] Internet Engineering Task Force, http://ietf.org.

[13] Web service Architecture, http://www-106.ibm.com/developworks/webservices/library/w-ovr/.

[14] http://www.webservice.org.

[15] http://www.atmarkit.co.jp.

[16] DongKu Sin et. Al., "Development of Standards for XML based e-Business Framework Security and Digital Signature", *NCA IV-RER-02103*, 2002.

[17] Steve Graham, Simeon Simeonov, Toufic Boubez, Doug Davis, Glen Daniels, Yuichi Nakamura, Ryo Neyama, "Bulding Web Service with Java", *SAMS*, 2002.

〈著 者 紹 介〉

문 기 영 (Ki-young Moon)
정회원

1986년 : 경북대학교 전자공학과 졸업
1989년 : 경북대학교 대학원 전자공학과 석사
1992년~1994년 : (주)대우정보시스템 기술연구소 대리
1994년 3월~현재 : 한국전자통신연구원 정보보호연구본부 능동보안기술연구팀 선임연구원/과제책임자
관심분야 : 전자상거래 보안, 분산시스템, 트랜잭션 등

박 남 제 (Nam-je Park)
정회원

2000년 : 동국대학교 정보산업학과 졸업
2003년 : 성균관대학교 정보보호학과 석사
2003년~현재 : 한국전자통신연구원 정보보호연구본부 능동보안기술연구팀
관심분야 : 전자상거래 보안, XML 보안, 무선인터넷 보안, 전자지불 등

송 유 진 (You-jin Song)
정회원

1982년 : 한국항공대학교 전자공학과 졸업
1987년 : 경북대학교 대학원 정보시스템 전공 석사
1995년 : 일본 Tokyo Institute of Technology (박사)
1988년~1996년 : 한국전자통신연구원 선임연구원
1996년~현재 : 동국대학교 정보산업학과/전자상거래대학원 교수
1998년~현재 : 한국정보보호학회 이사, ISO/IEC JTC1/SC27-Korea 전문위원
관심분야 : 암호 및 인증이론, 전자상거래보안 응용, 무선인터넷 보안, 전자화폐/전자지불, 컨텐츠 보호 등

손 승 원 (Sung-won Sohn)
정회원

1984년 : 경북대학교 전자공학과 졸업
1994년 : 연세대학교 대학원 전자공학과 석사
1999년 : 충북대학교 대학원 컴퓨터공학과 박사
1983년~1986년 : 삼성전자(주) 연구원
1986년~1991년 : LG전자(주) 중앙연구소 HI8mm 캠코더 팀장
1991년~현재 : 한국전자통신연구원 정보보호연구본부 네트워크보안연구부장/책임연구원
관심분야 : IC Card, Biometry, Active Network, 생체인식분야 등

박 치 항 (Chee-hang Park)
정회원

1974년 : 서울대학교 응용물리학과 졸업
1980년 : 한국과학기술원 전자계산학과 석사
1987년 : 파리6대학 전자계산학과 공학박사
1974년~1978년 : 한국과학기술연구소 연구원
1978년~현재 : 한국전자통신연구원 정보보호연구본부 본부장
관심분야 : 네트워크보안, 액티브 네트워크, 멀티미디어시스템, 미들웨어, 모바일 에이전트 구조 등