XML보안 환경에서 SOA에 관한 硏究

신승중*, 최재주**, 곽계달**
*한세대학교 컴퓨터공학과
**한양대학교 컴퓨터공학과
e-mail : expersin@hansei.ac.kr,

A Study On SOA(Service-Oriented Architecture) based for XML Security

Seung-Jung Shin*, Jae-Ju Choi**, Kae-Dal Kwack**
*Department of Computer Engineering, Hansei University
**Department of Computer Engineering, Hanyang University

요 약

다양한 비즈니스 변화는 기업 내부 및 기업 간의 E-비즈니스, B2B와 M&A 분야에서 서비스 및 시스템 통합의 필요성이 요구 되었다. 구현 방법으로 분산 객체 기술을 사용 되었으나 공개 표준 부재로 시스템 통합을 어렵게 하였다. XML기반 기술의 발달은 웹 서비스 통합 측면에서 유연성을 제공하였으나 정보 보안에 대한 취약점을 가지고 있었다. 이를 해결하기 위한 방안으로 디지털 서명과 WS-Security 논함으로써 XML 보안 환경 하에서 서비스 통합에 구현 방법을 제시 하는데 목적이 있다.

1. 서론

웹 서비스 등장은 비즈니스의 연계의 필요성 증가 및 시스템 연계 부족, 서로 다른 시스템과 어플리케이션 사이 데이터 교환의 필요성이 요구 되었다. 서로 다른 비즈니스 프로세스에서 XML(extensible markup language) 이 갖는 장점이 주목되어 웹 서비스에 대한 관심이 고조 되었다. XML 을 통한 데이터 교환은 기존 ERP (Enterprise Resource Planning) 시스템과 새로운 어플리케이션 간 데이터 교환 방식이 갖는 문제점을 효율적인 해결 방안으로 제시 되었다. 따라서, XML은 어플리케이션 간 인터페이스가 필요 분야에서 해결책으로 제시되었으며, 다양한 시스템과 어플리케이션간 통합을 위한 통신 언어이다.

웹 서비스는 서로 다른 플랫폼에 서로 다른 언어로 작성된 프로그램들간 표준 기반으로 서로 통신할 수 있도록 상호 운용성을 제공해 준다. 기존 CORBA(Common Object Request Broker Architecture), RMI(Remote Method Invocation), DCOM(Distributed Component Object Model)에서도 같은 개념이 존재하지만, SOAP을 이용하면 확장성 및 유연성 제공되었다. 웹 프로토콜인 XML, HTTP 및 TCP/IP 사용함으로써 통신 프로토콜을 위한 제반 비용 낮아지는 장점이 있다. 그러나 웹 서비스는 보안에 취약점이 발견 되었다. 보안 문제는 외부의 불법적인 침입 방지나 통신 내용을 보호뿐 아니라 사용자 인증, 데이터 무결성 보장, 송수신 부인봉쇄등 다양한 충족 사항이 요구된다. 온라인 인증은 디지털 키 관리와 전자 서명 및 데이터 암호화 등의 통합 처리 기법이 사용되어야 하며, 다양한 어플리케이션간의 상호 호환성 또한 확보되어야 한다.

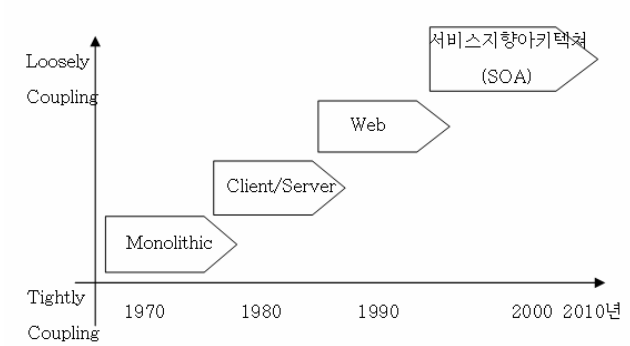
웹 서비스는 네트워크와 유연한 아키텍처를 통해 시간 및 장소, 어떤 장치의 구애 받지 않고 통합 서비스 환경을 지원해 준다. 기업 내부와 기업간 정보 교환 매우 효율적으로 전달 및 기업 내부의 효율성 증대, 새로운 사업의 기회를 창출 및 고객 요구에 좀더 빠른 대응이 요구 되고 있다. 특히, 웹 서비스는 새로운 시스템의 구축이 아니고 기존에 서비스 되고 있는 시스템을 통합 운영은 기업의 시스템 자원 관리 변화가 예상된다.

웹 서비스를 안전하게 구현하기 위해서는 네트워크 전송계층, OS, 응용 프로그램 레벨 등 다양한 관점에서 보안 사항을 고려해 보아야 한다. 그와 관련된 보안 기술도 고려해야 한다. 웹 서비스 개념과 함께 설계되고 있는 WS-Security 만으로는 광범위한 보안 요구 사항을 만족시킬 수 없으며, 현재 사용되고 있는 보안 기술과 WS-Security를 얼마나 적절히 혼합해서 사용하느냐에 따라 얼마나 안전한 웹 서비스를 구축 할 수 있는지 결정된다.

본 논문에서는 기존 시스템의 문제점을 파악하고 이를 해결하기 위해 웹 서비스 기반 시스템 구축에 필요한 보안 방안을 알아본다. 본 논문에서는 여러 가지 보안 기술 중 메시지 무결성, 기밀성, 사용자 인증 기능을 만족시키기 위해 제시된 WS-Security, XML Signature, XML Encryption에 대해서 자세히 알아보고 웹 서비스 시스템을 설계하고 구현한다.

2. 웹 서비스 선행 연구

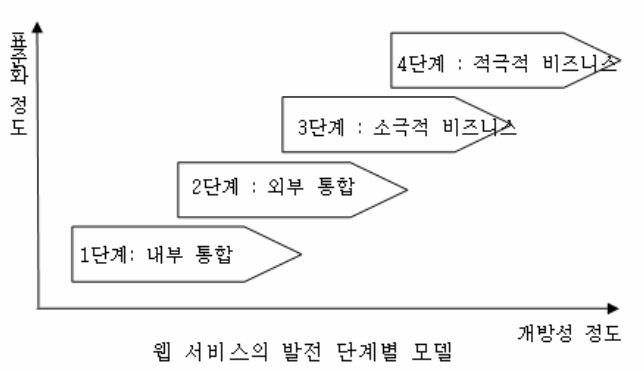
2.1 정보 시스템의 변화



시스템 환경 변화

2.2. 웹 서비스 보안 이슈 변화

웹 서비스는 웹 서비스들 간에 서로 연결이 가능하다는 특징을 가지고 있다. 이러한 웹 서비스의 특징은 보안에 대한 더 깊은 고려를 필요로 하며, 웹 서비스를 사용하는 유형별로 다양한 보안 요구 사항이 필요하다. 웹 서비스 모델을 바라보는 관점은 여러 가지가 있다.[11] 그 중 발전 단계별 웹 서비스 모델은 웹 서비스 모델을 1단계: 내부통합, 2단계: 외부 통합, 3단계:소극적 비즈니스, 4단계: 동적 비즈니스 네 가지 모델로 구분한다.



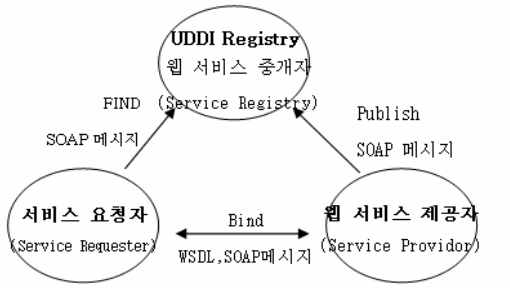
웹 서비스의 발전 단계별 모델

3. 웹 서비스 및 보안 관련 기술

3.1서비스 지향 아키텍쳐(SOA)

서비스 지향 아키텍처(Services-Oriented Architecture : SOA)는 서비스 통합 관점에서 각광 받고 있는 웹 서비스로 개념의 소프트웨어 아키텍처 이다.

SOA는 “서비스 제공자와 사용자가 합의된 계약(또는 인터페이스)을 통하여 유연하게 연계(Loosely coupled)된 소통을 지원하는 아키텍처를 만들기 위해 필요한 원칙들의 모음”으로 정의 된다.[1] 유연한 관계란 서비스 사용하는 자신이 필요로 하는 서비스의 가치에만 집중하고, 서비스 제공자는 사용자가 필요로 하는 서비스를 어떻게 구현할 것인가에 만 집중 하는 관계를 의미한다



웹 서비스 역할과 관련 표준 스펙

- 서비스 조립: 서비스는 다른 서비스와 조립할 수 있다. 이것은 로직이 다른 수준의 단위 정보로 표현되는 것을 허락하고 재사용과 추상화 계층의 생성을 장려한다.
- 서비스 자율성 : 서비스 로직은 명확한 경계 안에 존재한다. 서비스는 경계 안에서 독립적으로 구성되고 서비스가 통제를 실행하기 위해 다른 서비스에 의존 하지 않는다.
- 서비스 상태 정보를 유지하지 않는다. : 서비스는 느슨한 결합을 유지하는데 방해되는 상태 정보를 관리하지 않아야 한다. 특별한 경우에 상태 관리를 위임하더라도 서비스는 기본적으로 상태 정보를 관리하지 않도록 설계되어야 한다.
- 서비스 발견 가능해야 한다.: 사용하기를 원하는 서비스 요청자가 서비스를 발견하고 이해할 수 있어야 한다.
- 서비스 조립: 서비스는 다른 서비스와 조립할 수 있다. 이것은 로직이 다른 수준의 단위 정보로 표현되는 것을 허락하고 재사용과 추상화 계층의 생성을 장려한다.
- 서비스 자율성 : 서비스 로직은 명확한 경계 안에 존재한다. 서비스는 경계 안에서 독립적으로 구성되고 서비스가 통제를 실행하기 위해 다른 서비스에 의존 하지 않는다.
- 서비스 상태 정보를 유지하지 않는다. : 서비스는 느슨한 결합을 유지하는데 방해되는 상태 정보를 관리하지 않아야 한다. 특별한 경우에 상태 관리를 위임하더라도 서비스는 기본적으로 상태 정보를 관리하지 않도록 설계되어야 한다.
- 서비스 발견 가능해야 한다.: 사용하기를 원하는 서비스 요청자가 서비스를 발견하고 이해할 수 있어야 한다. [4]

서비스 발견 가능해야 한다.: 사용하기를 원하는 서비스 요청자가 서비스를 발견하고 이해할 수 있어야 한다. [4]

3.2 웹 서비스 및 보안 기술 분석

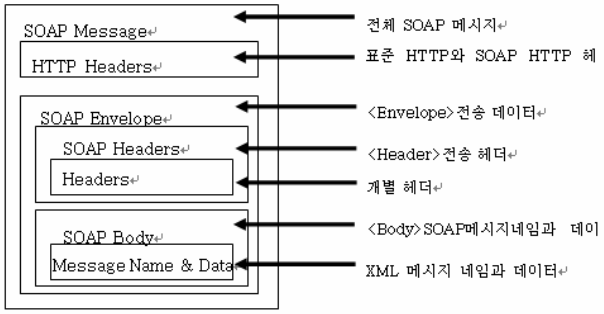
웹 서비스 보안은 하위계층인 네트워크 계층에서부터 전송계층, 어플리케이션 계층에 이르기 까지 여러 계층에서 처리될 수 있다. 보안 구현을 위해 XML 전자 서명을 이용하여 특정 부분에 대한 메시지 다이제스트를 생성하여 데이터를 구현 구분을 지원할 수 있으며, 시스템 보안 측면에서는 SSL, IPSec 보안 계층을 사용하여 보안 기술을 더욱 향상 시킬 수 있다.

3.2.1 웹 서비스 여러 기술

1)SOAP(Simple Object Access Protocol)

인터넷 표준인 XML 을 이용하여 웹 서비스 프로토콜로서 웹

서비스를 이용하기 위한 객체간의 통신 규격이다. 분산 환경에서 구조화된 정보를 교환하기 위한 목적으로 고안된 XML 기반의 경량 프로토콜이며, 단순성과 확장성을 설계 목적으로 사용한다



SOAP Message 구조

- Envelope : 메시지를 표현하는 XML 문서의 최상위 요소
- Header: 통신 주체들간에 사전 협의 없이 분산화 된 방법으로 특성들을 SOAP메시지에 추가하기 위한 필수 또는 선택적으로 나타내기 위해 사용될 수 있는 속성들을 정의한다.

2)WSDL(Web Services Description Language)

WSDL 은 SOAP메시지 집합과 해당 메시지가 교환되는 방법을 설명하는 XML 문서라고 할 수 있다. WSDL은 XML 문서로 되어 있어 해석 및 편집을 할 수 있다. XML 스키마 표준을 사용함으로써 다양한 플랫폼과 프로그래밍 언어에서 엑세스 할수 있는 웹 서비스 인터페이스를 정의하여 사용한다.

3)UDDI(Universal Description, Discovery, and Integration)

UDDI는 비즈니스 기업과 그들이 제공하는 서비스들에 대한 정보를 구조화된 방법으로 저장하는 개방형 레지스트리로 설계되어 있다. 클라이언트는 UDDI를 통해서 웹 서비스를 검색 할 수 있다. UDDI는 크게 서비스에 대한 기술, 탐색을 위한 표준 기반의 규격 부분, 웹 상에서의 비즈니스 레지스트리의 공동 운영 부분으로 이루어지며 XML 파일 형태로 되어 있다.

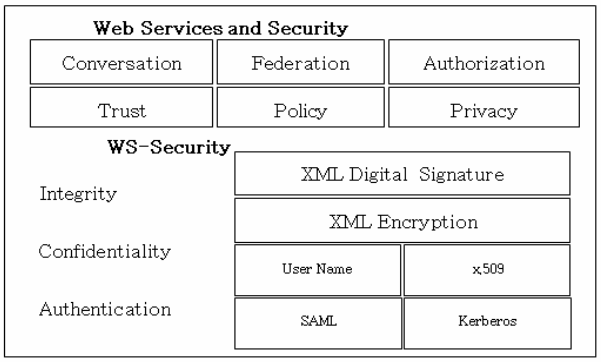
3.2.1 보안 기술 정의

- 암호화: 암호화란 메시지 내용을 타인이 볼 수 없게 인코딩하는 것을 정의 한다. 암호화는 실제로 공개키 기반 구조와 디지털 인증서의 사용에 있어서 중요한 위치에 있다.
- 비밀키 암호화 : 암호화와 복호화에 같은 키를 사용하는 방식이다. 예로 송신자는 전송하고자 하는 데이터를 키와 암호 알고리즘을 통해 암호문으로 변환해 수신자에게 전송하고 수신자는 동일한 키를 복호 알고리즘을 사용하여 원래의 평문으로 만들게 된다. 발신자와 수신자는 암호화를 통해 데이터 교환을 하기 이전에 안전하게 서로 키를 교환해야 한다.
- 공개키 암호화 :수학적 함수를 기반으로 하며 비밀키 암호화 방식과는 달리 두개의 키가 존재한다. 이중 하나는 누구든지 사용할수 있도록 공개하고, 다른 하나는 자신만이 알고 있는 것이다. 이때 공개되는 키를 공개키(Public key)라고 하고, 비밀스럽게 보관하는 키를 비밀키(Private key)라고 한다. 이러한 방식을 사용함으로써 비대칭적 암호화방식은 대칭적 암호화방식에서 문제된 키 관리와 분배의 문제점을 해결하고 있다.
- 디지털 서명: 디지털 서명(Digital Signature)란 비밀키를 이용하여 행한 서명과 원래의 변형되지 않은 문서 또는 데이터를 전송받은 수신인이, 서명한 사람의 비밀키에 대응하는 공개키를 사용하여 확인 절차를 거치는 공개키 암호화 방식과 값 변환 기능을 이용하여 문서 또는 데이터를 변환하는 전자서명의 한 유형이다.

4. 정보 보안의 방안

4.1 웹 서비스 및 WS-Security 보안 방안

4.1.1 웹 서비스 보안 스펙



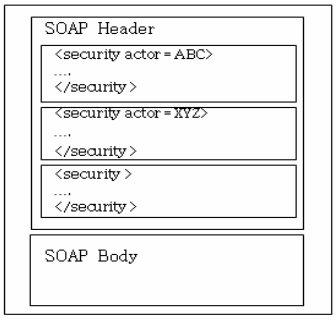
웹 서비스 보안 명세 구성

웹 서비스 보안 명세의 첫 번째 단계는 WS-Security 이다. WS-Security는 무결성과 기밀성을 제공하기 위해 SOAP을 어떻게 확장하고 메시지 내부에 보안 토큰을 어떻게 포함 하는지를 정의한다. 이는 X.509 인증서를 포함한 바이너리 포맷 데이터를 인코딩 방법에 대한 정의도 포함한다. 따라서 주 내용은 End-to-End 무결성 및 기밀성을 포함한 다중 보안 토큰, 신뢰 도메인, 암호화 기술을 지원하기 위한 명시 조건 등에 대한 기술이다.

WS-Policy	보안 수준에 대한 요구 사항, 제약조건, 정책 등을 규정한다.
WS-Trust	보안 도메인간 상호작용을 가능하게 하는 보안 신뢰 모델을 정의 한다
WS-Privacy	개인 정보에 대한 비밀성의 보안에 대해 정의한다.
WS-Federation	연합된 시스템간의 관계와 기타 정보 관리 방법을 정의한다.
WS-Authorization	웹 서비스 환경에서 권한 부여 데이터와 정책 관리방법을 정의한다.

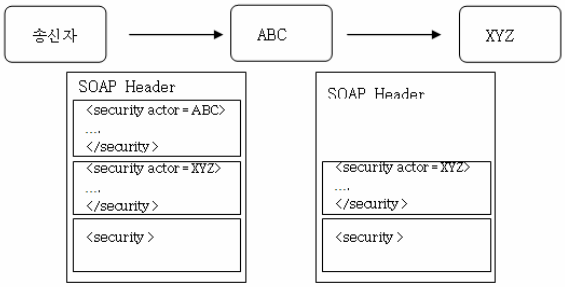
4.1.2 WS-Security

WS-Security는 2002년 4월 1.0 이 발표 되었다. 보호하고 사용되는 공개 키 등 키 정보를 안전하게 전파하는 데에 목적으로 두고 있다. XML-Signature, XML-Encryption 등 기존의 관련 표준을 모두 수용함으로써 기존 환경에 변화를 주지 않는다는 것이 특징이다.



SOAP 메시지의 Security

● SOAP 메시지의 Header 에 해당 메시지의 보안 관련 정보를 포함하는 Security 헤더를 두어 메시지 송신자의 신원정보, 송신자 인증, 무결성 인증과 관련한 정보들을 기록하고, Body에는 전송하고자 하는 내용과 이 내용을 암호화한 암호문을 저장한다. SOAP 메시지에 적용된 전자서명이나 암호문 생성 방법 또는 키 정보를 이 헤더 안에 저장할 수 있다.



처리된 Header 의 삭제

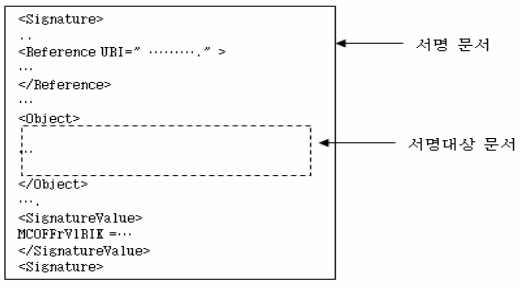
4.2 XML 정보 보안 방안

4.2.1 XML 전자 서명

XML 서명은 XML 형태로 전자 서명을 생성하고 표현하는 것을 기술하고 있는 W3C 권고안이다. 서명은 임의의 XML 데이터는 비XML 데이터로 나타낼 수 있다. 서명은 서명되는 데이터로부터 분리되거나 XML의 경우에는 서명되는 데이터가 XML 문서의 일부가 될 수 있다. 만일 서명이 분리되지 않는다면, 서명되는 데이터를 감싸거나 또는 서명되는 데이터에 의해 둘러 쌓여질 수 있다. 기본적으로 XML 서명키를 서명되는 데이터와 연관시켜는 방법을 정의한다

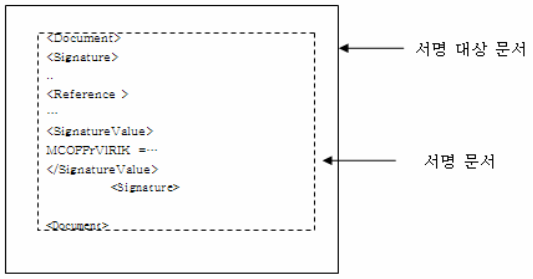
4.2.2 XML 전자 서명 기본 구조

● Enveloping Signature 형식의 XML 서명 문서



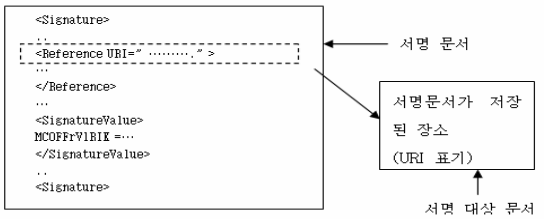
Enveloping Signature 형식의 서명 문서

● Enveloped Signature 형식의 XML 서명 문서



Enveloped Signature 형식의 서명 문서

● Detached Signature 형식의 XML 서명 문서



Detached Signature 형식의 서명

5. 결론

본 연구는 XML 기반 환경 하에서 서비스 통합은 유연한 결합성 및 호환성 제공되어 시스템 통합이 가능하게 되었다. 그러나 XML 기반 환경하에서 서비스지향 아키텍쳐의 통합은 보안에 대한 노출은 문제점의 해결이 과제로 남아 있었다. 데이터 연동 및 시스템 통합을 지향하기 위해 시스템은 항상 외부 시스템의 접근이 노출되었으며, 데이터 교환 및 변조 ,복제의 위험을 가지고 있었다. 앞 장에서 이 해결 방안으로 XML 문서 보안 및 XML 전자 서명의 구현 부분에 대해서 자세히 알아 보았다. 이로서 XML 문서 전자 서명의 구현 및 적용은 정보 보안의 해결책을 모색 하였다.

참고문헌

[1] Yefim V.Natis & Roy W.schulte,"Introduction to Service-Oriented Architecture"Gartner,2003.4
[2] 한국전산원, " 공공부문 SOA 도입전략" 2004
[3] BEA. SOA White Paper, 2005
[4] SOA 서비스 지향 아키텍처 : XML과 웹 서비스 통합을 위한 필드 가이드 지은이: 토마스 얼
[5] 김주한 외" 웹 서비스 보안 기술의 표준화 및 시장 동향" , 전자통신동향분석,2005년 2월
[6] W3C Proposed Recommendation,"XML Signature Syntax and Processing," February 2002
[7] 한국전산원" 차세대 웹서비스 표준화…" 2004
[8] 정보통신통신기술협회, "ebXML 비즈니스 트랜잭션 수행을 위한 XML 기반 보안 기술 적용 지침", 2003년 10월
[9] 공공정보화 웹 서비스 도입방안 연구 /한국전산원 한국전산원, 2003
[10] 웹 서비스 확산발전 방안 연구 /류광택 [저] 한국전산원, 2004
[11] 웹 서비스의 현황 및 비즈니스 모델의 변화 : 정보통신정책연구원