웹 서비스 기반 보안 토큰을 이용한 통합 인증 모델 설계

강철수° 이상훈 전문석
숭실대학교 통신연구실
luckix@hanafos.com°, iam@leesanghun.pe.kr, mjun@computing.ssu.ac.kr

Web Service-based Design of Integrated Authentication Model using Secure Token

Chul-Su Kang° Sang-Hun Lee Moon-Seog Jun
Dept. of Computing, Soongsil University

요 약

웹 서비스는 최근 가장 주목받고 있는 기술 중 하나이다. 오늘날 웹 서비스는 간단한 데이터 공유에서부터 대규모의 인터넷 판매 및 통화 교환, 애플리케이션 통합 시나리오의 범주까지 다양한 분야에서 전개되고 있다. 또한 웹 서비스는 모바일, 디바이스, 그리드 시나리오 등에도 적용되고 있다. 현재 웹서비스는 이기종간에 구축된 서비스를 통합하고 호환시키는데 많은 중점을 두고 있다. 여기서 반드시 필요한 부분이 이 이기종 간의 인증 부분이다. 서로 다른 시스템에 접근하기 위해서 사용자는 여러 번의 인증절차를 거쳐야 한다. 본고에서는 사용자의 인증절차를 통합하고, 접근 권한에 대한 제어를 위해 WS-Security의 표준안에 포함된 보안 토큰을 이용한 통합 인증 모델을 제시하고자 한다.

1. 서 론

최근까지 IT분야의 눈부신 발전과 더불어 인터넷의 급속한 확산으로 인하여 인터넷을 이용한 e-business는 매년 눈부신 성장을 하고 있다. 이러한 환경에서 가장 주목 받고 있는 기술이 '웹 서비스'이다.

오늘날 많은 분야에서 웹 서비스를 통해 기존의 각기 다른 환경에서 구현된 애플리케이션을 하나로 통합하려는 시도가 나타나고 있다. 서로 다른 서비스가 통합됨에 따라 각 서비스에 접근할 때 마다 로그인을 해야 하는 다중 인증 절차와 각 서비스마다 사용자에 대한 접근을 달리해야 하는 접근 제어에 대한 문제가 발생했다. 이러한 문제점에 대해 2004년 5월 OASIS에서는 SOAP Message에 대한 표준인 WS-Security 1.0을 발표 하고 인증절차를 위한 보안 토큰을 제시하였다.

본 논문에서는 WS-Security에서 제시한 보안토큰에 접근제어 정보를 포함한 보안토큰을 이용하여 인증절차를 간소화하고 사용자에 대한 권한 제어를 포함하는 통합 인증 모델을 제시하고자 한다.

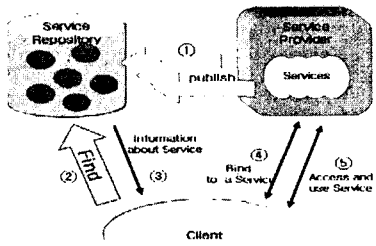
2장에서는 웹서비스에 관련된 전반적인 사항과 보안토큰에 관련된 연구를 살펴보고, 3장에서 보안토큰을 이용한 통합인증 모델을 제시하고, 4장에서 본 논문에 대한 결론과 앞으로의 발전방향을 제시하고 끝맺도록 하겠다.

2. 관련연구

웹 서비스는 표준화된 XML 메시지를 통해 네트워크 상에서 접근 가능한 연산들의 집합을 기술하는 인터페이스로 정의된다[1]. 본장에서는 현재 웹 서비스에 관련된 기술들을 알아보도록 하겠다.

2.1 웹서비스 개요

최근 들어 IT업계에서 화두가 되고 있는 웹 서비스(Web Services) 기술은 W3C(World Wide Web Consortium)에서 '인터페이스와 바인딩(binding)이 XML(eXtensible Markup Language)에 의해 정의되고 기술되며 탐색이 가능하고 URI(Uniform Resource Identifier)에 의해 식별이 되며, 인터넷 기반의 프로토콜을 통해 XML 기반의 메시지들을 이용하여 다른 소프트웨어 애플리케이션들과 직접적인 상호작용이 가능하도록 지원을 해주는 하나의 소프트웨어 애플리케이션[2]'으로 정의하고 있다.



[그림 1] 웹 서비스 기본 구조

서비스 요청자(Service Requester)는 개발자 관점에서 볼 때 웹 서비스를 찾고 호출하는 애플리케이션으로 서비스가 공개된 Repository에서 검색(Find)하여 서비스의 세부사항을 알아낸 다음 원하는 서비스에 바인딩(Binding)하여 실제로 해당 서비스의 기능을 이용하는 것이고, 서비스 제공자(Service Provider)는 웹 서비스로서 소프트웨어 애플리케이션을 제공하는 비즈니스 엔터티로서 비즈니스 관점에서는 웹 서비스의 소유주이며 개발자 관점에서는 웹 서비스를 호스팅 하고 있는 플랫폼이다. 웹 서비스 제공자는 웹 서비스를 사용할 수 있도록 서비스의 기능을 기술(describe)한 다음 접근할 수 있는 레지스트리에 웹 서비스의 세부사항을 공표

(publish)해야 한다. 마지막 요소인 서비스 브로커 혹은 서비스 레파지토리는 검색이 가능한 웹 서비스 저장소로서 서비스 제공자의 서비스의 세부사항(회사의 상세정보, 서비스 자체의 정보)등을 올려두고 서비스 요청자의 원하는 서비스를 발견하는 장소로서 무역에서 보면 중계무역상이나 검색엔진 혹은 쇼핑몰 등이 이에 해당한다고 하겠다. 이러한 웹 서비스 구조의 3가지 요소는 모두 상호 독립적이며 이들 간의 통신과정은 XML를 통해 보안적인 측면과 표준화를 통한 유연성을 확보하고 있다[3].

2.2 웹서비스 핵심 기술 요소

-WSDL(Web Service Description Language)

XML 기반의 웹서비스 기술 스크립트 언어로 웹서비스에 접촉하고 이용하기 위한 메시지 스키마을 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.[4]

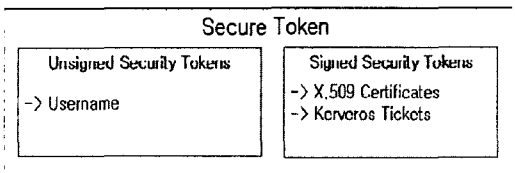
-UDDI(Universal Description, Discovery and Integration)

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.[5]

-SOAP(Simple Object Access Protocol)

XML기반 프로토콜로 복잡한 객체 데이터 타입도 쉽게 모델링 할 수 있게 해주며 RPC 프로토콜을 지원한다. HTTP뿐 아니라 FTP, SMTP, POP3등 기존의 프로토콜 상에서 동작 하므로 부가적인 비용이 발생하지 않으며 특정 벤더에 종속되 않는 공개 프로토콜로 웹서비스에서 사용되는 모든 메시지는 SOAP를 사용하여 통신한다.[6]

2.3 보안 토큰



[그림 2] 보안 토큰[7]

보안 토큰은 인증된 토큰(Signed Security Tokens)과 인증되지 않은 토큰(Unsigned Security Tokens)으로 나뉘어 진다. 인증되지 않은 토큰은 인증기관에 의해 승인되지 않은 보안 토큰으로, 보안 등급이 낮은 경우에 적용할 수 있는 정보로서, *Username* 정보가 있다. 인증된 토큰은 인증기관에 의해 승인되고, 그 인증기관에 의해 암호학적으로 서명된 토큰으로 X.509인증서[8]와 커버로스 티켓[9]등이 있다.

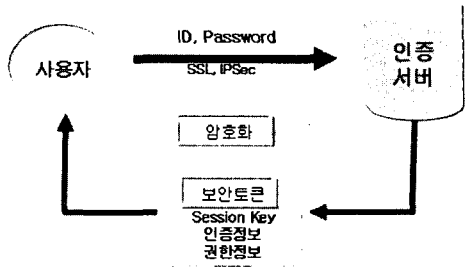
- 보안토큰 생성 절차

사용자가 여러 서비스로 구성된 웹서비스에 접근하고자 한다.

① 사용자는 ID, Password로 인정서버를 통해 인증 받음.

② 인증서버는 사용자에게 Kerveros Tickets, Session Key, 사용자 고유 ID, 사용자 권한 정보등을 담은 보안 토큰을 제공한다.

③보안 토큰은 암호화 되어 SOAP메시지에 포함된다.

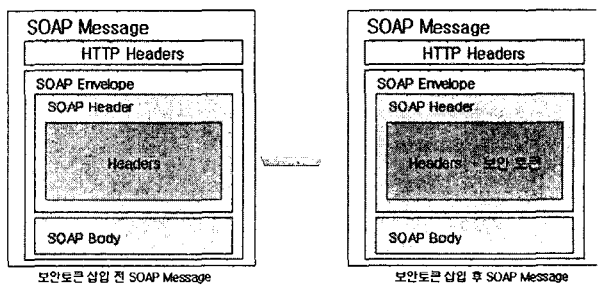


[그림 3] 보안 토큰 생성

위의 과정을 통해서 사용자는 보안토큰을 요청하게 되고 발행된 토큰은 SOAP메시지 전송에 대한 인증정보 및 권한 정보를 포함 하게 된다. 이 모든 과정은 SSL, IPSec과 같은 신뢰성 있는 경로를 통해 이루어 져야 한다.

3. 보안 토큰을 이용한 통합 인증

사용자가 여러 번의 인정과정을 거칠 필요 없이 구축된 인증 시스템을 통해 권한을 부여 받고 인증을 하는 방식을 통합 인증이라고 할 수 있다. 보안 토큰은 SOAP 메시지의 Envelope의 헤더부분에 삽입된다. 사용자는 자신이 부여받은 보안 토큰을 통해 인증과 동시에 권한을 부여 받게 되고 시스템은 사용자의 보안토큰을 통해 인증 및 접근제어를 하게 된다.



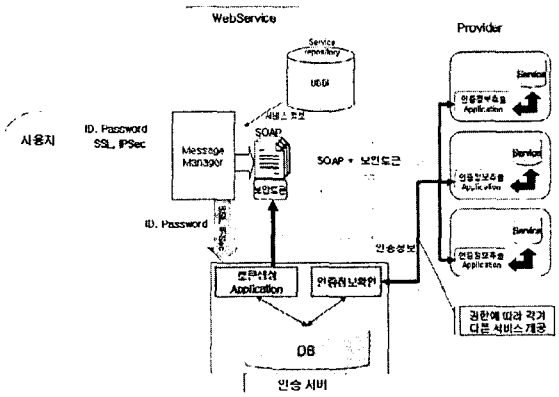
[그림 4] SOAP Message

3.1 인증 및 권한 요청

통합 인증 시스템은 보안 토큰을 포함한 암호화된 SOAP 메시지를 복호화 하고 포함된 보안 토큰을 참조하게 되고, 보안 토큰의 인증 정보를 인증서버에 전송한다. 서버에서 인증이 되면 사용자의 권한을 참조하게 된다. 여기서 보안토큰을 참조한 시스템은 보안토큰을 조작할 수 없다. 이 SOAP 메시지가 다른 서비스를 제공하는 시스템에 전송되더라도 포함된 보안토큰은 변경되지 않는다.

3.2 통합 인증 모델

앞서 2.3장에서 설명한 보안토큰과 인증 및 권한 요청을 포함하는 전체적인 통합 인증 모델을 제시하고자 한다. 전체적인 구조는 인증서버는 웹서비스에 대한 전체적인 인증을 담당하며 사용자는 여러 서비스에 접근 하더라도 서비스 제공자들은 사용자에게 반복적으로 인증을 요청하지 않고 인증 서버를 통해 사용자를 인증하고 권한을 제어한다.



[그림 5]웹 서비스 통합 인증 모델

사용자는 SSL, IPSec과 같은 신뢰성 있는 경로를 통해 사용자 정보를 제공하고 인증서버는 토큰생성 어플리케이션을 통해 사용자에게 보안 토큰을 제공한다. 제공된 보안토큰은 SOAP 메시지에 암호화 되어 삽입되며 SOAP 메시지는 신뢰성, 무결성, 부인 방지 등을 위해 다시 암호화와 서명 단계를 거쳐서 전송된다. 전송된 SOAP 메시지는 복호화 되고 서비스의 인정정보 추출 어플리케이션을 통해 인증정보를 추출한다. 추출된 인증정보는 인증서버에서 인증을 받게 되며 인증이 성공적으로 이루어 졌다면 서비스 제공자는 사용자의 리소스 접근 권한을 확인 후 서비스를 제공하게 된다. 하지만 인증이 제대로 이루어 지지 않는다면 SOAP 메시지는 삭제되고 접근을 거부하게 된다.

4. 결론 및 향후 발전 방향

본 논문에서는 웹서비스에서의 인증절차를 줄이기 위한 통합 인증 모델을 제시하였다. SOAP 메시지에 보안토큰을 같이 암호화 시켜 전송함으로서 보안토큰에 포함된 인증정보가 사용자의 로그인 정보를 대신하고 권한 정보를 통해 사용자의 접근 권한을 제어할 수 있도록 하였다. 이로 인해 사용자는 이 기종 간에 구축된 서비스에 접근 할 때 마다 해야 했던 인증과정을 한 번의 인증과정만을 함으로 사용자의 불편함을 줄일 수 있게 되었다. 인증 과정을 통합하고 줄였지만 보안토큰을 암호화하고 다시 보안토큰을 포함하는 SOAP 메시지에 대해 암호화와 서명 단계를 거침으로 보안 토큰의 무결성, 기밀성등 신뢰성에는 문제가 없다.

앞으로 본 논문에서 제시한 방안에서 여러 번의 암호화와 복호화로 발생할 수 있는 속도의 문제점을 개선하여 보다 신뢰성 있고 신속한 시스템을 만들 수 있도록 연구해야 할 것이다. 또한 보안 토큰이 아닌 다른 인증정보를 통한 여러 방안을 제시하고 본 논문에서 제시한 방법과의 비교를 통해 효율적인 방안을 찾아 나가는 노력을 기울여야 할 것이다.

참 고 문 헌

[1]David Orched, "Web Services Pitalls", http://xml.com/pub/a/2002/02/06/webservices.html, XML.com,Feb,2002

[2]http://www.w3.org/2002/ws/arch/2/06/wd-wsa-arch-20020605.html

[3]문기영, 박남제, 송유진, 손승원, 박치항, "안전한 XML 기반 웹서비스를 위한 웹 애플리케이션 보안 프레임 워크", 정보보호학회, 13권 6호,79-91, 2003.2.

[4]WSDL, http://www.w3.org./TR/wsdl

[5]UDDI, http://www.oasis-open.org/committees/uddi-spec

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

[7]Security in a Web Services World: A Proposed Architecture and Roadmap http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwssecur/html/securitywhitepaper.asp

[8]IETF, "Internet X.509 Public key Infrastructure Certificate and CRL Profile", Jan 1999, http://www.ietf.org/rfc/rfc2459.txt

[9]IETF, "The Kerberos Network Authentication Service(V5)", Sep 1993, http://www.ietf.org/rfc/rfc1510.txt