웹 서비스 상에서 안전한 서비스 등록 절차에 대한 연구

정혜련*, 서인석*, 윤혁중*
*한국전자통신연구원 부설 국가보안기술연구소
e-mail : hrchung@etri.re.kr

A Study of secure service registration on Web Service

HyeRyoun Chung*, InSeok Seo*, HyukJoong Yoon*
*National Security Research Institute

요 약

전자상거래가 활성화되고 이를 위한 표준화가 활발히 진행되면서 웹 서비스는 ebXML 과 함께 전자상거래의 대표적인 표준으로 자리매김하고 있다. 웹 서비스의 여러 표준 중 UDDI 는 서비스를 등록하는 레지스터리로 전화번호부와 같은 역할을 수행한다. UDDI 에 서비스를 등록하거나 수정, 삭제하는 경우 UDDI 레지스토리는 서비스 제공자에 대한 인증을 통해 등록된 서비스가 안전함을 보장해야 한다. 본 논문에서는 UDDI 레지스토리가 가져야 하는 보안요구사항을 분석하고, 기존 PKI 의 CA 을 연계하여 이를 해결할 수 있는 안전한 인증방안을 제시한다.

1. 서론

인터넷을 통한 전자 상거래가 활발해 지고, B2B 협업이 일반화되면서 이들 서비스를 등록, 검색할 수 있는 레지스터리의 필요성이 점차 높아지고 있다. 이러한 기능의 제공을 위해 웹 서비스는 UDDI 라는 기술을 제시하고 있다. UDDI 는 웹 서비스와 서비스를 제공하는 비즈니스를 등록하고 검색할 수 있는 방법을 제공하는 분산 레지스터리의 표준으로 WSDL, SOAP 과 함께 웹 서비스의 분야의 핵심 기술이라 할 수 있다.

기업은 자신이 제공하는 서비스를 UDDI 에 등록하고 사용자는 UDDI 를 검색함으로써 필요로 하는 서비스 제공자를 찾을 수 있다. 이와 함께 UDDI 는 각 레지스터리 노드 간의 데이터 복제를 통하여 여러 레지스터리 노드들이 서로 비즈니스 정보를 공유할 수 있도록 함으로써 글로벌 비즈니스를 가능토록 한다.

이미 Microsoft 와 IBM 이 각자의 사이트에서 UDDI 을 적용하고 있으며, 서로간의 미러링도 지원하고 있다. 또한 국내에서도 국내 웹 서비스 등록 및 체계적인 관리를 지원하기 위한 '웹서비스등록관리센터(WSRC-가칭)'을 오는 12 월에 설립키로 했다.

웹 서비스의 확대와 함께 UDDI 의 필요성 또한 절실해 지고 있는 실정이지만, 실제적으로 UDDI 를 어떻게 운영할 것인지, 어디에 위치할 것인지에 대한 구체적인 방법이 제시되고 있지 않다. 특히 보안에 대한 개념은 거의 전무하다고 할 수 있다. UDDI 명세 3.0 이 발표되면서 UDDI 보안에 대한 고려가 이루어지긴 하였지만 웹 서비스의 가장 큰 장점인 확장성과 유연성을 위해 보안 측면에서조차 개념적인 이론만을 제공할 뿐이다.

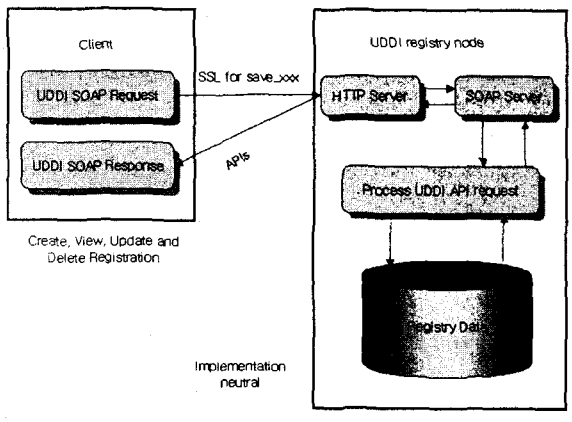
본 논문에서 서비스 제공자가 UDDI 에 서비스를 등록하거나 삭제, 수정하고자 할 때 사용자의 신원증명을 통해 악의적인 사용자가 거짓 서비스를 등록하거나 등록되어 있는 서비스를 변조, 삭제하는 것을 막을 수 있는 방법을 제안한다. 본 논문의 구성은 다음과 같다. 2 장에서는 UDDI 표준을 통해 UDDI 의 역할 및 개념에 대해 알아보고 3 장에서는 UDDI 가 가져야 하는 보안 요구사항과 이를 해결하기 위해 UDDI 명세 3.0 에서 정의된 정책 및 WS-Security 에서 정의된 보안토큰에 대해 검토한다. 마지막 4 장에서는 3 장에서 제시한 UDDI 보안 요구사항을 PKI 의 CA 시스템과 연계함으로써 안전한 서비스의 등록, 삭제, 수정할 수 있는 인증방법을 제시하고 5 장에서 이에 대한 결론을 도출한다.

2. UDDI

UDDI(Universal Description, Discovery, and Integration)는 인터넷 상의 전 세계 비즈니스 목록에 자신을 등재하기 위한 XML 기반의 레지스터리이다. UDDI 의 궁극적인 목표는 각 기업들이 웹 상에서 서로를 찾을 수 있도록 함으로써 온라인 트랜잭션을 간략하게 하기 위함이다. 서비스 개발자 및 제공자는 UDDI 비즈니스 레지스토리에 자신의 웹 서비스 정보를 등록하게 된다. 서비스 이용자는 어떠한 비즈니스 특정 서비스를 제공하는지 검색하거나, 특정 형식의 서비스를 제공하거나 특정 산업 분류에 속하는 기업을 검색하기 위해 또는 웹 서비스를 이용하기 위해 필요한 기술적인 상세 정보를 얻기 위해 UDDI 비즈니스 레지스토리를 사용할 수 있다.

UDDI 의 작동방법을 순서적으로 살펴보면 다음과 같다

1. 소프트웨어 회사와 표준기구 및 프로그램 개발자들은 tModel 로 정의되는 서비스 기술 모델을 레지스토리에 등록한다.
2. 기업들은 그들이 제공하는 비즈니스와 서비스의 기술을 UDDI 레지스토리에 등록한다.
3. UDDI 는 Unique Universal Identifier (UUID) 키로 알려진 프로그램식의 독특한 식별자를 할당함으로써 이러한 모든 엔터티를 계속적으로 유지한다.
4. 전자 상거래, 검색엔진, 비즈니스 어플리케이션 같은 기타 클라이언트들은 관심 있는 서비스를 발견하기 위해 UDDI 레지스터리를 사용한다.
5. 차례로 다른 비즈니스들은 이러한 서비스들을 호출하여 간단하고 동적인 통합(binding)을 수행한다.



[그림 1]클라이언트와 레지스토리 간 UDDI 흐름

UDDI 의 작동 순서에서 살펴보았듯이 UDDI 레지스토리에는 그들이 지원하는 비즈니스 및 서비스의 기술(description)이 포함되어 있다. 또한 웹 서비스가 지원하는 산업용 표준에 대한 참조, 분류법 정의, 식별 시스템을 포함하고 있다. UDDI 는 프로그래밍 모델과 스키마를 제공하고 이것은 레지스터리를 사용하여 규칙을 정의한다. UDDI 표준의 모든 API 는 XML 로 정의되어 있고, SOAP envelope 으로 싸여 있으며, HTTP 를 통해 전송된다. [그림 1]은 UDDI 의 메시지 전송을 나타낸다. 클라이언트가 HTTP 를 통한 클라이언트의 SOAP 요청을 레지스토리 노드로 전송하면 레지스터리 서버의 SOAP 서버는 UDDI SOAP 메시지를 관리하고 처리하며 클라이언트로 SOAP 응답을 반환한다. 레지스터리 정책상 데이터를 수정하도록 하는 클라이언트 요청은 보안 및 인증 처리가 된 트랜잭션이 되어야 한다.

서비스 개발자는 SOAP 요청 메시지를 통하여 서비스를 등록, 삭제, 수정 할 수 있다. 이러한 단계에서 UDDI 레지스토리는 보안 및 인증을 수행하여만 한다. 다음 장에서는 UDDI 레지스토리에 서비스를 등록하거나 삭제, 수정하고자 할 때 요구되는 보안 요구사항에 대해 논의하고 이를 해결하기 위해 제시되고 있는 해결방법을 살펴본다.

3. UDDI 레지스토리의 보안요구사항

UDDI 레지스토리가 가져야 할 보안 요구사항은 데이터의 관리, 사용자의 신원확인, 사용자 인증 및 인가, 메시지의 비밀성 및 데이터의 무결성 등을 꼽을 수 있다. UDDI 명세 3.0 은 이와 같은 보안 요구사항을 위해 많은 부분 보안 취약성을 해결하기 위한 노력을 하였는데, 취약한 보안을 해결하기 위해 다양한 정책과 discard_authToken 과 get_authToken 의 보안 정책 API 을 정의하고 있다.

UDDI 명세 3.0 은 레지스터리에 있는 데이터의 정확도를 결정하기 위하여 모든 핵심 데이터 유형의 디지털 사인 지원을 추가하여 데이터 무결성과 신뢰성을 보장토록 하였다. 또한 인증 및 데이터 접근을 위해 하나 이상의 신원확인 시스템 통합을 허용하고 있으며 신원확인 시스템은 UDDI 명세 3.0 에서 정의하고 있는 보안 정책 API 을 통해 접근 제어를 제공할 수 있다.

UDDI 명세 3.0 은 보안을 위해 정책적인 측면을 강조하고 있다. 여러 정책들 중 우리는 등록과 사용자 및 프라이버시 권한에 대한 정책에 집중할 필요가 있다. 해당 정책들은 authInfo element 을 제공하는 API 을 이용하여 획득함으로써 사용자의 신원확인과 인증, 인가를 수행한다. UDDI 명세 3.0 에서 사용되는 authInfo element 의 개념은 WS-Security 에서 사용되는 보안 토큰과 유사한 개념으로 보안 토큰은 사용자의 신원확인 정보를 포함한다.

본 논문에서는 WS-Security 에 정의된 보안토큰을 UDDI 에 서비스 등록, 삭제, 수정시 필요한 사용자 신원 정보로 사용함으로써 안전한 인증 절차를 통해 UDDI 보안 취약성을 해결하고자 한다.

이를 위하여 본 장에서 WS-Security 의 보안 토큰에 대해 알아봄으로써 다음 장에서 제안하게 될 안전한 인증방법에 대한 기초를 마련한다.

보안 토큰은 보안 관련 정보의 표현으로 X.509 인증서, Kerberos 티켓과 인증자, SIM 카드의 모바일 장치 보안 토큰, 사용자명등 여러 가지 형태로 표현될 수 있다. 서비스 제공자는 보안 토큰을 메시지와 결합시키고 소유증명함으로써 자신이 정당한 사용자임을 증명할 수 있다. 이 때 사용되는 보안 토큰은 이미 기존 프로토콜을 사용하여 신뢰할 수 있고 안전하게 제공되었다고 가정한다. 보안토큰을 발행받고 사용하는 방법은 다양한 시나리오가 존재하며, 종류가 다른 보안 토큰간의 연계를 위한 신임연합에 대해서도 소개하고 있다.

본 논문에서는 사용자의 신원확인을 위한 보안토큰을 X.509 인증서로 적용하고, 신원증명 시스템을 PKI 의 CA 와 연계시킴으로써 기존 프로토콜을 적용할 수 있도록 제안할 것이다. 해당 프로토콜에서 PKI 의 CA 시스템은 보안 토큰 브로커가 된다. PKI 의 CA 시스템은 신뢰성 있는 기관으로 보안 토큰 브로커로써의 조건을 충족할 수 있으며 X.509 의 인증서를 발행하는 기관이므로, 보안토큰 발행에 관한 부하를 최소화할 수 있다는 장점을 가진다. 다음 장에서 CA 시스템을 보안 토큰 브로커로 활용하여 인증을 수행함으로써 안전한 서비스를 등록, 삭제, 수정하는 절차에 대해 논의할 것이다.

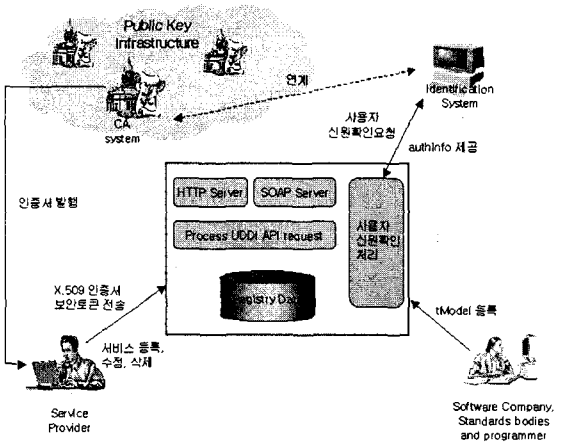
4. 안전한 서비스의 등록, 삭제, 수정 절차

3 장에서 설명하였듯이 UDDI 명세 3.0 은 보안상 취약한 부분을 해결하기 위해 기존 명세보다 정책 부분에 상당한 노력을 할애함으로써 보안상 취약성을 해결하기 위한 노력을 하였다. 이와 함께 OASIS 는 WS-Security 을 통해 웹 서비스 전반에 대한 보안에 대해 기술함으로써 웹 서비스의 가장 큰 문제점인 허술한 보안을 해결하기 위해 많은 표준기관과 업체들이 노력하고 있음을 알 수 있다.

그러나 UDDI 명세 3.0 이나 WS-Security 에 제안된 취약성 해결 방안들은 웹 서비스의 가장 큰 장점인 유연성과 확장성을 위해 광범위하게 기술함으로써 실제 UDDI 레지스토리를 사용함에 있어서 적용하기 다소 어려운 부분이 있다.

본 논문에서는 UDDI 명세 3.0 의 신원확인 시스템과 PKI 의 CA 와 연계시키고 CA 에서 발행한 X.509 인증서를 보안토큰으로 사용하여 안전한 인증 절차를 제안하고자 한다. 이는 기존 시스템을 활용하여 구축 시 소요되는 비용을 최소화하고 보다 잘 적용할 수 있도록 하기 위함이다. 제안되는 인증 절차에서 CA 시스템과 UDDI 레지스토리, 인증 시스템은 모두 신뢰할 수 있는 기관으로 가정하며, 서비스 제공자와 UDDI 레지스터리 간, UDDI 레지스터리와 신원확인 시스템간의 모든 트랜잭션은 SSL/ TLS 또는 GSSAPI 와 같은 기존 프로토콜에 의해 보호된다고 가정한다.

[그림 2]는 서비스 제공자가 서비스를 등록, 삭제, 수정하기 위해 수행해야 하는 일련의 절차를 나타낸다. 소프트웨어 업체와 표준 단체, 프로그래머들은 tModel 을 UDDI 레지스토리에 등록한다. 서비스 제공자는 등록된 tModel 에 맞추어 자사에서 제공하는 서비스를 등록하거나 수정, 삭제하게 된다. 해당 작업 수행시 서비스 제공자는 UDDI 레지스터리에 의해 신원을 확인 받는 인증 절차를 거쳐야만 한다.



[그림 2] 서비스의 등록, 수정, 삭제 절차

이를 위해 서비스 제공자는 기존 CA 시스템으로부터 발행 받은 X.509 인증서를 이용하여 보안토큰을 구성한다. UDDI 레지스터리로 최초 서비스 등록 혹은 수정, 삭제 요청 메시지를 전송할 때 서비스 제공자는 X.509 인증서 기반의 보안토큰을 UDDI 레지스터리로 전송한다. 보안토큰을 수신한 UDDI 레지스토리는 보안토큰 정보에 근거하여 신원확인 시스템으로 get_authToken 요청 메시지를 보냄으로써 사용자의 신원확인 정보를 얻고자 한다. get_authToken 메시지를 수신한 신원확인 시스템은 CA 시스템과 연계하여 보안토큰으로 수신한 X.509 인증서가 유효한지 검사하여 적합한 사용자인지 검증한다. 적합한 사용자임이 판별되면 신원확인 시스템은 authInfo element 를 UDDI 레지스토리로 전송한다. 신원확인 시스템에 의해 적합한 사용자임이 판별된 사용자는 이후 서비스 등록, 수정, 삭제 작업을 수행할 수 있다. 만약 신원확인 시스템에 의해 적합하지 않은 사용자로 판별되면 해당 세션을 강제 종료되고, 서비스 등록자는 서비스의 등록, 수정, 삭제 작업을 수행할 수 없게 된다.

이와 같은 시스템 구성은 기존 PKI 를 적용함으로써 보안토큰 브로커의 구축 비용을 최소화 하고 안전한 서비스 등록이 가능토록 한다. 또한 WS-Security 의 보안 토큰 개념과 UDDI 명세 3.0 의 신원확인 시스템을 적용함으로써 제안된 표준에 적합한 시스템 구성이 가능하게 된다.

5. 결론

본 논문에서는 UDDI 보안요구사항 중 특히 서비스를 등록하고,. 삭제 및 수정할 때 요구되는 사용자의 신원확인 및 사용자 인증, 인가에 대해 집중하여 신원확인 시스템과 UDDI 레지스토리의 상호 작동 방법 및 데이터 교환 방법 등을 제시함으로써 안전한 서비

스 등록을 위한 방안을 제시한다. 이를 위하여 1 개 이상의 신원확인 시스템을 수용하며, WS-Security 에서 제시된 보안토큰 개념을 사용한다.

사용되는 신원확인 시스템은 기존 PKI 의 CA 시스템과 연계된다. 본 논문에서 CA 시스템은 보안 토큰 브로커로써 이미 신뢰할 수 있는 기관이며, 보안 토큰의 한 종류인 X.509 인증서를 발행하는 기관이므로 보안 토큰 브로커의 조건을 모두 충족한다고 할 수 있다. 또한 기존 프로토콜을 수용함으로써 보안 토큰 브로커를 구축하는데 소요되는 비용을 최소화 할 수 있다.

그러나 이로써 모든 UDDI 의 보안요구사항이 충족된다고 할 수는 없다. 서비스를 등록하고, 검색하는 트랙잭션의 보호 뿐 아니라, UDDI 레지스토리 자체 보안 또한 무시할 수 없는 요소이며, X.509 보안토큰이 아닌 이종의 보안 토큰을 사용하는 서비스 제공자가 서비스를 등록하기 위해 보안 토큰간의 신임연합을 고려해야만 한다. 이 밖에도 UDDI 레지스토리와 신원확인 시스템의 운영 주체를 결정하는 문제 등도 UDDI 레지스토리 보안을 위해 간과할 수 없는 부분이다.

향후 UDDI 레지스터리 자체 보안과 보안 토큰간 신임연합을 위한 프로토콜 확대에 대한 연구와 함께 신원확인 시스템 구축을 통하여 보다 안전한 UDDI 서비스를 사용할 수 있도록 지속적인 연구를 수행할 예정이다.

참고문헌

[1] http://www.microsoft.com/
[2] http://www.w3.org/
[3] http://www.oasis-open.org
[4] http://www.ibm.com
[5] http://www.uddi.org/
[6] UDDI version 3.0 UDDI Spec Technical Committee Specification
[6] C# Web Service, Ashin Banerjee, Wrox
[7] Security in a Web Service World: A proposed Architecture and Roadmap, A joint Security Whitepaper From IBM corporation and MS corporation, April 7 2002
[8] Web Service Security (WS-Security), Bob Atkinson, Giovanni Della et al, December 18, 2002
[9] Internet X.509 Public Key Infrastructure Qualified Certificates Profile, S. Santesson, et al, March 2000
[10] WS-Security Profile for XML-based Tokens, Phillop Hallan-Baker, Maryann Hondo et al, August 28 2002