웹 서비스를 위한 통합접근 관리 연구

유석환° 차무홍 신동일 신동규
세종대학교 컴퓨터공학과
{shwyu°, bidon, dshin, shindk}@gce.sejong.ac.kr

A study of EAM for Web Service

SeokHwan Yu°, Moo-hong Cha, Dongil Shin, Dongkyoo Shin
Dept of Computer Engineering, Sejong University

요 약

오늘날 웹 서비스는 많은 관심을 받으며 발전하고 있다. 이러한 발전과 함께 다양한 시스템과 다양한 사용자를 관리해야하는 어려움 또한 직면한 상태이다. 각각의 시스템에서 사용자를 별도로 관리하는 것은 보안상의 문제뿐아니라 유지보수면에서도 비 효율적인것이다. 사용자 또한 여러 시스템에서 각각의 인증을 받는 불편함이 있다. 따라서 기업내의 모든 자원과 사용자에 대한 통합을 통해서 일관된 자원 및 사용자를 관리 가능하게하는 통합접근관리 기술의 도입이 보안상의 취약한 부분을 보완하게 해줄것이다. 본 논문에서는 XML 기반의 웹 서비스환경에서 통합접근 관리를 연구하였다.

1. 서 론

오늘날, 사람들은 매일 인터넷이라는 서비스 제공자를 통해 주요 뉴스를 읽고, 증권 및 날씨 정보를 얻으며, 온라인 쇼핑을 하는 등 다양한 서비스와 정보를 제공받고 있다. 웹 애플리케이션들은 HTML을 생성하기 위한 서로 다른 소프트웨어를 사용하여 작성되며, 인터넷 브라우저 또는 특정 클라이언트를 사용해야만 웹에 액세스할수 있다. 이러한 것은 HTML과 웹 서버 기반 기술의 한계에 일부 원인이 있고, 이 기술들은 주로 프리젠테이션에만 치중하고 다른 애플리케이션과 상호 잘 융할 수 없다.

웹 서비스의 탄생은 인터넷을 통해 정보를 교환할 수 있는 새로운 패러다임을 제시했으며, 이는 개방형 인터넷 표준과 기술에 기반을 두고 있다. 산업 표준을 사용하여 웹 서비스들은 네트워크를 통해 XML 기반 데이터를 전송하고 인터넷에서 사용할 수 있도록 제공함으로써 다양한 컴퓨팅 플랫폼, 모바일 장치 등을 사용하여 언제 어디서든지 액세스할 수 있게 해준다. 또한 웹 서비스는 개방형 표준과 프로토콜을 사용하는 유연성 때문에 인터넷과 인트라넷을 통한 EAI(Enterprise Application Integration), B2B(Business-to-Business)통합 및 A2A(Application-to-Application)통신을 용이하게 해준다. 이기종의 애플리케이션들과 분산 애플리케이션 아키텍처를 사용하는 조직에서 웹 서비스를 도입함으로써 통신 메커니즘을 표준화하고 서로다른 플랫폼에 상주하고 서로다른 프로그래밍 언어들로 작성된 애플리케이션들이 상호 작용할 수 있게된다. 본 논문에서는 웹서비스에대한 통합 접근관리에 대한 연구를 하였다[1].

2. 관련연구

2.1 웹 서비스

웹 서비스는 서비스 중심적 아키텍처의 개념에 기반을 두고 있다. 서비스 중심적 아키텍처는 최신 분산 컴퓨팅 기술이며, 애플리케이션 함수, 개체, 다른 시스템으로부터의 프로세스들을 포함하는 소프트웨어 컴포넌트들이 서비스로 제공 가능하게 한다. 웹 서비스는 프로그래밍 할 수 있는 인터페이스를 통해 인터넷 상에서 비즈니스 로직을 서비스로 제공하는 자기 설명적이고 모듈화된 비즈니스 애플리케이션이며, 서비스들을 찾고, 사용하고, 호출하는 방법을 제공하기 위해 인터넷 프로토콜을 사용한다. 웹 서비스는 XML 표준에 기반을 두고 모든 프로그래밍 언어, 프로토콜 또는 플랫폼을 사용하는 약결합된 애플리케이션 구성요소로서 개발될 수 있다. 이것은 비즈니스 애플리케이션을 누구나, 언제 어디서든지, 어떠한 플랫폼을 사용해서도 액세스할 수 있는 서비스를 제공한다.

웹 서비스는 방화벽을 통해 XML기반 RPC 메커니즘을 통해 호출 가능하고, XML메시징에 기반을 둔 다중 플랫폼, 다중 언어 솔루션을 제공한다. 또한 확장성에 영향을 주지 주지않고도 경량의 하부 구조를 사용하여 손쉽게 애플리케이션을 통합 가능하게 하고, 이종의 애플리케이션들이 상호 연동 하능하게 해준다[2].

2.2 XML기반 시스템에서 기존 보안 기술 적용의 문제점

기존 전자거래 인프라는 개별적으로 구축하여 운영되고 있어서 타 시스템과의 상호운영성이 떨어진다. 따라서, 타 시스템사이의 데이터 연동시 많은 비용이 소요되는게 현실이다.
하지만 XML 정보보호 기술은 세계표준으로 이종 시스템과의 연동시 표준을 따르도록 구축을 하면 기존 시스템에서 발생하는 호환성 및 상호연동성 문제를 감소 시킬수 있다.
또한 기존의 전자거래 시스템은 보안을 위해 기본적으로 사용자 ID, 패스워드, PKI, IPsec, SSL, TLS, S/MIME등을 사용한다. 하지만 이러한 기술은 보안을 위해서 효과적으로 사용되지만 이를 사용하는 기업간의 확장성이 떨어지는 단점이 있고, XML 기반의 시스템에서 XML 기술의 장점을 살리지 못한다. 예를 들면, SSL ,TLS와 같은 보안기술은 전송하려는 데이터 전체에 대한 암호화를 수행함으로써 XML문서와 같이 데이터의 일부만 암호화가 필요한 경우에는 비효율적인 방법이다. 따라서 XML을 사용하는 시스템의 보안을 위해서는 XML기반 보안기술의 적용이 필요하다.

2.3 관련 XML기반 보안 기술

2.3.1 XML 전자서명(XML Digital Signature)

XML 서명은 XML형태로 전자서명을 표현하는 것을 기술하고 있는 W3C 권고안이다. 서명은 임의의 XML 데이터 또는 비-XML 데이터를 나타낼 수 있다. 서명은 서명되는 데이터로부터 분리되거나 XML의 경우에는 서명되는 데이터가 XML 문서의 일부가 될수 있다. 만일 서명이 분리되지 않았다면, 서명되는 데이터를 감싸거나 또는 서명되는 데이터에 의해 둘러 싸여질 수 있다. 기본적으로 XML 서명은 키를 서명되는 데이터와 연관시키는 방법을 정의한다. XML 서명은 서명 값과 서명된 에이터를 연결하는 데 참조를 이용한다. 서명되는 데이터는 우선 해시되며 해시 값은 엘리먼트에 놓여진다. 그리고 엘리먼트는 다이제스트되어 암호학적으로 서명된다[3].

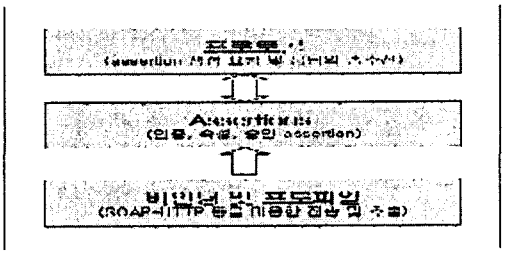
2.3.2 XML Encryption

기존의 보안기술은 데이터 전체에 대한 암호화를 수행함으로써 데이터의 일부만 암호화가 필요한 경우에는 비효율적인 방법이다.
이에 따라 데이터 중 일부분만을 암호화해 중간에 경유하게 되는 제 3자에게 특정 정보를 노출시키지 않으면서 최종 수신자에게 전달 할 수 있는 방법으로 현재 W3C에서 XML 기반의 표준화를 추진하고 있는 것이 XML Encryption이다. XML 전자서명과 통합 적용을 통해 송수신 메시지에 대한 기본적인 보안 요구를 만족시키기 위해 최적화되어 있다[4].

XML Encryption은 웹서비스와, ebXML프레임워크에서 메시지 기밀성 보장을 위한 표준 기술로 채택될 전망이다.

2.3.3 SAML(Security Assertion Markup Language)

SAML(Security Assertion Markup Language)은 주로 연합 환경에서의 보안 정보 교환을 위한 XML 기반의 프레임워크로서 Single Sign-on, 인증 서비스, 백 오피스 트랜잭션 문제들을 다루는 명세서이다.
보안 정보는 주체에 대한 주장들로 표현된다. 보안 도메인에서 정체성을 가지는 어떠한 엔터티나 주체가 될 수 있다. 주장들은 주체가 인증을 받았는지, 자원을 접근할 권한이 있는지, 특정 속성들을 가지고 있는지를 나타낸다[5].



[그림1 SAML 구조]

2.3.4 XACML(eXtensible Access Control Markup Language)

국제적인 컴소시엄인 OASI에 의해 표준화된 XACML은 XML 문서에 대한 접근을 정책리스트를 이용하여 제어할 수 있는 XML기반의 언어이다. XACML TC(Technical Committee)에서는 XACML로 정의된 기술로 정책과 인증을 표현하기 위한 XML 스키마를 제공하고 있다. 이 정책에서의 리소스는 XML을 사용하여 표현되는 어떠한 객체도 될 수 있으며 XACML은 XPath나 LDAP 등 다양한 프로토콜과 함께 바인딩하여 사용될

수 있으며 새로운 프로토콜과도 함께 사용될 수 있다. XACML은 인증시스템의 접근과 접근자 요청의 특징적인 역할에 대한 제어를 할 것으로 기대된다[6].

3. XML기반 웹서비스를 위한 통합접근관리 연구

3.1 XML 정보보호기술을 적용한 통합접근관리에 대한 연구

EAM[7]에 적용 가능한 XML정보보호 기술은 표준인증 메커니즘인 SAML(Security Assertion Markup Language)과 자원 접근관리 표준 명세인 XACML이 있다.

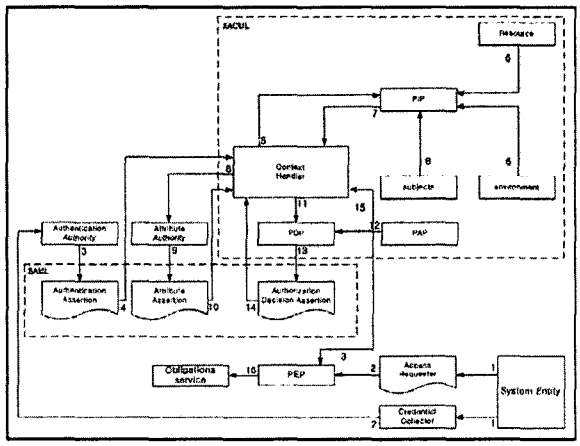
SAML은 일반 인터넷과 웹서비스를 위한 SSO와 접근제어를 위한 스키마를 정의하고 있어 EAM 솔루션으로 구축될 수 있다. SAML에서는 사용자의 인증 정보를 다룰 수 있는 인터페이스의 스키마나 전송규칙 등을 제정하며 기업의 정책을 결정하기 위한 수단과 방법, 파트너나 시스템의 통합에 대한 구체적인 방법에 대해서는 제공하지 않는다. 제공되지 않는 부분은 솔루션 구현에 따라 다양하게 이루어 질 수 있다.

XACML은 접근제어 정책을 통해 보안이 요구되는 자원에 대해 미세한 접근 제어 서비스를 제공 할 수 있는 XML 기반의 언어이다. XACML은 SAML PDP(Policy Decision Point)의 일부로서 역할을 수행 해 최종적인 자원 접근 요청에 대한 결과를 생성한다.

3.2 SAML과 XACML을 이용한 접근관리 아키텍쳐

SAML의 인증서는 기밀성과 무결성을 유지하기 위한 전자서명과 암호화가 이루어지므로 처리속도는 저하되지만 통합된 인증과 신뢰성있는 인증을 보장하는 것이 중요하다. SAML의 권한 결정 요청은 XACML 정책 서버에 의해 분석되고 접근의 허가 여부를 반환한다. Request는 접근 권한 제어에 대한 정보를 담고있고, Resource속성은 접근 하려는 리소스의 URI를 제공하고 이 리소스에 대한행위는 Action에서 제공한다.

그림에서 요청된 정보는 PEP를 거쳐 ContextHandler에게 전달되면, ContextHandler에서 요청자, 접근하려는 자원, 행위에 대한 속성을 PIP부터 전달받아 Request 쿼리를 작성하고 PDP에게 전달한다. 이 정보에 대한 접근의 결정을 PDP로부터 얻게된다. 접근정책은 시스템의 구현에 따라 자유롭게 설정할 수 있으며 특별하게 요구되는 사항은 별도의 스키마의 확장을 통해 유연한 정보 제공으로 접근제어를 할수 있다. Response는 접근 평가에서 허가, 거부를 알려주며 이것으로 접근자의 리소스에 대한 접근제어를 한다.



[그림2 SAML+XACML]

4. 결론 및 향후 과제

본 논문에서는 XML기반의 보안기술 명세를 적용하여 통합접근관리에 대한 연구를 하였다. 단일화된 신뢰성있는 인증 시스템은 세계시장을 형성하고 확장시키는 기반이 될것이다. 이것에 발을 맞추어 증가하는 데이터와 이에 따른 시스템의 확장과 유지보수는 중요한 문제이다. 암호화, 전자서명, 접근제어, 인증, 키관리와 같이 다양한 보안 기술들은 XML포맷을 이용하여 확장성과 유연성을 가지고 여러 분야에서 응용이 가능하다. 향후 과제로는 본 논문에서 연구한 접근관리와 키관리를 연동 가능한 시스템을 구현하는 것이다.

5. 참고 문헌

[1] Ramesh Nagappan, Robert Skoczylas, Rlma zpatel Srlganesh, "Delveloping Java Web Service", 2003
[2] Henry Bequet, "Java Web Service", 2003
[3] XML_Signature Syntax and Processing, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212
[4] XML Encryption, http://www.w3.org/Encryption/2001
[5] Security Assertion Markup Language, http://www.oasis-open.org/committees/security
[6] XML Access Control Markup Language, http://www.oasis-open.org/committees/xacml/index.shtml
[7]Gartner Research Note, J. Pescatore, Extranet Access Management 2H01 Magic Quadrant, http://www.gartner.com/reprints/ibm/104593.html