웹 서비스 기반의 SAML 인증 시스템의 설계

송준홍° 성백호 차석일 김현희 신동일 신동규
세종대학교 컴퓨터공학과
{song0424°, guardia, kiry, hyunhee, dshin, shindk}@gce.sejong.ac.kr

Design of SAML Authority System based on Web Service

Jun-hong Song° Baek-ho Sung Suk-il Cha Hyunhee Kim Dongil Shin Dongkyoo Shin
Dept. of Computer Engineering, Sejong University

요 약

SAML(Security Assertion Markup Language)은 웹 서비스 환경에 최적화된 인증과 권한 부여를 표준적이면서도 확장성 있는 구조를 제공하는 공개된 표준이다. ebXML과 같은 공개된 XML 기반 거래 프레임워크에 SAML을 적용함으로써 기업 간 협력형 비즈니스 모델 내에서 문제가 되었던 SSO(Single Sign-on)를 위한 사용자 관리 및 인증의 부담을 최소화 할 수 있다. 본 연구에서는 SAML에 대한 기술 분석과 함께 ebXML 및 웹 서비스 비즈니스 트랜잭션 내에서 적용 방안을 논의하고 웹 서비스 모델 기반의 SAML 인증 시스템을 제시한다.

1. 서 론

인터넷을 통한 기업 간 전자상거래는 독립적인 거래 모델에서 협력모델로 발전해 나아가고 있다. 이에 따라 필수적으로 각각의 서비스를 이용하는 사용자의 인증(authentication) 및 요청자원에 대한 접근 승인(authorization) 등에 있어 투명성 제공 문제가 비즈니스 운영의 중요한 선결 과제로 대두되고 있다.

OASIS는 점차 복잡해지는 사용자의 인증 및 속성 정보 관리 및 전달, 승인을 위해 SAML[1]을 제안하였다. SAML은 분산된 비즈니스 어플리케이션간의 SSO[2] 및 인증 과정에 적용됨으로써 기존의 각 업체 별로 상이했던 사용자 인증 및 승인 시스템의 상호운용성 문제를 제거하고 통일된 방식을 제공함으로써 웹 서비스 형태의 동적인 서비스 바인딩 시에도 효과적인 방안이 되고 있다.

따라서 본 연구에서는 SAML 기술의 분석을 통해 특정 어플리케이션에 종속되지 않는 웹 서비스 형태의 SAML 시스템을 설계하고 ebXML[3]기반의 적용 모델을 제시한다.

2. 관련 연구

2.1 SAML 개요

SAML은 경쟁 관계에 있던 S2ML[4]과 AuthXML[5]을 통합하여 e-비즈니스 프레임워크에서 인증 및 승인을 위한 표준적인 보안 기술을 제공하기 위해 OASIS의 STTC(Security Services Technical Committee)가 제안한 XML 기반의 보안 기술이다. SAML은 새로운 보안 기술을 제안하는 것이 아니라 기존의 보안 기술을 활용해 구성되며, 특정 업체의 방식이 아닌 표준적인 메시지 형식과 전송 프로토콜을 사용함으로써 플랫폼이나 솔루션 등에 독립적인 인증 및 속성 확인, 승인 등의 서비스를 제공해 줄 수 있게된다.

SAML은 인터넷상에서의 자원 요청자에 대한 인증, 승인, 속성 확인 등을 수행하는 역할을 하며 이는 XML 기반의 다른 보안 기술들[6]과 통합되어 전체 보안 시스템을 구성하는 요소 기술로서 기능을 가진다.

2.1.1 SAML 구조

SAML은 사실을 주장하는 Assertion과 인증 및 승인 등을 요청 및 수신하기 위한 프로토콜, 실제 인터넷 상의 네트워크와의 연동을 정의한 바인딩 및 프로파일로 구성된다. 개괄적인 구조는 그림 1과 같다.

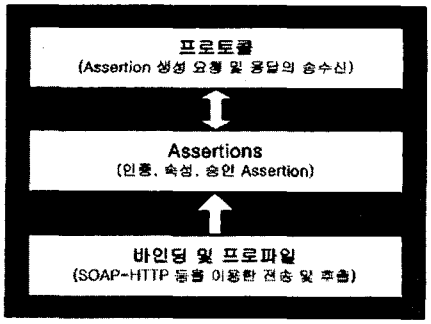

그림 1 SAML 구조

(1) Assertion

Assertion은 인증 및 승인, 속성 정보를 포함하는 XML 기반 구조를 가진다. 또한 Assertion의 인증을 위해 XML 전자서명을 적용한다.

Assertion은 3가지로 구성되며 다음과 같다.

- 인증 Assertion : 인증 Assertion은 인증기관(authority)에서 발행한 인증 요청자에 대한 성공적 인증과정 수행을 보증하는 Assertion이다. 이 Assertion에는 발행자, 인증 요청자 정보, Assertion 발생 시간, 기타 인증 관련 속성들이 포함된다.
- 속성 Assertion : 속성 Assertion은 속성관리기관에서 발행하며, 요청자에 대한 자격을 확인하는 Assertion이다.

- 승인 결정 Assertion : 승인 결정 Assertion은 승인기관에서 발행하며, 인증된 요청자가 요청한 자원에 대해 접근 허용 여부를 결정해 그 결과로서 발행하게 된다.

각각의 Assertion 발행 기관은 한 곳에 위치 할 수 있다.

(2) SAML 프로토콜

SAML 프로토콜은 XML 기반의 메시지 형태로서 요청 및 응답의 쌍으로 구성되어 각 Assertion에 대한 전송을 담당한다. 일반적으로 Assertion은 SAML 프로토콜의 응답을 통해 얻어진다.

(3) SAML 바인딩

SAML 바인딩은 SAML Assertion 요청 및 응답 프로토콜을 표준 메시지 전송 프로토콜과 연동함에 있어 처리되어야할 방식을 정의하고 있다. 현재 SOAP-HTTP 바인딩[7]이 기본적으로 사용된다.

SAML 프로파일은 SAML Assertion이 어떠한 방식으로 메시지 프레임워크 또는 프로토콜에서 삽입되고, 추출되는지를 명시한 것으로서 현재 웹 브라우저 프로파일[7]과 SOAP 프로파일이 정의되어 있는 상태이다.

2.1.2 SAML 사용 시나리오

단일 업체간의 비즈니스와는 달리 협력형 비즈니스 모델에 있어 사용자의 인증 및 권한부여 등의 문제는 더욱 복잡하다. 이를 극복하기 위해 SSO개념이 등장했으며, SAML의 Assertion은 SSO 구현 시 인증을 위한 토큰(token)으로서 핵심적인 역할을 수행한다. 그림 2는 SAML Assertion을 이용한 웹 기반 Pull 방식의 SSO 수행 시나리오이다.

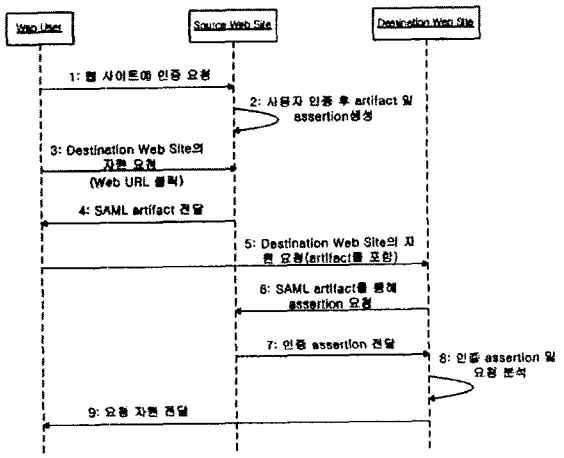

그림 2 SAML 기반 SSO Pull 모델

(1) 웹 사용자는 소스 웹사이트에 패스워드기반 인증을 수행한다.

(2) 소스 웹사이트는 사용자인증 후 인증 사용자에 해당하는 Assertion을 생성하고 Assertion을 참조하는 artifact를 생성한다.

(3) 웹 사용자는 목적지 웹사이트의 자원을 요청한다.

(4,5) 소스 웹사이트는 요청자에게 artifact를 전달함과 동시에 목적지 웹사이트로 경로 재 설정을 수행한다.

(6,7) 목적지 웹사이트는 수신한 artifact를 소스 웹사이트에 전달하고 해당 Assertion을 전달받는다.

(8,9) 목적지 웹사이트는 수신한 Assertion을 분석하고 적합한 요청일 경우 웹 사용자에게 요청 자원을 전달한다.

웹 사용자는 소스 웹사이트에서 수행한 1회 인증 과정으로 목적지 웹사이트에 재 인증과정 없이 자원을 전달 받게된다. 이때 소스 웹사이트는 인증 및 속성 Assertion을 발행하는 인증기관의 역할을 수행하며 목적지 웹사이트는 요청에 대한 평가를 수행하는 역할을 담당하다.

위의 과정은 '3:Destination Web Site의 자원요청' 단계에서 내부적으로 진행되며 사용자에게 SSO과정에 대한 투명성을 제공한다.

3. SAML 인증 시스템의 설계

본 연구에서 설계한 웹 서비스 기반의 SAML 시스템은 ebXML을 적용 모델로 하여 설계되었다. 즉, ebXML 기반의 비즈니스 수행 클라이언트가 SAML 인증기관으로부터 1회 인증을 수행으로 추후 ebXML 등록기/저장소 등의 서버 시스템 이용 시 요구되는 인증 과정을 제거 할 수 있게 되는 것이다.

그림 3은 시스템 구성 클래스간의 관계를 나타낸 클래스다이어그램으로써 SAML 요청 및 처리, 응답 관련 모듈이외에 송수신한 SAML 관련 메시지의 무결성 및 인증을 위해 XML 전자서명[8]의 생성 및 검증을 담당하는 모듈이 추가되어진다. 또한 웹 서비스기반의 시스템 구성에 따라 SOAP 처리 모듈이 모든 메시지의 송수신을 담당하는 모듈로서 역할을 수행한다.

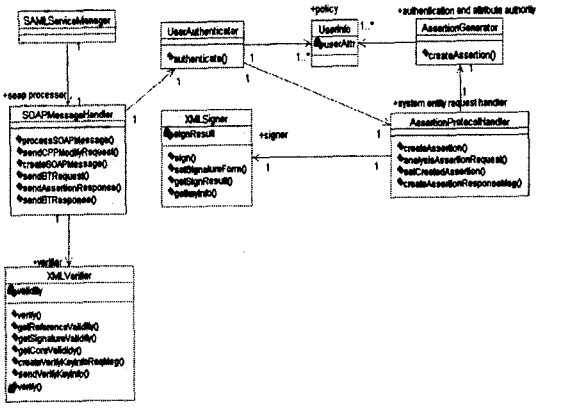

그림 3 SAML 시스템 클래스 다이어그램

- SAMLServiceManager : SAML 웹 서비스를 총괄하는 관리자 역할을 수행.
- SOAPMessageHandler : SOAP 메시지 처리와 관련된 작업과 메시지의 송수신을 담당.
- UserInfo : 사용자 인증을 위한 정보를 제공.
- XMLVerifier : XML 전자서명의 검증을 담당.
- XMLSigner : XML 전자서명을 수행한다. enveloped 방식의 서명 생성을 기본 서명 방식으로 함.

- **UserAuthenticator** : SAML 요청 클라이언트로부터 전달된 인증 정보를 통해 Assertion 생성을 위한 인증 수행.
- AssertionProtocolHandler : Assertion 요청 및 응답 프로토콜의 생성 및 처리를 담당하며, AssertionGenerator에 실제 인증된 클라이언트에 적합한 Assertion 생성을 요청.
- AssertionGenerator : SAML의 인증 및 속성 Assertion 생성 기관의 역할을 수행해 인증된 클라이언트의 Assertion을 생성하고 AssertionProtocolHandler에 전달.

그림 4는 클라이언트로부터 수신한 인증 및 속성 Assertion 생성 요청을 처리하는 유즈케이스(use case)를 시퀀스 다이어그램으로 도식화한 것이다.

(1) postAssertionRequest(req) : 클라이언트로부터 인증을 수행하기 위한 사용자 정보를 포함한 Assertion 생성 요청 메시지를 전달받는다. 클라이언트는 패스워드 기반의 사용자인증 정보를 전달한다.
(2) verify(req) : 전자서명을 검증을 요청한다.
(3) verify(req) : 수신 메시지에서 XML 전자서명 검증 공개키 정보를 추출 후 전자서명을 검증한다.
(4) authenticate(id, password) : 메시지에 대한 검증이 완료된 경우 Assertion 요청 클라이언트를 인증한다.
(5) createAssertion() : 인증이 완료된 경우 해당 요청 클라이언트의 Assertion 생성을 수행한다. 이는 아래의 과정 (6, 7, 8, 9)이 포함된다.

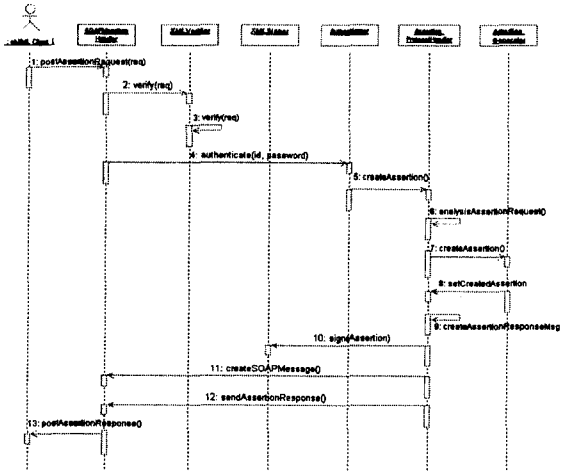

그림 4 Assertion 생성 시퀀스 다이어그램

(6) analysisAssertionRequest() : Assertion 요청 메시지를 분석하고 결과를 실제 Assertion 생성 객체에게 전달한다.
(7) createAssertion() : Assertion 요청의 분석 결과에 따라 Assertion을 생성한다.
(8) setCreatedAssertion : 생성된 Assertion을 전달한다.
(9) createAssertionResponseMsg() : Assertion 요청에 대한 응답으로 전달할 메시지를 구성한다.
(10) sign(Assertion) : 응답 Assertion을 전자서명 한다.
(11) createSOAPMessage() : Assertion 응답 메시지를 SOAP 형식으로 생성한다.
(12) sendAssertionResponse() : 메시지 전달을 요청한다.
(13) postAssertionResponse() : Assertion 요청 클라이언트에게 응답 메시지를 전달한다.

SAML 인증 시스템은 SOAP를 이용한 Assertion 요청 및 응답 프로토콜을 사용함으로써 ebXML 뿐 아니라 기타 인증 서비스가 요구되는 웹 서비스에서 시스템의 추가적인 변경 없이 사용할 수 있는 확장성 및 상호운용성을 제공한다.

4. 결론 및 향후 연구

SAML은 협력형 비즈니스모델 운영에 있어 반드시 필요한 표준화된 사용자 인증 정보 전달 수단으로서 다중 사이트간의 SSO를 가능케 할 뿐 아니라 요청에 대한 승인 결정 시 필요한 사용자 및 역할별 정보를 전달한다.

현재 SAML은 WS-Security 명세[9]와 Liberty Alliance 프로젝트[10]에서 표준적인 사용자 인증정보 전송을 위한 기술로 채택함으로써 적용 범위를 더욱 넓혀가고 있다. 이에 본 논문에서는 SAML 기술 분석을 수행하고, 웹 서비스기반의 SAML 인증 시스템을 설계함으로써 ebXML을 비롯한 XML 기반 전자상거래 프레임워크에 적용 할 수 있는 시스템 모델을 제안하였다.

향후 연구로는 본 연구에서 설계된 시스템의 구현을 통해 실제 비즈니스 수행 시 적용시킴으로써 설계된 모델을 검증하고 평가하여 보다 효율적인 SAML 기반의 인증 시스템으로 발전시켜나가야 할 것이다.

참고문헌

[1] Security Assertion Markup Language, http://www.oasis-open.org/committees/security/docs/cs-sstc-core-01.pdf
[2] Understanding Single Sign-on, http://www.intranetjournal.com/articles/200205/se_05_28_02a.html
[3] ebXML, http://www.ebxml.org
[4] Security Services Markup Language, www.oasis-open.org/committees/security/docs/draft-s2ml-v08a.pdf.
[5] AuthXML Draft, http://www.oasis-open.org/committees/security/docs/draft-authxml-v2.pdf.
[6] 송준홍, 차석일, 김현희, 성백호, 신동일, 신동규 "ebXML에서의 XML보안기술 적용 연구" 한국정보과학회 학술발표논문집(B), 제29권, 제 1호, pp796~798, 2002.
[7] SAML Bindings and Profiles, http://www.oasis-open.org/committees/security/docs/cs-sstc-bindings-01.pdf
[8] XML-Signature Syntax and Processing, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/
[9] Web Service Security Specification, http://www.verisign.com/wss/wss.pdf
[10] Liberty Alliance Project, http://www.projectliberty.org