웹서비스 통합 인증에 대한 SAML적용 모델 연구

이형석*, 정종일, 박병철, 신동일, 신동규
세종대학교 컴퓨터공학과
e-mail:{bestehen, jijeong, leon, dshin, shindk}@gce.sejong.ac.kr

A Study on the Application Model of SAML for Integrated Authentication in Web Services

HyoungSeok Yi*, JongIl Jeong, ByungChul Park, Dongil Shin, Dongkyoo Shin
Dept of Computer Engineering, Sejong University

요 약

웹서비스에 대한 높은 관심과 함께 그 실현이 점차 가시화 되고 XML로 이루어진 지원 기술들의 전폭적인 지지로 잠재력은 더욱 확대되고 있다. 웹서비스는 기존 웹 기반의 디스플레이에 그쳤던 단순정보 교환을 애플리케이션 차원에서 데이터를 통신할 수 있어 개발 가능성이 무한한 프레임워크로 각광받고 있다. 전자상거래 분야도 예외는 아니어서 웹서비스의 기본 개념을 이용하여 프레임워크를 구성하려는 노력이 진행되고 있다. 이에 따라 인증분야에서도 한계점이 드러나게 되었고 각 시스템마다 존재하는 많은 인증 정보관리 문제가 부각되고 있다. OASIS에서는 웹서비스의 등장과 함께 SAML이라는 표준 인증 방식을 제시하였다. SAML은 XML기반의 표준화된 인증방식을 취하여 안전성과 확장성뿐만 아니라 인증 간 상호운용성을 제공하는 강력한 기능을 가지고 있다. 본 논문에서는 SAML을 이용한 SSO(Single Sign On)와 접근권한에 대한 적용개념을 소개하고 SAML인증서버를 이용한 Web Services인증 모델을 제시하고자 한다.

서 론

각 기업들의 인트라넷 시스템과 웹서비스 [1]가 각광 받으면서 급속히 시장이 확대되고 있다. 정보시스템은 이제 대부분의 기업이나 기관에서 없어서는 안 되는 기반시스템이 되었으며 많은 업무가 정보시스템에 의해 처리되고 있다. 웹서비스는 XML(eXtensible Markup Language)을 기반 기술로 하여 다양한 기술들이 조합되어 탄생한 분산 객체 서비스이다. 웹서비스는 UDDI(Universal Description, Discovery and Integration) [2]에서 서비스를 검색하고 서비스제공자의 WSDL(Web Service Description Language) [3]로 통신 모듈을 생성하며 표준 프로토콜인 SOAP (Simple Object Access Protocol) [4]을 사용하여 통신한다. 서비스제공자와 요청자는 각 시스템의 메시지처리 점을 통해 정보를 요청하고 응답을 수신하게 된다. 기존의 HTTP방식의 정보와 더불어 데이터를 교환하는 표준이 생김으로써 서비스를 제공하는 시스템은 기하급수적으로 증가할 것으로 보인다. 이에 따라 증가하는 것이 보안 문제이다. 특히 넘쳐나는 인증정보와 시스템 리소스에 무분별한 접근은 보안상의 커다란 문제로 부각되고 있다. OASIS [5]는 이러한 문제점을 해결하기 위해 새로운 인증메커니즘을 작성하였다. SAML(Security Assertion Markup Language) [6]은 XML을 기반으로 작성된 assertion statement를 요청하고 응답하는 표준 인증 메커니즘이다. SAML은 크게 Authentication, Attribute, Authorization Decision statement로 구분할 수 있다. Authentication은 요청자의 정보를 제공하고 attribute는 요청자의 속성정보를 제공하며 Authorization Decision은 요청자가 특정 리소스에 접근했을 때 해당되는 접근 허가여부를 판단하기 위한 스키마를 정의하고 있다. 특히 Authentication과 artifact Assertion을 통한 Single Sign On(SSO) [7]의 구현이 가능하다. 본 논문에서는 SAML을 중심으로 한 여러 가지 형태의 인증 방식을 설명하고 웹서비스로의 적용 모델에 대하여 제시한다.

2. 관련 연구

2.1. Web Services 개요

일반적으로 인터넷을 통해 제공되는 일반적인 웹서비스와는 달리 Web Services는 표준 RPC를 통해 프로토콜에 의존적이지 않도록 배치되어 바인딩 될 수 있는 비즈니스 분산 객체이다. 표준 인터넷 프로토콜인 SOAP을 사용하여 기존의 HTTP와 같은 인터넷 프로토콜을 그대로 사용하므로 제반 비용이 작아지고 XML을 기반으로 하기 때문에 확정성과 유연성이 있다. 캡슐화된 어플리케이션으로 웹에 존재하는 콤포넌트의 재조립으로 새로운 웹서비스로의 구성이 가능하다. 웹서비스의 기본 구성 요소는 서비스 요청자, 제공자, 레지스트리로 나눌 수 있는데 서비스 제공자는 레지스트리에 제공하는 웹 애플리케이션 객체를 등록하고 요청자는 레지스트리에서 서비스를 검색하여 원

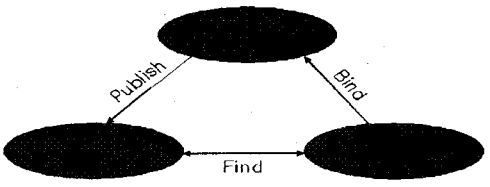

그림 1 웹서비스 구성요소

하는 서비스를 찾을 수 있고 WSDL을 사용하여 서비스와 통신하기 위한 모듈을 생성하여 제공자와 직접 통신할 수 있게 된다 [1].

2.2. Web Services 핵심기술 요소

- **SOAP(Simple Object Access Protocol)**

XML기반 프로토콜로 복잡한 객체 데이터 타입도 쉽게 모델링 할 수 있게 해주며 RPC프로토콜을 지원한다. HTTP뿐 아니라 FTP, SMTP, POP3등 기존의 프로토콜 상에서 동작하므로 부가적인 비용이 발생하지 않으며 특정 벤더에 종속되지 않은 공개프로토콜로 웹서비스에서 사용되는 모든 메시지는 SOAP을 사용하여 통신한다 [4].

- **WSDL(Web Service Description Language)**

XML기반의 웹서비스 기술 스크립트 언어로 웹서비스에 접촉하고 이용하기 위한 메시지 스키마를 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 [3].

- **UDDI(Universal Description, Discovery and Integration)**

일종의 디렉토리 서비스로서 웹서비스의 제공자는 자신의 서비스의 기능을 묘사하로 UDDI에 WSDL을 등록하게 된다. 서비스 요청자는 UDDI를 통해 등록된 웹서비스를 간단히 검색할 수 있으며 WSDL에 의한 클라이언트 생성으로 서비스 제공자와 통신할 수 있다 [2].

3. SAML(Security Assertion Markup Language)

인증과 권한 정보 교환을 위한 XML기반의 Security specification으로 OASIS에서 표준안을 제정하였다.

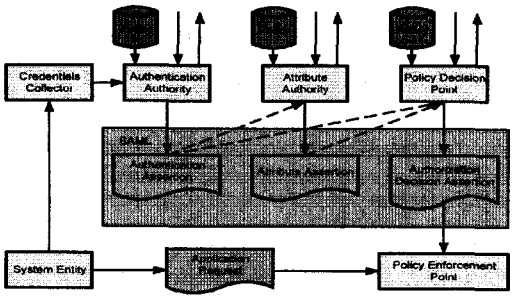

그림 2 SAML 아키텍처

XML스키마로 security assertion과 assertion의 요청, 응답에 대한 포맷을 정의하고 assertion사용에 관한 규칙들을 설명하고 있다 [그림 2]. SAML은 서비스간의 인증 상호운용성을 제공하고 Single Sign On을 실현할 수 있다. 가장 중요한 목표는 보안서비스를 요구하는 다른 시스템간의 표준 인증방식으로 상호운용성을 도모하는 것이라 할 수 있다. SAML은 크게 인증(Authentication), 속성(Attribute), 권한(Authorization)에 관한 내용을 saml system에 요청하고 이에 대한 응답으로 assertioin을 받게 된다.

Assertion은 발행자에 의해 만들어지는 하나 혹은 여러 개의 정보의 패키지로 Assertion의 정보를 인증의 근거로 사용한다. SAML에서는 세 가지 다른 종류의 assertion을 만드는 것을 허용하는데 여기에는 인증(Authentication), 속성(Attribute), 권한결정(Authorization Decision)이 있다. [그림 3]은 요청자에 의해 호출된 속성에 관한 assertion의 예이다.

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Request IssueInstant="2002-08-08T07:58:32.338Z"
MajorVersion="1" MinorVersion="0"
RequestID="a207b1a0-aaa4-11d6-9e6d-75a01a1d3688"
xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol">
<samlp:AttributeQuery>
<saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
<saml:NameIdentifier Format=""
NameQualifier="verisign.com/ams">uid150</saml:NameIdentifier>
<saml:SubjectConfirmation>
<saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:am:passwor
d</saml:ConfirmationMethod>
<saml:SubjectConfirmationData>password</saml:SubjectConfirmation
Data>
</saml:SubjectConfirmation>
</saml:Subject>
<saml:AttributeDesignator
AttributeName="//verisign.com/core/attr/email"
AttributeNamespace="verisign.com/ams/namespace/common"
xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"/>
</samlp:AttributeQuery>
</samlp:Request>
```

그림 3 속성 assertion의 예

인증은 요청 주체에 대한 고유 ID와 같은 인증 정보를 일컫는 것이고, 속성은 요청 주체에 대한 속성에 대한 정보를 제공한다. 즉 email주소, 시스템이나 조직에서의 역할(role)등이 될 수 있다. 권한은 시스템의 리소스에 접근할 수 있는지 여부에 대한 요청이며 이 요청은 시스템 Policy에 따라 접근 여부를 허가 또는 거부하게 된다. 요청과 응답에 대한 메시지는 SOAP을 통하여 이루어지게 된다 [6].

3.1. SAML을 이용한 SSO(Single Sign On)모델 - Pull

사용자가 여러 번의 인증과정을 확인 받을 필요 없이 연계된 하나의 인증 시스템을 통하여 여러 사이트에 접근할 수 있는 인증방식을 Single Sign On이라고 한다. SSO은 두 가지 방식으로 나뉠 수 있는데 pull모델과 push모델로 나뉠 수 있다. pull모델은 사이트 이동 시 artifact를 인증표처럼 사용하여 인증을 받게 된다. [그림 4]은 artifact를 사용한 PULL모델로서 과정을 설명한 것이다 [7].

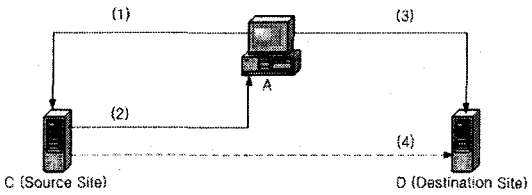

그림 4 SAML Single Sign On - Pull 모델

A는 C에 로그인하여 최초 인증을 받게 된다. 최초 인증 후 D에 접근을 하려고 한다.

(1) D에 접속하려는 요청을 C로 보낸다.

(2) C에서는 유일한 값의 artifact를 생성하여 Destination site의 위치와 함께 클라이언트에 응답하며 artifact는 저장된다.

(3) 클라이언트는 artifact와 함께 Destination site인 D로 인증요청을 한다. 이 과정에서 클라이언트의 사용자는 직접적으로 관여하지 않는다.

(4) D는 과정(3)에서 수신한 요청자의 artifact를 C에 전송

하여 저장된 artifact와 비교 후 인증을 확인하게 되고 적합한 인증자라면 요청자의 assertion을 응답 값으로 수신하므로 써 최종 D에 SSO하게 된다. 인증이 최종 확인되어 SSO에 성공했다면 C에 생성된 artifact는 삭제되게 된다.

(1)번부터 (4)번까지의 과정은 하나의 트랜잭션으로 처리되어 사용자는 한 번의 요청으로 모든 과정을 거쳐 인증을 받게 된다. 사용자의 개입 없이 D는 artifact에 의한 인증방식으로 C에서 assertion을 요청 수신하므로 pull모델이라 할 수 있다. 각 과정에서 artifact와 assertion에 대한 요청과 응답은 기밀성과 무결성이 보장되어야 하므로 SSL같은 채널 상의 보안이나 데이터 암호화 같은 보안사항이 요구된다. 또한 (1)~(3)까지의 과정은 HTTP의 GET방식에 의해서 이루어지고 assertion에 대한 요청과 응답은 SOAP통신에 의해 이루어지게 된다.

3.2. SAML을 이용한 SSO모델 - Push

다른 SSO방식으로 PUSH모델을 들 수 있는데 이는 기존의 HTTP에서의 POST방식으로 SAML assertion을 요청하고 응답하는 방식이다 [7].

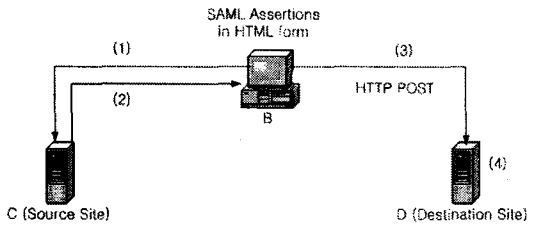

그림 5 SAML Single Sign On - Push 모델

(1), (2) 인터넷 프로토콜 상에서 GET방식으로 assertion을 요청하고 응답받게 된다.

(3) B는 클라이언트에 저장된 assertion을 HTTP POST 방식으로 전송하게 된다. 이 과정에서 표에서 보여주는 것과 같이 assertion은 hidden방식으로 Destination Site인 D로 전송된다. 최종적으로 수신된 assertion은 인증을 통해 SSO을 마치게 된다.

```
<HTML>
<BODY Onload="document.forms[0].submit()">
<FORM METHOD="POST" ACTION="<assertion consumer host name
and path>"> ...
<INPUT TYPE="HIDDEN" NAME="SAMLResponse" VALUE=" response
in base64 coding">
<INPUT TYPE="hidden" NAME="TARGET" Value="<Target>">
</FORM>
</BODY>
</HTML>
```

그림 6 POST 방식의 assertion 전송 form 예

위와 같은 동작을 위해 다음과 같은 HTML코드가 삽입될 수 있다.

```
<INPUT TYPE="Submit" NAME="button" Value="Submit">
```

이 방식은 두개의 트랜잭션으로 이루어지는데 최초 인증을 위해 assertion을 획득하는 과정과 POST방식에 의한 assertion전송 과정이 있다. HTTP의 전송 데이터 값을 그대로 hidden방식으로 사용자에 의해 전달되므로 이는 PUSH방식이라 할 수 있다. 이 방법 역시 assertion요청과 응답에 기밀성과 무결성을 유지해야만 한다.

3.3. SAML Authorization Decision 모델

SAML은 Authorization Decision Assertion을 이용하여 접근 권한에 대한 인증을 지원한다. 접근 권한 assertion은 리소스에 대한 적당한 권한을 가지고 접근하는 것으로 이에 부합하는 적당한 Action을 취할 수 있다. SAML Authorization Decision은 Single Sign On에 기반을 둔 다른 사이트로의 이동시에도 접근 권한 assertion을 사용할 수 있다.

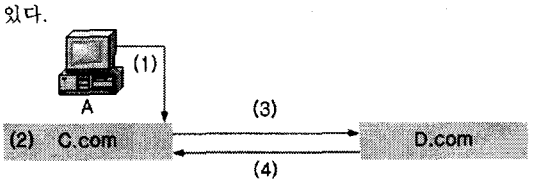

그림 7 SAML Authorization Decision 모델

C.com에 속해 있는 사용자A는 C.com에서 인증 되어 리소스에 접근하게 되고 특정 정보를 제공하고 있는 D.com에 접근한다. SAML Authorization Decision assertion은 사용자 인증정보와 접근하려는 리소스 URI, 사용자에 대한 role정보를 가지고 있기 때문에 D.com의 정책 서버의 결정에 따라 외부의 사용자에 대한 적당한 권한에 따른 리소스 접근을 가능하도록 해준다. 따라서 사용자A는 보안이 요구되는 리소스에는 접근할 수가 없게 된다.

3.4. 비즈니스 트랜잭션 모델

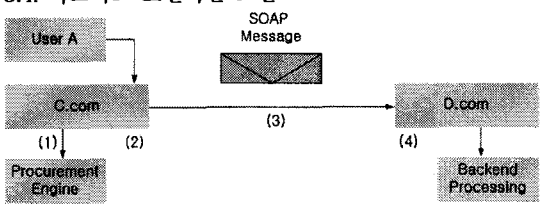

그림 8 비즈니스 트랜잭션 모델

SAML은 인증이나 권한정보 외에 ebXML이나 Web Services프레임워크에서 안전한 데이터의 교환을 위해 사용될 수 있다 [그림 8].

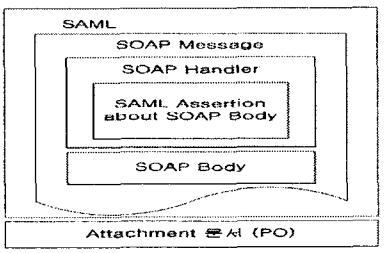

그림 9 비즈니스 트랜잭션 모델
SOAP attachment

(1),(2)사용자A는 C.com에서 인증을 받아 비즈니스 문서인 purchase order (PO)의 내용을 작성하고 request를 생

성한다. 이때 XML전자서명을 사용하여 인증을 보장할 수 있다.
(3) C.com은 SOAP message의 header내에 SAML assertions를 삽입함으로써 PO에 대한 보안 context를 작성하고 PO는 payload에 첨부하고 전송한다. SOAP메시지의 내부 구조는 [그림 9]과 같다.
(4) D.com은 SOAP메시지 내에 인증정보를 참조하여 검증을 실행하고 document와 header 내의 SAML assertions를 추출하여 PO를 처리한다.

4. 웹서비스 SAML 인증 아키텍처.

앞서 SAML의 다양한 인증모델을 설명하였다. 이러한 인증 모델을 이해함과 동시에 실제적인 서비스 아키텍처의 모델을 제시한다. 전체적인 구조는 SAML 서비스 시스템에서 여러 개의 웹서비스 제공자의 인증을 담당하게 되고 제공자끼리는 SAML 서버를 통하여 SSO를 할 수 있다 [그림 10].

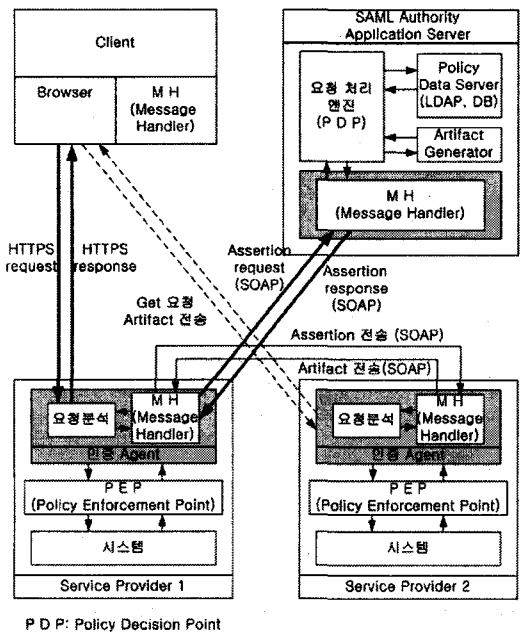

그림 10 웹서비스 SAML인증 아키텍처

또한 웹서비스 제공자의 리소스에 적합한 권한을 가지고 접근을 할 수 있다. SAML Authority 서비스에서 통합적으로 인증을 담당하고 있으며 웹서비스 제공자는 이 인증 애플리케이션서버를 통해 assertion을 발행 받게 된다. assertion의 요청과 수신은 SOAP메시지를 통하여 이루어지게 되며 artifact데이터는 GET방식을 통해 전송하되 SSL을 통하여 기밀성을 보장 한다. 최초의 HTTPS요청에 의해 접근을 하게 되고 인증의 기초정보를 인증agent는 SAML 서버로 SOAP메시지를 생성하여 전송한다. 서버의 요청처리엔진에서 적합한 assertion을 발행하고 Authority Decision요청일 경우 이에 대한 정보를 포함한 assertion을 응답하여 승인된 접근은 웹서비스를 제공받게 된다. 클라이언트가 다른 웹서비스로 이동시 artifact정보를 포함한 접근 요청을 하게 되며 이 artifact는 resource사이트에서 assertion을 Pull해서 가져오는 티켓 역할을 하게 된다. 최종적으로 assertion에 의한 접근을 허가 또는 거부하게 된다.

5. 결론 및 향후 연구방향

공개된 네트워크인 인터넷을 통한 global환경에서 데이터 교환은 효율성과 비용적인 면에서 커다란 이익이라고 할 수 있다. 그러나 증가하는 데이터와 이에 따른 시스템의 확장과 유지 또한 문제가 될 것이다. 웹서비스는 그 효율성과 확장성에서 무한한 잠재력을 가지고 있지만 보안과 이에 수반되는 비용의 문제는 또 다른 문제점을 야기할 수 있다. SAML은 이러한 부가적인 비용을 절감하는 통합인증 서비스를 제공할 수 있으며 사용자에 대한 속성과 접근권한에 대한 정보를 제공하므로 써 이를 이용하는 확장된 서비스를 제공할 수 있다.

SAML서비스는 효율적인 인증정보를 제공하는 동시에 XML전자서명, 암호화와 함께 유기적으로 서비스가 제공되어 질 수 있다. 본 논문에서는 많은 웹서비스 객체에서의 인증을 처리하기 위한 SAML 인증서비스 모델을 제시하였다. 제시된 모델을 중심으로 SAML API를 구현하여 실제 시스템을 구현할 계획이며 이에 제반해 발생하는 문제점에 대해 연구할 것이다. 웹서비스는 곧 우리의 생활 속으로 빠르게 진입할 것이다. 이에 대한 효율적인 보안체계를 준비하지 않으면 아무리 잠재력이 있는 웹서비스라 해도 보급이나 이를 이용하는 시장에 걸림돌이 될 것은 당연하다. 웹서비스 이용을 위한 기술의 개발과 함께 보안과 인증에 대한 관심 또한 동일한 시점에서 이루어져 취약점과 대책에 대해 연구가 진행되어야 할 것이다.

6. 참고 문헌

[1] Curbera, F.: "Unraveling the Web services web: an introduction to SOAP, WSDL, and UDDI" Internet Computing, IEEE, Volume: 6 Issue: 2, Mar/Apr 2002, Page(s): 86 -93
[2] UDDI, http://www.oasis-open.org/committees/uddi-spec/
[3] Blake, M.B.: "An agent-based cross -organizational workflow architecture in support of Web services" Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops on , 2002 Page(s): 176 -181
[4] Tsenov, M.: "Application of SOAP protocol in e-commerce solution" Intelligent Systems, 2002. Proceedings. 2002 First International IEEE Symposium , Volume: 3 , 2002 Page(s): 59 -62 vol.3
[5] OASIS, http://www.oasis-open.org/
[6] Security Assertion Markup Language (SAML), http://www.oasis-open.org/committees/security/
[7] Samar, V.: "Single sign-on using Technologies: Infrastructure for Collaborative Entecookies for Web applications" Enabling rprises, 1999. (WET ICE '99) Proceedings. IEEE 8th International Workshops on , 1999 Page(s): 158 -163