전자상거래에서의 사용자 인증에 관한 연구

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

A study for user authentication in e-commerce

Jongil Jeong° Seokhwan Yu Moohong Cha Dongkyoo Shin Dongil Shin
Dept of Coumputer Engineering, Sejong University

요 약

구매자 중심의 거대한 전자상거래 시장에서 사용자의 인증은 중요한 issue이다. 전자상거래 시스템별 개별적인 인증방식은 사용자에게는 불필요한 반복 인증과정 수행으로 인한 번거로움과 패스워드관리에 대한 문제를 야기 시키며 관리자에게는 사용자 정보관리를 위한 보안적인 면까지 고려해야하는 부담을 갖게 한다. 본 논문에서 제시하는 단일인증 방법을 통해서 사용자의 편의 증대와 효율적인 관리 그리고 기술적인 지원에 드는 비용을 줄일 수 있을 것이다.

1. 서론

인터넷을 바탕으로 활성화된 전세계전자상거래 시장의 규모는 2005년에 무려 5조 달러 이상으로 성장할 것으로 예상된다[1]. 거래형태별 기업간 전자 상거래 실적은 구매자 중심형, 판매자 중심형, 그리고 중개자 중심형으로 구분하며 이 중 구매자 중심형태의 실적비중이 가장 큰 것으로 나타난다[1].

구매자 중심의 거대한 전자상거래 시장에서 사용자의 인증은 중요한 issue가되고 있다. 인터넷을 통해 거래가 이루어지기 때문에 사용자들은 신뢰성과 안전성 보장을 요구하고 있다.

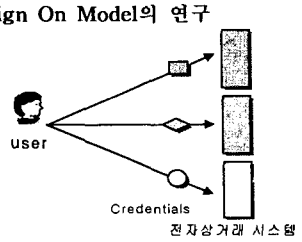
공개키 기반구조(PKI, Public Key Infrastructure)는 공개키 인증서를 기반으로 사용자인증에 필요한 메시지를 전송함으로써 메시지의 무결성, 부인방지, 기밀성 그리고 인증을 보장하고 있다. 이러한 인증방법은 사용자에게 신뢰성을 보장할 수 있다. 그러나 사용자 편의성 면에서 볼 때 기존 전자상거래 인증방법은 사용자가 거래를 원하는 사이트마다 개별적인 인증과정을 거쳐야하는 번거로움을 야기한다.

불필요하고 반복적인 인증절차로 인해 사용자와 시스템 관리자는 패스워드 관리에 대한 부담을 갖게 된다. 사용자는 전자상거래 시스템을 이용하기 위해 개별적으로 각 시스템마다 별도의 패스워드들을 보유해야하고 각 시스템마다 정확히 일치하는 패스워드를 선택해야하는 어려움이 있다. 관리자는 전자상거래 시스템 사용자들과 관련된 정보와 패스워드를 데이터베이스에 저장하고 관리하는 작업과 공개된 네트워크를 통해서 빈번하게 전송되는 사용자의 정보가 악의를 가진 제 3자에게 노출될 위험성에 대한 대책을 가져야한다.

단일인증을 통해서 반복적인 인증절차로 인해 사용자와 관리자에게 부여된 부담을 덜 수 있다. 특히, 보안 정보 교환을 위한 XML기반의 framework인 SAML(Security Assertion Markup Language)인증의 적용으로 반복적인 인증절차의 문제점들을 보완할 수 있다. 따라서 본 논문에서는 전자상거래에서 사용자 인증의 편의성과 잠재적인 보안문제의 해결을 위해 단일인증 모델 구현을 위한 SAML을 적용한 Single Sign-On 모델을 제시한다.

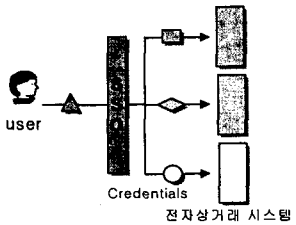
2. 관련연구

2.1 Single Sign On Model의 연구



[그림 1] Traditional logon procedure

[그림 1]은 사용자가 거래하기를 원하는 전자상거래 시스템의 숫자만큼 credential(User ID and password)이 필요하고 각 전자 상거래 시스템을 사용하기 위해서는 개별적으로 logon 절차를 거쳐야만 한다. 사용자들은 평균적으로 다섯 개에서 여덟 개의 패스워드를 사용하고 패스워드를 노트에 적어서 보관하거나 극히 단순한 패스워드들만을 사용한다. 허술한 패스워드 관리는 악의를 가진 제 3자 에게 쉽게 노출될 수 있으므로 보안이 취약해지는 결과를 초래한다.



[그림 2] SSO logon procedure

SSO(Single Sign-on)[2]이란, 단 한번의 logon만으로 기업의 각종 업무 시스템이나 인터넷 서비스에 접속할 수 있게 해주는 보안 응용 솔루션으로 최근 전자상거래 뿐만 아니라 각 기업들의 인트라넷 시스템과 웹 서비스가 대폭 확

장됨에 따라 SSO 시스템도 급속히 확대되고 있다. SSO를 도입하면 각각의 시스템마다의 인증 절차를 밟지 않고도 사용자에 부여된 1개의 계정만으로 다양한 시스템에 접근할 수 있기 때문에 사용자의 편의가 대폭 높아지고, 관리자 입장에서도 인증정책의 변경이나 권한 설정이 수월해져 관리비용 및 수고를 크게 덜 수 있다 [2].

SSO의 구현은 인증절차를 단순화하고 이질적인 platform과 application 환경에서 패스워드의 수를 감소시켜 관리와 잠재적인 보안문제를 해결할 수 있다. 따라서 application의 사용이 더욱 용이해지게 되고 기술적인 지원에 필요한 비용을 절감할 수 있다.

[그림 2]는 기존의 전자상거래 시스템과 사용자사이에 SSO layer를 두어 하나의 credential로 인증 후 각 application에 재 인증하지 않고 접근할 수 있음을 보여준다.

2.2 SSO 기술의 소개

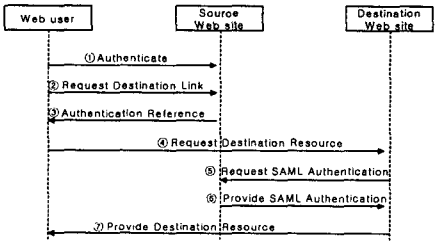
SSO구현을 위한 기술로는 Key-exchange 방식의 Kerberos와 Needham-Schroeder같은 전통적인 third party 인증 프로토콜이 있다. 이 인증 프로토콜들은 키 교환이나 키 확인 단계부터 시작하기 때문에 client application은 암호화와 인증을 위해 새로운 키나 확인된 키를 사용해야한다. SSO구현을 위한 또 다른 프로토콜로는 cookie와 SAML(Security Assertion Markup Language)같은 Token-based 방식이 있다. Key-exchange방식과 달리 Token-based 방식은 인증 token이 독립적으로 설치된 안전한 채널 상에서 전송된다. 안전한 채널이란 SSL/TLS가 대개 브라우저와 함께 사용되며 인증 token이 key를 전달하지 않고 안전한 채널 내에서 전송되는 것으로써 인증된 client key없이 설치된다는 것을 의미한다.

Token-based 프로토콜의 장점은 대다수의 서비스 제공자들이 이미 SSL 서버 인증서를 가지고 있고 브라우저를 통해서 적절한 암호기법의 구현이 모든 client machine상에서 가능하다는 것이다. 또 다른 장점으로는 사용자가 직접적인 관계가 없는 여러 개의 인증 token들을 사용할 수 있다는 것이다 [3].

SAML은 단일 인증 후 신뢰관계가 형성된 도메인간의 사이트 접근을 용이하게 하는데 적합한 표준으로서 token 역할을 하는 artifact를 전달하고 검증함으로써 SSO를 구현할 수 있다.

2.3 SAML을 적용한 SSO model의 연구

SAML을 사용한 시나리오로서 Single Sign-On을 위한 pull 시나리오와 Back Office Transaction 시나리오를 살펴본다.

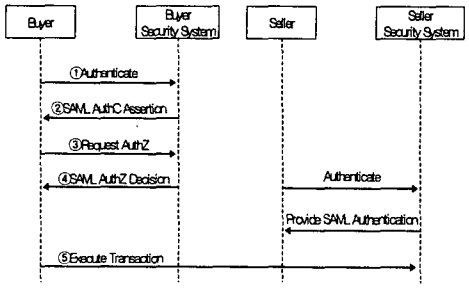


[그림 3] Single Sign-On push 시나리오

[그림 3]의 수행 과정은 다음과 같다.

① 웹 사용자는 source 웹 사이트에서 인증과정을 수행한다.
② 웹 사용자는 목적지 웹 사이트의 링크를 클릭 한다.
③ source 웹 사이트는 목적지 웹 사이트에 사용자의 인증 식별 참조를 전달하고 목적지 웹 사이트로 이동시킨다.
④ 웹 사용자는 목적지 사이트의 자원을 요청하고 인증 참조를 전달한다.
⑤ 목적지 웹 사이트는 인증 Assertion을 source 웹 사이트에 요청하면서 인증 참조를 전달한다.
⑥ source 웹 사이트는 Assertion을 전달한다.
⑦ 목적지 웹 사이트는 Assertion을 분석해 웹 사용자에게 자원을 제공한다.

[그림4]는 Back office Transaction 시나리오는 두 거래 당사자인 구매자와 판매자 간의 transaction과정을 나타낸다. 구매자 및 판매자 보안 시스템의 인증은 거래당사자 내부 처리를 따른다.



[그림 4] Back office Transaction 시나리오

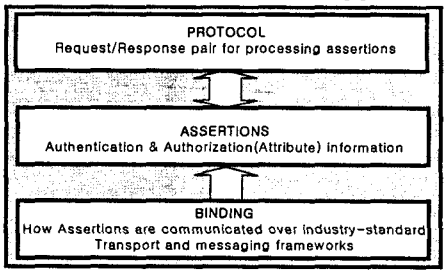
[그림 4]의 수행 과정은 다음과 같다.

① 구매자는 구매자 보안 시스템에 인증 요청을 보낸다.
② 구매자 보안 시스템은 Assertion을 전송한다.
③ 판매자는 판매자 보안 시스템에 인증요청을 보낸다.
④ 판매자 보안 시스템은 Assertion을 전송한다.
⑤ 구매자와 판매자는 Assertion을 교환한다.
이때 Assertion 내에는 거래 허용 승인을 위한 속성 정보와 인증정보가 포함된다.

2.4 SAML(Security Assertion Markup Language)

SAML[6]은 인터넷상에서의 자원 요청 자에 대한 인증, 승인, 그리고 속성확인 등을 수행하는 역할을 하며 이는 XML 기반의 다른 보안 기술들(XML Signature, XML Encryption, XKMS, XACML 등)과 통합되어 전체 보안 시스템을 구성하는 일부 요소로서 기능을 가진다.

SAML 명세는 Assertion, Protocol, Binding으로 구성되어 있다. 개괄적인 구조는 [그림 4]와 같다 [7].



[그림 4] SAML 구조

▲ Assertion

Assertion은 인증 및 승인 정보를 포함하는 XML 기반 구조를 가진다. Assertion 스키마의 구성은 [그림 5]와 같다 [6].

```
<element name="Assertion" type="saml:AssertionType"/>
 <complexType name="AssertionType">
  <sequence>
   <element ref="saml:Conditions" minOccurs="0"/>
   <element ref="saml:Advice" minOccurs="0"/>
   <choice maxOccurs="unbounded">
    <element ref="saml:Statement"/>
    <element ref="saml:SubjectStatement"/>
    <element ref="saml:AuthenticationStatement"/>
    <element ref="saml:AuthorizationDecisionStatement"/>
    <element ref="saml:AttributeStatement"/>
   </choice>
   <element ref="ds:Signature" minOccurs="0"/>
  </sequence>
  <attribute name="MajorVersion" type="integer" use="required"/>
  <attribute name="MinorVersion" type="integer" use="required"/>
  <attribute name="AssertionID" type="saml:IDType" use="required"/>
  <attribute name="Issuer" type="string" use="required"/>
  <attribute name="IssueInstant" type="dateTime" use="required"/>
</complexType>
```

[그림 6]Assertion 스키마의 구성

Assertion 엘리먼트는 하위에 여러 개의 엘리먼트들과 속성들을 갖는다. Conditions엘리먼트는 Assertion의 유효성을 검증한다. Advice엘리먼트는 Assertion 발행자가 제공하는 부가적인 정보를 포함한다. Statement와 SubjectStatement엘리먼트는 assertion기반의 다른 애플리케이션이 SAML assertion framework를 재사용할 수 있도록 하는 확장 지점의 역할을 한다.

AuthenticationStatement엘리먼트는 인증기관에서 발행한 인증 요청 자에 대한 성공적인 인증과정 수행을 보증한다. AttributeStatement엘리먼트는 인증 Assertion과 속성관리기관에서 발행하며 요청 자에 대한 자격을 확인한다. AuthorizationDecisionStatement엘리먼트는 승인기관에서 발행하는 인증된 요청 자가 요청한 자원에 대해 접근 허용 여부를 결정해 그 결과로서 발행하게 된다. Signature엘리먼트는 Assertion의 인증을 위해 XML 전자서명을 적용한다. 각각의 Assertion 발행 기관은 한 곳에 위치할 수 있다. [그림 6]은 AuthenticationStatement를 포함하는 Assertion을 생성한 결과이다.

```
<saml:Assertion AssertionID="00cda300-0d5e-8521-83c5-c2d9f6847b91"
                IssueInstant="2003-03-24T14:36:56Z"
                Issuer="verisign, Inc." MajorVersion="1" MinorVersion="0">
  <saml:Conditions NotBefore="2003-03-24T14:36:56Z"
                   NotOnOrAfter="2003-03-24T14:36:56Z" />
  <saml:Advice />
  <saml:AuthenticationStatement
                AuthenticationMethod="password"
                AuthenticationInstant="2003-03-24T14:36:56Z">
    <saml:Subject>
      <saml:NameIdentifier NameQualifier="sejong.ac.kr" >
                jijeong
      </saml:NameIdentifier>
    </saml:Subject>
  </saml:AuthenticationStatement>
</saml:Assertion>
```

[그림 7] AuthenticationStatement를 포함하는 Assertion의 결과

AuthenticationMethod속성의 값 password는 subject를 인증하는 방법을 나타낸다. subject를 인증하는 방법으로는 password방식 외에도 Kerberos, X.509 Public Key, XMKS Public Key, 그리고 XML Digital Signature 방식이 사용 될 수 있고 기타 다른 인증방식들도 사용할 수 있다.

AuthenticationInstant속성의 값은 subject를 인증한 시간을 나타내며 UTC데이터 포맷으로 인코딩 된 값이다. NameIdentifier엘리먼트는 subject의 이름과 security domain으로 subject를 식별하는 역할을 한다. NameQualifier속성은 충돌 없이 서로 다른 사용자 스토어로부터 이름을 통합할 방법을 제공한다. NameQualifier 속성은 생략이 가능하다 [6].

▲ Protocol

SAML 프로토콜은 XML 기반의 메시지 형태로서 요청 및 응답의 쌍으로 구성되어 각 Assertion에 대한 전송을 담당한다. 일반적으로 Assertion은 SAML 프로토콜의 응답을 통해 얻어진다 [8].

▲ Binding

"binding"은 SAML request/response메시지를 표준 통신 프로토콜로 교환하는 매핑으로 SAML request/response 프로토콜 전송 메커니즘으로서 SOAP을 사용한다 [8].

4. 결론

인터넷 전자상거래의 규모가 커짐에 따라 사용자가 사용할 수 있는 전자상거래 시스템의 수도 그만큼 증가하게 된다. 사용자가 이용할 수 있는 시스템이 다양할 수 록 인증을 거쳐야하는 과정은 더욱 복잡해질 것이다. 기존의 개별적인 인증방법에서 벗어나 Single Sign On 모델을 도입하므로 써 사용자는 전자상거래 시스템의 사용이 더욱 쉬워지게 되고 서비스 제공자는 기술적인 도움에 필요한 비용을 줄일 수 있을 뿐만 아니라 보안개선효과도 얻을 수 있게 될 것이다.

참고 문헌

[1] 산업자원부, 한국전자거래진흥원, 2003 e-비즈니스 백서, 2003.

[2] N. A. Nazario, *"Security Policies for the Federal Public Key Infrastructure"*, 19th NISSC, Baltimore, Oct. 22-25, 1996, pp.445-451.

[3] Single Sign On(SSO)
http://www.oasis-open.org/committees/security/docs/cs-sstc-bindings-01.pdf

[4] Research Report, Token-based Web Single Signon with Enabled Clients
IBM Research Zurich Research Laboratory 8803 Ruschlikon Switzerland

[5] Netegrity, Inc
"Security Assertions Markup Language(SAML)" The standard XML framework for secure information exchange.

[6] Jason Rouault,
"Introduction to SAML An XML based security Assertion Markup Language"

[7] Dournaee, "XML Security"