SAML기반의 보안 서비스 관리에 관한 연구

차석일, 김현희, 송준홍, 이형석, 신동일, 신동규
세종대학교 컴퓨터공학과
e-mail: {kiry, hyunhee, song0424, bestehen, dshin, shindk}@gce.sejong.ac.kr

A Study of Security Service Management based on SAML

Suk-Il Cha, Hyun-Hee Kim, Jun-Hong Song, Hyoung-Seok Lee, Dongil Shin, Dongkyoo Shin
Department of Computer Engineering, Sejong University

요약

인터넷에서 비즈니스 파트너 사이에 보안 정보를 교환하는 XML 프레임워크인 SAML (Security Assertions Markup Language)은 국제적 컨소시엄인 OASIS(the Organization for the Advancement of Structured Information Standards)에 의해 제정된 표준이다. SAML은 S2ML(Security Services Markup Language)의 원리와 구조를 재사용하고, 신뢰할 수 있는 Single Sign-On, 인증 서비스, B2B Transaction, Sessioning같은 기능을 가진다. 다양한 정책기반의 산업에서의 보안 시스템, 자바 어플리케이션 서버, XML 메시징 프레임워크와 다양한 오퍼레이팅 플랫폼사이에 인증, 승인과 함께 프로필 정보를 교환하기 위해 사용된다. 본 논문에서는 SAML의 기반으로 인터넷에서 여러 기업들이 보안문서를 교환할 때 여러 가지 솔루션과 함께 쓰고 공유하는 안전한 언어에 대해서 논한다.

1. 서 론

SAML(Security Assertions Markup Language)은 XML에 기반을 둔 인터넷 비즈니스 파트너 사이의 보안 정보 교환을 목적으로 하는 프레임워크이다. 이것은 공통의 산업 명세를 만드는 국제적인 컴소시엄인 OASIS(the Organization for the Advancement of Structured Information Standards)에 의해 표준화되었다. SAML은 Netigrity사에서 제정된 S2ML(Security Services Markup Language)의 공인되고 신뢰된 기능만을 정의하고, 가능한 많은 원리와 구조를 재사용 하였기 때문에, S2ML과는 유즈케이스를 접하는 범위와 목적에서 차이점이 있지만 주요 목적인 보안서비스의 제공과 서로 다른 시스템들 사이에 상호이용이 가능하게 하는 것이라는 점에서 유사점을 가진다[1].

SAML 명세는 S2ML과 비교할 때, 새로운 기술을 정의하지는 않으나, 인증과 승인에 대한 새로운 표준을 제시한다. 시스템에 의해 전송되는 기술된 정보나 출력 값을 XML을 사용하여 간단히 표현 할 수 있다[2].

전통적으로 보안은 기업내부의 일이었지만 현재 대부분의 기업들은 그들의 전자상거래시에 편의성과 확장성을 도모하기 위해 서로 다른 기업간에 웹으로 제휴를 맺고 있는 경우가 많다. 이러한 상황은 B2C에서의 사용자 혹은 B2B에서의 XML 기반의 문서 교환에서부터 시작한다. 처음 한 사이트에서 서비스를 제공하면 다른 사이트도 보안을 공유하게 되고, 웹은 다양한 업무가 항상 상주하게 된다. 이러한 전자상거래시에 SAML은 다음의 이점을 가진다.

첫 번째로 상호 운용성이 있다. SAML을 사용해서 전자상거래 사이트, 서비스 제공업자, 회사들은 사용자에 관한 정보를 안전하게 교환 할 수 있다. 현재 보안 솔루션을 교환하기 위한 중간 과정의 필요 없이 사용자와 웹 서비스의 인증된 정보에 관한 정보를 안전하게 교환할 수 있다. SAML은 서로 다른 시스템 하에서 보안에 관한 자료를 전달하기 위한 공통 언어이다.

두 번째로 개방된 솔루션을 들 수 있다. SAML은 SOAP(Simple Object Access Protocol), Biztalk과 ebXML(Electronic Business eXtensible Markup Language)같은 다양한 XML 문서 교환뿐만 아니라 HTTP, SMTP, FTP와 같은 다양한, 산업 표준 전송 프로토콜도 지원하도록 설계된다.

마지막으로 사이트간에 Single Sign-On기능을 들 수 있다. SAML을 이용하면 사용자는 사용자 인증을 한 사이트나 기업에서 받은 후에 인증해준 사이트나 기업과 서로 인증된 파트너 기업의 사이트를 검색할 수 있다[3][4].

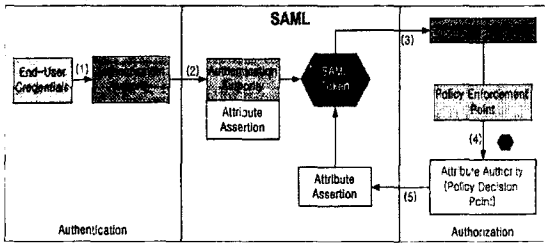
2. 범위와 목적

주장(Assertion)은 식별자, 속성 정보, 권한 부여의 선언을 제정하는 SAML 기관에 의해 만들어진 자료이다. 기본적인 SAML 객체들은 인증 주장(Authentication assertion)과 속성 주장(Attribute assertion)으로 나뉜다.

SAML 주장들은 요청/응답 프로토콜을 사용하는 주체들에 의해 받아들여지고 갱생되며, SAML 주장들은 ebXML(Electronic Business eXtensible Markup Language)과 같은 산업 표준 전송 메시징 프레임워크들에 내장된다. 인증 주장은 인증을 위한 설명을 포함하고 있으며, 속성 주장은 인증 결정을 만들기 위해 사용되어진 서비스에 대해 식별자, 그룹, 역할 그리고 다른 사용자의 프로필 정보와 같은 속성을 가진다. SAML 주장은 상업용 웹 브라우저, HTTP(Hypertext Transfer Protocol), MIME(Multi-Purpose Internet Mail Extensions), SOAP(Simple Object Access Protocol), ebXML(Electronic Business eXtensible Markup Language)등과 같은 산업 표준 전송에 따르는 바인딩 SAML정보와 메시징 프레임워크를 가지기 때문에 표준 인터넷 프로토콜 상에 공유된다. 각각의 경우를 살펴보면, 상업용 웹 브라우저에서 SAML 주장들은 쿠키나 URL문자를 통해 웹 브라우저로 전달된다. 이러한 전달은 HTTP상에서 소스 사이트에서 목적지 웹사이트를 경유하는 동안 헤더 또는 HTTP POST를 통해 운반된다. MIME은 MIME 보안 패키지로 패키징된다. SOAP에서는 부담을 줄이고 안전성을 높이기 위해 SOAP 문서의 포장 헤더를 묶어두는 방법을 쓴다. ebXML에서는 기업 임금 부담에 SAML주장을 묶어두기 위해 MIME기반 패키징 구조를 제공한다. SAML은 새로운 암호의 기술 또는 보안 모델을 정의하지 않으므로 XML기반으로 사용하고 있는 산업 표준 보안 기술을 묘사하는데 사용된다. 또한 제휴한 웹사이트들 사이에 이전을 제공하지 않기 때문에 인증 환경에서 SAML의 사용을 전제로 하는 조건으로 행해져야만 한다. 현재 SAML은 인증 정책을 표현하는 데이터 포맷을 정의하지 않기 때문에 보안 시스템의 인증과 승인 서비스는 구현하는 시스템에 따라 다양하다[5].

3. 유즈케이스 모델

SAML의 정의는 유즈케이스에 기본으로 둔다. 그 중 가장 기본적인 유즈케이스는 아래[그림 1]과 같이 보호된 자원을 접근하는 최종사용자로 표현된다. [그림 1]에서는 SAML의 각각의 요소들의 진행과정을 보여주고 어떻게 인증서를 안전하게 보내는지를 보여준다[6].



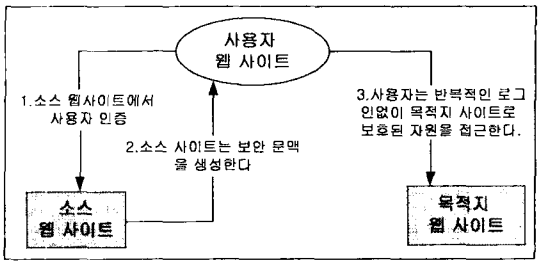
[그림 1] 기업과 소비자간의 보안문서 전달 과정

(1) 최종사용자는 인증기관(Authentication Authority)에 증명서를 보낸다.
(2) 인증기관은 사용자 디렉토리에 사용자 증명서를 주가하고 하나 이상의 속성 주장과 함께 인증 주장을 생성한다. 최종사용자는 토큰에 어셈블리된 SAML 주장들에 의해 인증되고 식별된다.
(3) 최종사용자는 SAML 토큰을 사용한 보호된 자원으로 접근을 시도한다.
(4) PEP(Policy Enforcement Point)는 자원을 보호하기 위해 최종 사용자의 요청을 차단하고, 속성 기관 (잘 알고 있는 SAML 보안 엔진 또는 기업 어플리케이션)에 최종 사용자의 SAML 토큰(인증 주장)을 제출한다.
(5) 인증기관(Attribute Authority) 또는 PDP(Policy Decision Point)는 정책기반으로 결정한다. 만약 자원을 접근하는데 인증된다면, 사용자의 SAML 토큰을 추가하는 속성 주장을 생성한다. 최종 사용자의 SAML 토큰은 single sign-on관계로 제휴를 맺은 믿을 수 있는 기업 파트너에게 건네줄 수 있다[4][5].

4. SAML 유즈케이스 시나리오

4.1 믿을 만한 환경의 Single Sign-On

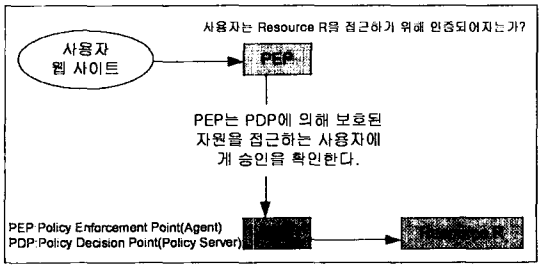
사용자는 웹사이트 자료와 함께 인증된 후 다른 웹사이트(목적지 웹사이트)에 자기 자신을 재 인증하지 않고 다른 웹사이트의 보호된 자원을 접근한다.



[그림 2] Single Sign-On (SSO)

4.2 인증 서비스(Authorization Service)

이 모델에서 사용자는 보호된 자료나 웹 서비스에 인증을 받는다. 자료(PEP) 보안 관리자는 PDP를 통해서 자료에 대한 인증을 검사한다. 보통 사용자는 웹서버의 동적 자료에 대해 요청을 보내고, 웹서버는 요청서비스를 받아들이기 전에 사용자 정보를 체크한다. 이 시나리오에서, 보안 서비스는 증명서 관리자, 인증관리, 속성관리, PDP로써 역할을 한다. 백 엔드 어플리케이션은 PEP로써 역할을 한다.



[그림 3] 인증 서비스

4.3 B2B 전송(Business-To-Business Transaction)

이 시나리오는 XML문서 기반의 트랜잭션에 포함된 파트너들에 대해 설명한다. 이 모델에서는 각 파트너가 자신의 보안 시스템을 통해 인증하거나 또는 3rd-party의 보안 서비스 엔진을 사용해서 인증 가능하다. 이 경우 파트너는 트랜잭션을 인증하기 위해 자신의 보안시스템으로 제공된 인증 데이터를 교환한다. 파트너는 중개자처럼 B2B 교환을 사용하여 기업 트랜잭션을 들어갈 수 있다. 이 중개자는 트랜잭션에 포함된 파트너에 의해 만들어진 결정을 위해 부가적인 포인트를 주어 트랜잭션 처리를 통해 정렬하기 위한 인증과 인증된 데이터를 추가한다. 이

모델에서 파트너는 PEP같이 주된 역할을 한다.

4.4 세션(Sessioning)

이 시나리오는 최종사용자는 single sign-on 서비스의 부분인 웹사이트로 항해하는 것처럼 유지되는 세션의 기술을 포함한다. 소스 웹사이트는 인증관리, 속성관리와 세션관리로써 역할을 한다. 소스 사이트는 PDP와 PEP로써 역할을 한다.

5. SAML 기본 구조

기본적인 SAML 주장들은 인증(Authentication)과 속성(Attribute)의 2가지 다른 타입으로 구성된다.
인증은 시스템 엔터티의 일치를 입증하는 과정이다.

```
<saml:Assertation
  MajorVersion="1" MinorVersion="0"
  AssertionID="186CB37D-5C81-4716-8F65-F0B4FC4B4A0B"
  Issuer="                    "
  IssueInstant="2001-05-31T13:20:00-05:00">
  <saml:Conditions
    NotBefore="2001-05-31T13:20:00-05:00"
    NotAfter="2001-05-31T13:25:00-05:00"/>
  <saml:AuthenticationStatement
    AuthenticationMethod="password"
    AuthenticationInstant="2001-05-31T13:21:00-05:00">
    <saml:Subject>
      <saml:NameIdentifier>
        <SecurityDomain>"                    "</SecurityDomain>
        <Name>"cn=Alice,co=example,ou=sales"</Name>
      </saml:NameIdentifier>
    </saml:Subject>
  </saml:AuthenticationStatement>
</saml:Assertion>
```

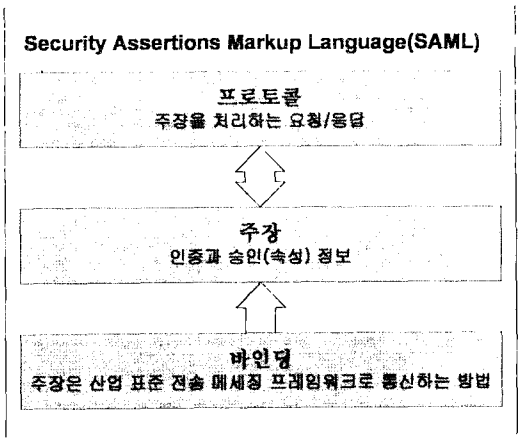
[그림 4] 인증 주장(Authentication Assertion) 예

속성은 생성된 SAML 주장의 시스템 엔터티에 관한 것이고 여러 가지 프로토콜의 사용에 따라 바뀐다.

```
<saml:Assertation…>
  <saml:Conditions>…</saml:Conditions>
  <saml:AttributeStatement>
    <saml:Subject>
      <saml:NameIdentifier>
        <SecurityDomain>"                    "</SecurityDomain>
        <Name>"cn=Alice,co=example,ou=sales"</Name>
      </saml:NameIdentifier>
    </saml:Subject>
    <saml:Attribute>
      <AttributeName>"NetWorthSummary"</AttributeName>
      <AttributeNamespace>"                    "</
    AttributeNamespace>
      <saml:AttributeValue>
        <CreditSummary>
          <HistoryScore>"Excellent"</HistoryScore>
          <CurrentAssets>"Loaded"</CurrentAssets>
        </CreditSummary>
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

[그림 5] 속성 주장(Attribute Assertion) 예

SAML 프로토콜 명세에서 응답자는 지정된 타입의 주장을 한 쌍의 요청/응답으로 정의된 메시지를 요청자에게 보낼 수 있도록 되어 있는 프로토콜을 사용한다.
SAML 바인딩 명세는 여러 가지 산업 표준 전송 프로토콜과 메시징 프레임워크를 통해 SAML 주장에서 요청지 웹에서 목적지 웹까지를 통신하는 방법을 정의한다.
주장 바인딩은 HTTP(Hypertext Transfer Protocol), MIME(Multi-Purpose Internet Mail Extensions), SMTP(Simple Mail Transfer Protocol), ebXML(Electronic Business eXtensible Markup Language), SOAP/XP, BEEP로 지정된다[4][5][7].



[그림 6] SAML의 기본 구조

6. 결론

앞으로 인터넷 전자상거래 시장에는 SAML로 구현한 전자상거래 보안 기술 컴포넌트가 나올 것이다. 이것은 유즈케이스 시나리오를 이용한 인증 서비스, B2B Transaction, 최종사용자를 위한 세션 기술을 포함할 것이다. 이것은 single sign-on 기술로 서로 다른 웹사이트를 접근할 때 인증을 유지되는 기술이다. 이러한 기술뿐만 아니라, SAML은 현재 다양한 부분에서 활발한 활동을 하고 있으며 빠른 속도로 더 나은 기술의 개발이 진행될 것으로 예상된다.

7. 참고문헌

[1]S2ML: Security Services Markup Language, Version 0.8a, January 8, 2001.http://www.oasis-open.org/committees/security/docs/draft-s2ml-v08a.pdf
[2][XML-SIG] D. Eastlake, J. R., D. Solo, M. Bartel, J. Boyer , B. Fox , E. Simon. *XML-Signature Syntax and Processing*, World Wide Web Consortium. http://www.w3.org/TR/xmldsig-core/
[3]http://www.oasis-open.org/commitees/security/
[4]http://xml.coverpages.org.saml.html
[5]http://www.netegrity.com
[6]http://www.fawcette.com/xmlmag/2002_02/magazine/columns/collaboration/edejesus/
[7]Charles P. Pfleeger "Security in Computing" Prentce Hall PTR, Upper Saddle River, NJ07458