프로토콜 바인딩 기법을 적용한 단일인증기반 이질적 인증시스템의 통합에 관현 연구

권오현[0] 황 준 김영찬
중앙대학교 컴퓨터공학과
{ohkwon[0], yckim}@sslab.cse.cau.ac.kr

A study on Integration of SSO-based heterogeneous authentification systems using protocol binding

Ohyun Kwon[0] Jun Hwang Youngchan Kim
Dept. of Computer Science and Enginerring, Chung-Ang University

요 약

인터넷의 사용이 날로 증가함에 따라 전자상거래가 인터넷을 통해 활발하게 이루어지는데 있어서 금융권 및 각종 기타 기관에서는 인증서 기반의 전자서명을 사용하고 있다. 이러한 인증서 기반의 시스템은 궁극적으로 SSO(Single Sign-On)를 지향하는데, 동일 인증기관 내의 모든 서비스는 단 한 번의 접속으로 모두 사용할 수 있게 하는 것이 그 목적이다. 그러나 SSO는 동일 인증기관이라는 제약사항이 따르기 때문에 인터넷을 이용하는 사용자들이 각 인증기관별로 인증서를 따로 관리하게 되는 불편함이 생기게 된다. 따라서 본 논문에서는 OASIS에서 발표한 SAML을 이용하여 다른 이질적인 인증 기관간의 인증을 통합 할 수 있는 방법을 제시하고자 한다.

1. 서 론

최근 웹 서비스에 대한 사용자 요구가 늘어나고 있는 추세이며, 이에 인터넷을 상거래에 활용하는 노력이 전자상거래라는 형태로 등장하고 있다. 이러한 전자상거래에서 가장 중요하게 대두되는 부분이 보안이다.

전자상거래는 서면 방식이 아닌 비 대면적인 전자적 거래정보교환으로 이루어지기 때문에, 거래에 있어서의 각종 정보가 불법노출, 부당거래, 자원의 불법적인 접근, 서비스 거부 등의 보안 침해를 받을 수 있다.

이에 대한 대안으로서 금융권 및 각종 기타 기관에서는 인증서 기반의 전자서명을 사용하고 있다. 이러한 인증서 기반의 시스템은 궁극적으로 SSO(Single Sign-On)를 지향하는데, 이는 동일 신뢰기관(CA) 내의 모든 서비스는 단 한 번의 접속으로 모두 사용할 수 있게 하는 것이 그 목적이다. 그러나 SSO는 동일 인증기관이라는 제약사항이 따르기 때문에 이질적인 보안 시스템에 관해서는 사용할 수 없게 된다. 그 결과 사용자는 각각의 인증기관별로 인증서를 따로 관리해야 하는 불편함이 생기게 된다.

따라서 이질적인 인증기관간의 통합을 해줄 수 있는 표준이 필요한데, 본 논문에서는 이를 해결하는 방안으로서 OASIS의 표준안인 SAML을 제안하고, SAML을 이용하여 불필요한 인증절차 없이 이질적인 신뢰된 인증기관 내의 서비스를 이용할 수 있는 구조(SSO)를 설계 및 구현하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서 관련연구, 3장에서는 본 논문에서 제안하는 SAML을 이용한 SSO를 설계할 것이며, 4장에서는 제안 기법에 대한 성능을 비교분석하고, 마지막으로 5장에서는 결론 및 향후 연구과제를 제시한다.

2. 관련 연구

2.1 PKI(Public Key Infrastructure) 인증 시스템

PKI는 공개키 알고리즘을 위한 키 관리 구조로서 X.509기반으로 자신의 공개키를 공표하고, 개인키를 비밀스럽게 간직함으로서 이증의 보안을 거치는 기반구조이다. 먼저 인증을 하는 인증기관(CA)는 인증서에 포함된 Public Key를 사용하여 사용자의 인증서를 확인하고, 인증기관이 소유한 Private Key를 사용하여 전자서명(Digital Signature)을 생성하여 인증서에 첨부하게 된다. 이러한 인증과정을 통해 사용자의 신분확인이 끝나면, 인증된 클라이언트는 인증기관 내의 모든 서비스를 이용할 수 있게 되는 형태의 기본 구조로 되어 있다. 기본적으로 SSO를 그 목적으로 하고 있지만 이질적인 환경에서의 SSO를 지원하지 못하는 단점이 있다.

2.2 커베로스(Kerberos) 인증 시스템

커베로스는 개방된 컴퓨터 네트웍 내에서 서비스 요구를 인증하기 위한 티켓 기반 인증 시스템이다. 커베로스는 사용자가 인증 과정으로부터 암호화된 "티켓"을 요청할 수 있게 해주는데, 이 티켓은 서버에 특정 서비스를 요구하는데 사용될 수 있도록 인증역할을 하는 방식이다. 하지만 커베로스 또한 이질적인 환경에서의 SSO를 지원하지 못하는 단점이 있다.

2.3 SAML(Security Assertion Markup Language)

SAML은 국제 컨소시엄인 OASIS(the Organization for the Advancement of Structured Information Standards)에서 제정된 표준이며 S2ML(Security Services Markup Language)의 원리와 구조를 재사용하고, 신뢰할 수 있는 Single Sign-On, 인증 서비스, B2B Transaction, Sessioning같은 기능을 가진다. SAML 구

조는 SAML 주장(Assertion), 프로토콜(Protocol), 바인딩(Binding)과 프로파일(Profile)로 분류할 수 있는데, 이 중에서 주장은 인증, 속성, 권한으로 구성되고, 전자서명으로 승인된다. 이른바 SAML의 주장이 단일인증의 필수요소를 내포하고 있으며, 프로토콜 바인딩을 통해서 보안 도메인 또는 여러 권한 정책을 가지는 여러 사이트에서 단일인증을 실현할 수가 있다. 즉, 본 논문에서는 이러한 특성을 가지고 있는 SAML을 이용하고자 한다.

2.4 SOAP 프로토콜

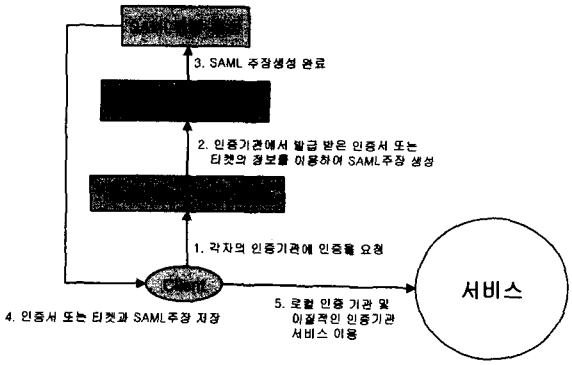
SOAP은 웹상에서 구조화되고 활자화된 정보를 교환할 수 있도록 디자인된 가볍고 간편한 XML프로토콜로서 HTTP, SMTP 등과 같은 기존 프로토콜과 병합하여 사용 될 수 있으며 메시지 시스템으로부터 RPC에 이르기까지 광범위한 프로그램에서도 사용할 수 있는 프로토콜이다. SOAP 메시지는 [그림]과 같이 구성되어 있으며, 문서화된 XML데이터를 보낼 방법을 정의하는 프로토콜로 정의되기 때문에 SOAP 자체적으로 인코딩하는 방법을 표준안에 명시하고 있다. 따라서 본 논문에서는 SOAP스키마만 알고 있다면, 어느 시스템에서든 사용할 수 있도록 설계되어 있는 SOAP프로토콜을 사용하여 이질적인 인증시스템 간에 통신수단으로 사용하고자 한다.

3. 제안하는 Single Sign-On 설계

3.1 기본 설계

SSO(Single Sign-On)은 사용자가 네트워크에 한번 로그온 하여, 허가된 모든 자원에 접근할 수 있도록 하는 것을 의미한다. 그러나 인증기관이 다른 경우에는 다른 인증기관을 거칠 때마다 다시 인증을 받아야 한다. 따라서 본 논문에서는 이러한 문제의 해결을 위하여, 서로 다른 이질적인 인증기관 중 가장 대표적인 PKI와 Kerberos간의 통합을 SAML Assertion을 생성하여 이질적인 인증기관 간의 SSO를 가능하게 하는 메커니즘을 제안한다.

사용자는 각자 자신이 속한 인증기관에서 인증을 받은 후에 SAML 주장 생성 모듈에 의해 SAML 주장을 생성한다. 이 때 생성되는 주장은 인증 주장이며, 이 인증주장을 기반으로 속성주장과 승인결정주장을 생성하게 된다. [그림 1]에서 보듯이 클라이언트는 각자의 인증기관에 해당하는 CA 또는 TGS에 인증을 요청하면, 인증기관에서는 클라이언트의 요구사항을 검토하고 타당성 여부를 판정하여 인증서 또는 티켓을 발급하게 되며, 발급된 티켓은 SAML주장생성 모듈을 통과하면서 SAML 인증주장을 생성하게 된다. 클라이언트는 이 SAML 주장을 이용해 서비스내의 허가된 모든 영역을 다른 인증 절차 없이 사용할 수 있게 된다. 또한 이질적인 인증기관 서비스를 이용할 때는 SOAP프로토콜을 통해 전송된 SOAP 메시지를 분석하여, SAML 주장이 생성되었음을 확인 후 서비스 사용을 허가해주게 된다. 이때 문서의 보안은 신뢰성이 있는 인정된 SSL을 사용함으로서 본 논문에서 요구하는 신뢰성 있는 SSO를 만족하게 된다.



[그림 1] SSO 인증 메커니즘

3.2 구체적인 설계

3.2.1 SAML 인증주장

인증서의 내용을 기반으로 SAML 주장을 생성하여 나온 결과물은 텍스트 형태의 XML문서이다. 본 논문에서의 제안기법은 SAML의 표현기법을 사용한다. [그림 2]는 클라이언트에게 요청받은 인증기관에서 SAML주장생성 모듈을 통과해 생성된 인증주장이다. 이는 서울여자대학교의 PKI인증 시스템인 "grid.swu.ac.kr"이라는 인증기관에 중앙대학교 시스템 소프트웨어연구실의 happydate라는 이름의 클라이언트가 인증을 받아 생성된 인증 주장을 표현하고 있다. 또한 CA역할을 수행하는 "grid.swu.ac.kr"의 AuthenticationMethod는 PKI기반의 X.509를 사용하고 있으므로 AuthenticationMethod의 값은 'X509-PKI'가 되어짐을 볼 수 있다.

```
<saml : Assertation
  ......................
  Issuer="grid.swu.ac.kr"
  ......................
  <saml:AuthenticationStatement
    AuthenticationMethod="X509-PKI"
      ......................
      <saml : NameIdentifier>
        <SecurityDomain>"happydate.cse.cau.ac.kr"</SecurityDomain>
        <Name>"cn=happyate sn=sslab co=cau o=ac ou-kr"</Name>
  ..............................
</saml:Assertion>
```

[그림 2] SAML 인증주장

3.2.2 SAML 속성주장

생성된 SAML인증주장은 시스템의 구성에 관한 것이고 사용하는 프로토콜에 따라 바뀔 수 있다. [그림 3]는 Kerberos인증 시스템 내의 서비스인 "grid2.swu.ac.kr"에게 메시지를 "Hello"로 표현하는 속성주장을 보여주고 있다

3.2.3 SAML 응답

SAML 프로토콜에서 응답자는 지정된 타입의 주장을 한 쌍의 요청/응답으로 정의되어 있는 메시지를 요청자에게 보낼 수 있도록 되어있는 프로토콜을 사용하고 있다.[그림 4]

```
<saml : Assertation
  ..... .............
    <saml: NameIdentifier>
  <SecurityDomain>"happydate.cse.cau.ac.kr"</securityDomain>
   .... ........................
   <saml:Attribute>
     <AttributeNamespace>"grid2.swu.ac.kr"</AttributeNamespace>
     <saml:AttributeValue>
      <CreditSummary>
         <message>"Hello"</message>
        ........................
</saml-Assertion>
```

[그림 3] SAML 속성 주장

```
<samlp : Response
  ....................
  Issuer-"grid.swu.ac.kr"
  StatusCode-"Success">
  <saml : Assertation
    ..... ........................
    Issuer-"grid.swu.ac.kr"
    <saml:Conditions
      NotBefore-"2003-09-20 22:53:58-24:00"
      NotAfter-"2003-09-20 22:53:58-24:00"/>
  ....................
</samlp:Request>
```

[그림 4] SAML 응답

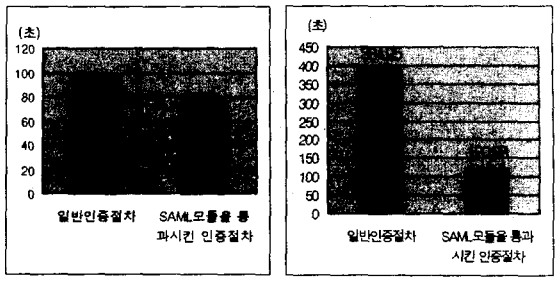
3.2.4 SAML 바인딩

SAML 바인딩은 여러 가지 산업 표준 프로토콜과 메시징 프레임워크를 통해 SAML 주장에서 요청서비스에 이르기까지 일련의 통신방법을 정의한다. 본 논문에서는 2.4에서 설명한 SOAP메시지를 통한 SOAP/XP 바인딩을 사용할 것이다. 따라서 이질적인 서비스를 사용하고자 할 때는 SOAP프로토콜을 통해 전송된 SOAP메시지의 바디 내에 SAML 요청/응답을 분석하여 SAML 주장이 생성되었음을 확인 후 서비스 사용을 허가해주는 방식이다.

4. 성능 평가

일반적으로 사용되어지는 각 인증기관별 인증서를 따로 발급받아 이질적 인증기관을 통과할 때마다 다시 인증을 받는 방법과 본 논문에서 제안하는 SAML을 이용한 인증방법을 비교분석한다. 실험환경으로는 X.509 PKI 인증시스템과 Kerberos V5 인증 시스템을 사용하였다. 또한 각 인증시스템은 일반적인 사양으로 구성되어 있으며 커널버전 2.4.2를 사용하였다.

[그림 5]은 이질적인 인증 시스템간의 연동이 이루어졌을 경우, 일반인증절차와 SAML모듈을 통과시킨 인증절차의 결과이다. (a)의 일반인증절차는 PKI에서 인증을 받은 후에 Kerberos 인증절차를 다시 한 번 거치는 경우와 Kerberos에서 인증을 받은 후에 PKI 인증 절차를



(a) (b)

다시 한 번 거치는 경우의 평균치를 나타낸다. 본 논문에서 제안하는 SAML모듈을 통과시킨 인증절차의 평균치가 일반인증절차보다 적은 시간이 소요되는 것을 볼 수 있다. (b)의 경우는 각 인증시스템에서 사용하고자 하는 서비스가 50개씩으로 증가시켜 보았을 때의 결과이다. (a)와 (b)의 결과에서 알 수 있듯이 인증시스템을 통과하는데 걸리는 시간이 가장 큰 비중을 차지하고 있음을 알 수 있다. 따라서 본 논문에서 제안하는 메커니즘을 사용할 경우 현격한 성능의 향상을 가져옴을 알 수 있다.

5. 결론 및 향후 연구과제

본 논문의 실험 및 성능 평가에서 보듯이 제안한 인증시스템은 이질적인 인증 시스템을 통과할 때는 현격한 성능향상을 보여주었다. 따라서 인증시스템의 종류가 다양하고 이질적인 인증환경 내의 서비스 이용이 많은 시스템에서는 SAML모듈을 통과한 인증방법이 효과적일 것이다. 하지만 제안하는 시스템은 인증기관에서 발급된 인증서 또는 티켓이 모듈을 거쳐 SAML주장을 생성하게 되므로 SAML주장 생성 모듈을 통과하는데 걸리는 부가적인 오버헤드가 발생하게 된다. 따라서 로컬 인증기관 내의 서비스만을 이용 할 시에는 오히려 부하를 증가시키는 불필요한 요소가 될 위험이 있다.

6. 참고문헌

[1]SAML기반의 보안 서비스 관리에 관한 연구, 차석일, 김현희, 송준홍, 이형석, 신동일, 신동규, 정보과학회 2002년 춘계학술대회, VOL.29, NO.01, pp.0793~0795

[2]Eve Maler, Prateek, Mishra, "SAML assertion and profile", http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf,

[3]SAML V1.1 Standard Specification, OASIS, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security, 2003