Shibboleth e Google Apps

Francesco Malvezzi

Università di Modena e Reggio nell'Emilia

17 giugno 2009

Panoramica

- funzionamento di default di Shibboleth;
- autenticazione SAML con Google Apps;
- indicazioni su come integrare Google Apps con Shibboleth 2.0;
- qualche considerazione sulla sicurezza.

SAML (Security Assertion Markup Language)

- *XML-based framework for marshaling security and identity informations and exchanging it across domain boundaries*
- Standardizza le fasi, il tipo ed il formato dei messaggi nelle asserzioni di autenticazione autorizzazione.
- Riferimenti: SAML v2.0 Basics di Eve Maler (`http://www.oasis-open.org/committees/download.php/12958/SAMLV2.0-basics.pdf`)
- SAML definisce vari casi d'uso (profili), cioé combinazioni di scambi di messaggi con certi protocolli in una certa sequenza.

Shibboleth

Shibboleth è un potentissimo sistema di autenticazione e single sign-on per il web conforme alle specifiche SAML2.
Oltre alla flessibilità e all'adesione agli standard, offre un livello di sicurezza molto elevato.

Attori in un'autenticazione Shibboleth

In una autenticazione tutta Shibboleth gli attori sono:

- Identity Provider: convalida l'identità degli utenti e rilascia i loro attributi;
- Service Provider: protegge una risorsa web.

Profilo SAML di Shibboleth (Shibboleth-IdP 1.3)

Il flusso è:

- l'utente che desidera accedere a una risorsa protetta (SP) viene ridiretto sulla pagina di login dell'IdP Shibboleth;
- ad autenticazione avvenuta, Shibboleth IdP ridirige il browser dell'utente al servizio richiesto. Il browser veicola un identificativo opaco che identifica la sessione si autenticazione;
- il Service Provider dietro le quinte, con una chiamata SOAP autenticata e cifrata, richiede gli attributi dell'utente all'IdP ed usa l'identificativo opaco come chiave;
- se del caso il Service Provider usa gli attributi utente per l'autorizzazione o le proprie elaborazioni

Esempio

https://idem-moodle.unimore.it

Log della transazione:

```
08:53:31.132 - INFO [Shibboleth-Audit:675] - 20090611T065331Z|
urn:mace:shibboleth:1.0:profiles:AuthnRequest||https://moodle-
idem.unimore.it/shibboleth|urn:mace:shibboleth:2.0:profiles:sa
ml1:sso|https://omissis.unimore.it/idp/shibboleth|urn:oasis:na
mes:tc:SAML:1.0:profiles:browser-post|_9ed0c14985de917958a3465
ba2af9825|malvezzi|urn:oasis:names:tc:SAML:2.0:ac:classes:Pass
wordProtectedTransport||_74e40c1730e9d3bacdeb6aa340cb9220|_829
059b4672ee9761ce66d0224d125af,|
08:53:31.265 - INFO [Shibboleth-Audit:675] - 20090611T065331Z|
urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding|_374fe50aeec
1c9a11ae960f7ece81987|https://moodle-idem.unimore.it/shibbolet
h|urn:mace:shibboleth:2.0:profiles:saml1:query:attribute|https
://omissis.unimore.it/idp/shibboleth|urn:oasis:names:tc:SAML:1
.0:bindings:SOAP-binding|_000c346ca1098d2abaf170311df68797|mal
vezzi||uid,eduPersonPrincipalName,surname,eduPersonScopedAffil
iation,givenName,commonName,transientId,eduPersonTargetedID,em
ail,|_74e40c1730e9d3bacdeb6aa340cb9220|_9ef9ca67cdefd88bff0094
8db540d35e,|
```

Da notare

- il browser utente non trasporta mai dati personali (solo il token);
- per ottenere gli attributi utente il Service Provider si autentica con un certificato utente x509.

Un impostore dovrebbe avere il controllo dello SP per possedere sia il nome DNS (per ottenere il token dopo la ridirezione), sia la chiave privata per autenticarsi sull'IdP.

Google Apps

- Google Apps è un insieme di utility tra cui un web client di posta elettronica.
- Permette autenticazione con Single Sign-On con un profilo SAML2.
- È disponibile gratuitamente per le istituzioni universitarie.

Profilo SAML di Google Apps

Il flusso è:

- l'utente che desidera accedere alla webmail gmail viene ridiretto sulla pagina di login dell'IdP SAML;
- ad autenticazione avvenuta, lo IdP SAML ridirige il browser dell'utente al servizio richiesto su https. Il browser veicola lo Id dell'utente che è quanto basta a Google Apps per fornire l'accesso alla giusta casella di posta.

Integrazione di Google Apps con Shibboleth

Il documento base è: “Achieving Single Sign-on with Google Apps and Shibboleth 2.0” di Will Norris, University of Southern California (`https://shibboleth.usc.edu/docs/google-apps/`)
In due parole: c’è una fase di configurazione di Google Apps dell’interfaccia web e una fase di configurazione di Shibboleth IdP per supportare il profilo SAML2SSO Profile e per rilasciare, anziché un identificativo opaco, lo Id utente.

Notazione del NameID

Notare l'eleganza di Shibboleth 2 che definisce attributi utenti e identificativi della sessione con la stessa notazione:

```
<resolver:AttributeDefinition id="principal"
 xsi:type="PrincipalName"
 xmlns="urn:mace:shibboleth:2.0:resolver:ad">
    <resolver:AttributeEncoder xsi:type="SAML2StringNameID"
    xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
    nameFormat="urn:oasis:names:tc:SAML:1.1: \
    nameid-format:unspecified" />
</resolver:AttributeDefinition>
```

Un’aggiunta al attribute-filter.xml

Consiglio di non rilasciare il TransientID a Google Apps:

```
<AttributeFilterPolicy id="releaseTransientID">
        <PolicyRequirementRule xsi:type="basic:NOT">
               <basic:Rule
               xsi:type="basic:AttributeRequesterString"
               value="google.com" />
        </PolicyRequirementRule>
        <AttributeRule attributeID="transientId">
            <PermitValueRule xsi:type="basic:ANY" />
        </AttributeRule>
</AttributeFilterPolicy>
```

attribute-filter.xml

Esempio

`http://start.studenti.unimore.it`
Log della transazione:

```
09:58:58.868 - INFO [Shibboleth-Audit:898] - 20090603T075858Z|
urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect|iabgflpcipa
hmkopifecbdpjgllgbboffmfdbmfm|google.com|urn:mace:shibboleth:2
.0:profiles:saml2:sso|https://idp.unimore.it/idp/shibboleth|ur
n:oasis:names:tc:SAML:2.0:bindings:HTTP-POST|_a414f70a09ed7527
a59534b9f61885f4|malvezzi|urn:oasis:names:tc:SAML:2.0:ac:class
es:PasswordProtectedTransport|eduPersonScopedAffiliation,princ
ipal,|malvezzi|_672d691e34e23c24f459709fef47b40c,|
```

Conclusioni

- Shibboleth è molto flessibile;
- per adattare Shibboleth a Google Apps bisogna accettare alcuni compromessi di sicurezza;
- d'altra parte i compromessi di sicurezza sfigurano di fronte agli ovvi compromessi sulla tutela della privacy degli utenti.