Shibboleth, SAML e SSO

Francesco Malvezzi

Università di Modena e Reggio nell'Emilia

30 marzo 2009

Introduzione

Lo scopo di questo tutorial è:

- fare conoscenza con Shibboleth;
- dare qualche cenno su SAML.

In particolare capire come interagiscono i componenti dell'autenticazione/autorizzazione quando Shibboleth è la soluzione di Single Sign On.

Cosa offre Shibboleth

Shibboleth offre:

- Autenticazione su un backend da fornire;
- Reperimento e rilascio di attributi utenti da uno o più backend;
- Single Sign On (SSO);
- Federabilità;

Shibboleth non è:

- Un sistema di Identity Management;

Significa che il processo di accreditamento/gestione degli utenti deve essere già gestito (LDAP + procedure di popolamento/modifica/cancellazione).

Perché Shibboleth

- Open Source (SAML);
- Rodato;
- Sicuro.

SAML

- blog di Tom Scavo (`http://trscavo.blogspot.com/2004/10/saml1.html`)
- SAML v2.0 Basics di Eve Maler (`http://www.oasis-open.org/committees/download.php/12958/SAMLV2.0-basics.pdf`)

XML-based framework for marshaling security and identity informations and exchanging it across domain boundaries

SAML standardizza le

- asserzioni (informazioni di autenticazione, passaggio di attributi);
- protocolli (coppie di scambi di messaggi);
- binding (protocolli di comunicazione - HTTP POST, HTTP Artifact, SOAP);
- profili (asserzioni, protocolli e binding applicati a casi d'uso)

per le autenticazioni, passaggio di attributi ecc.

SAML e Shibboleth

- Chi sposa l'implementazione SAML di Shibboleth non ne ha bisogno di una conoscenza approfondita.
- La conoscenza di SAML è fondamentale per la interoperabilità di prodotti differenti.
- *Dire di un prodotto che è SAML enabled è come dire che è LDAP enabled* (Scott Cantor)

N.B.: Shibboleth è reference implementaion di SAML2.0, ma è compatibile con SAML1.1

Gli attori dell'archiettura Shibboleth

Identity Provider (IdP) gestisce l'autenticazione, il Single Sign On ed il rilascio degli attributi delle identità contenute per sistema di Identity Management;

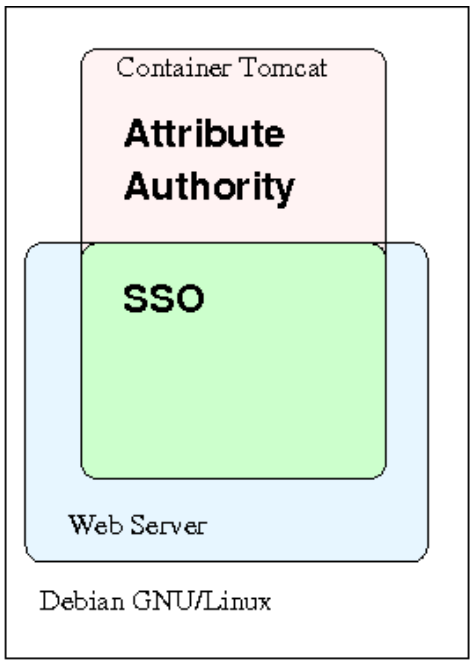
Service Provider (SP) protegge l'accesso alle risorse web (anche autorizzazione, grazie agli attributi rilasciati dall'IdP);

Where Are You From Service (WAYF) permette all'utente la scelta della sua home organization (dove sono le sue credenziali);

metadati catalogo dei partecipanti, per la verifica di sicurezza e per condividere le preferenze di ciascuno.

Anatomia dello Identity Provider

Lo IdP shibboleth è un'applicazione java dispiegata dentro un contenitore J2EE (Tomcat, Jboss, ecc. . .).
Può essere presente un web server come reverse proxy.
Le funzioni che svolge sono:

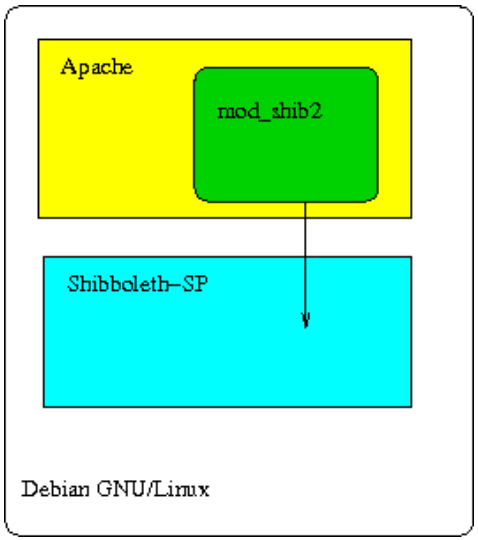


Autenticazione e SSO porta 443, url */idp*: ridirige l'utente a un form di login (valutate le esigenza della controparte) o ritrasmette le informazioni di avvenuta autenticazione se è presente una sessione valida;

Attribute Authority (AA) porta 8443: rilascia gli attributi degli utenti autenticati.

Anatomia del Service Provider

Lo SP shibboleth è un demone scritto in C++ con cui il server web dialoga (mod_shib2 nel caso apache, filtro ISAPI per IIS).



Shibboleth-SP
intercetta le richieste a risorse
protette e ridirige l'utente al WAYF o all'IdP;

Ricevute le informazioni di autenticazione, apre una comunicazione verso lo Attribute Authority dell'IdP per reperire gli attributi.