Toward campus portal with shibboleth middleware

Eisuke Ito and Masanori Nakakuni
itou@cc.kyushu-u.ac.jp, Kyushu University
nak@fukuoka-u.ac.jp, Fukuoka University
Outline

1. Background
2. Shibboleth
3. Campus portal
4. Solution
5. Conclusion
1. Background

- Closed/Private web services increase in University
  - WebCT, e-Syllabus, researcher & resources, student portal, etc...
  - Those systems are independently implemented.

- Single ID/PW and SSO (Single Sign-on)
  - Unify ID&PW (Single ID/PW)
  - SSO
    - Reverse proxy type SSO system will be installed.
    - Shibboleth SSO system is installing.

- But, Information sources are still distributed.
  - Campus portal is required to realize one stop service
1. Background (Cont.)

- Problem: it is difficult to gather information from private services
- Distributed web SSO (single sign on) systems are developed
  - such as *OpenID* and *Shibboleth*
  - NII of Japan deploys Shibboleth SSO
    - Common (Uniformed/standardized) SSO platform may appear.
  - Kyushu university is installing Shibboleth IdP
- Common platform makes easy to exchange data between systems.
Goal

• We are constructing common SSO platform with Shibboleth.
• On the platform, we may establish something method for information exchange between private services.
• And make a university portal
Outline

1. Background
2. Shibboleth
3. Campus Portal
4. Solution
5. Conclusion
SAML

- SAML (Security Assertion Markup Language)
  - XML based data exchange protocol defined by OASIS
  - http://docs.oasis-open.org/security/saml/v2.0/
- 3 players
  - User and browser
  - IdP (Identity Provider)
    - User account, authentication
  - SP (Service Provider)
- SAML assertion
  - Authentication
  - Attribute
  - Authorization Decision
- SAML over HTTP
- SAML over SOAP
1. A user accesses to an SP.
2. SP checks authenticated or not. If not, SP make a SAML authentication request.
3. SP returns redirection message to IdP.
4. User enter his/her credential to the IdP.
5. IdP returns message to redirect SP
6. SP decides to provide service or not, based on returned SAML assertion.
7. SP provides service to the user.

IdP must be fixed for SP.
Shibboleth

• A Web SSO middleware (developed by Internet2)
  – http://shibboleth.internet2.edu/

• Assumption
  – User may belong with an organization.
  – The organization may issue one’s credential such as ID/PW for user authentication.

• 4 Players
  – User and browser
  – IdP (Identity Provider)
  – SP (Service Provider)
  – DS (Discovery Service) ....
    • User selects his/her IdP (or Organization)
    • It was called WAYF (Where are you from?) in Shibboleth ver. 1.x

• Attribute based authorization
  – Organization may manage user account
  – User’s attributes may be also manage users attributes
1. A user accesses to an SP.
2. SP checks authenticated or not. If not, SP makes a SAML authentication request.
3. Select his/her IdP in DS process
4. SP redirects to the IdP.
5. User enter his/her credential to the IdP.
6. IdP returns message to redirect SP
7. SP decides to provide service or not, based on returned SAML assertion.
8. SP provides service to the user.
3. Campus Portal

- Portal is a web site that is a major starting site for users when they get connected to the web or that users tend to visit as an anchor site.
- Campus portal
  - One stop service for users
  - Good notice board for officials
The start page of google apps (iGoogle) …. (Start page is not available, now.)

- It can include various site information with google gadget.
- It can use SAML based authentication (Shibboleth)
Yahoo! JAPAN
An image of campus portal

Mash up private services into portal

Private services of Kyushu U

- MyLibrary
  - "Keynote speech of President"

- WebCT
  - "WebCT" checkbox
  - "WebCT" checkbox
  - "WebCT" checkbox

SaaS/Cloud style service
Problem of campus portal

• Difficult to integrate independent private services
  – How to extract information pieces from each sites?
  – How to pass through user authentication?
    • This is a barrier.
    • Common web SSO may make easier to break this barrier.
Outline

1. Background
2. Shibboleth
3. Campus Portal
4. Solutions
5. Conclusion
4. Solutions

• We need a data exchange method between private services.
• We studied 4 methods
  1. HTTP proxy
  2. HTTP binding
  3. Artifact binding
  4. Unsolicited Response

• Above 2, 3, and 4 are proposed by M. Aoyagi et al. in this article.
(1) HTTP Proxy

• User entrusts ones credential to portal.
  – Portal must be trustworthy.

• Portal acts as proxy of user (browser)
  – it sends user’s ID/PW to SP or IdP.
(2) HTTP Binding

- Portal, SP, and IdP exchange SAML data directory.
  - After authentication at IdP, SP returns response, and returns information of SP using agent.
(3) Artifact Binding

- IdP and SP exchange artifacts, where artifacts include session information.
(4) Unsolicited Response

- IdP sends unsolicited response to SP.
- SP receives the unsolicited response, and invokes response process.
Comparison of each methods

- Each methods is familiar with SAML and Shibboleth

<table>
<thead>
<tr>
<th></th>
<th>HTTP Proxy</th>
<th>HTTP Binding</th>
<th>Artifact Binding</th>
<th>Unsolicited Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP</td>
<td>Specify IdP</td>
<td>Specify IdP</td>
<td>Specify IdP Additional SOAP process</td>
<td>Must supports unsolicited response.</td>
</tr>
<tr>
<td>IdP</td>
<td></td>
<td></td>
<td>Additional SOAP process</td>
<td></td>
</tr>
<tr>
<td>Portal</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Demerit</td>
<td>Portal becomes security bottle neck</td>
<td></td>
<td>Can’t apply this method if communication between IdP and SP is limited.</td>
<td></td>
</tr>
</tbody>
</table>
Prototype of HTTP Proxy

• **Environments**

  - **IdP**
    | OS   | CentOS 5.1 |
    | Web  | Tomcat 6.0 |
    | IdP  | Shibboleth |

  - **SP**
    | OS   | CentOS 5.1 |
    | Web  | Apache2.2  |
    | SP module | mod_shib2.2 |
    | Service | PukiWiki |

  - **Portal**
    | OS         | FreeBSD 7.0 |
    | Web Server | Apache 2.2  |
    | Programming | Ruby 1.8    |
    | HTTP User Agent | Mechanize 0.8 |

• **Results**

  – Success to integrate other service into portal.
  – But, not portable
5. Conclusion

• Common Shibboleth SSO platform makes easy to exchange data between closed/private services.

• On the platform, we may establish something method for information exchange between private services for campus portal.

• We studied 4 methods:
  – HTTP proxy
  – HTTP binding
  – Artifact binding
  – Unsolicited Response ... (better than other)

• In the future,
  – Construct Shibboleth IdP
  – Shibbolize SPs
  – Make campus portal which integrates private services.