UPKI update from Japan

SP / IDP CASES

Eisuke Ito, Eiji Abe, Yoshiaki Kasahara
Kyushu University
ito.eisuke.523@m.kyushu-u.ac.jp
Outline

1. Introduction
2. Shibboleth SSO
3. Problems of IdP
4. Analysis
5. Conclusion
1. Introduction

1. Introduction
2. Shibboleth SSO
3. Problems of IdP
4. Analysis
5. Conclusion
1. Introduction

- Protected services in University
  - E-Learning, e-Syllabi, Researcher activity DB, Student portal, …
  - E-Journal, Google Apps, Windows Live, …
- Shibboleth SSO (Single Sign-on)
  - Distributed SSO Middleware
  - Identity Providers (IdP), Service Providers (SP). (and Discovery Service (DS))
- Federation
  - A trust relationship between Identity Providers (IdP) and Service Providers (SP).
  - NII of Japan deploys Shibboleth SSO Federation
  - Kyushu University joins this federation
History

Joined UPK

- LDAP
- Password manager
- University authN platform
- University ID

kitenet
(Wireless LAN)

UPKI
UPKI Initiative
Server Cert. service
eduroam.jp
GRID
SSO trial
UPKI-Fed Trail
UPKI-Fed Federation

Shibboleth IdP
Join UPKI-Fed (JP Federation)
In this presentation,

 Show a case study of shibboleth IdP and SP operation in Kyushu University
 Report some problems of shibboleth IdP operation.
 Report results of two month operation.
2. Shibboleth SSO

1. Introduction
2. Shibboleth SSO
3. Problems of IdP
4. Analysis
5. Conclusion
2. Shibboleth SSO

- Before Shibboleth
  - Kyushu U
    - Students 18,000
    - Staffs 7,000 (prof. 2500)
  - Campus wide authentication system (since 2007.)
  - IDM and LDAP server
    - IDM: Identity management system (Meta Directory)
    - LDAP server is used as password authenticator.
Dataflow of IDM

Students

- Student DB
- Student list
- Learning System (PCs, Server, WBT)
- Twice in a Year

Stiffs

- Personnel DB
- Staff list
- IDM (Identity Management Sys.)
- Daily

- ID Card
- ID Card
- LDAP
- Account activation
- Staff
Integrated Services

- WebCT (e-Learning)
- NetAcademy2 (English study)
- kitenet (WiFi)
- Campus licensed software
- Space management system
- Cute.Anyware (E-journal proxy by Library)
- Webmail (Primary e-mail service)
- Course registration and grade point management sys.,
- Researcher activity DB
# SSO Policy

<table>
<thead>
<tr>
<th></th>
<th>Internal service</th>
<th>Out sourced service</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Usability oriented</strong></td>
<td>• Webmail&lt;br&gt;• WebCT (e-Learning)&lt;br&gt;• Software download site (licensed software)&lt;br&gt;• University portal</td>
<td>• E-Journal services&lt;br&gt;• RefWorks&lt;br&gt;• Google Apps</td>
</tr>
<tr>
<td><strong>Security oriented</strong></td>
<td>• Financial system&lt;br&gt;• Grade point management system</td>
<td></td>
</tr>
</tbody>
</table>

Shibbolize!
3. Problems of IdP

1. Introduction
2. Shibboleth SSO
3. Problems of IdP
4. Analysis
5. Conclusion
3. Problems of IdP

Attributes matching

Attribute filtering

LDAP  \rightleftharpoons  \text{IdP}  \rightleftharpoons  \text{SP}
Attributes matching

Existing schema (attributes)  mismatch  eduperson schema

LDAP  Open LDAP (rewrite)  IdP

Solutions

Add/Change schema  Attributes Translation  Schema Matching

OpenLDAP’s rewrite module

OpenLDAP’s rewrite module

attribute-resolver.xml
Attribute filtering

OK
Serves all attributes

IdP

No
Against privacy policy

Internal SPs
- MyLibrary
- EZproxy
- WebCT

External SPs
- Google
- RefWorks
Solutions for attribute filtering problem

1. Write filter rules for each SP.

2. Two IdPs

3. Filtering script

- Open LDAP (rewrite) rules
- LDAP
- IdP
4. Analysis

1. Introduction
2. Shibboleth SSO
3. Problems of IdP
4. Analysis
5. Conclusion
4. Analysis

Shibboleth IdP and SPs in Kyushu University

- LDAP
  - SJSDS (Solaris)
- Open LDAP
  - OpenLDAP, CentOS
- Shibboleth IdP
  - Tomcat (CentOS)
  - (VMware)
  - (Windows XP)
- Internal SPs
  - MyLibrary
  - EZproxy
  - WebCT
Kyushu University Library
http://www.lib.kyushu-u.ac.jp/
Results

- Two months operation
- No serious trouble.
- Some trivial matters.
  - Some users bookmark the IdP site.
    - 404 Not Found: /idp/Authn/Password 7time(s)
    - He/She can’t access to the service which he/she wants.
Statistics: Unique users


<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Students</td>
<td>1815</td>
<td>18000</td>
</tr>
<tr>
<td>Staffs</td>
<td>467</td>
<td>7000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(2500)</td>
</tr>
<tr>
<td>Total</td>
<td>2291</td>
<td>25000</td>
</tr>
</tbody>
</table>

![Graph showing the increase in unique users over time from Jan. 2010 to Jan. 2011.](graph.png)
Top 200 users (10% users) occupy 41.2% access.
Statistics: Daily access
Most user access at afternoon.
5. Conclusion

- A case study of Shibboleth IdP in a university
- Two problems for IdP construction
  - Attribute matching
  - Attribute filtering
- Two months operation
  - No serious trouble.
  - Got statistics
    - No over load
Thank you for your attention.