APPLICATION OF SINGLE SIGN-ON (SSO) IN DIGITAL CAMPUS

Jian Hu, Qizhi Sun, Hongping Chen

College of Information Engineering, North China University of Technology, Beijing, China
hujian@ncut.edu.cn, sunqzo@163.com,chp-lover@163.com

Abstract

System isolation, inconsistent information, verifies frequent and so on are the problems facing with of the campus network construction. In order to solve the problems above, we integrated B / S architecture applications with the Single sign-on (SSO) system. A unified personnel database has been established using LDAP server, and creates dynamic groups to manage elements of the database. CAS and Form technology were used to achieve the integration of internal campus network applications and other black-box system with SSO.

Keywords: Single sign-on; LDAP； CAS

1 Introduction

Nowadays along with the university information system development, more and more B / S architecture applications were deployed. These systems play an important role in the university information system. But they were developed in a particular period for different applications and using different techniques. The growing number of systems brings convenience for users, but also exposed a wide range of issues: Between the isolated systems, there is information redundancy and information inconsistent, so its difficult to maintain; Too many log in points, each system has its own authentication mechanism, If a user wants to access some systems, he/she must log on several times, which brings inconvenience to the user; Users must to remember many usernames and passwords, it could result in password fatigue and lead to password disclosure, so it have security risks.

Single sign-on is a good solution to these problems. The so-called single sign is that after a user logs on a system can logs on other systems which integrated into a single sign system without re-authentication. Our single sign-on implementation mechanisms: Using LDAP to establish a unified personnel database, so that personnel information between various systems was unified and information redundancy were reduced. At the same time it will provide authentication information for single sign-on. Establish single sign-on authentication service center and integrate all existing applications with the center.

2 Instruction of SSO

During the implementation of single sign-on deployment, we mainly use two techniques: LDAP technology and single sign-on (SSO). The following is a brief introduction of these two technologies.

LDAP is short for Lightweight Directory Access Protocol. LDAP server is used to store and retrieve information, which is similar to ordinary relational database[1]. The main differences between LDAP servers and the general relational database are as follows: LDAP using tree model rather than rational model to organize information; Mainly provides data query services, the query speed faster than the ordinary relational database; Excellent ability to copy the information makes it highly robust. LDAP tree information organization model is similar to the actual hierarchical relationships between the various departments of an organization. So using LDAP to store personnel information made management easier. In the LDAP products we have chosen a powerful Directory Server Enterprise Edition (DSEE) which was developed by SUN.

There are a lot of single sign-on products and its implementation techniques are also varied. We can simply divide it into two types: pseudo-single sign-on and true single sign-on.

Pseudo-single sign-on refers to realize single sign-on by simulate the form submit. As shown in Figure 1. Typically, users enter the correct username and password and then click the submit button, they will enter the application system. Throughout the process, the user authentication information submitted via GET/POST method. Pseudo-single sign-on system simulated the login process and submits authentication information to the application system to achieve single sign-on. To save time and reduce the degree of difficulty, this method is used by a lot of portal systems.

978-1-4244-6769-3/10/$26.00 ©2010 IEEE

The true SSO system is divided into different categories. Such as: cookies-based, agent-based gateway-based. They generally follow the following principles. A SSO Web Authentication Center and establish a trust relationship with all business systems; the entire log through the SSO authentication center; SSO certificate whether the current access to Web applications is legitimate through a variety of ways. In the SSO products we have chosen Central Authentication Service (CAS). CAS is originally created by Yale University to provide a trusted way for an application to authenticate a user. It has a library of clients for Java, .Net, PHP, Perl, Apache, uPortal, and others.

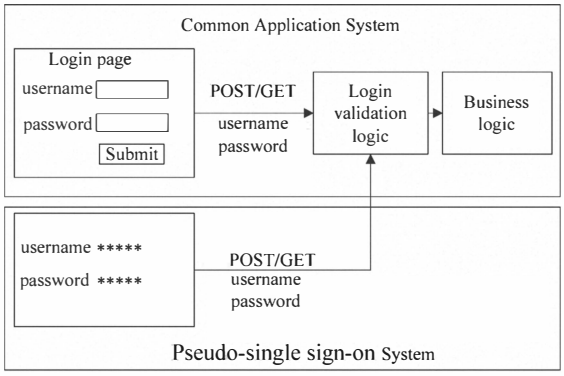

Figure 1. Pseudo-single sign-on system

3 A specific analysis of SSO implementation

In the implementation of SSO project, we need to establish a unified database of persons using LDAP server. Then integrate other systems using SSO.

3.1 Set up LDAP server

In the process of LDAP server set up, the directory tree structure design is very important. A good designed directory information tree not only could save query time but also could facilitate the management. One structure of directory information tree is based on hierarchical of an Organization (Figure 2).

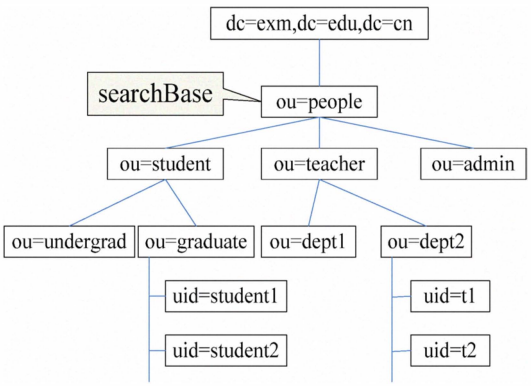

Figure 2.The directory information tree based on hierarchical of an Organization

The advantage of this structure is its clear structure and easy to manage. It also has some disadvantages. (1) It is difficult to adjust the person's branch. If we want to do this we must delete a people in on branch and add this people in anther branch. (2) If we change the tree's structure we must delete all people and add all people.

In order to solve these problems, we use the following design pattern. Everyone is placed under the ou=people. We do not need to use add and delete operation for element adjustment. Then we build dynamic groups to manage elements.

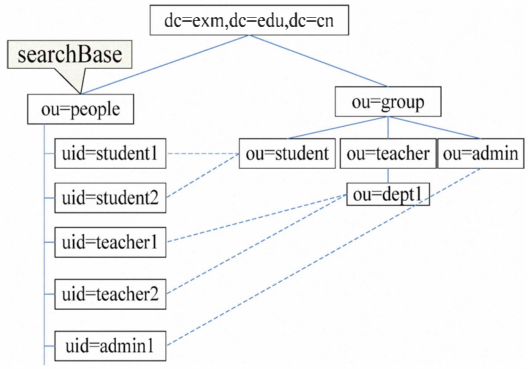

Figure 3.The directory information tree based on hierarchical of an Organization and dynamic organization

3.2 SSO principle

First of all, we briefly describe the principle of single sign-on. Figure 4.[2]
1) Client access to a business system.
2) SSO client will redirect the client browser to the SSO server.
3) The user to enter username and password for authentication.
4) The user through the certification and back to the business system with a ticket.
5) SSO client to confirm whether the user is legitimate.
6) Legitimate users, get user information and then access business systems.

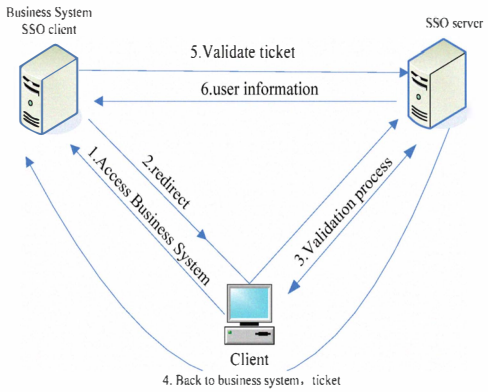

Figure 4. SSO schematic

The user logs on the system can logs on other systems which integrated into a single sign system without re-authentication.

3.3 SSO server deployment and client integration

We use CAS as the SSO server. CAS server deployments are mainly related to the following aspects.[6]

1) Deployment of CAS war package.
2) Connect to the LDAP server.
3) Modify the tickets survival time.
4) Custom server-side pages.

We integrate business systems with library of CAS clients. The following are examples of JSP system integration. Add client-side jar package and add the interceptor code in the file of web.xml. Code is as follows.[6]

```
<filter>
 <filter-name>CASFilter</filter-name>
 <filter-class>
   edu.yale.its.tp.cas.client.filter.CASFilter
</filter-class>
 <init-param>
<param-name>
   edu.yale.its.tp.cas.client.filter.loginUrl
</param-name>
<param-value>
   http://casServer:port/cas/login
</param-value>
</init-param>
<init-param>
<param-name>
   edu.yale.its.tp.cas.client.filter.validateUrl
</param-name>
<param-value>
   http://casServer:port/cas/proxyValidate
</param-value>
</init-param>
<init-param>
<param-name>
   edu.yale.its.tp.cas.client.filter.serverName
</param-name>
<param-value>clientServer:port</param-value>
</init-param>
</filter>
<filter-mapping>
<filter-name>CASFilter</filter-name>
 <url-pattern>/servlet/*</url-pattern>
</filter-mapping>
```

The following code is for getting user information.

```
session.getAttribute(CASFilter.CAS_FILTER_USER);
session.getAttribute("edu.yale.its.tp.cas.client.filter.user");
```

In the SSO integration also involves the ASP, PHP and. NET systems. We do not introduce them one by one.

4 Technical difficulties and innovation

In the construction of LDAP server, we have adopted a dynamic group to manage personnel information. It does not reduce the query speed, simultaneously to facilitate the management and programming. In the single sign-on integration, we combination CAS with pseudo-single sign-on achieved the integration of black box systems. In order to reduce the difficulty, we canceled the SSL certification.

5 Conclusions

Through the single sign-on project construction, a unified database of persons was established. We integrated the isolated system that is not only convenient for the customer but also convenient the manager. In the construction of the Digital Campus Enterprise Service Bus was also used to achieve synchronization of information between databases.

References

[1] HU Kai-sheng, Application of LDAP in a Uniform Identity Authentication System for Digital Library. Computer Knowledge and Technology,Vol.6,No.10, 2010(4):2334-2336.

[2] MIDI.SSO(Single Sign-on) in Action. http://www.cnblogs.com/yinhaiming/articles/1411264.html,2009

[3] LAI Shen-lu,LI Xin,JI Jun-chuan. Application of Pluggable SSO Technology. Computer Engineering,Vol.34, No.14, 2008(7):121-125.

[4] Xin Wang, Henning Schulzrinne,Dilip Kandlur, Dinesh Verma. Measurement and Analysis of LDAP Performance. IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 16, NO. 1, 2008(2)

[5] Sahana K. Bhosale, Architecture of a Single Sign on (SSO) for Internet Banking. Wireless, Mobile and Multimedia Networks, 2008

[6] Tao zhang, Binkun Liu. CAS Single sign-on in Tomcat. http://www.ibm.com/developerworks/cn/opensource/os-cn-cas/index.html,2008(4)

[7] T. Small, D. Hennessy, and F. Dawson, “Calendar attributes for VCard and LDAP,” RFC 2739, Internet Engineering Task Force, Jan. 2000