Research of Security Identity Authentication Based on Campus Network

Guo Zhenghui ¹, Han Xiujuan ²

¹ College of Computer Science and Technology Henan Polytechnic University, Jiaozuo Henan, China
guozh@hpu.edu.cn

² College of Computer Science and Technology Henan Polytechnic University, Jiaozuo Henan, China
hanxj@hpu.edu.cn

Abstract—With the development computer technology of campus network, more and more application systems become popular. These application systems are independent each other, everyone has its own different account information in different systems and must save its different account information. Based on the above fact, the paper analyzes common authentication scheme, then propose a security single sign-on way. The method implement a security uniform identity authentication using PKI, LDAP, CAS. In this way user can access all corresponding application systems when they login only one time. This approach can allow users to easily manager their account information.

Index Terms—LDAP, Authentication, SSO, PKI

I. INTRODUCTION

With the continuous increased infrastructure in campus network and development technology of the electronic information, more and more application systems are rapidly used in campus network. These systems are independent each other, such as office automation, campus network accounting system, financial tracking system, educational management system, library loan system, etc. Each system has its own authentication database that is different from other and users in each system have their own accounting information. It is difficult for users and administrators to manage the accounting information of many different systems. So the more number of applications system, the more complicated. So these systems urgently need the support of SSO. Based on the above face, the paper presents a SSO[1-2] method after analysis of several different common authentication systems. It allows users to login once to access all mutual trust systems, at the same time SSO confirm the identity of communications and provide data security. This authentication method uses LDAP as its database that is a simplified version of X500, X509 is a part of X500. Judging from the nature of data, the certificate data store in LDAP, the information user generated come from LDAP. This paper will use CAS as authentication method and add plug for support of certificate method.

II. ANALYSIS OF COMMON AUTHENTICATION METHOD

A. General Authentication Method

General authentication is each application has its own independent authentication method and is mutually coupled from other systems. When users access different application systems, they must enter corresponding information. At present this authentication method is adopted by many application systems, and each system’s authentication and authorization are different from others.

B. Authentication Method of LDAP and Radius

LDAP is Lightweight Directory Access Protocol[3], based on the X.500 standard, but significantly simpler and more easily adapted to meet custom needs. Unlike X.500, LDAP supports TCP/IP, which is necessary for Internet access. The LDAP protocol enables corporate directory entries to be arranged in a hierarchical structure that reflects geographic and organizational boundaries. LDAP directories are arranged as trees, please see Fig. 1. One of the most important features of both X.500 and LDAP is the ability to search for user-specified resources.

Radius (Remote Authentication Dial In User Service) is a networking protocol that provides centralized Authentication, Authorization, and Accounting management for computers to connect and use a network service. It runs in the application layer, uses UDP as transport, and supports a wide variety of authentication schemes.

The above two protocols can provide unified authentication methods, both run in the application layer, based on C/S mode. They supports a wide variety of authentication schemes and have a variety client

![Figure 1. Example of ldap of a figure](image-url)
development environment, such as SDK for C, SDK for JAVA, SDK for Perl, etc. Radius can store its accounting information in LDAP database. But they are not SSO; logging in different systems need enter different user information, do not have Characteristic behavior of a single sign-on.

C. Kerberos Authentication Method

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. It is the implementation of SSO and allows nodes communicating over a non-secure network to prove their identity to one another in a secure manner. It makes use of a trusted third party, termed a key distribution center, which consists of two logically separate parts: an Authentication Server and a Ticket Granting Server. Kerberos works on the basis of "tickets" which serve to prove the identity of users. please see authentication process of Fig. 2, it is the realization of C/S of SSO. The SSO referred in this paper is based WEB mode and is a simplified version of Kerberos to implement security unified identity of cross-domain. The service ticket stored in KDC can only be used once compared to Kerberos.

Figure 2.  Kerberos authentication process of a figure.

III. IMPLEMENTATION OF CERTIFICATE REPOSITORY

PKI is public key infrastructure, it enables users to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization. A public key certificate is a cryptographically signed digital structure that guarantees the association between at least one identifier and a public key. The X.509 document defines the format of a public key certificate and of certificate revocation list. An LDAP directory represents the perfect repository for public user information and public key certificates and offers distributed access to the data it stores[4]. Like a database schema, a directory schema defines how data is represented in the directory. In order for the directory to serve as a repository for the certificate, the directory schema should be open and extensible.

Please see Fig. 3, it show how to use LDAP as certificate database. All the basic information of users stored in LDAP, CA issued certificates and CRL is also stored in LDAP. All certificate original data user requested come from LDAP, then CA signature it. The certificate use the standard PKCS#12 and use pfx format[5]. User download it and import it to system to provide individual account security and personal identification. Once user has his certificate, he can use it to login in application system while he can also choose traditional user/password way. This paper recommends using certificate method, at the same time authentication system will get user information from certificate. Only the certificate is signed successful, application system can implement SSO based PKI.

IV. IMPLEMENTATION OF SSO

SSO is an integrated part of campus network, user only need to provide a one-time credential and then can access all mutual trusted application system[6]. Now the best integration solution of application systems is based SOA that use Web Service to achieve the target. CAS is Central Authentication Service and a single sign-on protocol for the part of SOA. Its purpose is to permit a user to access multiple applications while providing their credentials only once. Please see Fig. 4, when a user accesses a site that uses CAS, that site redirects the user to CAS. Once CAS has verified a user's identity, it forwards them back to the original site. CAS attaches a unique ticket number to the URL of the protected service. The protected service sees this ticket. It sends this ticket to CAS. CAS tells the

Figure 3.  Certificate database based on LDAP of a figure

Figure 4.  CAS authentication process of a figure.
protected service whether the ticket is good and if so, the Case ID that was used to obtain the ticket. The protected service reacts accordingly, allowing access if the ticket is good.

The extension of authentication is as follows:

A. Step 1

When user access a protected resource, CAS Client analysis of whether the request contains Service Ticket, if included, then skip to step C, if not, redirect to the CAS URL with target address.

B. Step 2

If the user has certificate, system will pop up a dialog box to let user select appropriate certificate and identify user. If user has no certificate, system will let user use traditional user/password method. After authorization authentication system will write TGC cookie and redirect target url with service ticket.

C. Step 3

CAS client filter obtain http request, get the service ticket and post it to CAS, if valid, access applications, if not, skip to step A.

For the safety of TGC, accessing CAS use https, ticket only be use once. This paper presents dual authentication in CAS - certificate and LDAP. This requires extension of user authentication interface, CAS separate authentication interface from authentication protocol. The extended authentication provided by CAS is “AuthenticationHandler” which has support and authenticate methods where users implement their codes. In order to dual authenticate with certificate and LDAP, this paper implement “Credentials” and corresponding “CredentialsToPrincipalResolver”.

V. CONCLUSION

With the development of campus network technology, independent application systems do not suite to direction of campus network. So SOA-based architecture using Web Service is the best solution for loosely couple up. At this time SSO is a part of it, login once to access the application systems of mutual trust, without second logon. Based on fact, this paper implement a SSO method using PKI, LDAP, CAS, etc and provide a security identity authentication. Users only login once can access many mutual trust systems.

REFERENCES