Research and Design of Web Single Sign-On Scheme

Xin-e YOU，Yan ZHU
Loudi Vocational & Technical College ,Loudi，417000，China
Email:hnldyxe@163.com

Abstract—The thesis designs an easy to use, safe, efficient solution of Web Single Sign-On, referring to the design idea of Kerberos protocol based on ticket access and using Single Sign-On model of Broker-Agent-Based. In this program, the use of URL redirects and Cookie technology achieve Single Sign-On, can be implemented, and has a good application and promotion of value.

Keywords-Single Sign-On; Cookie; Ticket

I. INTRODUCTION

Today in information technology for rapid development, B/S structure application system, that is easy to extend, easy to maintain, low to the cost of development and so on, gradually occupies most of the market share. The application systems based on Web in the same department or enterprise business applications co-exist quite common. These systems are often set up at different times by different technicians and technologies, each with its separate identity authentication services, and manage the corresponding data of users. Users need to remember multiple accounts and passwords. So the management will be not only tedious, low efficiency, and occupy too much system resources, resulting in decreased efficiency of the system implementation, but also there is a security risk that leak the user's login credentials. Technology for Single Sign-On(SSO) is an effective way to solve the above problems. SSO means users only need to take the initiative to conduct a network authentication, and then you can access all of its authorized network resources without the need for active participation in other re-authentication process[1].

By analysing advantages and disadvantages in SSO model, the thesis designs an easy to use, safe and efficient solution of Web SSO by referring to the design idea of Kerberos protocol based on ticket access and using SSO model of broker-agent-based.

II. COMMON SINGLE SIGN-ON MODEL

SSO model can usually be divided into Broker-Based SSO, Agent-Based SSO and Gateway-Based SSO[2].

A.The model for Broker-Based SSO

Figure 1 shows the model for Broker-Based SSO that consists of the client, Authentication Server, and application system. In the model, authentication server is at the core, which is equivalent to a broker. When users log initially and pass the authentication, the authentication server sends an electronic identity to the user, and the user can access to applications with the logo, so as to achieve the purpose of SSO.

The advantage of the model is that central authentication server is unified to authenticate users, and the central database maintains and manages the user's identity information. However, the model also has some shortcomings. It needs to amend the original application system to meet the authentication mechanism used, while transforming old system is a difficult task. Moreover, in the model all the user's login information is taken over by the system and users must input a user login name and password, so anonymous users can not log in.

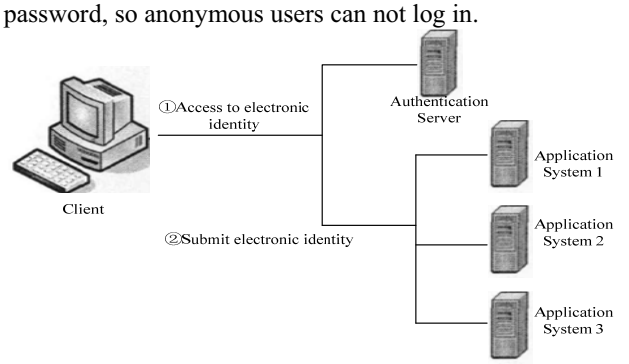

Figure 1. The model for Broker-Based SSO

B. The model for Agent-Based SSO

Figure 2 shows the model for Agent-Based SSO that consists of the client, application system and agent software[3]. Agent software can be installed on the client and application system. The role of agent software carries out authentication for different application systems, and each agent software can work by different authentication means.

The model ensures the safety of the channel and SSO, with good flexibility and implementation. However, the model has a big flaw that the user's login information is stored locally, which increases the risk of password disclosure. What's more, when a new application system is added, we must develop an appropriate agent program, which is more complex and has a huge workload for maintenance.

978-1-4673-2207-2/12/$31.00 ©2012 IEEE

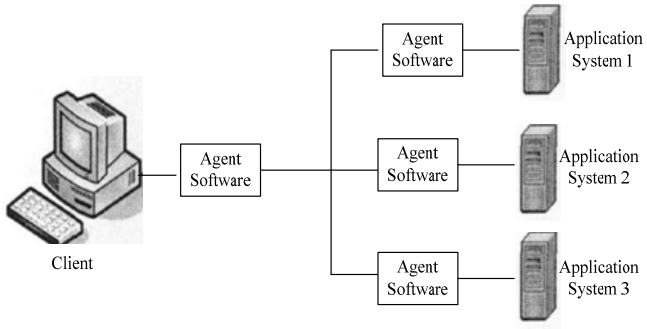

Figure 2. The model for Agent-Based SSO

C. The model for Gateway-Based SSO

Figure 3 shows the model for Gateway-Based SSO that mainly consists of the client, gateway and application system. In this model, the firewall is set up at network entrance or an encrypted communication equipment for a special purpose is set up as a gateway, and all service requests are intercepted by the gateway to put in a trusted isolated network. If the client passes the gateway authentication, they will gain access to visit resources for the application service[4]. If the gateway service can be identified by IP addresses, and a IP-based rule with a combination of database is established at the gateway, the gateway will be used to implement SSO.

The model hardly changes application system, as long as configuration and gateway have mutual authentication. Users can easily encrypt and transmit data of application systems, and implementation and maintenance is relatively simple[5]. However, this model is largely dependent on a gateway, demanding all aspects of gateway's performance. If a gateway is used, the gateway failure may cause paralysis of the entire system, while the use of multiple gateways need to consider how to update user information database at the gateway in time synchronization that make it consistent. This model is more stringent for network environment, which limits its use.

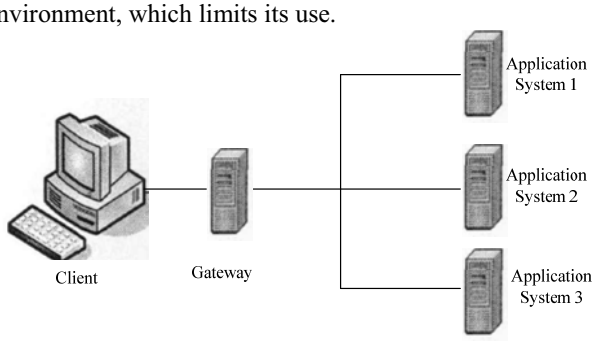

Figure 3. The model for Gateway-Based SSO

III. THE DESIGN OF SINGLE SIGN-ON PROGRAM

Single Sign-On is an effective means of integrating applications which has a very important role in the enterprise. In the design of SSO program, we should follow the easy to use, safe, efficient and implemented principles.

A..Design ideas

(1) In the determination of authentication method, the combination of "user name/password" traditional authentication and digital certificate authentication is used. The client first use "user name / password" approach to Authentication Server (AS) for authentication. After the initial certification, according to the required level of the application system's security, it determines whether the client is demanded to show the digital certificate for further certification.

(2) In the determination of the model for SSO, we use a hybrid model for Broker-Agent in accordance with the advantages of Broker and Agent. On one hand, Broker model is used to centralize authentication. On the other hand, the authentication agent is added to Web application system, and the agent user complete authentication in the application system to enhance implementation of SSO services.

(3) In the design of SSO process, referring to the design idea of Kerberos protocol based on ticket access, a variety of related tickets are generated for the user , which contain the user's authentication information or authentication information of visiting a Web application. Jump among the relevant entities in Login process and parameters transmission can be completed by URL redirection.

(4) SSO server sends authentication token of Cookie to the user's browser that passes identity authentication through a SSL secure channel. When the user enter authentication server once again, that will automatically carry the Cookie, so authentication may be waived. That realizes "single sign-on for one time, always roaming."

B.The overall model

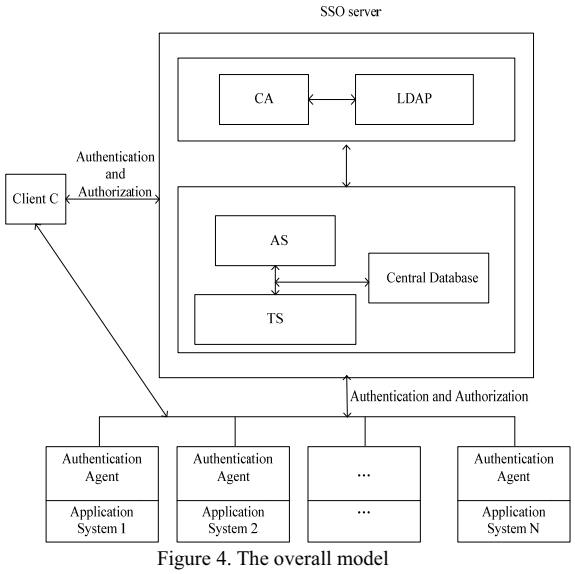

Figure 4. The overall model

Figure 4 shows the overall model for system. Single Sign-On is achieved by SSO server and SSO authentication agent. SSO server mainly consists of Authentication Server (AS) and Ticket Server (TS). The role of the main entities in the model is as follows:

(1) AS: AS is the core component to achieve SSO and provides centralized authentication service. PT (Primary

Ticket) is generated for authenticated users, and it can be used multiple times in the effective time. AS caches PT, and sends a Cookie to the user browser, whose content is the user's identity PT_ID.

(2) TS: According to user-owned PT, TS generated ST (Service Ticket) of visiting a Web service for the user, and ST is a one-time use. In addition, it is an important function of TS to respond to ST authentication request of SSO authentication agent.

(3) SSO authentication agent: SSO authentication agent is placed in the Web application system, which sends the verification request of ST to TS, verify the user's identity in the system from results obtained.

C.The design of Single Sign-On process

Table 1 shows symbols and meaning used in Single Sign-On process.

TABLE 1. SYMBOLS AND MEANING USED IN SINGLE SIGN-ON PROCESS

symbol	meaning
C	user
App	Web Application
PUK_X	Public Key of X
PRK_X	Private Key of X
Kc	Key of Cookie encrypted in AS
K(t)	t as the key value of symmetric cipher algorithm
K[m]	use Key to encrypt m
H(m)	deal with m with Hash

Users that have not been authenticated by AS, directly access to a Web application, and the login process is shown in Figure 5. The step is as follows:

(1) User C that has not been authenticated by AS, directly sends the request of access to system resources to a Web application.

(2) SSO authentication agent in Web application intercepts the user's request. If any identifying information and ST_ID parameters in the request are not found, the user will not be certified by AS. The use's browser is redirected at the entrance to the AS authentication, and uniquely identity AppID in SSO from Web application is added to URL request parameters.

(3) If AS finds that Cookie in the user's HTTP request header information does not contain PT-ID, the user does not pass the identify authentication. Pop-up the login window, and ask the user to input user ID and password.

(4) When the user enters user ID and password, the client generates a random number, and then encrypted user ID and password are sent to AS. AS decrypts, and a central database authenticates user ID and password. if the authentication is pass, validated, the level of AppID security will be inquired, which determines whether users need to present their digital certificates for further authentication.

Operation Description: C→AS: IDc||K(H (psw))[r1]||K(r1)[psw]||H (IDc||r1||psw)

In which, IDc is identified as C; psw is the user login password; r1 is a random number.

(5) If certified, according to user ID, AS queries the identity SSO_userID in SSO system, determines whether the user has been permitted to access the AppID corresponding to Web application, and gets the identity App_userID in Web applications. AS generates PT for the user, which contains the user's SSO_userID, and AS cache PT. Meanwhile, AS transmits a Cookie to user's browser through a secure transmission channel, Cookie's name=token， value=k_c[PT_ID], in which PT_ID is the user's own PT identity.

(6) According to the user's PT, TS generates ST visiting Web application, and then cache ST, which contains AppID, App_userID and the user's PT.

(7) The user's browser is redirected to Web application by AS, with ST_ID in the URL parameters.

(8) SSO authentication agent in Web application system obtains ST_ID, and resquests TS to verify ST, whose information contains ST_ID and AppID in Web application.

(9) According to ST_ID, TS queries ST in the cache, from which identity App_userID is got in Web application. The verified results, which will be encrypted as follows, are sent to the SSO certification agency. The message is as follows:

$PUK_{App}[K_s]||$
$K_s[ST\_ID||App\_userID]||PRK_{TS}[H[ST\_ID||App\_userID]]$

TS generates session key Ks, and the authentication results ST_ID | | App_userID are encrypted with Ks. Ks is encrypted with public key PUK_{App} in Web application, and it is ensured that only the corresponding Web application can obtain Ks and decrypt the results. What's more, TS signs to the verified results with private key, which ensures that the results are actually from the TS and is not tampered with. For valid ST, TS immediately removes it from the cache.

(10) SSO authentication agent in Web application side, firstly, decrypts the symmetric key Ks with private key, and then decrypts the validation results with Ks and verifies the signature value with private key of TS. Finally, the user's identity App_userID is got within the Web application, and the user's identity information is recorded in the session to achieve the user's login in the system, and then the necessary services are provided to the user.

After the above process, the user has completed the authentication and had a PT in AS cache. The user has accessed the application system with ST. When users go to access other application system, Cookie that contains PT_ID is automatically carried. as long as PT entities corresponding to PT_ID are still in valid time range, which has not been removed by system, the user will be dispensed to the user authentication. The process no longer requires the user's active participation, which is transparent to the users. The purpose for " Single Sign-On for one time, always roaming" is achieved.

IV. SAFETY ANALYSIS

(1) The safety of identity authentication

In this scenario, the traditional "user name / password" authentication is combined with the digital certificate authentication. According to the security level of Web application, one of two ways is used with flexibility, which not only reduces the hardware cost, but also ensures the security.

When the traditional "user name / password"

authentication method is used, to prevent password disclosure which is resulted in as eavesdroppers monitor users and send a request to AS, the user password Hash encrypts random numbers generated on client for the key. The password value is encrypted by regarding random number as the key, so as to achieve the purpose of ensuring the user's password.

When a digital certificate authentication mode is used, USBKey hardware and PIN are the two necessary conditions of completing authentication for the user. The signature and encryption operations are completed in the hardware, and private key can not be exported, which ensures the user's safety of private key.

(2) The safety of Cookie

The Cookie which contains PT_ID, is the user's certificate to log in again, so its safety is more important. The transmission of Cookie uses SSL secure channel[6], and AS sends session Cookie. once users close the browser, Cookie will immediately disappear, together with Cookie contents encrypted by AS. Many ways ensure the safety of Cookie.

(3) The safety of ST

ST results contains users' identity authentication in an application system. The program encrypts the results with the session key encrypted and signs on verification results with the private key so as to ensure the confidentiality, authentication and integrity. In this scenario, the validation results include ST_ID, which is relevant to a specific authentication requests. When SSO authentication agent receives verification results, it will compare the validation results ST_ID with ST_ID of the request, and if not, the message playback can be identified, so it is invalid that the attackers validate replay of the ST results. After successful authentication for ST, TS will immediately remove it from the cache, so it is invalid that the attackers replay ST_ID in URL parameters.

V. CONCLUSION

The thesis makes a comprehensive introduction to popular Single Sign-On model currently. Through the analysis and comparison of the advantages and disadvantages of various models, the hybrid model based on Broker-Agent is designed, and Broker-Based approach combined with agent authentication design Single Sign-On solution, which not only ensures the channel security and Single Sign-On, but also has good flexibility and can be implemented. The traditional "user name / password" authentication is combined with digital certificate authentication, and the system's security level determines whether the client need to present their digital certificate, which ensures the security and reduces the cost. Referring to the design idea of Kerberos protocol based on ticket access , a variety of tickets are generated for users, so as to achieve Single Sign-On with Cookie. Single Sign-On solution designed in the thesis is efficient, safe, easy to implement, and has the application and promotion of value in Information integration of enterprises.

ACKNOWLEDGMENT

Our research was supported by the Research Foundation of Education Committee of Hunan Province, China(Grant No.09C1271), the Planned Science and Technology Project of Hunan Province, China(Grant No.2010GK3015).

REFERENCE

[1] H. Ji,Z. Lin, cResearch and design of single sign-on scheme", Computer Engineering and Design, Vol.30, pp.2862-2864, 2009.

[2] X.H. Zhang,Z.K. Fan, "Optimized Design of Web Single Sign-On Based on Authentication Protocol", Computer Engineering, Vol.36, pp.146-148,2010.

[3] B. Wei,Z.Xu, "Defense approach against application level DDoS attacks based on authentication mechanism", Computer Engineering and Design,Vol.31, pp. 231-235,2010.

[4] F. Liu,Z. Wang, "Portal Single Sign-on Scheme Based on CAS", Computer Systems Applications,Vol.20, pp.77-80,2011.

[5] Z.G. Liang, "Design of Single Sign-on for hybrid architecture based on Web service", Journal of Computer Application,Vol.30, pp. 3363-3365,2010.

[6] W.H. Feng,Y.L. Liu, "Design and implementation of unified authentication system on cookie", Computer Engineering and Design,Vol.31, pp.4971-4975,2010.

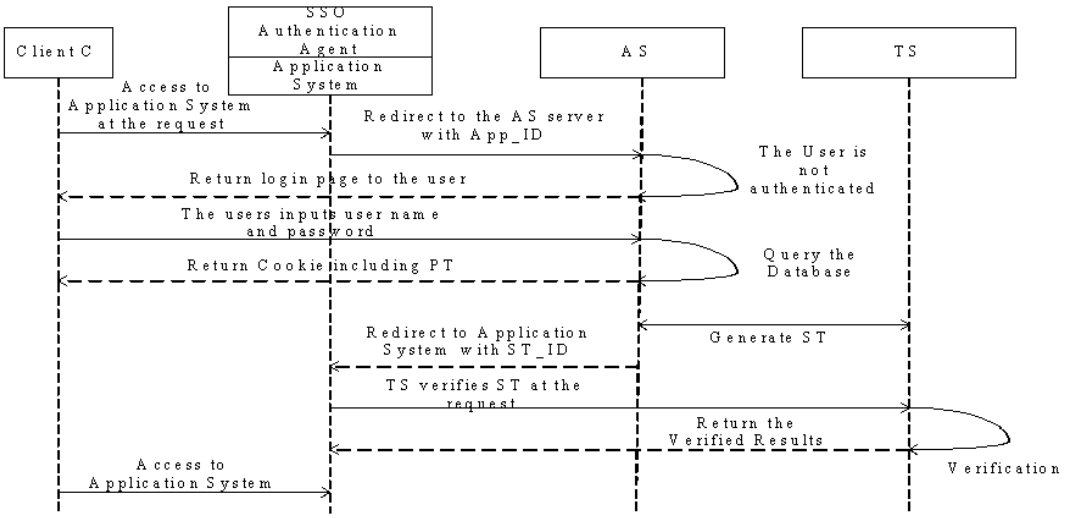

Figure 5. Single Sign-On Authentication Process