Research on the SSO Key Technology Based on Web

Yu-rong GUAN\(^1\)\(^*\) and Fei ZHOU\(^2\)

\(^1\)Huanggang Normal University, Huangzhou, Hubei, China
\(^2\)Huanggang Normal University, Huangzhou, Hubei, China

\(^*\)Corresponding author

Keywords: SSO, Cookie, Session, Unified identity authentication.

Abstract. "Once logged in, full network roaming" is the primary purpose of single sign on, which allows users to log in from an entry and access all applications. This paper mainly introduces the SSO system related technical support, from the unified identity authentication technology, Cookie technology and Session authentication mechanism to several single sign on design model based on Web, also from the safety and feasibility analysis of the implementation process of SSO, solve user and administrator problems, improve the convenience of network the user's work efficiency and operation.

Introduction

With the continuous development of information technology, the application platform based on Web is very extensive, such as e-mail, online shopping website, etc., these are great application platform provides efficient management mechanism for enterprises, schools, hospitals and so on, also provides a great convenience for people's life. In my school as an example, the construction of digital campus in the supporting facilities, has been the realization of the network, network teaching and comprehensive information management and other functions, with the financial management system, teacher management system, student management system, office automation system, and with the actual needs of the school informatization construction, application system will become gradually increased. As a result, each application system has different development languages, and the background database is used differently, but some of the information in the database is the same. Each of the systems to their identity database to use authentication authentication mode respectively, which resulted in not only for users to remember different application system user name and password of trouble, and will also cause the system administrator leads to repeated problems occur due to the user information database in each application into multiple in short, the heavy burden to the user and the system administrator and serious waste of resources. In the face of the Web application system more and more, the traditional identity authentication and login mode has obviously restricted, service performance and efficiency of the office so that the identity authentication system to establish a safe, efficient, integrated and unified, to achieve a single point between each application system has become an inevitable trend on the development of the current application.

Unified Identity Authentication Technology

The so-called unified authentication between different application systems in a network, take a unified way to detect the user identity authentication process is not a legitimate user, is in the process of communication between users and servers, with a way to confirm the identity of the user or the right limit, then the identity of the different users the distribution of access control [1]. It consists of two aspects: identification and authentication. Identification depends on the user's user name, password, password, fingerprint, handwriting, sound, etc. authentication is the process of judging the correctness, validity and validity of the information presented.
The core of unified identity authentication is a unified authentication mode [2]. After users login to the unified authentication service, all application systems supporting unified authentication service can be used. It is the general certification process: the user enters the unified identity authentication system, login input registered user name and password; unified identity authentication system and user session is established, at the same time send user access authentication token; user authentication token to access the application system of a unified identity authentication service support access; applications received access authentication token, the token to the unified identity authentication system, judge its legitimacy; legitimacy of unified identity authentication system, token judgment if legitimate, then the results will be returned to the application system; application system allows users to access.

**The Single Sign on Design Model**

SSO can effectively improve the security of the system, and more convenient to the user information management, improve the efficiency of applications, is that when the user access to the application system more need to authenticate the identity, only need a login in the initial state of identity authentication, can access other applications within the scope of authority. SSO[3] can be centralized management of different application system distributed users, system administrators only need user information and data management in a unified identity authentication system, configure different permissions, the use of the distribution of different application system.

The design model [4] of SSO can be classified the Gateway-Based SSO, the Broker-Based SSO, the Agent-Based SSO, the Token-Based SSO, the Agent and Broker -Based SSO, and etc.

Gateway-Based SSO respectively by the client and gateway and application server is composed of three parts, a checkpoint gateway as the client access the application server must pass through, it is connected with the client, and the other end is connected with the application server. The gateway records the user identity information and the IP address of the application server it accesses, so the gateway can easily implement single sign on. The SSO model set, just placing a gateway, authentication module and the corresponding configuration, the authentication module can be set to a IP address access mode based on when the client through authentication gateway, to get permission to access the application server permissions, after identifying the gateway the IP address of the application server, if combined with the gateway information in the database, then the IP address is the user to access the application server notes, can achieve single sign on. A single sign on this model depends on the performance of the gateway, the gateway determines the authentication efficiency, not suitable for large user authentication; on the other hand, the safety factor is low, the gateway can easily become the target of hacker attacks, but once it is broken, affect the safety of the whole system.

Broker-Based SSO is a client, authentication server and application server that is composed of three parts, of which the authentication server acts as a broker, it is connected with the client, and the other end is connected with the application server. When the user first login, if the identity authentication, the authentication server will send users a user identity, and use this identity can access the application server, to achieve single sign on purpose. The SSO model for authentication provides a safe and independent "third party", the use of electronic identification authentication server to send authenticated user, application server access without authentication by the authentication server again, so as to reduce the recognition time, also easy to expand the application system for other. Large scale user authentication. Due to the single sign on this model, the electronic identification is necessary for users to access the application server certificate, so in addition to safe and effective configuration of the "third party" authentication server, must also make changes to each application system, so that the application system can identify electronic identification.

Agent-Based SSO is also composed of three parts, namely client, proxy and application server, which can design different functions according to different settings. If the agent program settings on the client, it will replace the user to the application server automatically sends the user name and password; if the agent is arranged in the application server, it will replace the application server to the
user authentication or redirection etc. In the single sign on model, each application server must install the corresponding proxy program, this will cause the development difficulty and the cost to be too high, simultaneously also does not have the good versatility.

For users, the auxiliary SSO to simplify the login process, the interoperability problems are reduced to the minimum, but also does not affect the system's business processes, business efficiency and network throughput, all users on learning to use single sign on access should be more rapid, simple and sensitive. For the administrators, to achieve single sign on and cannot interfere with management of computer software and hardware resources, network environment, and the management of the SSO should not increase too much extra work or the emergence of new vulnerabilities, from the development perspective, the application of single sign on access should be independent, including the design and implementation of the code and the main business does not have such coupling, basically does not affect the original system, do not need to change or only takes up a small change can be used to access the system of single sign on any of the old and new, from the information security point of view, to risk can be expected to resist the highest level of risk will not be expected to a minimum.

Cookie Technology and Session Mechanism

Netscape invented the technology known as cookie [5]. When a user requests a Web page, the server also provides a cookie file in addition to the requested page. The browser receives the cookie file stored in the host's cookie list, just some cookie file or string, rather than the executable, so even containing the virus, no formal operation path, so it will not cause damage. Cookie contains 5 domains, namely, domain name Domain, path Path, content Content, expiration time Expires, and secure Secure.

Session is a mechanism used to maintain the state between the client and the server. Session refers to the time elapsed when the browser enters the Web page to close the Web page, which is how much time the user visits the page. The value of the Session variable is stored in the server, using a session ID to distinguish which user is session variable, the value by the user's browser when accessing the Web page back to the server, when you need to create a session for a user request, the server needs first to the access request to test the existence of session ID if the inspection, existing, so that has created the session does not need to create; if the test does not exist, it will create a session, and at the same time the production of a session ID.

The Single Sign on Implementation

Combined with the SSO model based on agent, according to the design of unified identity authentication system process, analysis of the application of Cookie technology and Session mechanism of SSO process in the design to their actual needs of the implementation of a single sign on system.

When a user accesses the application Web page for the first time, the application verifies that the user has legitimate user access credentials. If the user has and legally access the application, otherwise it will return to the authentication server.

The authentication server verifies that the user has a token issued by the authentication server, so as to verify whether the user is a legitimate user. If the user has a valid authentication token, then the authentication server sends a user credentials to the user that can access the application, or it will be required to log in again.

The user is returned to the unified authentication system login page and is asked to log in again. The user to enter a user name and password, the authentication server verifies the user's legal identity, if the legal identity authentication server, it will send to a user access token, and sends a unified identity authentication system can access credentials and one can access the application's access credentials. The relationship between the access token and the document is also recorded, and the user accesses
the application according to the token provided in response to the corresponding credentials. If the user’s identity is not legitimate, then access to the application is denied.

When the legitimate user access to another application, because the legitimate user already holds the access token can be used to access token authentication server access credentials to access the application, we can access to the application.

From the above process can be seen, if the user's legal identity, then not only will return to the user identity authentication server legitimate messages, and will return the authorization information, and will the legal identity information and authorization information is encapsulated in cookie, the user's browser to receive cookie, information will be written to the session, after the user access to the other again application of the system, you can use session with information, smoothly through the verification, which do not use the username and password to log in again, you can directly according to the function module in session application system access authorization information.

In reality, SSO has a more complex structure. The user information database is not absolutely single, involved in a large user base in the enterprise, the user information based on the different types of large scale, cannot do all the user information stored in a single centralized database, which requires the SSO mechanism should allow the user information stored in the storage unit is different, therefore, need to the emphasis is the unified authentication system has no effect on substantive single sign on. The authentication server is not absolutely single, the whole system can have two or more sets of authentication server, the authentication server and even different products are also allowed, for the completion of the single sign on a higher level, the authentication server through a communication protocol between standard authentication information exchanges.

Conclusions

The single sign on authentication mechanism manages the dispersed user identity information in the network. It can cross domain access through one authentication, and has gradually become a practical application in recent years. This paper discusses the SSO technology related technical background, analyzes the implementation scheme of Web SSO based on typical, combined with the digital campus environment, further research support Web services framework, the SSO authentication service has good scalability and integration, can not only support the existing application system and user authentication, should be flexible and convenient use mode, reduce the resource waste and technology, to provide a convenient user support.

Acknowledgements

I thank reviewers for constructive reviews and suggestions that improved the quality of this paper. This essay is the fruit of our several months’ consisting work. This work was supported by the guidance project of science and technology research plan of Hubei Provincial Department of Education, project number is B2017190, project name is research and application of single sign on key technology based on Web.

References