Research and practice about the identity authentication technology

Yun Xia, Fu
The College Of Computer & Information
China Three Gorges University
Yichang, Hubei Province, China
512716030@qq.com

Keywords: identity authentication; Single sign-on model; Kerberos authentication

Abstract. During the rapid development of the network, this is very important that the system is security.we should will be thinking about the problem ,it is the system's first line of security . How do we protect and build it?In this paper, we introduce about Kerberos authentication and certification process; At the same time we introduce the Cookie technology and LDAP directory service methods. At last ,We have been established a unified identity authentication ,it is single sign-on model. we will rely on the model. During the running of the system,I t will be ensured the safety and reliability.

Preface

Today , the variety of application service about network is very wide.we can see at any time in our life. It is used to identify the identity authentication in Network application system. The different identity of the user authorization has different operation, Users need to remember a lot of user name and password,but the Password is easy to forget.

The system is not convenient to manage user's data, it will be caused data inconsistencies in the database.It will be established a centralized identity authentication module in the application system for identity authentication, As long as the user authentication is right, the user's operation is very convenient,it is very easy switching between subsystems in the portal. Users do not need to remember the login name and password, the management about network resources is unified and centralized. The operation mechanism and environment of colleges and universities is very especially, With the rapid development of university informatization construction pace, we must establish and improve in the unified identity authentication system, it will be unified management about the function of centralized management.

Kerberos Protocol

In order to realize the identity authentication, we use Kerberos protocol.It allows the computer through the exchange to encrypt the message with another computer on the network to prove identity. If authentication is successful, it will creat secret key during the two computers .If you have secret key,you will communicate dialogue each other, it will be prevented the attack about eavesdropping and replay.[1] There is two compositions about Key Distribution Center .They are authentication server and award tickets server.

First ,we will introduce the term ,it will be used in the below article. AS: the authentication server;TGS:ticket grant server;TMC: ticket management server; TGT: ticket grant license ticket. It will be introduced using Kerberos technology to realize the authentication process.

The first step, the Kerberos client apply for the bill TGT from the AS authentication server .

The second step, when the customer reveive message from AS, it will be checked the correct in the authentication database, users will be confirmed that the user is legitimate,they belong to confirm the Kerberos client,it will be generated a session key. At the same time it will be used the Kerberos client's secret key to encrypt the session key, and produce a bill TGT. Part of the TGT is the Kerberos client entity name, address, time stamps, restrictions of time and the session key. After the AS generated TGT, it will be sended the TGT to Kerberos client.

© 2016. The authors - Published by Atlantis Press

The third step, the Kerberos client received TGT from AS, then it will be used its own secret key to decrypt, get the session key.After it will use the declassified information to reconstruct certification request list,and it will send a request to the TGS ,so it will apply for the notes,it will access to the application server AP.

The fourth step, TGS use its secret key to decrypt the TGT, at the same time it will be used the TGT session key encrypted authentication information and to the customer request and the authentication information decrypted with the information in the TGT.After the TGT can generate a new session key to the customer and the application server is used, combined with its own secret key encryption session, finally generate a paper.TGS generated after the TGT, sends the TGT Kerberos client[2].

The fifth step, the client will receive the response from the TGS, the client will receive the session key for Shared with application server .At the same time, client will generate a new access to the application server authentication,he may use the authentication to encrypt the application server session key,. At last it will send the bill to the application server.

The sixth step , the request will be confirmed from the application server .

While they finished certification during the AS and TGS each orther, they will get the session key, they can encrypt data transmission with the session key.In the Kerberos protocol ,there are two advantages about AS and TGS dual authentication: first ,it will reduce the user key exposure, it can reduce the accumulation of the attacker to the related user key cipher;The second is the authentication process has the advantages of single sign-on SSO users get the TGT has not expired, complete to any server in the system authentication without having to enter the password.

LDAP Protocol

The LDAP protocol is a connection-oriented TCP protocol implementation, it defines the LDAP client and the communication process between the LDAP server and message format.It will be monitor in service port of LDAP server . After receiving the request ,it will be made by the client, so it will establish a connection, and will start session.During the process of each step and each session request, the server has to reply. The LDAP directory server supports distributed directory service. If the directory structure is relatively large, it will use multiple servers to storage respectively the different parts .During the directory server connecting is used to a pointer.The LDAP server directly connected to the directory, and return the results to the client application [2] [3].

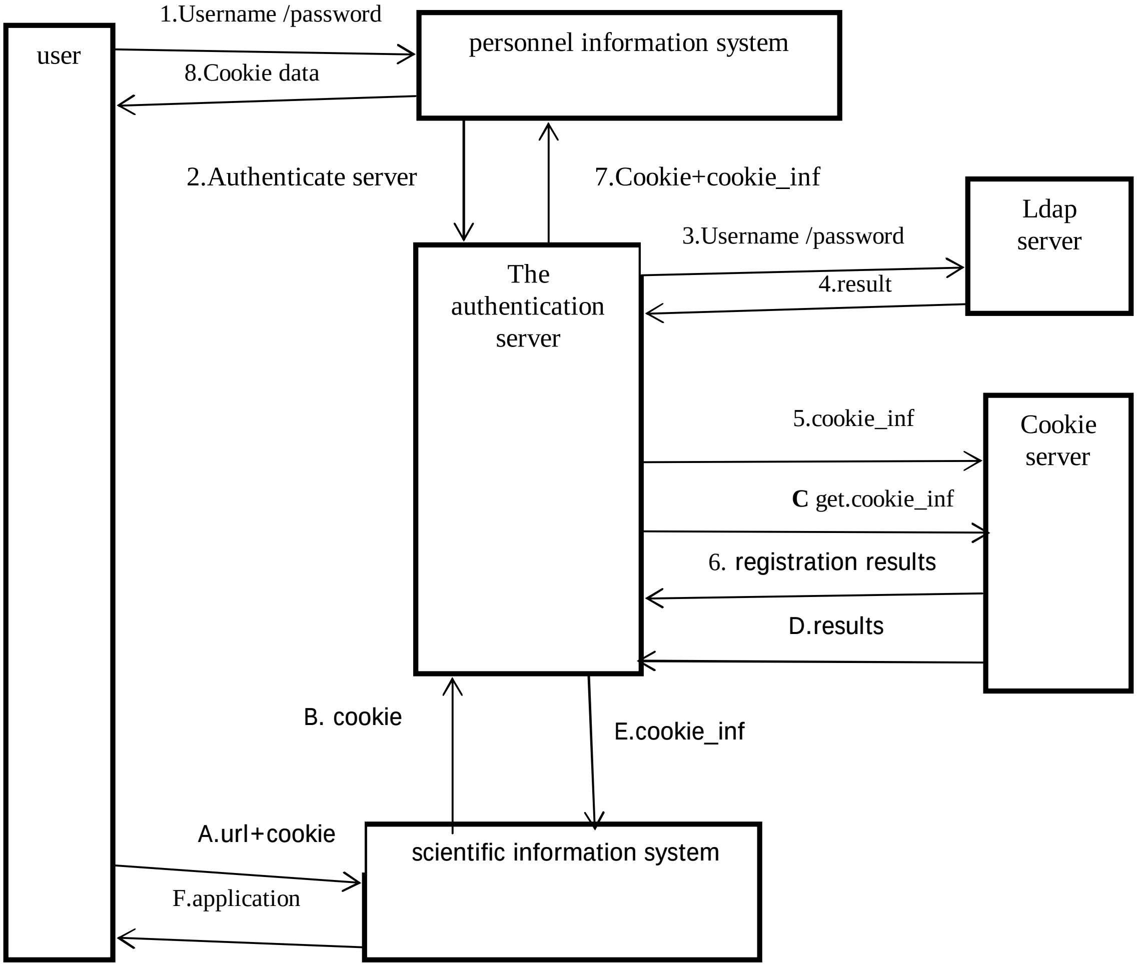
Authentication Scheme T Of SSO

Our purpose will integrate the campus all application,so we have to achieve a login more traffic through the unified portal of entry.We achieve single sign-on ,we will achieve certification based on the secondary authentication,we can distinguish the legitimacy of the user. At last, we will realize single sign-on (sso).In this design, we use cookies to realize single sign-on (sso), and solve the problem of Cookie cross-domain sharing.our ultimate goal is the following nodes: first ,we will integrate the information resources and the related system aboutour campus system; second we will realize unified portal, a single sign-on (sso), implement different service.

The single sign-on system can be made up of three parts: the first part is unified authentication server; another part is user data center;The third part is a identity authentication system. Sso server is installed on the unified authentication Server,it will provide services for the system of single sign-on.SSO Agent is a part of the WEB application system, it will be installed in the WEB application server. It will provide user login information, visit the notes, etc.

We will follow design criteria when we built the framework of the system. First part is system based on WEB environment, running under the IE browser, use Cookie technology. The second part, the user operation will be quick and convenient. Because we used LDAP application platform, we will manage the system through authentication server, user hasonly one password to login the system. The third part is securite about the system. We used Role Based Access Control,we will ensure our information to be stolen and to be tampered.

We use cookies technologyin oue system, the Cookie is mainly used to maintain the state of the user and the server, it is a small piece of text information, it will be transfered along with the user's request page between Web servers and browsers.Every time the user access to the site, the Web application will read cookies contain information.Cookies contain mainly information include the name of the Cookie, the Cookie value, the validity of the Cookie, domain name, URL path, safety signs.Use cookies and Cookie_ inf to save the user authentication information, including cookies stored on the client side, while Cookie_inf stored in Cookie Server, in Cookie_inf contains user authentication need relevant information, such as the ID number of cookies, produce Cookie Web Server code, use MD5 encrypted information, user information encryption.We will use LDAP in the digital campus identity information ,the LDAP is very import.We will collect organization structure information、 resources、authority through LDAP directory structure. We will storage the identity authentication of the library through the database to the LDAP structure. It will be simpled ,we can unify storage of information, we will avoid data redundancy, ,we will cooperate convenient operation.



Users will login through their own username/password, first this information will be verified on the authentication server. If this information is legal, then the urser information will be checked on the LDAP server. The result of the validation and the information will be bring from database of legitimate users , it will be write a Cookie in the server. Users get certification paper, urser will access all application system within the effective time (time stamp). Because of the Cookie records the user access to the WEB application system of information, so the urser access to the WEB application system again, in the same browser will put the record sent to the server, this purpose is that the server can read original client information form saved. First step is judged the user is logged or is not login. we will verify the ticket from the cookies to Cookie Server, the urse will get the result from Cookie – inf.

If the login can direct access to the scientific research information system, so as to realize and achieve the function of the single sign-on.

Analysis Of The System Safety

We design the single sign-on authentication system, we will trust between authentication server and application server each other, this ticket is safety and reliable in the passing data . Therefore ,we issue certificate to the application server and the authentication server .It will provide security through using SSL technology , we will establish secure channel to avoid network eavesdropping. System use paper timestamp of the authentication process , if these exceeding time limit for the timestamp bills, then it will be discarded and it will be not used again. We protect the communication parties from message replay attack ,we use serial number in the SSL technology, the serial number be encrypted as a load of packets sent.During the SSL handshake, system can produce different random numbers to mark the SSL handshake, so replay attack at bay.

Conclusions

In this system, we use Kerberos protocol, cookies and Cookie - inf, LDAP technology. We design the single sign-on authentication system. We will protect the information security during using SSL protocol , in the system we will ensure the data during the network environment,it will be more accurate, safe and reliable. With the development of computer technology, there will be more identity authentication protocol and various implementation techniques, these protocols are constantly to perfect and improve their system hidden trouble existing in the practical application of authentication.

Acknowledgements

This work was financially supported by the Shanghai Natural Science Foundation (0666666), Innovation Program of Shanghai Municipal Education Commission (060000) and Shanghai Leading Academic Discipline Project of Shanghai Municipal Education Commission (0555555).

References

[1] Proceedings of 2010 Second International Conference on E-Learning, E-Business, Enterprise Information Systems, and E-Government (EEEE 2010) Volume 2[C]. 2010

[2] V.Geetha,Pranesh.V.Kallapur. Web Security: Research Challenges and Open Issues[A]. Advances in Computer, Communication, Control and Automation (3CA 2011 V121) [C]. 2011 [9] Pranesh V.Kallapur,V.Geetha. Web Security: A Survey of Latest Trends in Security Attacks[A]. Advances in Computer, Communication, Control and Automation (3CA 2011 V121) [C]. 2011

[3] Mehdi Sadeghzadeh,Saied Jafarian. Black Hole Attack Detection Using Trap Packet[A]. Proceedings of 5th International Conference on Intelligent Systems(ICIS'2015)[C]. 2015