Advanced Engineering Forum *Online: 2012-09-26*
ISSN: 2234-991X, Vols. 6-7, pp 843-847
doi:10.4028/www.scientific.net/AEF.6-7.843

Security Strategy Research and Design based on Agency Identity Authentication

Xie Chuan

Hangzhou Vocational & Technical College, Hangzhou 310018, China

Xiechuan999@163.com

Keywords : Security strategy; Agency; Authentication; LAN

Abstract. The application of LAN in enterprises has become wider and wider, it brings efficiency and convenience to management and production, but at the same time, security threat is increasing. This threat is influenced by the factors such as network environment, network management and the level of the staff. Therefore it causes the realization of LAN security strategic planning is not entirely reliable, reflecting mainly in the subjective factors such as network user identity authentication. Through research, on the basis of the application of Single Sign-On technology and introducing the agency identity authentication system, a new security strategy is built up, which can improve the whole LAN security.

Introduction

Security strategy is defined as a set of rules used for all safety activities in a safe area. These rules are established by a safety authority organization in the safe area, described and implemented by a safety control mechanism. According to the authorization nature, security strategies can be classified into identity based policy, rule based policy and role security policy. Identity based security policy is the strategy which ensures the network application security by confirming the operator identity in the network application. The most important feature of it is having "short board effect".

The study thinks that the weakest link of network security strategy is the operator norm, namely the identity authentication management. Nowadays, identity authentication mainly uses "user name", "password" and other informations. Therefore, the hidden danger of identity authentication lies in: identity authentication information length is not enough; there's no record of non encrypt form; it is not modified within the prescribed period, and may be repeated; or it could repeat because of different network application, etc..

Due to these factors mostly belong to the operator's subjective behaviours, it is difficult to overcome these security risks only with the operators own constraints in the circumstance that the same user uses different application systems simultaneously. Thus, the study attempts to set up a proxy authentication system to solve the above problems, namely minimizing the subjective factors influencing network security by "agent" password and security management.

Agency Identity Authentication

Common network identity authentication generally adopts SSO (Single Sign-On) technology, as shown in figure 1. This technology requires modifications of every application system codes and fails to support unlocal applications, such as public Email, MSN, QQ and so on. Meanwhile, the security also exists the above problems.

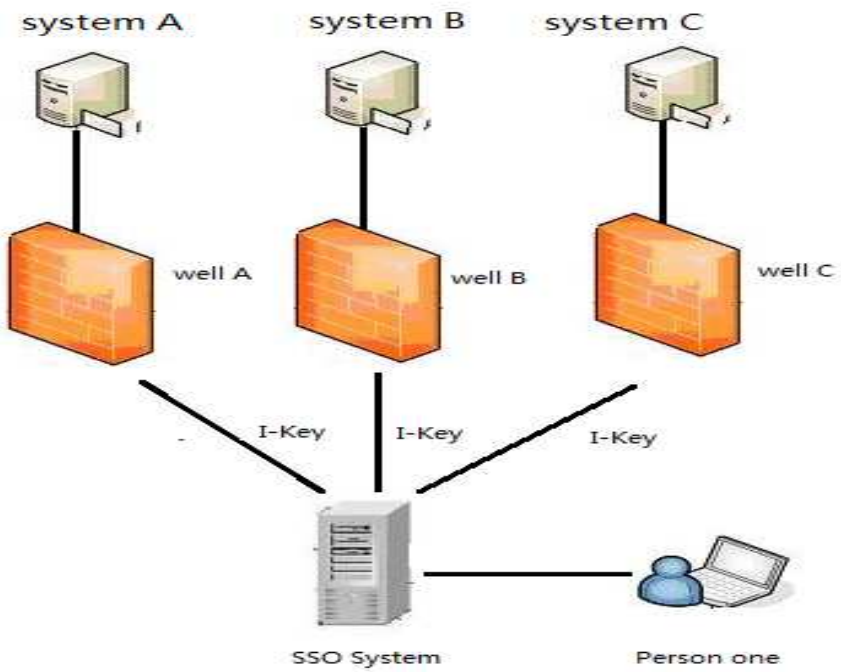

Figure 1. SSO Technology

The research uses single sign-on to make an access strategy which only requires a user certificate to access different systems and all hardware and software resources in the Internet, improving the security of the network system, namely: Agency identity authentication (PSO, Proxy Sign On) network security strategy, as shown in figure 2.

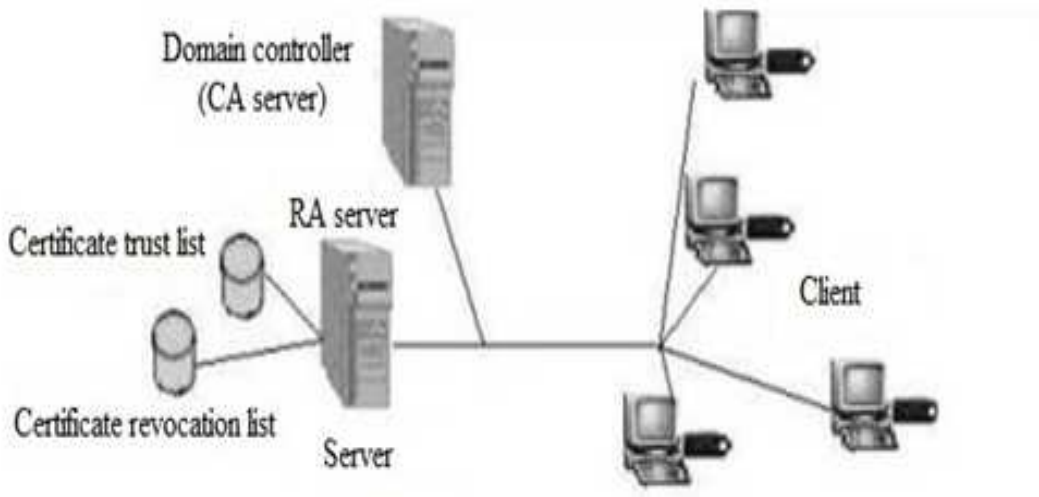

Figure 2. Conception of agency identity authentication strategy

System Design

The server monitors user login Session through the C session Management unifiedly, in which each SSO information is stored in the corresponding session. C Authorization Server controls Agent by Session settings, new item and expired events.

Server design is shown in figure 3.

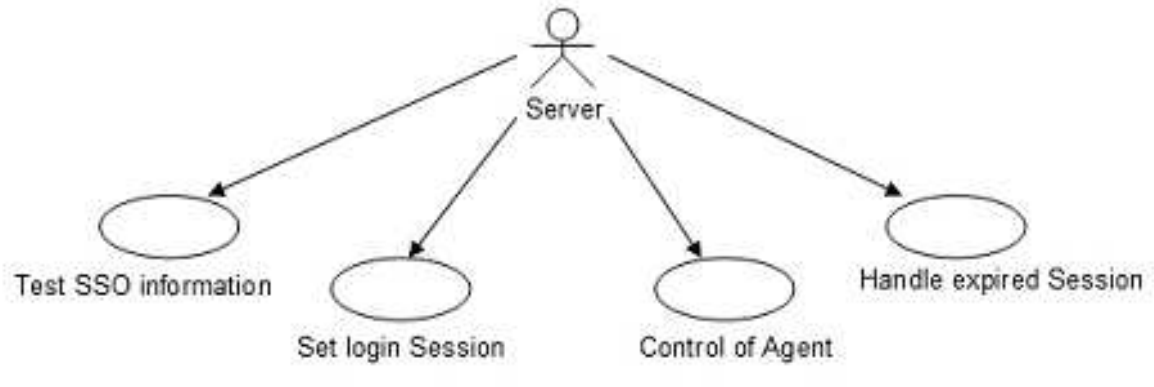

Figure 3. Server design

Analyzing and repackingdata packets through the interception of C SSO Firewall, sending to the designated target, and giving feedback of the authorized server Session changes. Agency design is shown in figure 4.

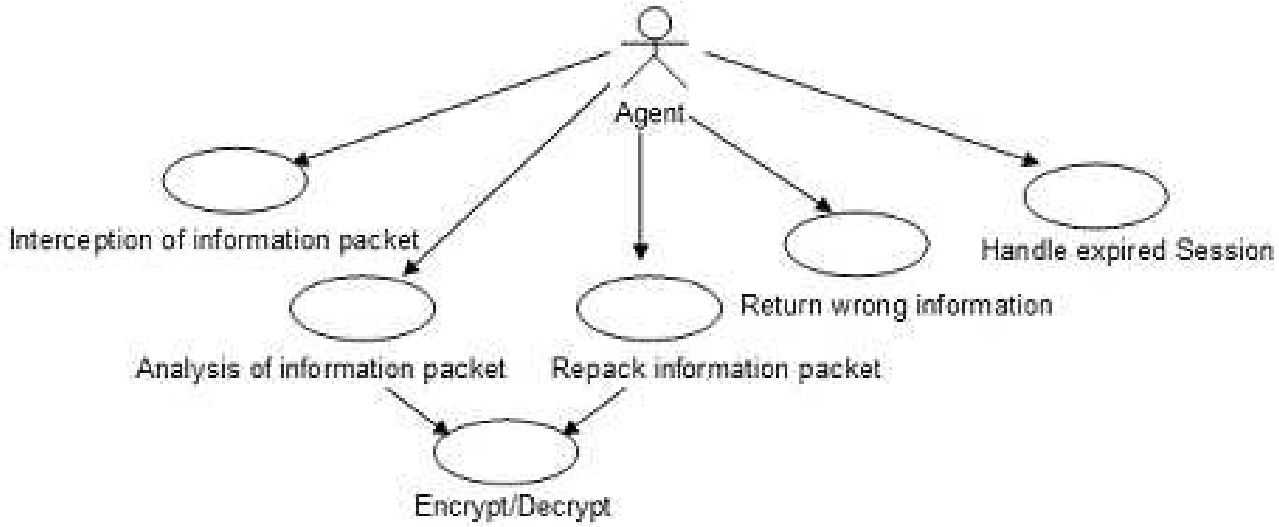

Figure 4. Agency design

Client Design

Start two aspects operation through the CHookDll class. Obtain basic information of the hook object program, package into the CApplicationInfo class and pass to the CDatabaseConn class for database operation. The CDatabaseConn class gets the corresponding database information by adopting the CXMLConfigLoader methods.

System Sequence

System sequence is shown in figure 5.

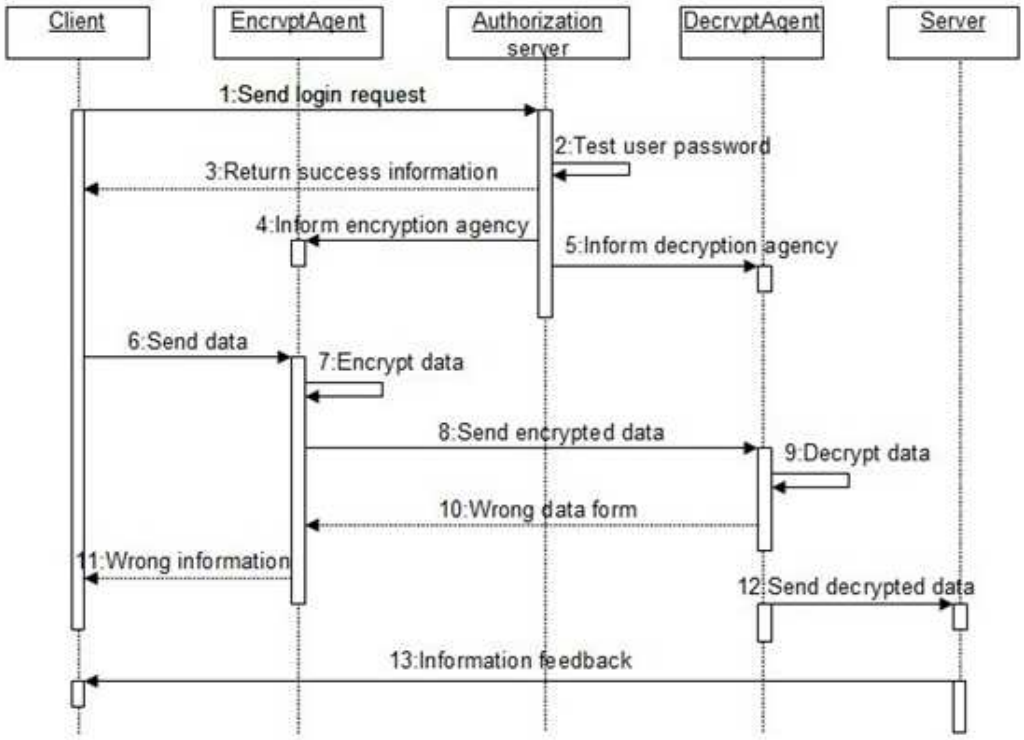

Figure 5. System sequence

Background Database Design

(1)User List

Set user list for the storage of system user information. The structure is shown in table 1.

Table 1 User List

List	Type	Major key	Instruction
UserID	Integer	PK	List Indec
User	Varchar	—	User
Pass	Varchar	—	Password
Purview	SmallInt	—	User limitation

(2)Application List

Set application list for the storage of program information in the system. The structure is shown in table 2.

Table 2 Application List

List	Type	Major key	Instruction
AppID	Integer	PK	List Indec
Name	Varchar	—	Program
Process	Varchar	—	Process name
Comment	Varchar	—	Program notes
Type	SmallInt	—	Program types C/S or B/s

Conclusion

The research practice chooses equipment management, material management, sales management, security management and other systems, which all have their own user identity authentication information and manage the application access authorization of their users. Integrate the above

systems through the proxy identity authentication system in the practice, forming a new strategy for network security. Realizing unified identity authentication by adopting the strategy, which is suitable for the currently common used C/S and B/S architectures. To enterprises users, this agency identity authentication mode integrates the user group identification information, enhancing network access and authentication security based on in the formation of unified user identity authentication. At the same time, users can log on many application systems simultaneously through C/S or B/S, and the uniqueness of the log also can be guaranteed. Thus, it constructs a high security access strategy for the network application system.

References

[1] Yongxiang,Xu. Unified User Managment System Design[J]. Computer Engineering,2003,29(5):120- 123.

[2] Manshan, lin, Heqing, Guo. SSO Technology Situation and Development[J]. Computer Application,2004,24(6):248- 250.

[3] Wei, Han, Zhihua, Fan. Application Research of SSO Technology in Web Service based on SAML[J]. Computer Engineering and Design,2005,26

[4] Ting, Zhang, Jixiu, Geng. SSO Implementation Patterns Research in Web[J]. Computer Simulation,2005,2

[5] Shenlu, Lai, Xin, Li, Chuan, Jun. Pluggable SSO Technology Application[J]. Computer Engineering. 2008(14)

[6] Xiaohui, Zhou. Solution of Cross-domain SSO based on Digital Certificate[J]. Journal of Changchun University of Technology (Nature Science). 2010(06)

[7] Dazhi, Li, Sihan, Qin. Design and Implementation of Identity Authentication based on PAM[J]. Computer Science. 2005(02)

[8] Yinfeng, Lin, Zhonghua, Feng. Design and Implementation of Campus Network Unified Identity Authentication based on LDAP[J]. China High Technology Enterprises. 2011(10)

[9] Rongxin, Fu, Fanren, Kong. Research on Resource Sharing Platform Authentication Mechanism based on Shibboleth[J]. Journal of Hezhou University. 2011(02)