An Improved Single Sign-On Model: Design and Implementation

Degang Sun[1], Hui Deng[2], Rui Mao[3]

Institute of Information Engineering, University of Chinese Academy of Sciences, Beijing 100093, China

sundegang@iie.ac.cn, denghui@iie.ac.cn, maorui@iie.ac.cn

Keywords: Single-Sign-On, Identity Authentication, Access Control.

Abstract. The application of single-sign-on is a technology which aims to manage the access control of the internal systems of enterprises. The traditional single-sign-on models cannot simultaneously meet the requirements in implementation, manageability, system pressure, and security. In this paper, based on the traditional models of gateway and broker, we propose an improved model that integrates the advantages of these two models. Both theoretical analysis and experimental results indicate that our proposed model have good performances in implementation, manageability, system pressure, and security.

1. Introduction

Nowadays, the identity authentication is a basic requirement for most application systems. At present these systems mainly use the user ID and password as a means of identity authentication. According to statistics, a typic -al web users have 25 accounts[1]. Because of the independence of these systems, users are forced to register each website alone. Manag- ing a large number of accounts and passwords as part of the daily work brings a lot of trouble to these users. Meanwhile, users frequently choose weak password and reuse them on several websites, which leads to the leak potential hazard of password.

The concept of single sign-on (SSO) is brought forward in this context[2-3]. SSO is a property of access control of multiple related, but independent software systems, with which an authorized user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or password [4]. In this way, the users only need to login one time and then they can access all authorized resources. SSO introduces great benefits such as less required number of user IDs and passwords and higher security of the system[5].

In this paper, we first introduce the traditional single-sign-on models and gives the theoretical analysis of implementation, manageability, system pressure, and security of these models. Then we propose an improved model on the basis of the traditional single-sign-on ones.

2. Single-Sign-On Model

To realize single-sign-on system mainly has three common models:the broker-based single-sign-on model(SSO), the agent-based single-sign-on(SSO) model and the gate- way-based single-sign-on(SSO) model.The following will introduce of the three models respectively.

2.1 The Broker-based Single-Sign-On (SSO).

The broker-based single-sign-on[6] system model consists of clients, authentication server, and the application server. Represented by the classic Kerberos protocol, all authentication work is completed by authentication server. The certification process is: before access to the system resources, all the clients forward to the authentication server for authentication. The authentication server returns an identity token to the user and the user brings the token to access other application servers[7], so as to realize single-sign-on (SSO).Figure 1 illustr- ates the broker-based single-sign-on model.

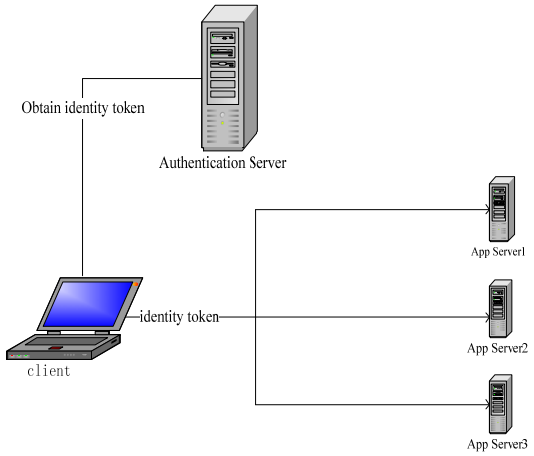

Fig. 1 The broker-based SSO

2.2 The Agent-based Single-Sign-On (SSO).

In an agent-based single-sign-on(SSO) [8]model, an agent program automatically authenticates user identity for different applications. This agent can work in different ways. It can use password or encryption keys to authenticate automatically, thus taking the certification burden away from the user. Agent can also put in the server,acting as a "translator" between the server authentication system and client authentication method. Figure 2 illustrates the agent-based singl- e-sign-on model.

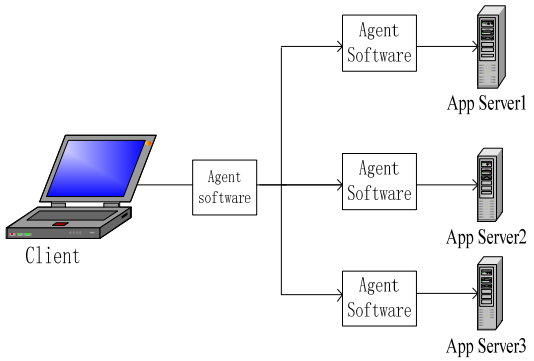

Fig. 2 The agent-based SSO

2.3 The Gateway-based Single-Sign-On (SSO).

In the gateway-based single-sign-on (SSO) [9]model, the gateway acts as a hurdle, isolating the client and application server. Among them, the gateway is responsible for maintaining a record user identity information and its access to IP address of the application resources of forms. The gateway realizes single-sign-on (SSO) through this form. After authenticated successfully, clients can access the application server resources authorized to him [10] . Figure 3 illustrates the gateway-based single-sign-on model.

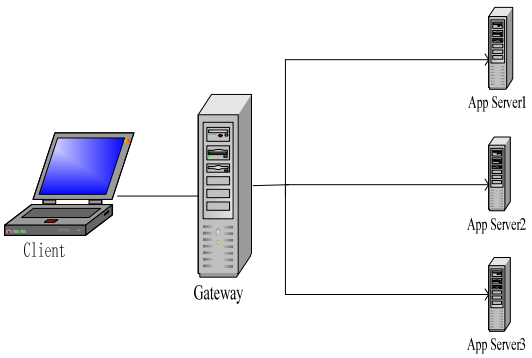

Fig. 3 The gateway-based SSO

3. Model Evaluating

For single-sign-on(SSO) model,we used to measure the performance from aspects of implementation,security,manageability,and the system pressure.Possibility of implement means the complexity of the system implementation,namely the complexity of the existing system integrating to single-sign-on (SSO).Manageability refers to how to manage user information.Safety is used to measure whether system is vulnerable to attack.The system pressure means the pressure which the system bears under user authentication proc- ess.

3.1 The Broker-based Single-Sign-On (SSO).

(1)Implementation: The broker-based sing- le-sign-on is essentially a kind of ticket-based [11] single-sign-on model. In this way you need to modify the target system and the original part of user authentication of each application system should be modified to validate access tickets.At the same time, when application system changes, the client should also be modified, whicn will introduce the difficulties in implementation.

(2)Manageability: This model stores the information such as user information, applicat- ion server information centrally, which is unified managed by the central database [12] . So the management is convenient, which is the main feature of this model.

(3)Security: The model generally adopts the way of timestamp to ensure security of validating ticket, which is vulnerable to replay attacks [13] . Therefore, this model cannot achieve a high security.

(4)The system pressure: All authentication and authorization work are done by authentication server. A central server problems can cause paralysis of the entire system [14] , so the system pressure is heavy.

3.2 The Agent-based Single-Sign-On (SSO).

(1)Implementation: The agent-based single-sign-on (SSO) makes it easy to integrate the application system [15] into single-sign-on system,but the agent needs to design and realize the interaction with original applicatio- ns. That means the requirement of develop- ments is quiet high for the agent supplier.

(2)Manageability: The agency can't help manage information. We need to store the user name and password in the local [16] . Each application server has its own authentication module. The application server not only needs to manage themselves but also needs to manage agent configuration information. Thus information is decentralized.

(3)Security: The model often uses encrypt- ion authentication protocol, the communicat- ion of agent program should be safe, but the agent itself stores the user authentication information and agent configuration information. Security is focused on the safety of the agent itself, which must be able to ensure the security of sensitive information and ensure that they are not being gave away or misused.

(4)The system pressure:Each application server has agents,the certification of work completed done by each agent.There is no centralized authentication so that the system presure is small.

3.3 The Gateway-based Single-Sign-On (SSO).

(1)Implementation:Under this model, the change of client does is not big, as long as we configure the gateway for mutual authenticat- ion module. When the application system is changed, the clients just need to modify the configuration of gateway, the client's change is very small.

(2)Manageability: All clients through the gateway to access the resources, all user information is stored in the database gateway[17], the way of centralized storage is convenient to manage. However, when using multiple gateways, how to synchronize data and keep the consistency will be a problem[18].

(3)Security: The gateway can be a firewall, or communication encryption server[19], which can promise the safety in the process of data transmission.

(4)The system pressure:The gateway does the work such as authentication and authorization, it also needs to store informa- tion (the user information,application server information), which brings a great system pressure.

4. An Improved Single-Sign-On(SSO) model

4.1 An improved Single-Sign-On (SSO) model.

The broker-based single-sign-on model will change the authentication module of the original system and is vulnerable to replay attacks.For the agent-based single-sign-on (SSO),user information is stored in the local, which exists the risk of password leak. As to the gateway model, the system burden will be a problem. However,the broker-based single sign-on model can store identity information centrally.The gateway model can guarantee the security of data in the process of data transmission and the deployment is quick. Combining the advantages of broker-based SSO and gateway-based SSO model together, we hand over the authenticat- ion work to the authentication server and the authorization work to the gateway.Therefore we put forward an improved single-sign-on model.Figure 4 illustrates the improved single-sign-on model.

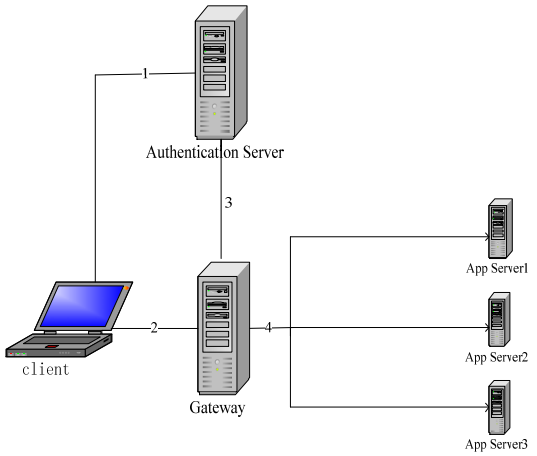

Fig. 4 The improved single-sign-on model

(1)The user certificates identity through authentication server, after the success of the certification, authentication server queries the user access to the server list of all the application systems, identity token and returns them to the user.

(2)The user select the application to click and generates the HTTP request. The application server establishes a connection with the gateway and then transmit user ID, app name, identity token to the gateway.

(3)The gateway will submit information to the authentication server;

(4)The gateway returns the authorized information of user back to the application server. The application server conducts access control and returns the results to the client browser. Users can view the results.

4.2 System Implementation.

The system is implemented based on our improved SSO model, which involves five entities: the smart client, authentication server, resource server reverse proxy server, gateway, and application server.

Authentication server is the most important part in the system. It implies authentication of client and interaction with user database. Resource server used to store the server information, user information, permissions, etc. Smart client application is installed on the smart client, which is mainly used for the interaction with the application server and authentication, showing the list of application systems which users can access. The gateway is mainly used to encrypt communication information and responsible for pulling access information for the user's HTTP request. The reverse proxy server is mainly used to forward the user's request. Figure 5 illustrates the system structure.

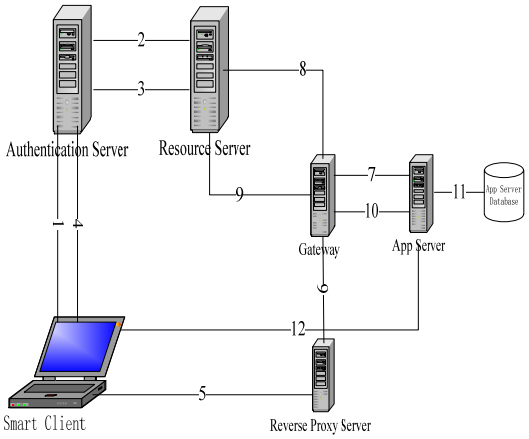

Fig. 5 The system structure

The System working process is as follows:

(1)After the computer system startup, the user start the smart client desktop applications and insert the USB key and input pin code, the intelligent desktop and unified authentication server build a connection.

(2)The authentication server downloads the user's identity information and certificates from the resource server and authenticates the user's identity

(3)After the successful authentication, the authentication server queries the user access to the server list of all the application from resource server

(4) The authentication server returns identity token, the list of application systems users can access, to the intelligent desktop.

(5) The intelligent desktop will receive token and keep it in memory. The application list is presented to the user. When the user selects the application on the list to click, generating an access request, forwarding the request to the reverse proxy server.

(6)The reverse proxy server forwards the request to the gateway.

(7)The gateway forwards client requests to the application server and the application server will forward user ID, token, app name to the gateway;

(8)The gateway submits the user ID, token, app name to resource server, in order to get the user authorization information.

(9)Resource server queries user request and authenticates token from the gateway. If the token is invalid, it returns empty information. Otherwise it returns the authorization information to the gateway.

(10)The gateway returns authorized information of user back to the application server.

(11)The application server conducts access control, connecting the database application system, transferring the access request to the database. The database server processes the request and returns operation results to the application server

(12)The application server returns the result to the client browser.

Figure 6 illustrates the system working process.

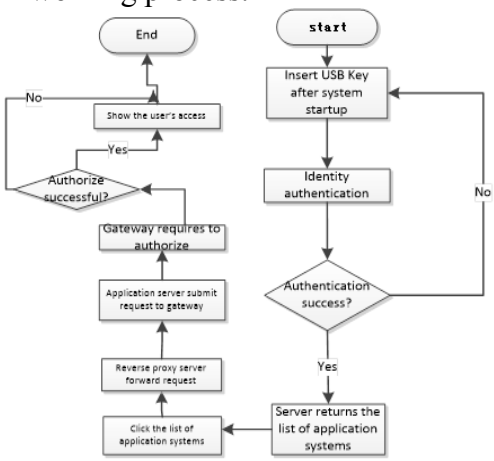

Fig. 6 The system working process

4.3 System Performance.

(1)Implementation: As to gateway-based model, the deployment is convenient and the change is small. In the improved-model, we make full use of the advantage. When application systems change, the change of client is small. The integration into system is easy and the possibility of implement is strong.

(2)Manageability: The advantage of broker-based SSO is that information stored centrally. Therefore the management of authentication information is convenient.

(3)Security: The authentication of system is based on a USB Key, which is a tool combining software with hardware. This kind of authentication is a strong one-time pad double factor authentication mode. The Key intern contains single-chip computer or smart card chip, which can store the user's keys or digital certificates. We use the password algorithm of user identity authentication that USB Key built-in [20] to ensure the safety of authentication. Second, we use the proxy server forwarding HTTP request to application system, so as to protect the security of application system. Moreover, the gateway guarantees the privacy of data in the process of data transmission by encryption thus improves the security.

(4)The system pressure: Through the improved SSO model,we separate the authentication and authorization process, reducing the pressure of the gateway. And the proxy server can also reduce the system stress and improve performance.

4.4 System Testing.

The system uses reverse proxy server to optimize system performance. We compare the system performance between the system which uses the reverse proxy server and the system which does not use the reverse proxy server by test tools, called LoadRunner. We send HTTP request and compare the system response time respectively in the number of concurrent users for 10, 20, 30... 100 cases. Figure 7 illustrates the results.

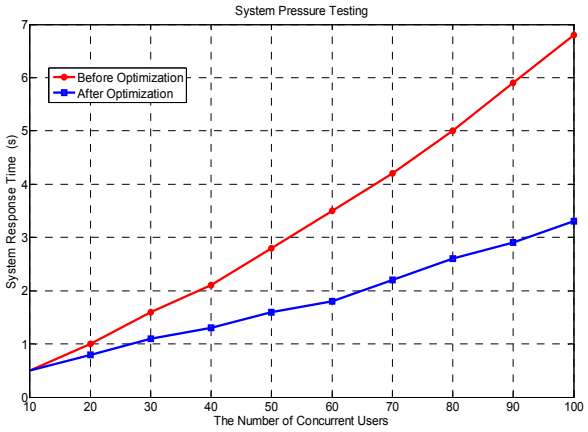

Fig .7 System Testing Results

From the figure 7, we can see that the system response time under two conditions is similar when there are not too many concurrent users. But when the concurrent users increases gradually, the performance difference is more and more obvious. When the 100 concurrent users access, the response time of system that uses reverse proxy server is almost twice as fast than which does not use the proxy. There the system obtains the good effect by using reverse proxy server.

5. Summary

In this paper, we combine the broker-based and gateway-based. Therefore we can not only store identity information centrally, which is convenient to system management and maintenance, but also use the advantage of gateway-based model that the deployment is convenient and the change of system is small, guaranteeing the security of data transmission. In the system, the authentication server completes the identity authentication. The gateway is mainly responsible for authorizat- ion work that user access to the application system. We reduce the burden of the system by separating the authentication and authorization work from each other. Besides, we use a proxy server to forward the request. The system has obtained the good effect in the aspects of possibility of implement, security, manageability and the system pressure.

References

[1]. Mayer A, Mladenov V, Schwenk J. On the Security of Holder-of-Key Single Sign-On[C]//Sicherheit. 2014: 65-77.

[2]. Ren Dong，Liu Lianzhong．Design on Secure Single Sign-on Model for Wbe Application Environment [J]． Computer Engineering and Applications，2002，38(24)：174—176

[3]. Binu S, Misbahuddin M, Raj P. A Single Sign on based secure remote user authentication scheme for Multi-Server Environments[C]//Computer and Communications Technologies (ICCCT), 2014 International Conference on. IEEE, 2014: 1-6.

[4]. Chun K L, Katuk N. A usability study of social media credentials as a single-sign-on mechanism: Student access to online teaching materials [J]. Journal of Industrial and Intelligent Information Vol, 2014, 2(3)

[5]. Tiwari P B, Joshi S R. Single sign-on with one time password[C]//Internet, 2009. AH-ICI 2009. First Asian Himalayas International Conference on. IEEE, 2009: 1-4

[6]. Lei W, Liang X J, Zhang H. Design on a Single Sign-On Scheme[J]. Applied Mechanics & Materials, 2010,

[7]. Mavrogiannopoulos N, Pashalidis A, Preneel B. Security implications in Kerberos by the introduction of smart cards[C]//Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. ACM, 2012: 59-60.

[8]. Hardwaj M, Singh S, Singh M. IMPLEMENTATION OF SINGLE SIGN-ON AND DELEGATION MECHANISMS IN ALCHEMI .NET BASED GRID COMPUTING FRAMEWORK[J]. International Journal of Information Technology and Knowledge Management, 2011, 4(1): 289-292

[9]. Pham D, Sood A K. An intrusion tolerance approach to enhance single sign on server protection[C]//Dependability (DEPEND), 2010 Third International Conference on. IEEE, 2010: 98-103

[10]. Wu Y, Suhendra V, Guo H. A gateway-based access control scheme for collaborative clouds[C]//the proceedings of 7th International Conference on Internet Monitoring and Protection. 2012.

[11]. Manshan Lin,Heqing Guo. The status and development of Signle sign-on(SSO)[J].Computer Applications, 2004 (S1): 248-250

[12]. Milenković I, Latinović O, Simić D. Using kerberos protocol for single sign-on in identity management systems[J]. JITA-Journal of Information Technology and Applications (Banja Luka)-APEIRON, 2013, 5(1).

[13]. Dua G, Gautam N, Sharma D, et al. Replay attack prevention in Kerberos authentication protocol using triple password[J]. arXiv preprint arXiv:1304.3550, 2013.

[14]. Luo F. A Design and Realization of SSO based on CAS[J]. International Journal of Engineering Practical Research, 2013.

[15]. Hursti J. Single sign-on[C]//Proc. Helsinki Uiniversity of Technology Seminar on Network Security. 1997.

[16]. Hajivali M, Fatemi Moghaddam F, Alrashdan M T, et al. Applying an agent-based user authentication and access control model for cloud servers[C]//ICT Convergence (ICTC), 2013 International Conference on. IEEE, 2013: 807-812.

[17]. Hayhow R, Gleeson B M. System and method for authenticating a network gateway: U.S. Patent 8,621,595[P]. 2013-12-31.

[18]. XU Fang-heng,CHEN Xuan,LONG Dan. New distributed multi-user single sign-on system model [J]. Application Research of Computers, 2012, No.9 (09):3355-3357

[19]. Wu Y, Suhendra V, Guo H. A Gateway-based Access Control Scheme for Collaborative Clouds[C]// In the International Conference on Internet Monitoring & Protection. 2012:54-

[20]. Meng Y X, Dong J Y, Yin Y H, et al. Transparent encryption technique for Word documents based on USB Key in Manufacturing System[C]//Applied Mechanics and Materials. 2013, 252: 323-3