Research on Network Security and Identity Authentication

Jin Meng[1, a], Jing Zhao[1,b], Ming-shun Xing[1,c] , Tie Ma[1,a] and Hai-yan Zhao[1,a]

[1] Department of Network service, Xi'an Communication Institute, Xi'an 710106, China

[a]51375908@qq.com, [b]813086903@qq.com, [c]583822272@qq.com

Keywords: Authentication, Authentication Protocol, USB Key, VIKEY

Abstract: With the rapid development of computer networks and the popularity of network applications, network security has been people's increasing attention. Network security is an important issue under Network environment, and authentication technology plays a very important role for network application security. Through the study of reason perish analysis and system design, providing efficient and practical solutions for network security applications system. The purpose of this paper is to research on authentication mechanisms and authentication protocols, analysis characteristics and application environments of the network authentication system, which develop the VIKEY online dynamic two-factor password authentication system.

Introduction of Network Authentication Technology

Authentication is a process of confirming a claimed identity. Authentication includes identity authentication and message authentication. The former is used to identify the user's identity, the latter is used to ensure the integrity and anti-repudiation of information communication parties [1]. As openness and complexity of the network connection, authentication environments are more complex. Through a comprehensive analysis of network operation of various factors, authentication can be summed up under the network environment have the following characteristics:

- Authentication means can't be achieved with single state;
- An attacker can eavesdrop authentication information of communication channel , intercept a legitimate user's identity and legal status impostor access network;
- Considering the issues of encryption efficiency and reliability: encryption algorithm needs a large number of complex calculations, the introduction of the authentication mechanism in the network, the network security is strengthened, but the decrease in the efficiency of network communications.
- The user has uncertainty and mobility.

Therefore network authentication must be considered appropriate security means ,which are authentication integrity, non-repudiation of the information, replay attacks and transport security, also be considered to avoid the user's identity forgery, tampering, repudiation, posing, etc. authentication is the first hurdle of network security system, Fig.1 shows logical structure of the safety system.

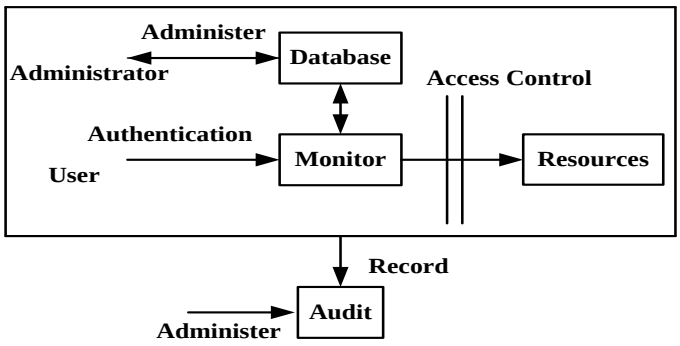

Fig.1. Logical structure of the safety system

Before users access to network system, we access the monitor determines whether users can

access based on user identity and authorization database a resource by identity authentication system. The user should be authorized by the security administrator to configure the database as needed. Audit in accordance with auditing system records the user's request and set behavior, while a non-real-time intrusion detection system in real time whether the intrusion. Access control and audit system relies on the "Information" of the authentication system, which is the identity of the user [2].

The Design Principles of VIKEY Identity Authentication System

VIKEY authentication system is a client / server model of online two-factor. This system can solve the problems of identity authentication access network for all types of enterprises and institutions. VIKEY authentication system consists of an authentication server and authentication client components. Authentication server stores a variety of user authentication information, as well as some local security parameter information. The authentication server will be placed in the actual use environment in an internal network of enterprises and units of the network by a firewall access control protection. Authentication client located in any host to be authenticated user authentication client includes a small USB key, and manipulate small USB key driver. VIKEY authentication system has a lot advantage of concise design, certification principles of advanced equipment and flexible, low-cost, safe and reliable performance [3].

Fig.2 shows the use process of PIN, the figure shows a small USB key, use the PIN to authenticate users. The encryption algorithm in the block diagram is selected by the small USB key manufacturers in accordance with relevant national regulations. Random numbers are generated by small USB key itself. VIKEY authentication system also supports this algorithm to achieve a random number of encryption algorithms.

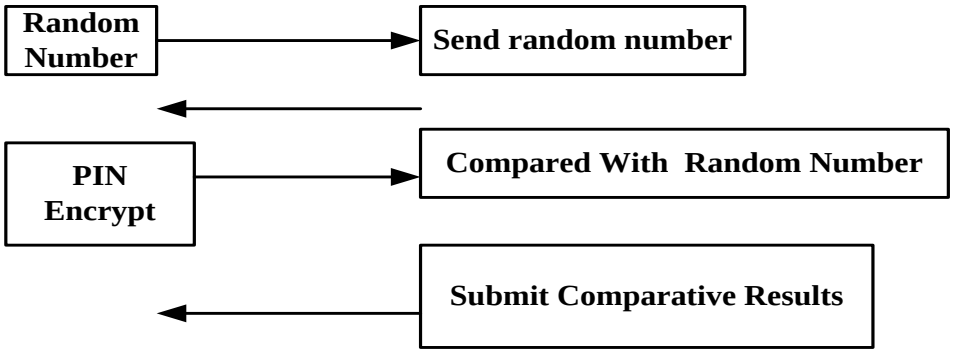

Fig.2. The use process of PIN

Small USB key generates a random number and sends it to the authentication agent, certification agency uses a random number to encrypt PIN and sends the results to a small encryption key; USB reads PIN small key from the key file, and Compare decryption results are consistent with the original random number: If results are consistent, small key to change the security status register through key authentication state. PIN is not stored anywhere in the key file except a small USB key. The small key USB key file is protected by the access control logic, and this ensures security of the small USB key.

The Network Access Certificates of VIKEY Identity Authentication System

After initialization is completed, the user can use the authentication information of small USB key to prove their identity. We need to be done interaction to complete the following three message authentication between the client and the authentication server [4]. Fig.3 shows the message exchanges process, where marked is expressed as:

- Rand: represents a random number Rand that authentication server generates, as a challenge authentication.
- ID, M1, N2 Rand: represents authentication packets that the client sends the server-side.

- N3: represents results authentication information that authentication server sends the user.

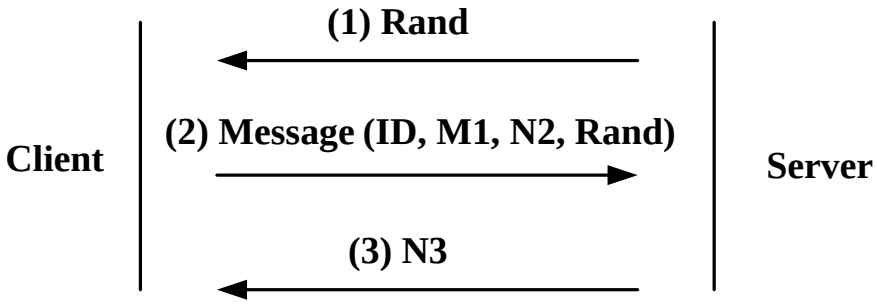

Fig.3. The message exchanges process

Detailed authentication steps of authentication protocol are as follows:

- In order to achieve the client authentication, the server generates a random number Rand, and sends to the clients' certification agency.
- certification agency generates a random number N after receiving Rand, and calculate:N2=H(N1)=H(H(N)), the client removes a small unique ID number from USB key in , the client authenticates information M1 that will be used to identify the next N2, forming the message (ID, MI, N2, Rand)which will be sent to the server .
- After the server receives the message (ID, M1, N2, Rand), use of local private key RSA to decrypt the message, and get the information about message (1D, M1, N2, Rand).
- The server sends the authentication result to the client.
- The client receives the authentication result and updates user information.

Certification process of this client and the authentication server is completed, and user network authentication ends, user can control a transparent proxy server to visit resources on the resource server.

The Design Principles of Authentication server

Authentication server includes two parts: control server and authentication server. The control server controls access and forwards packet for client requests; the authentication server completes the interaction between the client and authentication agent. Authentication Server stores decrypted private packet key RSA and user information, so its safety is very important. In order to better protect authentication server, the security and reliability of the authentication Server operating system is critical. Towards a secure operating system, codes don't not belong to their own operating system must not become a secure operating system, because the system there is any backdoor or flaw that are unknown. The use of open source operating system is a good option, we use cropped Linux. Authentication server application develops with ANSI-C standard. Fig.4 shows the network structure of authentication server.

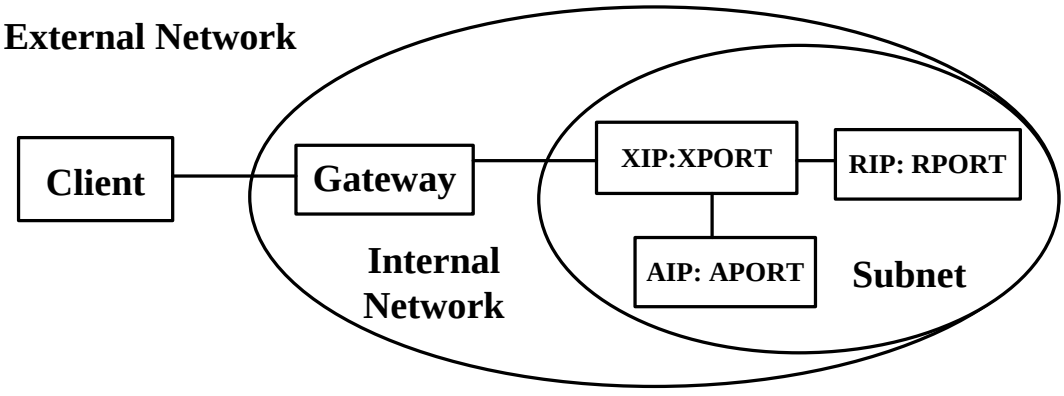

Fig.4. The network structure of authentication server

XIP:XPORT represents network address and port of control server; RIP: RPORT represents the network address and port number of server which provides resources services (such as providing

services for the HTTP port number is 80, FTP port number is 21, TELNET port number is 23) .AIP: APORT represents the network address and port of authentication server. Network divides into three parts: the external network, internal network and protected subnet. The authentication server and the resource server are in protected subnet [5].

The control server controls the request of user. Its functions are as follows: accept the client's request, determine whether the request requires authentication, activate the authentication process and forward satisfactory packets to the destination, which can reduce the pressure on the authentication server authentication and improve efficiency certification .The function modules of control server are as follows: define resources, decide which resource requires authentication can access; receive and forward data packets; activate the certification process; obtain certification results. Through a comprehensive analysis of network operation of various factors, authentication can be summed up under the network environment the following characteristics: Authentication means can't be achieved with single state; An attacker can eavesdrop authentication information of communication channel , intercept a legitimate user's identity and legal status impostor access network; Considering the issues of encryption efficiency and reliability: encryption algorithm needs a large number of complex calculations.

Conclusions

Network authentication technology has been matured, people will slowly realize the urgently needs for identity authentication system with the increasing popularity of the Internet. As authentication technologies get greatly development, so it is an integral part of modern life foundation. The paper has successfully established VIKEY authentication system, and analyzed certification principles and advantages of the s VIKEY system, indicating that it is a concise, secure and efficient scheme. The system is a dynamic two-factor authentication system based on client/server access under network environment, using a dynamic password authentication mechanism to achieve transparent authentication services in a network environment.

References

[1] A Hess and G Sch after Realizing a flexible access control mechanism for active nodes based on active networking technology[C] In IEEE International Conference on Communications (ICC 2004), Paris, France, June, 2004.

[2] YANG WENXIANG, LYNCH, BEVERLY P. On Knowledge Management and the Role of the in the Process of Knowledge Management [J], Chinese Librarianship, 2006, (21): 10-11.

[3] Matthew Connolly．Mobilizing the ’s Web Presence and Services：A Student- Collaboration to Create the’s Mobile Site and iPhone Application[J]．The Reference Librarian, 201 1(52):27-35.

[4] Daniel Chudnov. A Mobile Strategy Web Developers Will Love[J]． Computers in 1ibraries，2010(5): 24 -26.

[5] Matthew Connolly． Mobilizing the Library’s Web Presence and Services：A Student-Library Collaboration to Create the Library’s Mobile Site and iPhone Application[J]． The Reference Librarian, 2011(52):27-35.