한국산학기술학회논문지
Vol. 12, No. 3 pp. 1350-1355, 2011

A Secure Authentication Model Using Two Passwords in Client Server Systems

Jae-Woo Lee[1*]
[1]**Division of Computer Science & Information, Kyungbok College**

클라이언트 서버 시스템 환경하에서 2개의 패스워드를 사용하는 안전한 인증 모델

이재우[1*]
[1]경복대학 컴퓨터정보과

Abstract It is very important issues to protect many system resources using authorized client authentication in distributed client server systems. So it is not enough to prevent unauthorized opponents from attacking our systems that client authentication is performed using only the client's identifier and password. In this paper, we propose a secure authentication database modeling with two authentication keys such as a client authentication key and a server authentication key. The proposed authentication model can be used making high quality of computer security using two authentication keys during transaction processing. The two authentication keys are created by client and server, and are used in every request transaction without user's extra input. Using the proposed authentication keys, we can detect intrusion during authorized client's transaction processing because we can know intrusion immediately through comparing stored authentication keys in client server systems when hackers attack our network or computer systems.

요 약 클라이언트 서버 환경하에서 정당한 클라이언트를 인증하고 시스템 자원들을 보호하는 일은 매우 중요한 이슈 중에 하나이다. 즉, 인가받지 않은 사용자들에 의해 시스템이 보안 공격을 막아내기 위해서는 사용자의 아이디와 패스워드로는 불충분하다. 본 논문에서는 클라이언트 인증키와 서버 인증키를 사용하는 안전한 데이터베이스 인증모델을 제안하였다. 제안모델은 2개의 인증키를 사용하여 보안성을 높이고자 하였는데, 클라이언트와 서버간 데이타베이스 트랜잭션을 처리할 때 서로의 인증 패스워드를 관리하여 사용자의 별도의 입력 작업 없이 사용자 패스워드에 더하여 인증패스워드를 사용함으로써 시스템의 보안성을 높여줄 수 있는 안전한 인증모델을 제시하고자 하였다.

Key Words : Authentication Database, Secure Transaction, Client Server System

1. Introduction

Information technologies enable us to do many automated business processing in anywhere. And we live in information society owing to the brilliant growth of information technologies including the Internet.

In this information society, many information processing requests generally are performed in client server environment that a client requests information to a server systems in networks. So, we can always get various information easily that we need without restriction of our location. That is obviously benefit of using computer systems, but there have been also many risks that many unauthorized users attack our networks and computers for acquiring many kinds of information or destroying our resources. Therefore various security services or policies should be needed against such attacks to protect our networks or computer systems. There are several types of security attacks in networks and computer

*Corresponding Author : :Lee,Jae-Woo(jwlee@kyungbok.ac.kr)
Received December 22, 2010 Revised (1st February 23, 2011, 2nd March 09, 2011) Accepted March 10, 2011

security such as interruption, interception, modification and fabrication [1-3].

In this paper, we propose a secure authentication model with two authentication keys such as a client and server authentication key. The proposed client authentication algorithm can be used making high quality of computer security using two authentication keys during transaction processing. The two authentication keys are created by client and server, and are used in every request transaction without user's extra input. Because they are stored in client's disc and server's authentication database, through exchange and distribution of the authentication keys. Using the proposed authentication keys, we can detect intrusion during authorized client's transaction processing because we can know intrusion immediately through comparing authentication keys stored in client server systems when hackers attack our networks or computer systems.

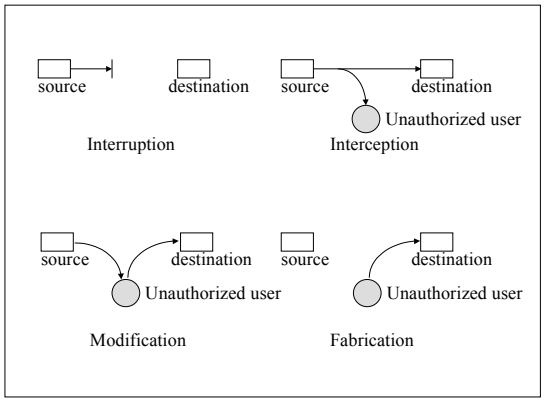
This paper is composed of 4 sections. In section 2, we describe briefly security attacks and various security services especially client authentication. In section 3, we define two authentication keys in client server systems and propose secure transaction processing algorithm. Finally, in conclusion we establish more secure transaction processing and plan future work.

2. Security Services and Authentication

2.1 Security Attack

Various security attacks can occur in distributed client server systems to destroy our computer systems such as interruption, interception, modification and fabrication. Interruption is concerned with availability in client server systems, and interception is an attack on confidentiality. Modification is concerned with integrity and fabrication is an attack on authentication [1,2,4,5].

As shown in Fig. 1, interruption is a security attack that resources of systems or networks are destroyed or become unavailable by interrupting transmission between sender and recipient. Interception is illegal action that an unauthorized opponent gains many information in networks for information stealing. And then, the stolen information will be used in accessing, copying, spreading for others. Modification is a security attack that transmission between sender and recipient is modified by opponent's attacks, such as changing values or altering data file. And those are transmitted modified in networks, and an authorized user misunderstood them. Fabrication is a security attack that unauthorized user access networks or systems for transmitting illegal transaction as authorized client [1,2,6].



[Fig. 1] Security Attacks in Distributed Client Server System

2.2 Security Services for Preventing Attack

Many security services are needed in networks and systems to protect our computer systems against those security attacks as described in section 2.1. Security service is a protection technology and policy that enhances the security of resources of computer systems. Various security services are applied to computer systems such as authentication, access control, confidentiality, integrity and non-repudiation. Among them, we think that authentication is most important security service because we should protect our system resources using authorized client authentication in distributed systems [1-3,5].

Authentication service is to assuring whether a client is authentic or not, by using user's ID, password or internet protocol address, etc. In distributed client server systems, a server system requires a user's ID and password for preventing unauthorized users from using resources of the server. Authentication is focus on fabrication attack [1,7].

As above mentioned, security services are needed for protecting our resources of computer systems. But it is not always secure that we use various security services, because of repeated and specialized attacks by hackers. So, it is very

important that all of messages should be encrypted by protocol of sender and receiver in networks. And then even though hackers gain many kinds of information about our networks or server systems, the stolen information or message is no useful to them [2,6,9,-11].

3. Authentication for Secure Transaction

3.1 Authentication Key Exchange and Distribution

In section 2, we have described security attacks and security services. Generally a user's ID and password are used for client authentication, and those are not enough to secure the user's transaction processing. In this paper, we use more complex authentication keys for secure transaction processing in client server systems, client's authentication key and server's authentication key. For exchange and distribution of authentication keys, when exchange session is opened for a client's transaction processing in client server systems, the client creates an authentication key for communicating with a server system using a random function, randomized(). And then the client requests a transaction using the user's ID, password and client authentication key. When the server receives the client's requesting, the server checks the client's ID and password with client authentication profile. And the server saves the client's authentication key in server system's database. After checking those client's messages, the server creates a server authentication key using the function, randomized(), for communicating with the client. The our proposed authentication key exchange and distribution session procedure is summarized as follows:

Step 1 : Input a client's ID and password for log-in

Step 2 : Create client's authentication key, Cak using a random function, Randomize()

Step 3 : Send the client's ID, password and Cak encrypted to server

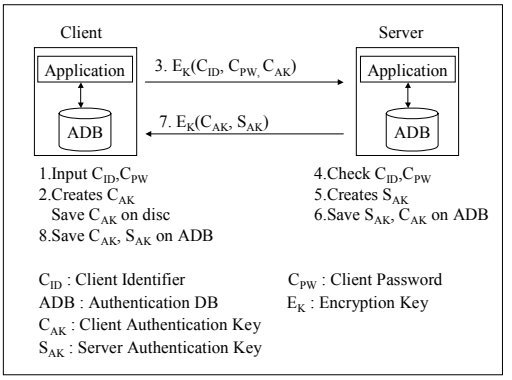
And then the server receives the client's ID, password and client authentication key, Cak

Step 4 : Checks the client's ID, password

Step 5 : Create server's authentication key, Sak using a random function, Randomize()

Step 6 : Save the Sak and Cak to server's authentication database, ADB

Step 7 : Send the server's Sak and Cak encrypted to the client



[Fig. 2] Authentication Key Exchange and Distribution

And the client receives the server's authentication key, Sak

Step 8 : Checks the received Cak with saved Cak

Step 9 : Save the server's Sak to client's authentication database, ADB

As shown in Fig. 2, before a client requests transaction processing to an application servers, the client creates it's own authentication key for exchange and distribution. And the client sends message to server system with the client's ID, password adding to the client authentication key. Our proposed authentication algorithm uses two authentication keys for making high quality of computer security besides client's password, the one is client's authentication key and the other is server's authentication key. Authentication key is created by a random function, randomize(). And the client and application server store the session password in it's own local disc or database. After the key exchange and distribution session, the client gains server authentication key for secure transaction processing.

For more secure transaction, authentication keys are exchanged and distributed periodically. It is more secure that the authentication key are changed frequently.

3.2 Design of Authentication Database

The above two authentication databases, the client's ADB(Authentication Database) and the server's ADB, are

used for secure client authentication. The database has authentication keys and authentication passwords. In our proposed authentication model, the authentication password of the server's ADB becomes the client's authentication key. Also, the authentication password of the client's ADB becomes the server's authentication key. Using the authentication keys we can select authentication password for secure transaction processing.

The authentication database table has two fields, client's key(Cak_i) and server's key(Sak_i). As shown in table 1 the layout of authentication table, Cak_1, Cak_2, ..Cak_i, ..,Cak_n are set of client's authentication key. And server's authentication keys are defined as Sak_1, Sak_2, ..Sak_i, ..,Sak_n. For selecting the authentication keys, the client and server system create a random number as authentication key using a function such as randomize(), and store to authentication database.

[Table 1] Authentication Database in Client ADB

Authentication Key	Authentication Password
Cak1	*Sak1*
Cak2	*Sak2*
...	...
Caki	*Saki*
...	...
Cakn	*Sakn*

[Table 2] Authentication Database in Server ADB

Authentication Key	Authentication Password
Sak1	*Cak1*
Sak2	*Cak2*
...	...
Saki	*Caki*
...	...
Sakn	*Cakn*

3.3 Secure Transaction Processing Using the ADB

The client requests information processing using the authentication keys, client's authentication key and the server's authentication key. For secure transaction processing the client uses it's ID and password with the two authentication keys. After the client requests transaction processing to the server, the server systems always send an authentication key for next transaction processing. That is, the client uses the former authentication key for getting authentication password from ADB. The our secure transaction processing is summarized as follows:

Step 1 : Select the client's authentication password, Sak, using the former client's authentication key, Cak from ADB

Step 2 : Send request messages to server system with the client's ID, password and Sak

And then the server receives the client's ID, password and client authentication password, Sak , server authentication key

Step 3 : Checks the client's ID, password as the authentication profile

Step 4 : Check the client's authentication password, Sak,, from selecting ADB

Step 5 : Select an authentication key using random number from ADB, the server's Sak and Cak

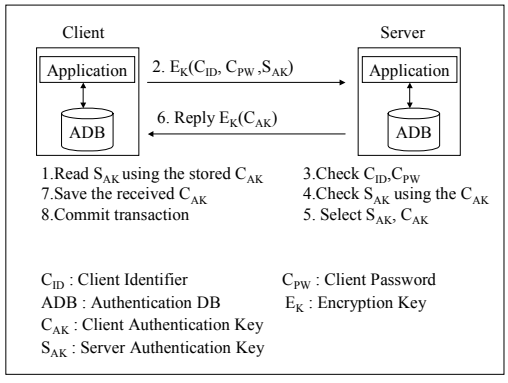
Step 6 : Send reply messages with the server's Cak to the client for next transaction processing

And the client receives the server's authentication key, Cak

Step 7 : Save the received Cak for next transaction processing

Step 8 : Commit transaction

As shown in Fig. 3, a client uses a ID and three passwords for secure transaction processing, ID, password, client authentication key and server authentication key.



[Fig. 3] Secure Transaction Processing

3.4 Purpose of the two Authentication Keys

For more secure transaction processing, it is not enough to use only the client's identifier and password. Our proposed authentication model use more complex password system without extra input operation during the user's transaction processing. Using the two authentication keys, we can detect intrusion during unauthorized client's transaction processing. Because we can know intrusion immediately through comparing the secret two authentication keys stored in client server systems when hackers attack our networks or computer systems. As shown in Fig. 3, a client uses three passwords, Cpw, Cak and Sak, for secure transaction processing. If an unauthorized user accesses our server systems, the user should know the two authentication keys besides ID and password.

4. Conclusion

In distributed client server systems, it is one of the most important problems that we should protect many resources of systems using authorized client authentication. But it is not easy to identify whether a client is authorized or not using only ID and password. There are many security attacks created by many opponents in networks or computer systems. In this paper, we have explained various security attacks and security services. And we have described client authentication security services for preventing the security attack. For secure transaction processing we propose a secure authentication procedure with two authentication keys, the client's authentication key and the server's authentication key. The proposed client authentication algorithm can be used making high quality of computer security using two authentication keys during transaction processing. The two authentication keys are created by client and server, and are used in every request transaction without user's extra input because of storing to client's disc and server database when a session is opened first. And using the authentication keys, we can detect intrusion during authorized client's transaction processing. Because we can know intrusion immediately comparing the two secret authentication keys stored in client server systems when hackers attack our networks or computer systems.

In the future, we will verify this authentication model by experimenting various cases of security attacks. And further research to protect computer system resources from various security attacks should be done and intrusion detection also will be considered.

References

[1] William Stallings, Network Security Essentials : Application and Standards, Prentice Hall, 1999.

[2] William Stallings, Cryptography and Network Security : Principles and Practice, Prentice Hall, 1999.

[3] Charlie Kaufman, Radia Perlman and Mike Speciner, *Network Security : Private Communication in a Public World*, Prentice Hall, 1995.

[4] Ravi Sandhu and Pierangela Samarati, "Authentication, Access Control, and Audit," *ACM Computing Surveys*, 28(1), pp.241-243, March 1996.

[5] B.C. Neuman and Theodore Ts'o. Kerberos, "An Authentication Service for Computer Networks," *IEEE Communications*, 32(9), pp.33-38, September 1994.

[6] Shai Halevi and Hugo Krawczyk, "Public-key Cryptography and Password Protocols," *ACM Transactions on Information and System Security*, 2(3), pp.230-268, August 1999.

[7] James Giles, Reiner Sailer, Dinesh Verma, and Suresh Chari, "Authentication for Distributed Web Caches," *Lecture Notes in Computer Science*, Vol. 2502, Springer-Verlag, pp.126-145, 2002.

[8] Ferdinand J. Dafelmair, "Survivability Strategy for a Security Critical Process," *Lecture Notes in Computer Science*, Vol. 2434, Springer-Verlag, pp.61-69, 2002.

[9] Jonathan Katz, Rafail Ostrovsky, and Moti Yung, "Forward Secrecy in Password-Only Key Exchange Protocols," *Lecture Notes in Computer Science*, Vol. 2576, Springer-Verlag, pp.29-44, 2002.

[10] Yasunori Ishihara, Shuichiro Ako, and Toru Fujiwara, "Security against Inference Attacks on Negative Information in Object-Oriented Databases," *Lecture Notes in Computer Science*, Vol. 2513, Springer-Verlag, pp.49-60, 2002.

[11] Donk-Kwan Kim, Seung-Soo Shin, "Three-Factor authentication system based on one time password," Proceedings of the KAIS Fall conference, The Korea Academia-Industrial cooperation Society, pp.25-28, 2008.

Jae-Woo Lee [Regular member]

- Aug. 2004 : Korea University, Computer Science and Engineering, PhD
- Jan. 1987 ~ Feb. 1999 : Ssangyong Information & Communication Corp., Engineer
- Mar. 1999 ~ current : Kyungbok College, Dept. of Computer Science, Professor

<Research Interests>
Project Management, Distributed Database System