Journal of Theoretical and Applied Information Technology
15 May 2012. Vol. 39 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PASSWORD BASED TWO SERVER AUTHENTICATION SYSTEM

[1]VIGNESH KUMAR K, [2]ANGULAKSHMI T, [3]MANIVANNAN D, [4]SEETHALAKSHMI R, [5]SWAMINATHAN P

[1]M.Tech, SOC, SASTRA University, Thanjavur, Tamil Nadu, India

[2]M.Tech, SEEE, SASTRA University, Thanjavur, Tamil Nadu, India

[3]Senior Associate Prof., SOC, SASTRA University, Thanjavur, Tamil Nadu, India

[4]Professor, SOC, SASTRA University, Thanjavur, Tamil Nadu, India

[5]Dean, SOC, SASTRA University, Thanjavur, Tamil Nadu, India

E-mail: [1]k_vignesh_kumar@yahoo.co.in, [2]t.angulakshmi@gmail.com

ABSTRACT

User Authentication in computer systems is an important cornerstone in today's computer era. The concept of a user id and password is one of the easiest ways for authentication. It is not only the easiest way, but also cost effective and highly efficient. Today, we can see the password cracking and hacking in everywhere. At present we are using the single server system for this sort of password based authentication. Traditional protocols for password-based authentication assume a single server which stores all the information (e.g., the password) necessary to authenticate a user. When an attacker obtains the information stored on the server, he can obtain all the passwords which were stored in the server via launching an off-line dictionary attack. To address this issue, a number of schemes have been proposed in which a user's password information is shared among multiple servers, and these servers cooperate in a threshold manner the user wants to authenticate. In this paper, a new efficient two-server password-only based authentication is proposed. In addition, the system is secure against offline dictionary attacks mounted by either of the two servers.

Keywords: *Password Authentication, Two Server Concept, Offline and Online Dictionary Attack*

1. INTRODUCTION

Password based user authentication systems are low cost and easy to use. A user only needs to memorize a short password and can be authenticated anywhere, anytime, regardless of the types of access devices he/she employs. Password based authentication system is still gaining popularity even in the presence of several alternative strong authentication approaches, e.g., two factor authentication and biometrics. The reason for this is, it does not require any additional devices or tokens like in biometrics and two factor authentication systems respectively. In two factor authentication system the loss or theft of the token not only risks disclosing the secrets inside but also disables the authentication functionality. The best example of this two factor authentication system is our current ATM system, in which the ATM card is one factor and the PIN number is another factor. So if the ATM card is lost means, the authentication functionality will be disabled. As far as biometrics is concerned, the security is very effective and efficient in this system but the only concerns are the cost of hardware and software complexity.

Traditional protocols for password-based authentication assume a single server which stores all the information (e.g., the password) necessary to authenticate a user. Password based authentication is the most commonly used entity authentication technique, due to the fact that no secure storage is required, and a user only needs to memorize his password and then can authenticate anywhere, anytime. Most of the existing password based authentication schemes assume the single-server model where a single server exists in a system. The major drawback of the single server model is that the server may result in a single point of failure, in the sense that compromise of the server reveals all user passwords held by the server. The server is compromised by means of an offline dictionary attack. In recent years, much attention has focused on designing password based authenticated key exchange protocols which can resist any kind of intruder's attack. To solve this problem, a new kind of authentication structure called the multiple server authentication was proposed. In such schemes, the capability of verifying a password is split between two or more servers, and more than a certain threshold number of servers need to collude to recover the password. Till now, few multiple server schemes were proposed. In these multiple server authentication settings, the two-server authentication protocol [5] [6] [7] is the simplest and the most acceptable to users. Six two server protocols have been proposed [2] since 2003.

2. BACKGROUND AND RELATED WORKS

In recent years, much attention has focused on designing password based authenticated key exchange protocols which can resist offline dictionary attack by an intruder. To solve this problem, a new kind of authentication structure called the multiple server authentication was proposed. In such schemes, the capability of verifying a password is split between two or more servers, thus securing the system from intruders. In these multiple server authentication system, the two-server authentication protocol is the simplest and the most acceptable to users. Some of the authentication systems based on two server concept are discussed below.

Mukesh et al.'s [4] proposed a robust finger print based two-server authentication and key exchange system, this is the first biometric two-server authentication scheme. In this scheme, the user's password is replaced by the random string generated by fingerprint template, the user need not memorize it. In Brainard et al.'s [2] two-server password system in which one server (called Blue Server or Service Server, SS for short) exposes itself to users and the other (called Red Server or Control Server, CS for short) is hidden from the public. While this two-server setting is very interesting, it is not a password-only system, both servers need to have public keys to protect the communication channel from users to servers. This setting makes it difficult to fully enjoy the benefits of a password system. Subsequently, Katz et al. Proposed a two-server password-only authenticated key exchange, the authors claimed that this is the first provably-secure two-server protocol for the important password-only setting (in which the user need remember only a password, and not the server's public keys), and is the first two-server protocol (in any setting) with a proof of security in the standard model. Recently, a practical two-server architecture was proposed by Yang et al. [3] and an efficient password-only two-server authenticated key exchange system, this scheme is a password-only variant of the one introduced by Brainard et al.'s. None of the existing two-server password based authentication schemes enables a user to use the same password over multiple service servers, which is deemed an important feature of the two-server model. Yanjiang Yang proposed a new scheme [1], enabling this prominent functionality.

3. TWO SERVER SYSTEM

The concept of a user id and password is a cost effective and efficient method. Identifying and allowing the authorized user to access the resources is one of the key aspects of authentication system. In today's computer era, there are so many vulnerabilities occurred based on internet. So, we have to design the application with high security. If there are any flaws, then it will be easily broken and an intruder can easily intrude. A single server system is a system in which the password will be stored in a single server as shown in Fig. 1. While considering the authentication system based on a single server, there are some drawbacks. The single server system is vulnerable to all sorts of attacks from intruders. The intruder can hack the system by trying all possible keys till the system gets compromised is the most successful in the single server system and exhaustive search also can be successful as shown in Fig. 2.

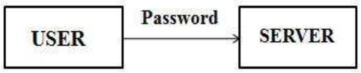


Figure.1 Block Diagram of a Single Server System

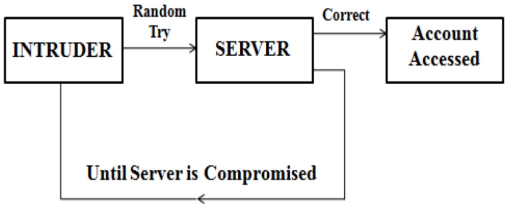


Figure.2 Example of single server system hacked by Intruder

So, it's necessary to introduce the concept of two server authentication system. In the case of a single server system, the hacker can easily compromise. But in the two server system it cannot be easily compromised by the attacker. The purpose of this paper is to present the two server authentication system which does not use any sort of cryptographic techniques such as encryption, hashing. A two server system is a system in which the system consists of two servers and the password will be split into two halves and stored on both the servers. So in this system the intruder has an additional burden of compromising both the servers simultaneously in order to take over or hack the system.

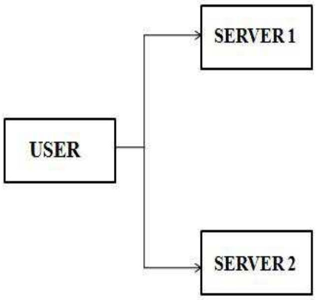


Figure.3 Block Diagram of Two Server System

4. PASSWORD BASED TWO SERVER AUTHENTICATION SYSTEM

4.1 Existing Works

There are so many papers presented about this two server authentication system. The proposed systems are Biometric based fingerprint authentication, key exchange based authentication and password only with no key exchange protocol type etc. Zung Yang who illustrated the concept of a "Practical Password Based Authentication System For Key Exchange", the only problem with that concept is the ease of understanding. Even though that is effective, that is not an easy job for a novice user to understand. Because he used so many complex functions by means of encryption and computation, which are difficult to understand as well to implement also. We proposed a two server password only based authentication system which is effective as well as easier to implement.

4.2 Proposed Work

Here we recommend to use the two servers namely front end server and back end server. There is no special preference for any server. Because in Yang's project, they used one as SS (Service Server) and another one as CS (Control Server). That is not in this case. There are some series of steps.

4.2.1 Registration phase

In the registration phase, the user has to enter the password and another one random number which should be at least two less than the length of the password.

(i.e.) 1<R<L-2,
R - Random Integer
L - Length of the Password

For example the user registered with the password," 1234567". In our system, the user should also enter a random number. Here let it be "3". It could not be an integer greater than 5 in this case. Upto this, the registration phase is over. Users are not allowed to set null password as well as zero as the random number.

4.2.2 Authentication phase

In this phase the entered password is divided into two shares according to that random number which was entered during the registration phase. In our example, the password 'P' is divided into 'P1' and 'P2'. Here the share of P1 is" 123" and P2 is" 4567" as in Fig.4. So, the share of P1 is authenticated by the Front end server and the P2 is authenticated by the back end server. In case of a legitimate user, if he enters the correct password, he is authenticated by the two servers. Next, we will check for an intruder.

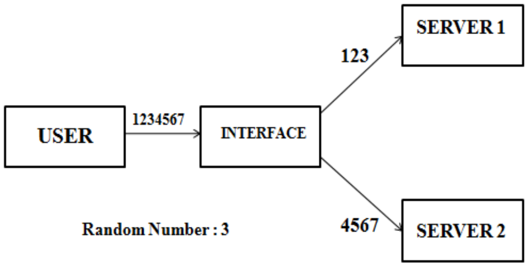


Figure.4 Block diagram of a two server authentication with an example

4.3 Security Analysis

4.3.1 Brute force attacks

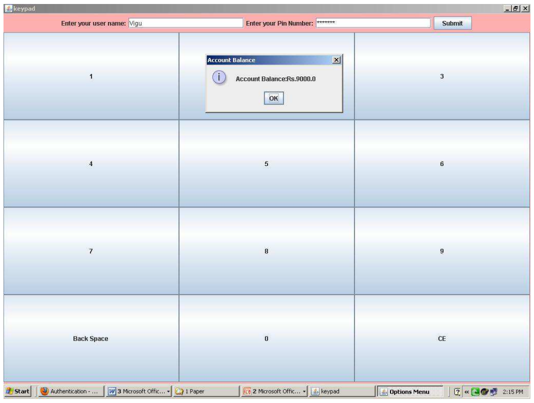
In case of any Brute force attacks, it may be either Dictionary attack or exhaustive search, this method works. For example consider a scenario, if an intruder wants to crack the password, then he is going to try all the possibilities starting from integer '1'. Here the valid password is "1234567" and the random number is" 3". All the single and two digit tries are easily rejected by the system since the random number is 3. The front-end server is compromised after he entered 123.But the backend server is not compromised still and his next try will be '124'. But in this case the front end server is decompromised and the user is blocked. Because, once the front end server is compromised, again it should not be decompromised. In this case we can easily identify the intruder due to the rollback of front end server from compromised to decompromised state. Hence our two server system is effective against exhaustive search or brute force attacks.

4.3.1 Strengthening Condition

Once the front end server is compromised in first attempt, the backend should be compromised within five attempts. Probably only the legitimate user can compromise the server in first attempt. Incase due to some careless, he may enter the wrong password for backend server. However the five attempts are too much for that legitimate user. The next condition is once the front end server is compromised it should not be decompromised again. So from the above mentioned strengthening conditions it is clear that the proposed system has good security against hacking

5. APPLICATION DEVELOPMENT AND SIMULATION DETAILS

In this work the application development and simulation model are done using Netbean IDE 7.1 and Microsoft Access. A simple banking application with authentication system and database management has been developed. Netbean IDE is used for compiling the Java code and developing the front-end GUI window. Screenshot of the GUI window is shown in Fig.5. Microsoft Access is database management tools, the bank account details, password, random numbers etc. of the banking application are stored in it and it is the back-end of the application. Screenshot of the back end is shown in Fig.6. The front-end and the back-end are interfaced using an ODBC connection. The ODBC (Open Database Connectivity) is a standard C application programming interface for accessing Database Management Systems. ODBC accomplishes DBMS independence by using an ODBC driver as a translation layer between the front-end GUI window and the back-end Microsoft Access. The application uses ODBC functions through an ODBC driver manager with which it is linked, and the driver passes the query to the DBMS.

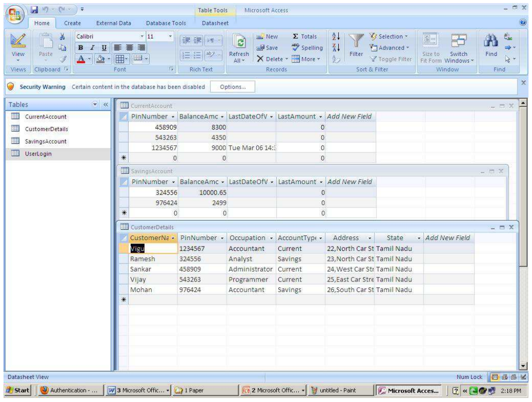


Enter your user name: Vigu
Enter your Pin Number: *******

Account Balance

Account Balance:Rs.9000.0

Figure. 5 Front End of the banking application displaying the account balance of a user



Security Warning Certain content in the database has been disabled

CurrentAccount

PinNumber	BalanceAmc	LastDateOfV	LastAmount	Add New Field
458909	8300		0	
543263	4350		0	
1234567	9000	Tue Mar 06 14::	0	
0	0		0	

SavingsAccount

PinNumber	BalanceAmc	LastDateOfV	LastAmount	Add New Field
324556	10000.65		0	
976424	2499		0	
0	0		0	

CustomerDetails

CustomerNa	PinNumber	Occupation	AccountTyp	Address	State	Add New Field
Vigu	1234567	Accountant	Current	22,North Car St	Tamil Nadu	
Ramesh	324556	Analyst	Savings	23,North Car St	Tamil Nadu	
Sankar	458909	Administrator	Current	24,West Car Str	Tamil Nadu	
Vijay	543263	Programmer	Current	25,East Car Stre	Tamil Nadu	
Mohan	976424	Accountant	Savings	26,South Car St	Tamil Nadu	

Fig. 6 Back end of the banking application displaying the database details of the bank customers

6. CONCLUSION

In this paper, we proposed a password-based authentication that is built upon a novel two-server model. Compared with previous solutions, our system possesses many advantages, such as the elimination of key exchange system, avoidance of any sort of cryptographic techniques such as encryption, hashing and high efficiency with provable security. In contrast to existing multi-server password systems, our system has great potential for practical applications. It can be directly applied to fortify existing standard single-server password applications, e.g., FTP and Web applications. By employing two servers, the system is able to offer considerably more protection of sensitive user data than any single-server approach could permit. The main advantages of our system are it is not resilient to any brute force attacks, two servers cannot be easily compromised by an intruder and easy to implement as no complex cryptographic approaches are followed.

Establishing an appropriate formal model for two-server password based authentication, and in turn proving the security of our proposed scheme within the model are among our future work. Another future work is to study the performance of our scheme by implementing and experimenting the scheme in a real-world application scenario.

REFERENCES:

[1] Yanjiang Yang, "Enabling Use of Single Password over Multiple Servers in Two-Server Model ", Computer and Information Technology (CIT), 2010 IEEE 10th International Conference.

[2] B. Kaliski and M. Szydlo J. Brainard, A. Juels. Nightingale: "A new two-server approach for authentication with short secrets", in Proceedings of the 12th USENIX Workshop on Security, pages 1-2. IEEE Computer Society, 2003.

[3] Dexin Yang , Bo Yang "A Novel Two-Server Password Authentication Scheme with Provable Security", IEEE Transaction 2010 10th IEEE International Conference on Computer and Information Technology (CIT 2010).

[4] Mukesh, R.Damodaram, A.Subbiah Bharathi,V. "A robust fingerprint based two-server authentication and key exchange system", 3rd International Conference on Communication Systems Software and Middleware and Workshops, 2008 Bangalore, pp. 167-174.

[5] Xun Yi, "Security Analysis of Yang et al.'s Practical Password-Based Two-Server Authentication and Key Exchange System", 2011 4th International Conference.Network and System Security (NSS).

[6] Jiang Huiping. "Strong password authentication protocols", 2010 4th International Conference Distance Learning and Education (ICDLE).

[7] Shuo Zhai, "Design and implementation of password-based identity authentication system", 2010 International Conference Computer Application and System Modeling (ICCASM).