American Journal of Applied Sciences 5 (12): 1630-1634, 2008
ISSN 1546-9239
© 2008 Science Publications

A Non-Exchanged Password Scheme for Password-Based Authentication in Client-Server Systems

[1]Shakir M. Hussain and [2]Hussein Al-Bahadili
[1]Faculty of IT, Applied Science University, P.O. Box 22, Amman 11931, Jordan
[2]Faculty of Information Systems and Technology,
Arab Academy for Banking and Financial Sciences, P.O. Box 13190, Amman 11942, Jordan

Abstract: The password-based authentication is widely used in client-server systems. This research presents a non-exchanged password scheme for password-based authentication. This scheme constructs a Digital Signature (DS) that is derived from the user password. The digital signature is then exchanged instead of the password itself for the purpose of authentication. Therefore, we refer to it as a Password-Based Digital Signature (PBDS) scheme. It consists of three phases, in the first phase a password-based Permutation (P) is computed using the Key-Based Random Permutation (KBRP) method. The second phase utilizes P to derive a Key (K) using the Password-Based Key Derivation (PBKD) algorithm. The third phase uses P and K to generate the exchanged DS. The scheme has a number of features that shows its advantages over other password authentication approaches.

Keywords: Password-based authentication, KBRP method, PBKD algorithm, key derivation

INTRODUCTION

The client-server distributed system architecture consists of a server, which has a record of the username-password database and a number of clients willing to exchange information with the server. A server is always protected by not exchanging information with a client unless it is assured of its registration (i.e., being authorized or authenticated). A password-based authentication (password authentication) approach is widely used to ensure high level of security in such systems. In conventional password authentication approach, the client usually exchanges either its password or a variation of it (e.g., encrypted form) with the server. By receiving the password, the server compares the received password with the one stored in the username-password database, to grant or deny the client access to the system.

In this case, client has no chance of being authenticated or allowed to access the system unless it exchanges its password or a variation of it across the network. This phase in the authentication process may expose the client password to be composed by an adversary or a man-in-the-middle. There are many methods have been proposed to secure the exchanged password during this phase of the authentication process, such as:

- Encrypted key exchange (EKE) algorithm[1]
- Authenticated key exchange secure against dictionary attacks (AKE)[2]
- Threshold password-authenticated key exchange[3]
- Password-based authentication and key distribution protocols with perfect forward secrecy[4]
- Simple Password Exponential Key Exchange (SPEKE)[5]
- The secret public key methods[6]
- Open Key Exchange (OKE)[7]

They all have their own drawbacks. In this work a new algorithm is proposed to be used for password-based authentication in client-server applications, without the exchange of the actual password or any variation of it. Instead, a Password-Based Digital Signature (PBDS) is derived and transmitted over the network. This signature is derived using an efficient highly secure scheme that utilizes the Key Based Random Permutation (KBRP) method[8] and the Password-Based Key Derivation (PBKD) method[9]. The main features of the new scheme include:

- It does not need to exchange the password or any close variation of it (e.g., encrypted form)
- The length of the derived signature is flexible and it is greater than the actual password length

Corresponding Author: Shakir M. Hussain, Faculty of Information Technology, Applied Science University, P.O. Box 22, Amman, 11931, Jordan Tel: +962-6-5609999 ext: 1266

- Any image of the password can not be extracted from the digital signature
- The possible number of digital signatures is equal to half of the key length; even though, if the intruder traps all the exchange signatures he can not construct the user password
- The entropy of the derived signature has no effect on its security strength

In order to demonstrate the strength of this new scheme, a number of scenarios are simulated and the exchanged digital signatures are computed for different passwords.

LITERATURE REVIEW

In client-server system, authentication is a way that can ensure the client has authorization to access the server. There are many factors that are used to verify a user's identity for security purposes. These factors are categorized as: something you know such as a password or PIN, something you have such as a credit card and something you are such as a fingerprint or other biometric[10,11].

The password authentication is widely used in many systems and applications each time the password needs to be verified. In cryptography, a password-authenticated key agreement method is an interactive method to establish cryptographic keys based on one or more party's knowledge of a password. Password-authenticated key agreement encompasses methods such as: Balanced password-authenticated key exchange, Augmented password-authenticated key exchange, Password-authenticated key retrieval, Multi-server methods and Multi-party methods. In the most stringent password-only security models, there is no requirement for the user of the method to remember any secret or public data other than the password[11].

A clear-text password exchanged in password-based authentication is not a secure form of authentication, because the user's passwords are passed over the link in unencrypted form. For this reason, a number of techniques have been developed to securely exchange the password over the network. In what follows we will refer to some of them.

A Password Authentication Protocol (PAP) uses a two-way handshake to perform authentication. Once the communication link is established, using the Link Control Protocol (LCP), the client sends a username and password to the server. The server uses its own authentication scheme and user database to authenticate the user and if the authentication is successful, the server sends an acknowledgment to the client and a user gets access to the system[12].

Another password authentication technique is the challenge-response protocol which is a more secure form of password authentication. In this technique, the server picks a random number (the challenge) and sends it to the user. Then the user computes a secret function on this challenge with the help of the password (the response). Therefore, in this technique the password is never transmitted in clear. Despite this important fact, challenge-response protocols can not be penetrated by eavesdroppers. If the challenge and response from a successful authentication are captured, eavesdroppers can perform a dictionary attack and get the password. Besides, challenge-response protocols are also plaintext-equivalent. So they can be easily defeated by an intruder who captures the password file, as well as one who can eavesdrop[13].

One variant of the challenge-response mechanism is the one-time password, in which the user uses a different password for every authentication. If these one-time passwords are derived from a human password, it still vulnerable to dictionary attacks. This approach is also vulnerable to several attacks ranging from stolen passwords to man-in-the-middle attacks[12,14].

A stronger authentication protocol known as Encrypted Key Exchange (EKE) was presented by Bellovin and Merritt. EKE uses a combination of symmetric (secret-key) and asymmetric (public-key) cryptography. In the most general form of EKE, the two communicating parties encrypt ephemeral public keys with a symmetric cipher, using their shared secret password as a key. EKE protects from off-line dictionary attacks by giving a passive attacker insufficient information to verify a guessed password[15].

EKE represented the strongest level of password-based authentication protocols available. EKE's greatest failing is that it still suffers from a plaintext-equivalence, requiring that both user and host share the same secret password, while a verifier-based mechanism requires only a verifier to be stored will be called. A system that uses plaintext-equivalent authentication becomes instantly compromised once the password database is revealed[13,14].

Asymmetric Key Exchange (AKE) is another framework that also used in password authentication. AKE is a theoretical concept that describes the outline of a family of key-exchange protocols[16]. AKE does not encrypt any of the protocol flows. Instead, it uses predefined mathematical relationships to combine exchanged ephemeral values with established password parameters.

AKE describes a swapped secret approach, in which each party computes a secret and then applies a one-way function to that secret to generate a verifier, which is handed to the other party. Designing a verifier-based protocol is considerably more difficult than designing a conventional shared-secret authentication protocol. This is one of the reasons why such protocols are relatively rare in practice[12].

A secure remote password (SRP) protocol is one possible interpretation of AKE that is believed to be simple, fast and highly secure. SRP is a secure password-based authentication and key exchange protocol designed to resist both passive and active attack. It solves the problem of authenticating clients to servers securely when the user of the client software must memorize a small secret (like a password) and no other secret information[12].

Password Authenticated Key Exchange (PAKE) is where two or more parties, based only on their knowledge of a password, establish a cryptographic key using an exchange of messages, such that an unauthorized party (one who controls the communication channel but does not possess the password) cannot participate in the method and is constrained as much as possible from guessing the password.

There are two major types of PAKE protocols: balanced and augmented PAKEs[17,18]. The scenario where both parties are having the password is the balanced type. An augmented PAKE has the same goals as a balanced one, but in this type, one party (commonly referred to as the client) has the password, while the other party (commonly referred to as the server) does not have the password. Instead, the server only has a password verification data derived using a one-way function of the password. This type of PAKEs is worthful for practical purposes because even an adversary obtains a password verification data from the server, the adversary still needs to launch offline dictionary attacks for getting the corresponding password.

THE PROPOSED PASSWORD AUTHENTICATION SCHEME

The evident weaknesses and complications encountered in the password-based authentication methods have contributed to create the need of stronger solutions and new protocols. This work presents a detailed description of the proposed Password-Based Digital Signature (PBDS) authentication scheme. It makes use of the KBRP method[8] and the PBKD algorithm[9].

```
P:      Array holds permutation with values 1 to N
K:      Array holds derived with key of size N
S:      Array holds digital signature of size n = N/2
SEED: A random number in the range 1 to N
j = SEED
for(i = 1 to n)
    S[i] = K[P[j]]
    j = P[j];
    if(j = = P[j])
        j = P[j]%N+1
```

Fig. 1: The PBDS scheme

In order to explain this new scheme, it is useful to provide a brief description of the KBRP and PBKD. KBRP is used to generate a pseudo randomized Permutation (P) of a given size from a certain password. PBKD is used to derive a strong Key (K) of the same permutation size using P.

The proposed scheme consists of three phases. These are: (i) generate P, (ii) derive K and (iii) derive a unique digital signature (DS) for password authentication. Phase one consists of processes which are similar to those in the KBRP method. Phase two mainly contains the key derivation process as introduced in PBKD.

The third phase of the process uses the outcomes of the two previous phases to derive DS which is going to be exchanged between the two communicating parties for authentication. The size of DS is half-size of K. The elements of DS are randomly selected from K according to P. First, a preset number (seed) that lies between 1 and P size (K size), is selected. This seed refers to a position in P. The content of this position, then, refers to another position on K. The content of this position is selected as a first element for DS. At the same time, the content of this position is used to indicate a position on P; its content will be used to locate a position on K from which we obtain the next element of DS. This process will continue until DS is completely assembled. Figure 1 outlines the processes of the new proposed scheme.

It is clear from the above discussion that the elements of DS are randomly selected from K without using a random number generator. Instead, P is used to indicate the position of the selected elements.

AUTHENTICATION MECHANISM

In client-server distributed system architecture, authentication is one of the main issues that need to be carefully considered. Normally, it is done through a

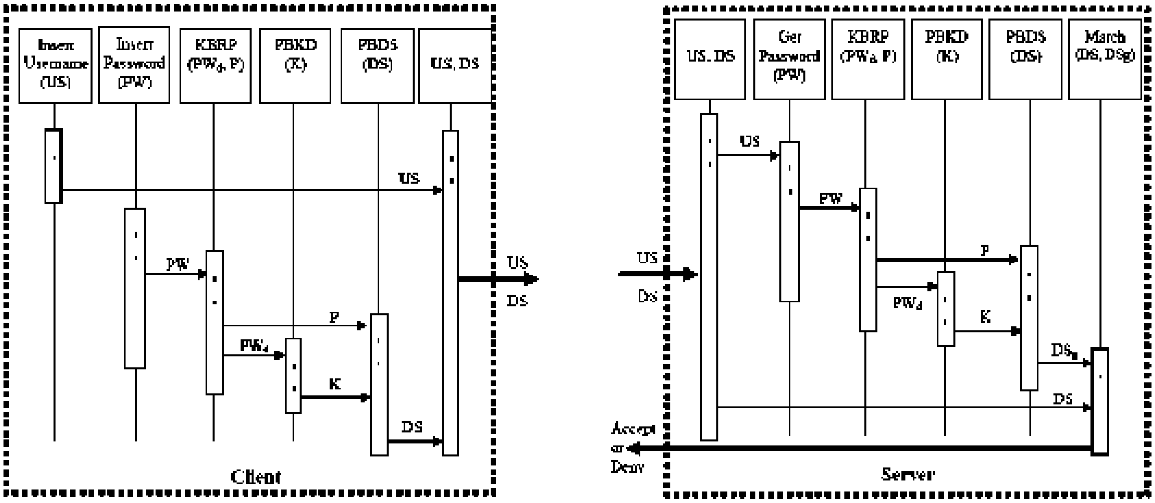

Fig. 2: The authentication mechanism of the PBDS scheme

login session, in which the client exchanges a username and password combination in one or more communication sessions, in plain or encrypted forms. The server, in turns, compares the received combination of the client username and password with its database. If they match then the client gains access to the system resources; otherwise, it is denied. However, many techniques have been proposed to ensure secure authentication communication session. But still these techniques can be overcame which may reveal the client password to the adversary.

In this new scheme the client does not exchange the password, instead, in addition to the username; it exchanges an associated digital signature that is derived by using the PBDS algorithm, in a single or dual communication session. Upon receiving the combination of the user name and the digital signature, the server retrieves the client password from its database and generates a digital signature using the PBDS algorithm. If the received and the generated digital signatures match then the client gains access to the system resources; otherwise, it is denied. Figure 2 shows the new scheme authentication mechanism.

Table 1: Constructed digital signatures using different passwords. (P: Permutation K: Derived Key DS: Digital Signature)

		Digital Signature (DS)			
Password	Seed	Binary		Hexadecimal	
John		**P:**	25 23 22 10 16 15 3 13 1 18 30 21 19 14 9 8 28 5 31 29 2 11 17 7 12 26 4 24 27 32 20 6		
		K:	00111000011001011000100001 11011		
	7	**DS**	1001101101001000	9B	48
	12	**DS**	0100000100110110	41	36
	20	**DS**	1111001010111111	F2	FB
Shakir		**P:**	27 8 12 20 32 19 4 7 25 6 13 21 29 1 28 16 26 18 24 5 23 3 11 30 15 22 14 31 2 10 17 9		
		K:	0111101001000011101100010 1001100		
	7	**DS**	1000111100001001	8F	09
	12	**DS**	0100110010001111	4C	8F
	20	**DS**	0011110000100100	3C	24
Albahadili		**P:**	13 14 3 9 31 5 11 21 4 1 32 20 22 30 18 26 28 2 29 17 6 23 19 27 10 7 15 25 12 816 24		
		K:	0100010000110111011010001 0001111		
	7	**DS**	1110110110001100	ED	8C
	12	**DS**	1110111000101110	DD	2D
	20	**DS**	1101110001011101	DC	5D

IMPLEMENTATION

In order to demonstrate the strength of the new proposed algorithm, it is implemented using C++ language. The code takes two input data: the permutation size and any string of characters (password). Then the permutation, P and the derived key, K, are obtained. From K and P the digital signature is constructed in order to be exchanged over the network for authentication. The size of the digital signature is determined as half size of the input derived key.

Three illustrative examples are considered using different passwords of different lengths. The size of permutation and derived key are chosen to be 32-bit length for these examples. Table 1 shows the results obtained for the permutation, derived key and three different digital signatures which are derived using the same P and K according to different seed values. One of the main features of this proposed algorithm is that the password elements can not be extracted even all the possible digital signatures are constructed by an adversary. In addition, the adversary has no chance to determine any of the valid digital signatures.

CONCLUSIONS

This research presents a new authentication scheme that enhances the security of the client-server systems. In standard password-based authentication algorithms, the password or a variation of it is exchanged over the network between the client and the server. In contrast, the new scheme does not exchange the password or any of its variations over the network. Instead, a password-based digital signature is derived and exchanged. The new scheme has the following main features:

- It does not need to exchange the password or any close variation of it (e.g., encrypted form) over the network
- The length of the derived signature is flexible and it is greater than the actual password length
- The entropy of the derived signature has no effect on its security strength
- The possible number of digital signatures is equal to half of the key length
- Any image of the password can not be extracted from the digital signatures
- The password can not be constructed even all associated digital signatures are trapped

It can be implemented locally at the client or as a mobile agent at the server.

ACKNOWLEDGEMENTS

This research received financial support towards the cost of its publishing from the Deanship of Research and Graduate Studies at Applied Science University, Amman - Jordan.

REFERENCES

1. Bellovin, S.M. and M. Merrit, 1992. Encrypted key Exchange: Password-based protocols secure against dictionary attacks. Proceedings of the IEEE Symposium on Research in Security and Privacy, pp: 72-84.
2. Mihir Bellare, David Pointcheval and Phillip Rogaway, 2000. Authenticated key exchange secure against dictionary attacks. Advances in Cryptology-EUROCRYPT 00. Lecture Notes in Computer Science, 1807: 139-155.
3. Philip MacKenzie, Thomas Shrimpton and Markus Jakobsson, 2006. Threshold password-authenticated key exchange. J. Cryptol., 19 (1): 27-66.
4. Hung-Min Sun and Her-Tyan Yeh, 2006. Password-based authentication and key distribution protocols with perfect forward secrecy. J. Comput. Syst. Sci., 72 (6): 1002-1011.
5. Jablon, D., 1996. Strong password-only authenticated key exchange. Comput. Commun. Rev., 26 (5): 5-26.
6. Gong, L., M. Lomas, R. Needham and J. Saltzer, 1993. Protecting poorly chosen secrets from guessing attacks. IEEE J. Selected Areas Commun., 11 (5): 648-656.
7. Lucks, S., 1997. Open key exchange: How to defeat dictionary attacks without encrypting public keys. Proceedings of the Security Protocol Workshop '97.
8. Hussain, S.M. and N.M. A-Ajloni, 2006. Key Base Random Permutation (KBRP). J. Comput. Sci., 2 (5): 419-421.
9. Hussain, S.M. and H. Al-Bahadili, 2008. A password-based key derivation algorithm using the kbrp method. Am. J. Applied Sci., 5 (7): 777-782.
10. Forouzan, B.A., 2008. Introduction to Cryptography and Network Security, McGraw Hill.
11. Brainard, J., A. Juels, R. Rivest, M. Szydlo and M. Yung, 2006. Fourth Factor Authentication: Somebody You Know. ACM CCS, pp: 168-78.
12. Thomas Wu, 2005. The Secure Remote Password Protocol, Stanford University.
13. Bresson, E., O. Chevassut and D. Pointcheval, 2004. New Security Results on Encrypted Key Exchange. Public Key Cryptography (PKC 2004), pp: 145-158.
14. Stallings, W., 2006. Cryptography and Network Security: Principles and Practice, Prentice-Hall.
15. Abdalla, M., P.A. Fouque and D. Pointcheval, 2005. Password-based authenticated key exchange in the three-party setting. Public Key Cryptography (PKC 2005), pp: 65-84.
16. Menezes, A., P. Oorschot and S. Vanstone, 1996. Handbook of Applied Cryptography, CRC Press.
17. IEEE, 2004. P1363.2/D15: Standard Specifications for Password-Based Public Key Cryptographic Techniques.
18. Wong, D.S., A.H. Chan and Feng Zhu, 2005. Password authenticated key exchange for resource-constrained wireless communications. Proceedings of the 4th International Conference on Networking (ICN'05), pp: 827-834.