Secure Password Authentication Scheme over Insecure Network

Aye Aye, Tin Mar Kyi
University of Computer Studies (Mandalay)
ayeayeucsm@gmail.com tinmarkyi@gmail.com

Abstract

Passwords are essential to ensure the privacy and security of personal data at home, at organization or World Wide Web. Simple passwords can be easily guessed and cracked with attacker's experience. The better solution is to use One Time Password. Many researchers proposed the various password authentication schemes to be secure user login. However, the previous authentication schemes are neither efficient, nor invulnerable to various categories of attacks. The purpose of this paper is to overcome these problems. Ticket is created by third party (RC) for password secrecy and RC is structured for authentication. In this paper, a new Ticket oriented password authentication is proposed to achieve all proposed goals. Furthermore, this scheme also provides the integrity, confidentiality and mutual authentication.

Keywords: One Time Password, Password Authentication, RC, Ticket

1. Introduction

Authentication is the key for information security since if the authentication mechanism is compromised, the rest of the security measures are by passed as well [54]. One-time password (OTP) schemes, where each password is used only once, offer available alternative or a supplement to traditional password schemes.

One Time Password is crucial in application: for example, cloud computing layer's security, banking security, mobile application security and privacy approval applications. For example, the storage of user's noteworthy data must be secure. Access to company network via remote access is to be controlled by one-time-password. If the user's password is compromised, the intruder could learn the password by guessing, intercepting, impersonating the user's communication and modify the user's password.

The main contribution of this paper are (1) to propose a new efficient ticket oriented password authentication scheme (2) to prevent replay attack and modification attack (3) to propose third party architecture in communication networks .

This paper is organized as follows. Section 2 illustrates the related work. The basic concepts of the proposed scheme are presented in Section 3. In Section 4, the goals for a new password authentication scheme are proposed. The proposed password authentication scheme is presented in Section 5. Section 6 compares the proposed scheme with other password authentication schemes. Evaluating Performance of proposed scheme is calculated in Section 7. Finally, Section8 presents our conclusions and future work.

2. Related Work

Lamport (1981) [7] introduced the first hash-based one-time password authentication scheme to defeat wiretapping or sniffing, but his scheme involves very high hash overhead and practical difficulty. Password-based authentication schemes have been widely deployed to verify the legitimacy of remote users.

From the Lamport's method, Haller and Yeh derived S/KEY one-time password scheme [6, 8] and Yeh's scheme, respectively [5]. Some researchers further pointed out that S/KEY scheme is not secure. To solve the above high hash overhead and password resetting problems, Shimizu proposed the CINON protocol [4].

Hsiang et al. pointed out that Yoon et al's scheme's pitfalls. They claimed their scheme can against parallel session attack, masquerading attack and password guess attack. However, Hsiang et al.'s scheme is vulnerable password guess attack, masquerading user attack and masquerading server attack [3].

Koner et al.[9] propose an efficient and reliable three entity user authentication technique that verifies the authenticity of user as well as remote server. User authenticity is verified by applying password, smart card and biometric property of user simultaneously. This 3-E is insulated from parallel session attack and impersonation attack

In 2012, Wang [1] proposed a password based authentication scheme between a smart card owner and smart card via an untrusted card reader to get the guarantee that the card reader will not be able to impersonate the card owner in future without the smart card itself.

3. Basic Concepts

Our scheme employs some basic concepts, such as one-way hash function, e.g., SHA-512, discrete logarithm problem, Diffie–Hellman key agreement protocol, asymmetric cipher RSA and signature cipher DSA. We briefly describe these basic concepts in this subsection [3].

3.1. One_Way Hash Function

The A one-way hash function $h: a \rightarrow b$ is a function with the following properties:

- The function h takes a message of arbitrary length as the input and produces a message digest of fixed-length as the output.
- The function h is one-way in the sense that given a, it is easy to compute h(a) = b.

However, given b, it is hard to compute h^{-1} (b) = a.

- Given a, it is computationally infeasible to find a' such that a'= a, but h(a') = h(a).
- It is computationally infeasible to find any pair a, a' such that a'= a, but h(a') = h(a).

3.2. Diffie-Hellman Key Exchange Protocol

The scheme allows two parties communicate each other in a secure communication with the agreed session key. Its security is based on solving discrete logarithm problem. Assume that Alice and Bob are to agree on a session key over insecure networks. The parameters g and p are public. Then, they do the following steps to agree on a session key [3].

- Alice randomly chooses a large number **a** and sends Bob $A = g^a \bmod p$.
- In the mean time, Bob also randomly chooses a large number **b** and sends Alice $B = g^b \bmod p$.
- After that, Alice and Bob can calculate their session key as $K = B^a \bmod p = A^b \bmod p = g^{ab} \bmod p$. Without knowing **a** and **b**, no one can listen on the Alice–Bob channel.

4. Goals for A New Password Authentication Scheme

In this paper, we first propose a new password authentication scheme to achieve the following ten goals. The ten goals solve the problems in client-server oriented schemes.

G1. No password is transmitted over the network.

G2. The scheme must generate strong initial password strength.

G3. Ticket cannot be revealed and modified by the user.

G4. No one can impersonate a legal user to login the server.

G5. The next password cannot be guessed even if the previous password is broken.

G6. The scheme must resist the replay attack, guessing attack and modification attack.

G7. The scheme can overcome the small login number problem and big login number problem.

G8. The scheme must be efficient and practical.

G9. The scheme can achieve mutual authentication. Not only can server verify the legal users, but users can verify the legal server.

G10. The scheme must support authentication, confidentiality and integrity properties.

5. Proposed Password Authentication Scheme

This system intends for secure one_time _password client/server authentication over insecure network. This scheme consists of three entities User, RC and Server. The overview of this system will be explained in Figure 1.

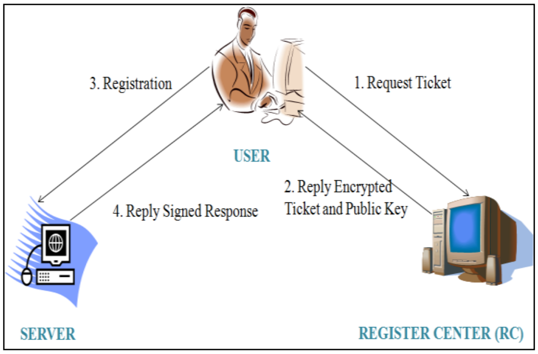

Figure 1. System Model for the Proposed Password Authentication Scheme

5.1. Notation

The following notations are used throughout the paper.

- ID denotes the user identity.
- PW denotes the password of user A.
- RC denotes the trusted third party, Register Center. RC is responsible for generating Ticket to user.
- S denotes the server. Server authenticates users and allows to use the resource if the user is legal.
- A denotes user’s Diffie-Hellman public key.
- B denotes RC’s Diffie-Hellman public key.
- a denotes Diffie-Hellman key private of user.
- b denotes Diffie-Hellman private key of RC.
- p denotes a large prime number.
- g denotes the primitive element in Galois field GF(p).
- Ticket denotes the approval to register to Server. It means a request by the user to login the server.
- LT denotes the life time of Ticket.
- T denotes the timestamp.
- n denotes the number of login.
- h denotes a public one-way hash function with fixed-length output, e.g. MD5or SHA-1.
- Enc denotes encryption algorithm, such as RSA.
- Sign denotes the signature algorithm, e.g. DSA.

- Authenticator denotes the success or fail reply information.
- The expression “X⇒Y: M” represents the message M sent from X to Y through a secure channel.

5.2. Three Phases of Scheme

Our scheme consists of three parts, namely, registration phase to RC, registration phase to server and login phase. In the registration phase, RC issues Ticket to the users who request registration. Ticket is used by user and sent to the server to complete registration process. Once the user registers with the server successfully, he/she can use the resources of server through the login phase.

In the login phase, a user sends his/her identifier (ID) and (n_1) times of hash. Then the server compares the identifier (ID) and verifies the one-time hash password to authenticate user decide whether the login request should be accepted or not. The registration phase is done only once by the user when a new user wants to join the system. The login phase and authentication phase are performed every time the user wants to login.

5.2.1. Registration to RC

When the user wishes to use the resources of system, user must apply for Ticket from RC first. Both sides of user and RC use Diffie-Hellman protocol to support discrete logarithm problem. To prevent guessing attack and modification attack Ticket is encrypted using asymmetric cryptosystem. Timestamp oriented authentication system is configured to defend replay attack. Figure 2 shows the registration process of the scheme.

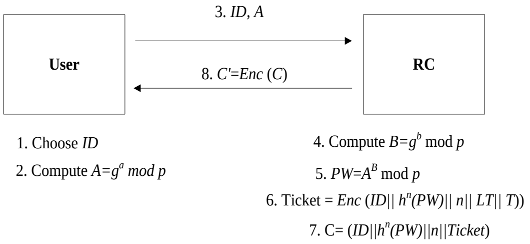
3. ID, A
User
RC
8. $C'=Enc\ (C)$
1. Choose ID
2. Compute $A=g^a \ mod\ p$
4. Compute $B=g^b$ mod p
5. $PW=A^B$ mod p
6. Ticket = $Enc\ (ID||\ h^n(PW)||\ n||\ LT||\ T))$
7. C= $(ID||h^n(PW)||n||Ticket)$

Figure 2. Registration to RC

The details of this phase are described in the following steps.

1. User chooses the identifier ID.
2. User computes A using Diffie-Hellman protocol.
3. User ⇒ RC: ID, A. RC calculates B and generates Ticket.
4. After generating Ticket, RC calculates C= (ID||hn(PW)||n||Ticket) and then send C to user by encrypting asymmetric cipher.

5.2.2. Registration to Server

After the user gets Ticket from RC, he/she sends Ticket, identifier and one-way hash value to server. Afterwards, server will perform the following steps. Figure 3 shows the registration to server phase.

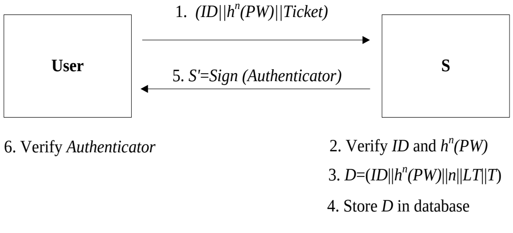
1. $(ID||h^n(PW)||Ticket)$
User
S
5. $S'=Sign\ (Authenticator)$
6. Verify $Authenticator$
2. Verify ID and $h^n(PW)$
3. $D=(ID||h^n(PW)||n||LT||T)$
4. Store D in database

Figure 3. Registration to Server

1. User→S: ID, hn(PW) and Ticket. User A issues a registration request to server S.
2. After receiving the registration request, S compare ID and hn(PW) with the values embedded in Ticket.
3. Then, S stores D in server’s database.

S →User: Authenticator. Server S sends the signed message to User, where message stands for success or fails registration information.

4. When, the message arrives, User verifies the message to check whether the server is legal or not. If the server is correct, User completes registration process successfully. Otherwise, server is rejected and repeats the registration phase.

5.2.3. Login to Server

When the user login to system, server will perform the following steps. Figure 4 shows the details of login process.

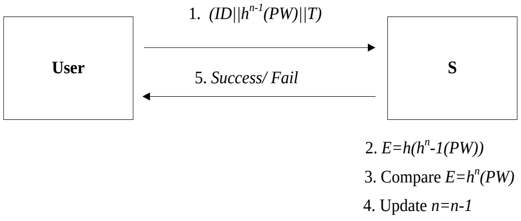

Figure 4. Login to Server

1. A→S: ID, hn-1(PW) and T. User issues a login service request to server S. T is the timestamp of this login. T can prevent from replaying attack.

2. After receiving the login service request, S calculates E=h(hn-1(PW),

3. Then, S compares E= hn(PW)where hn(PW) is one-time password maintained by S.

4. If it is equal, S updates the value of n.

5. S→A: Success/ Fail. Server S sends the login response to user.

6. Comparisons with Password Authentication Schemes

In this section, the proposed scheme will be compared with other password authentication scheme based on ten goals for evaluating a new password authentication scheme. Table1 shows the comparative goals among password authentication schemes. The proposed scheme is more efficient and better scheme as shown in Table1 result.

In our scheme, Diffie-Hellman key exchange protocol is used to generate more secure and stronger initial password. The trusted third party, RC provides mutual authentication and protects replay attack, guessing attack and modification attack. Liao et.al is superior to other schemes except the proposed scheme. Their scheme based on discrete logarithm problem and one-way hash function. Although their scheme is very efficient and low computing complexity, the main weak point of their scheme is the server has to keep the secret value (x) secretly. If (x) is broken up, their scheme will be destroyed.

Therefore, the proposed scheme uses Diffie-Hellman key protocol to generate initial password and one-way hash to compute one-time password. The proposed scheme is more secure, more efficient and achieves the not only confidentiality and integrity but mutual authentication also. In addition, public key cryptosystem is used for the purpose of secure scheme. Table 1 shows the evaluating result to achieve our goals.

Table 1. Comparisons among password authentication scheme

	Proposed Scheme	Liao's Scheme	Lamport's Scheme
G1	Y	N	N
G2	Y	N	N
G3	Y	N	N
G4	Y	Y	Y
G5	Y	Y	N
G6	Y	N	Y
G7	Y	N	N
G8	Y	Y	Y
G9	Y	N	Y
G10	Y	N	N

Y: Supported; N: Not Supported

7. Evaluating Performance of Scheme

This section is divided into two components: (1) how to achieve cryptographic properties such as confidentiality, integrity and mutual authentication (2) how to resist password attacks.

7.1. Confidentiality, Integrity and Mutual Authentication

The properties of confidentiality, integrity and mutual authentication are discussed and how to achieve these properties in the proposed scheme are discussed.

7.1.1. Confidentiality and Integrity

Confidentiality is the protection of transmitted data from passive attacks [10]. To achieve the confidentiality property, asymmetric encryption cipher is used in the proposed scheme.

Ticket is encrypted using public key cipher and the registration response of RC to user is also encrypted once more as discussed in the following equations:

$$Ticket= AsymEncrypt\ (ID||hn(PW)||LT||n||T) \quad (1)$$

$$D= AsymEncrypt\ (ID||h^n(PW)||n||Ticket) \quad (2)$$

As with confidentiality, integrity can apply to a stream of messages, a single message, or selected fields within a message. The connection-oriented integrity service addresses both message stream modification and denial of service [10]. To ensure the integrity, the server signs the response to user at registration phase.

$$S'=Sign_{priv}(Authenticator) \quad (3)$$

The receiving message arrives to the user; user verifies the authenticator by using server's public key.

$$V'=Verify_{pub}\ (Authenticator) \quad (4)$$

For the purpose of confidentiality and integrity, the purposed scheme is designed as described above.

7.1.2. Mutual Authentication

Simple definition of mutual authentication is two parties can authenticate each other respectively. In this scheme, server can authenticate whether the user is authorized user or impersonator. Server decrypts Ticket and compares the external identifier (ID) and hash password with internal ID and h^n(PW) of Ticket.

Moreover, the user can also authentication whether the server is correct or not by verifying the signature response of server. If the verification process is successful, the user labels that the server is authorized server.

7.2. Password Attack Resistance

The nature of password guessing attack, replay attack and impersonation attack are explained and the resistance formulas are described using equations.

7.2.1. Resistance to Password Guessing Attack

Most of the existing password authentication schemes are weak for generating initial password, where the attacker intercepts and store them locally and then attempts to use a guessed password to verify the correctness of his/her guess using theses authentication messages. In the proposed scheme, Diffie-Hellman protocol is used to generate strong and secure initial password. Additionally, the attacker will fail to guess password.

$$PW=A^{B} \bmod p \qquad (5)$$

The initial password is hashed using one-way hash function to be more secure and to prevent password guessing attack.

$$One\_Time\_Password=h^{n}(PW) \qquad (6)$$

7.2.2. Resistance to Password Replay Attack

Having the intercepted password, the attacker can impersonate and masquerade like the legal user. To resist the replay attack, the following equation will be computed.

$$\Delta T>=T'-T \qquad (7)$$

If the subtraction result is greater than ΔT, the system will define the unauthorized and deny the login request.

7.2.3. Resistance to Modification Attack

An attacker attempts to modify intercepted communications to masquerade the legal user and login to the system. The proposed scheme is intended to prevent modification attack. Eq. (1) and (2) achieve this attack resistance. Even if the attackers achieve the previous password, they find awkwardly to get the new password ($h^{n-1}(PW)$) because this scheme is one_time_password scheme.

8. Conclusion and Future Work

In this paper, a new password authentication scheme is designed for user's privacy over insecure communication networks. In terms of ten goals are achieved rather than other password authentication schemes. The advantages of this scheme are presented as follows. This authentication scheme not only reduces the small and big (n) attack of Lamport's one-time-password, but also prevents password guessing attack by the use of Diffie-Hellman key exchange protocol. Three-party ticket authentication architecture also supports mutual authentication and resists from modification and guessing attack. The life-time based password authentication scheme prevents the replay attack from eavesdroppers. The weak point of the proposed scheme is that user must communicate with unfriendly characters at registration and login process. For instance, current authentication system requires typing multiple hexadecimal numbers in login phase. Future implementation may wish to consider methods to improve the case of usage of the system. Multiple participants who can access multiple services in authenticated way may be additional research.

References

[1] Yongge Wang . Password Protected Smart Card and Memory Stick Authentication Against Off-line Dictionary Attacks, 2012

[2] I-EnLiao, Cheng-ChiLee and ,Min-Shiang Hwang, "A password authentication scheme over insecure networks", *Journal* of Computer and System Science, 2006.

[3] Debiao He, Jianhua Chen, and Jin Hu "Weaknesses of a Remote User Password Authentication Scheme Using Smart Card", International Journal of Network Security, Vol.13, No.1, PP.58-60, July 2011

[4] A.Shimizu, A dynamic password authentication method by one-way function, IEICETrans. Inform.Syst. J73-D-I(1990)630–636.

[5] T.-C.Yeh, H.-Y.Shen, J.-J.Hwang, A secure one-time password authentication scheme using smart cards, IEICETrans.Commun.E85-B(2002)2515–2518.

[6] N.Haller, The S/KEY one-time password system, RFC Technical Report1760, February1995.

[7] L. LAMPORT, Password Authentication with Insecure Communication, Communications of the ACM 1981, 24:770–2.

[8] N.Haller, The S/KEY(TM) one-time password system, in: Proceedings of Internet Society Symposium on Network and Distributed System Security, Internet Society, 1994, pp.151–158.

[9] C.C.Lee, C.T.Li, and S.D.Chen, “Two attacks on a two-factor user authentication in wireless sensor networks,” Parallel Processing Letters, vol.21, no.1, pp.21–26, 2011.

[10] William Stallings, “Cryptography and Network Security Principles and Practices, Fourth Edition”