Computers & Security Vol.18, No.8, pp.727-733, 1999
Copyright © 1999 Elsevier Science Limited
Printed in Great Britain. All rights reserved
0167-4048/99$20.00

Password Authentication Schemes with Smart Cards*

Wen-Her Yang and Shiuh-Pyng Shieh

Department of Computer Science and Information Engineering, College of Electrical Engineering and Computer Science, National Chiao Tung University, Hsinchu, Taiwan 30010.

In this paper, two password authentication schemes with smart cards are proposed. In the schemes, users can change their passwords freely, and the remote system does not need the directory of passwords or verification tables to authenticate users. Once the secure network environment is set up, authentication can be handled solely by the two parties involved. For a network without synchronized clocks, the proposed nonce-based authentication scheme is able to prevent malicious reply attacks.

Keywords: password authentication, smart card, ID-based scheme, clock synchronization.

1. Introduction

The rapid progress of networks facilitates more and more computers connecting together to exchange great information and share system resources. Security is then an important issue for computer networks. There are two basic requirements for network security: secrecy and authentication. Secrecy protects sensitive data against eavesdropping and modification. Authentication prevents forgery and unauthorized network access. The common approach to provide authenticity is the use of passwords. Password authentication has been used for a long time, mainly because it is easy to implement and use.

In conventional password authentication schemes, each user has an identifier (ID) and a secret password (PW). If a user requests to enter a network system, he must enter his ID and PW to pass the system authentication. A possible verification approach is to directly store and maintain a directory of users' IDs and PWs in the network system. Upon receipt of a user's login request, the network system searches the password directory table to verify whether or not the submitted password matches with the one stored in the table. If they match, the user is regarded as an authorized user and is permitted to enter the system. Otherwise, the login request is denied. Since the password is stored in plain-text form, this approach is clearly under the threat of revealing the password.

There are many schemes [Evans74, Lennon81] proposed to resolve the password revealing problem. These schemes often hash the password with a one-way function and store the hash value, instead of the plain password, in the directory table. In this way, the secrecy of passwords can be ensured even if contents of the directory table are disclosed. However, in the schemes, the system must protect the directory table against intruders' modification. Otherwise, the directory table may be replaced and users may be masqueraded. There are a number of authentication protocols [Kehne92, Kohl93, Neuman93, Otway87, Shieh96, Syverson93] which use a trusted third party to ensure authentication and security in an open network system. In these authentication protocols, secret information, such as secret keys, must be stored in a directory table on the authentication server. Therefore, the attacks to the directory table still exist in these authentication systems.

* This work was supported by the National Science Council, Taiwan under contract NSC86-NSPO(A)-PC-FA06-02.

Recently some enhanced authentication schemes [Chang91, Chang93, Okamoto89, Shieh97, Tsujii78, Wang96] are proposed to eliminate the drawback of using directory tables. These schemes all adopt the concept of ID-based signature scheme [Shamir85] in conjunction with smart cards [Peyret90]. The ID-based schemes have the following advantages: (1) neither secret nor public keys need be exchanged, (2) the public key directory table is not needed, and (3) the assistance of a third party is not needed. The first ID-based signature scheme was proposed by Shamir [Shamir85]. He uses the well-known public-key encryption algorithm RSA [Rivest78] with smart cards to implement ID-based signature. Shamir's ID-based scheme enables communicating parties to verify each other's signature without exchanging private or public keys.

In Shamir's ID-based scheme, the secret key corresponding to an ID is fixed, and cannot be changed. Thus, a user with an assigned ID cannot choose his secret key by himself. Since the concept of timestamps [Denning81] is not employed, the scheme is weak against the attack of replaying previously intercepted signature. It is hence not suitable for user authentication in network systems. Chang and Wu's scheme [Chang91] has a similar problem. A user's password is generated by the password generation center, rather than by the user himself. However, users are used to choosing their own passwords. This approach is against users' habit and may not be accepted by many users. Furthermore, the scheme suffers from the threat of password leakage [Chang93].

Based on Elgamal's signature [Elgamal85] and Shamir's ID-based schemes, Wang and Chang include the concept of timestamps in an improved authentication scheme [Wang96]. In their scheme, however, replay attacks cannot be avoided completely and user's identities may be forged. A legitimate user can impersonate other users and pass the system authentication. That is because the information about user identities is not included in the verification procedure of their scheme. The remote system can only determine validity of the authentication message, but cannot identify who really sent this message. Furthermore, these schemes are all based on ID-based schemes, they share the problem that a user cannot change his password after registration. If a user's password is compromised, he can no longer use his current ID, but needs to apply for a new one. This makes users inconvenient to use in a real network system. Since some weaknesses exist in these schemes, a more secure and practical authentication scheme for network systems is proposed in the following section.

In this paper, We propose two new password authentication schemes with smart cards. The proposed schemes can resolve the security problems in the above schemes [Chang91, Shamir85, Wang96]. Our method keeps the merits of ID-based schemes, but eliminates the weakness that users cannot change their passwords. In the new schemes, a user can freely choose and change his password at will. If his password is accidentally revealed, he can simply change it to another secure password without re-registering for a new ID. This paper is organized as follows. A new timestamp-based password authentication scheme is presented in section 2, which only needs one message for authentication. For the networks that clocks cannot be easily synchronized, we propose a nonce-based password authentication scheme in section 3. The security of our schemes will be analyzed in section 4. Finally, a conclusion is given in section 5.

2. Timestamp-Based Password Authentication Scheme

In the proposed scheme, we assume the existence of a trusted key information center in the network to issue personalized smart cards to users when joining the system. The proposed timestamp-based password authentication scheme can be divided into three phases. In the *registration phase*, the key information center sets up the authentication system and issues smart cards to the users who request registration. In the *login phase*, a user attaches his smart card to a terminal and keys in his identifier (ID) and password (PW). Then the terminal sends a login request message to the remote host. In the *verification phase*, the remote host verifies the correctness of submitted message and determines whether the login request should be accepted or not.

Registration Phase

The key information center is not responsible for authenticating users, but for generating key information, issuing smart cards to new users and serving password-changing request for registered users. Let U_i denote the ith user who submits his identifier ID_i and chosen password PW_i to the key information center to request for registration. Here, PW_i must be sent over a secure channel. Upon receipt of the request, the key information center will perform the following steps:

1. Generate two large prime numbers p and q, and let $n = p\ q$. For security reasons, the length of p and q is recommended to be 512 bits at least.

2. Choose a prime number e and an integer d which satisfy

   $$e \cdot d \ (\mathrm{mod}(\ p - 1) \cdot (q - 1)) = 1. \qquad (1.)$$

   Here e is the public key of the key information center that should be published, and d is the secret key that must be kept privately.

3. Find an integer g which is a primitive element in both GF(p) and GF(q), where g is the system's public information.

4. Calculate the user's secret information S_i as

   $$S_i \equiv ID_{i.}^{\ d} \pmod{n}. \qquad (2.)$$

   According to the encryption algorithm RSA [Rivest78], the following equation would be obtained.

   $$ID_i \equiv S_i^{\,e} \pmod{n} \qquad (3.)$$

   Even if one knows ID_i, e, and n, it is hard to crack S_i without the knowledge of d. This is a discrete logarithm problem [Adleman79]. The integer d can be evaluated only when n is factorized to p and q, which is very difficult because the length of n is 1024 bits.

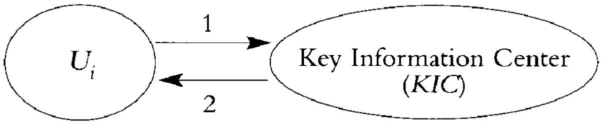
5. Generate the smart card's identifier CID_i of U_i and compute h_i by

   $$h_i \equiv g^{PW_i \cdot d} \pmod{n} \qquad (4.)$$

   Here CID_i is for validating the legality of smart cards in the *verification phase.*

6. Write n, e, g, ID_i, CID_i, S_i and h_i to the memory of smart card and issue the card to U_i.

   Once the authentication system is set up, the key information center is not needed except when new users request to join, or registered users request to change passwords. The integer pair p and q will not be used any more and should be thrown away secretly. When a new user requests to join, the center repeats step 4 through 6. The procedure of *registration phase* is shown in *Figure 1.*



1. U_i - >*KIC* : ID_i, PW_i

2. *KIC* - >U_i : a smartcard containing {ID_i, CID_i n, e, g, $S_{i,}$ h_i }

Figure 1. Registration Phase

Login Phase

When U_i wishes to login a remote host, he must insert the smart card into a card reader and enter his identity ID_i' and password PW_i'. If ID_i' is identical to the ID_i which is kept in the memory of the smart card, the smart card will perform the following steps:

1. Generate a random number ri and calculate the following two integers:

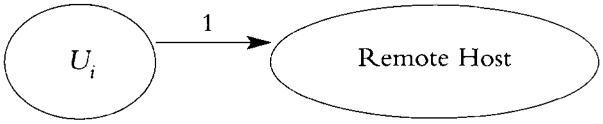
   $$X_i \equiv g^{ri \cdot PW_i'} \pmod{n} \qquad (5.)$$

   $$Y_i \equiv S_i \cdot h_i^{ri \cdot f(CID_i, T)} \pmod{n} \qquad (6.)$$

Where T is the current time used as a time-stamp and $f(x, y)$ is a one-way function. The one-way function is a function relatively easy to compute but significantly harder to undo or reverse. That is, given (x, y) it is easy to compute $f(x, y)$, but given $f(x, y)$ it is very difficult to compute x.

2. Send a login request message M containing ID_i, CID_i, X_i, Y_i, n, e, g and T to the remote host.

   In Figure 2, the transaction of *login phase* is depicted.



1. U_i - > host : M = { ID_i, $CID_{i,}$ X_i, $Y_{i,}$ n, e, g, T}

   $X_i \equiv g^{ri \cdot PW_i'}$ (mod n)

   $Y_i \equiv S_i \cdot h_i^{ri \cdot f\,(CID_i, T)}$ (mod n)

Figure 2. Log-in Phase

Verification Phase

The *verification phase* is executed by the remote host to determine whether U_i is allowed to login or not. Let T' be the time when the remote host receives the message M. Upon receipt of message M, the remote host will perform the following steps to verify the correctness of M.

1. Verify that ID_i is a valid user identity and CID_i is a legal smart card identity. If not, the log-in request is rejected.

2. Compare T with T', if the difference between T and T' is longer than the valid period, M is considered as an invalid message and the host computer will reject the login request. According to different network environments, the length of the valid period can be adjusted.

3. Check whether the following equation holds:

   $$Y_i^e = ID_i \cdot X_i^{f\,(CID_i, T)} \qquad (7.)$$

   The equation will hold when the password PW_i', keyed in by U_i, matches PW_i registered in the key information center. That is because:

   $$Y_i^e = (S_i \cdot h_i^{ri \cdot f\,(CID_i, T)})^e = S_i^{e} \cdot (g^{PW_i\,d})^{ri \cdot f\,(CID_i, T)\;e}$$

   $$= ID_i \cdot (g^{e \cdot d})^{ri \cdot PW_i \cdot f\,(CID_i, T)}$$
   $$= ID_i \cdot g^{ri \cdot PW_i \cdot f\,(CID_i, T)} \qquad (8.)$$

   and

   $$ID_i \cdot X_i^{f\,(CID_i, T)} = ID_i \cdot g^{ri \cdot PW_i \cdot f\,(CID_i, T)} \qquad (9.)$$

4. If the equation holds, the remote host believes that the message M is sent by U_i, and the password PW_i' matches PW_i. Therefore, U_i is allowed to log in the remote host, otherwise the login request is rejected.

Comparing to other schemes, our authentication scheme allows users to freely change their passwords at will. If a user U_i wants to change his password, he can submit his smart card and newly chosen password PW_i^* to the key information center over a secure channel. The center will compute the new *hi'* as

$$h_i' \equiv g^{PW_i^* \cdot d} \text{ (mod } n) \qquad (10.)$$

and write it into U_i's smart card to replace the original h_i. After getting the updated smart card, U_i is able to use the new password PW_i^* to login the network system.

The proposed password authentication scheme can withstand the problems that have appeared in other schemes [Chang91, Shamir85, Wang96]. With the timestamp T, the attack of replaying previously intercepted messages is avoided. However, note that if system clocks are not well synchronized, and transmission delay is long and unpredictable in a network environment (e.g., a wide area network) [Gong92], a potential replay attack exists in all schemes that employ the concept of timestamps. In the next section, we will propose a nonce-based authentication scheme to protect users against this attack in this network environment.

3. Nonce-Based Password Authentication Scheme

The nonce-based password authentication scheme is an extended version of the timestamp-based scheme. In the nonce-based scheme, the timestamp T is replaced with a nonce number N to withstand the replay attack. The nonce-based scheme consists of three phases. The *registration phase* is the same as the timestamp-based scheme described in the previous section, hence the description of the phase is skipped. The *login phase* and *verification phase* are described as follows respectively.

Login Phase

In order to login a remote host, U_i inserts his smart card into a terminal and enters his identity ID_i and password PW_i'. If ID_i matches the one kept in the memory of smart card, the following steps will be performed.

1. The smart card sends an initial message $M_1 = \{ID_i, CID_i\}$ to request for a login session.

2. Upon receipt of the message M_1, the remote host verifies the validity of ID_i and CID_i. If any one of these two is not valid, the login request is rejected and the connection will be closed. Otherwise, the remote host reserves ID_i and CID_i for the *verification phase*, and then evaluates a session nonce $N = f(CID_i, rj)$ and sends it back to the smart card. Here, rj is a random number and $f(x,y)$ is a one-way hash function. The session nonce N will be kept for future use.

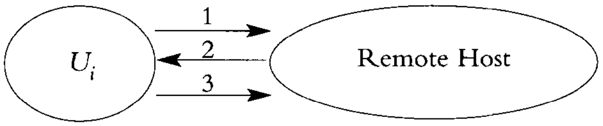
3. Upon receipt of the session nonce N, the smart card generates another random number ri and calculates the following two integers:

$$X_i \equiv g^{ri \cdot PW_i'} \pmod{n} \quad (11.)$$

$$Y_i \equiv S_i \cdot h_i^{ri \cdot N} \pmod{n} \quad (12.)$$

4. The smart card sends an authentication message M_2 containing X_i, Y_i, n, e and g to the remote host.

In the nonce-based scheme, three message transmissions are required to complete the login phase. The transaction of the new *log-in phase* is depicted in *Figure 3*.



1. U_i - > host : $M_1 = \{ ID_i, CID_i\}$
2. host - > U_i : $N = f(CID_i, rj)$
3. U_i - > host : $M_2 = \{ X_i, Y_i, n, e, g\}$
   $X_i \equiv g^{ri \cdot PW_i'} \pmod{n}$

   $Y_i \equiv S_i \cdot h_i^{ri \cdot N} \pmod{n}$

Figure 3. Log-in phase in the nonce-based scheme

Verification Phase

Upon receipt of message M_2, the remote host will do the following steps to decide whether U_i is permitted to log in or not.

1. Check whether the following equation holds:

$$Y_i^e = ID_i \cdot X_i^N \quad (13.)$$

   Where ID_i and CID_i are derived from the smart card and N is the session nonce generated by the remote host in the *login phase*.

2. If the equation holds, the remote host believes that:
   (a) the authentication message M_2 is truly sent by U_i,
   (b) the password PW_i', keyed in by U_i, matches PW_i registered in the key information center,
   (c) and the session nonce N that the smart card used to evaluate Y_i is identical to the one the remote host generated. That is, message M_2 is fresh and is not a replay message.

Since M_2 is proved as a legal and fresh authentication message, U_i is allowed to login the remote host. With the session nonce N, the nonce-based password authentication scheme can protect users against the replay attack even if the system clocks are not synchronized. In the next section, we will analyze the security of the two proposed schemes.

4. Security Analysis and Discussions

The strength of our schemes can be demonstrated by the following security attacks. In the proposed timestamp-based scheme, if a forger wants to masquerade U_i to pass the system authentication, he must find two integers x and y that satisfy the following equation.

$$y^e = ID_i \cdot x^{f(CID_i, T)} \qquad (14.)$$

Although the forger can get a pair of integers (y^e, $x^{f(CID_i, T)}$) that make the equation hold. The pair (y, x) is unattainable because computing (y, x) from (y^e, $x^{f(CID_i, T)}$) is a discrete logarithm problem. In another case, assume that the smart card CID_i of U_i is exposed to an intruder, say U_j ($j \neq i$). In this case, U_j cannot access the network systems since he does not have PW_i. One possible way for U_j to acquire PW_i is to crack $h_i \equiv g^{PWi \cdot d}$ (mod n). This is infeasible, because h_i is stored in the tamper-proof smart card and cannot be retrieved directly. Even if U_j can compromise h_i, PW_i remains secure because of the discrete logarithm problem. As to U_i, he can use the same ID_i to re-register a new smart card CID_i' to the key information center. From then on, the old smart card CID_i that U_j obtained is automatically disabled.

In the nonce-based scheme, the potential replay attack will not succeed. Considering the following scenario, an intruder eavesdropped an old authentication message from a login session of U_i associated with a session nonce N. He may replay the old authentication message to request for a new log-in session. Following the steps of *login phase*, the intruder first sends $M_1 = \{ID_i, CID_i\}$ to the remote host. Upon receipt of M_1, the remote host generates a new session nonce N' and replies it to the intruder. Then the intruder replays intercepted authentication message M_2 to the remote host. The login procedure will fail in the *verification phase*, because the verification equation does not hold as follows:

$$Y_i^e = ID_i \cdot X_i^N \neq ID_i \cdot X_i^{N'} \qquad (15.)$$

The authentication message M_2 that the intruder replayed is considered invalid. Consequently, the login request is rejected and the attack fails.

Exponential computation is considered to be very time-consuming. In our schemes, only two exponential computations are needed for the smart card to initialize a login session. This feature makes our schemes effective, since the smart cards usually do not support powerful computation capability. It is noticeable that the remote host performs the verification of users without any prior knowledge, and all the elements used in the *verification phase* are generated or provided on users' side. It means that the remote host does not need to register in the same key information center as users. Therefore, our authentication schemes are suitable for cross-domain network applications, such as electronic commerce systems.

5. Conclusions

In this paper, two practical password authentication schemes are proposed which are based on the concepts of ID-based schemes and the smart cards. These schemes do not need the directory of passwords or verification tables to authenticate users. Their security is based on the difficulty of factoring a large number and the discrete logarithm problem. Once the secure network system is set up, the authentication can be handled solely by the two parties involved. Unlike in other ID-based authentication schemes, users are permitted to choose and change their passwords freely in the two proposed schemes.

The proposed timestamp-based scheme needs only one message for authentication, but requires synchronous clocks. And the proposed nonce-based scheme is immune from the replay attack, but requires three authentication messages. In the networks with tightly synchronized system clocks, such as local area networks, the timestamp-based scheme is advised. On the other hand, the nonce-based scheme is suitable for a large network where clock synchronization is difficult, such as wide area networks, mobile communication networks, and satellite communication networks.

References

[Adleman 79] L. Adleman, "A subexponential algorithm for the discrete logarithm problem with applications to cryptography," *in Proc. 20th IEEE Symp. Foundations of Computer Science*, pp. 55-60, 1979.

[Chang 91] C. C. Chang and T. C. Wu, "Remote password authentication with smart cards," *IEE Proceeding-E*, Vol. 138, No. 3, pp. 165-168, 1991.

[Chang 93] C. C. Chang and S. J. Hwang, "Using smart cards to authenticate remote passwords," *Computers and Mathematical Applications*, Vol. 26, No. 7, pp. 19-27, 1993.

[Denning 81] D. E. Denning and G. M. Sacco, "Timestamps in key distribution protocols," *Communications of the ACM*, Vol. 24, No. 8, pp. 533-536, 1981.

[Elgamal 85] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, IT-31(4), pp. 469-472, 1985.

[Evans 74] A. Jr Evans, W. Kantrowitz and E. Weiss, "A user authentication system not requiring secrecy in the computer," *Communications of the ACM*, Vol. 17, pp. 437-442, 1974.

[Gong 92] L. Gong, "A security risk of depending on synchronized clocks," *ACM Operating System Review*, Vol. 26, No. 1, 1992.

[Kehne 92] A. Kehne, J. Schonwalder and H. Langendorfer, "A nonce-based protocol for multiple authentication," *ACM Operating Systems Review*, Vol. 26, No. 4, pp. 84-89, Oct. 1992.

[Kohl 93] J. Kohl, C. Neuman, "The Kerberos network authentication service (V5)," *Internet RFC 1510*, Sep. 1993.

[Lennon 81] R. E. Lennon, S. M. Matyas and C. H. Meyer, "Cryptographic authentication of time-invariant quantities," *IEEE Transactions on Communications*, COM-29, No. 6, pp. 773-777, 1981.

[Neuman 93] B. C. Neuman, and S. G. Stubblebine, "A note on the use of timestamps as nonces," *ACM Operating Systems Review*, Vol. 27, No. 2, pp. 10-14, April 1993.

[Okamoto 89] E. Okamoto, and K. Tanaka, "Identity-based information security management system for personal computer networks," *IEEE Journal on Selected Areas in Communications*, Vol. 7, No. 2, pp. 290-294, Feb. 1989.

[Otway 87] D. Otway and O. Rees, "Efficient and timely mutual authentication," *ACM Operating Systems Reviews*, Vol. 21, No. 1, pp. 8-10, Jan. 1987.

[Peyret 90] P. Peyret, G. Lisimaque and T.Y. Chua, "Smart cards provide very high security and flexibility in subscribers management," *IEEE Transactions on Consumer Electronics*, Vol. 36, No. 3, pp. 744-752, 1990.

[Rivest 78] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signature and public-key cryptosystem," *Communications of the ACM*, Vol. 21, No. 2, pp. 120-126, 1978.

[Shamir 85] A., Shamir, "Identity-based cryptosystems and signature schemes," *Proceedings CRYPTO'84*, pp. 47-53, Springer, Berlin, 1985.

[Shieh 96] S. P. Shieh and W. H. Yang, "An authentication and key distribution system for open network system," *ACM Operating Systems Review*, Vol. 30, No. 2, pp. 32-41, 1996.

[Shieh 97] S. P. Shieh, W. H. Yang and H. M. Sun, "An authentication protocol without trusted third party," *IEEE Communications Letters*, Vol. 1, No. 3, May 1997.

[Syverson 93] P. Syverson, "On key distribution protocols for repeated authentication," *ACM Operating Systems Review*, Vol. 27, No. 4, pp. 24-30, 1993.

[Tsujii 78] S. Tsujii, T. Itho, and K. Kurosawa, "ID-based cryptosystem using discrete logarithm problem," *Electronic Letters*, Vol. 23, pp. 1318-1320, Nov. 1978.

[Wang 96] S. J. Wang and J. F. Chang, "Smart card based secure password authentication scheme," *Computers and Security*, Vol. 15, No. 3, pp. 231-237, 1996.