LETTER

A Security Enhanced Timestamp-Based Password Authentication Scheme Using Smart Cards*

Al-Sakib Khan Pathan[†a)], *Nonmember* and Choong Seon Hong[†b)], *Member*

Summary
The intent of this letter is to propose an efficient timestamp based password authentication scheme using smart cards. We show various types of forgery attacks against Shen et al.'s timestamp-based password authentication scheme and improve their scheme to ensure robust security for the remote authentication process, keeping all the advantages of their scheme. Our scheme successfully defends the attacks that could be launched against other related previous schemes.

Key words:
Authentication, Cryptanalysis, Forgery Attack, Smart Card

1. Introduction

With the staggering growth of distributed systems and networking, and plummeting costs of networking devices, remote authentication has become an important task in many network applications. One of the major hurdles in remote authentication process is ensuring robust security while using possibly insecure channels for communications between the participating parties: the user and the authentication server. Various works addressed this issue from diverse perspectives which include password-table driven schemes, id-based schemes, timestamp based schemes, nonce-based schemes etc. Nonetheless, many of the works which dealt with this issue are able to provide only the unilateral authentication, where the server messages are usually considered to be completely secured and only the legitimacy of the user(s) could be verified. As the adversaries could intercept the login requests from the users and might pretend to be the legitimate server(s) to the users, there must be some type of mechanism to ensure authentication in both directions, which is termed as *bilateral or mutual authentication*. One of the mutual authentication (or, verification) schemes proposed earlier is Shen et al. scheme [1], which is based on the initial timestamp-based scheme proposed by Yang and Shieh [2]. In this letter, we present an improved timestamp-based mutual authentication scheme [13] which is adapted from Shen et al. scheme. We also show a new type of attack and some already identified attacks and weaknesses of Shen et al. scheme. We eliminate the weaknesses and vulnerabilities of Shen et al. scheme.

The rest of the letter is organized as follows; Section 2 states related works, Section 3 states Shen et al. scheme, Section 4 notes down different types of attacks against [1], Section 5 presents our improved scheme, Section 6 contains security analysis, and Section 7 concludes it.

2. Related Works

In 1999, Yang and Shieh [2] proposed two password authentication schemes with smart cards one of which was the timestamp-based password authentication scheme. In 2002, Chan and Cheng [3] showed that [2] is vulnerable to forged login attack and an adversary could be able to impersonate as a legal user to pass the system authentication. Fan et al. [4] presented a cryptanalysis of [2] and showed another type of attack which was different than that of [3] and also proposed an enhanced scheme which could withstand Chan-Cheng attack and the attack that they demonstrated in their paper. But later, [5] showed that, Fan et al. scheme was still insecure and vulnerable to forged login attack. Again, [6] showed two other attacks on Fan et al.'s enhanced scheme. Shen et al. [1] came up with one enhanced scheme based on [2] which they claimed to be efficient enough to protect the authentication process from forged login or forged server attacks. Unfortunately, later [7], [8] and [9] showed that the improved scheme proposed by Shen et al. was still vulnerable to the forgery attacks. Wang and Li [10] proposed another improved scheme based on Yang-Shieh scheme [2] assuming that the remote host had an extra storage for storing certain information.

Our proposed scheme is different than all of the mentioned schemes and overcomes the drawbacks of these existing schemes. Moreover, it ensures all of the advantages that were present in the previous schemes.

Manuscript received December 14, 2006.
Manuscript revised June 05, 2007.
† The authors are with the Department of Computer Engineering, Kyung Hee University, Giheung, Yongin, Gyeonggi 449-701, South Korea.
* This work was supported by MIC and ITRC projects. Dr. C. S. Hong is the corresponding author.
a) E-Mail: spathan@networking.khu.ac.kr
b) E-Mail: cshong@khu.ac.kr

3. Review of Shen et al.'s Scheme

3.1 Basic Terms

U_i – The ith user seeking for authentication, KIC – The Key Information Center, ID_i – The identity of the user U_i, PW_i – The password chosen by U_i, CID_i – The identity of the smart card associated with U_i, $f(.)$ – A one-way hash function. A one-way function is a transfer function f where given p, it is fairly easy to compute, $q = f(p)$ in the forward direction, but given q, it is computationally very difficult to find out a p using the inverse such that, $p = f^{-1}(q)$.

3.2 Shen et al.'s Timestamp-Based Scheme

Registration Phase: The KIC sets up the authentication system and issues smart cards to U_i who requests for registration. It is assumed that, this phase occurs over a secure channel. The steps that are followed in this phase are:

1. U_i securely submits ID_i and PW_i to the KIC and in turn the following operations are done by the KIC.
2. Two large prime numbers p and q are generated, and let $n = p \bullet q$
3. A prime number e and an integer d are chosen which satisfy, $e \bullet d \equiv 1 \bmod (p-1)(q-1)$, where, e is the public key of the KIC that should be published and d is the secret key that is kept undisclosed.
4. An integer g is found which is a primitive element in both GF(p) and GF(q), where g is the public information of the KIC.
5. $S_i = ID_i^d \bmod n$ is computed as U_i's secret information.
6. h_i for U_i is computed such that, $h_i = g^{PW_i \bullet d} \bmod n$.
7. CID_i is computed as, $CID_i = f(ID_i \oplus d)$, where $\oplus$ stands for an exclusive operation.
8. Then the information n, e, g, ID_i, CID_i, S_i, h_i and $f(.)$ are written into the smart card's memory and the card is issued to U_i.

Login Phase: When U_i needs to login to the system, the smart card should be attached to the login device and ID_i and PW_i need to be keyed in. After that, the smart card performs the following operations:

1. Generates random number r_i and computes X_i and Y_i :

   $X_i = g^{r_i \bullet PW_i} \bmod n$ and $Y_i = S_i \bullet h_i^{r_i \bullet f(CID_i, T)} \bmod n$

   Here, T is the current timestamp.
2. Sends the login request message, $M = \{ID_i, CID_i, X_i, Y_i, n, e, g, T\}$ to the remote server.

Verification Phase: After the server has received the message M, it carries out the following steps:

1. Checks the validity of ID_i. If the format of ID_i is incorrect, the server rejects the request.
2. Checks whether $CID_i' = CID_i$ or not, where, $CID_i' = f(ID_i \oplus d)$. If the result is positive, the following steps are performed otherwise the request is rejected.
3. Checks whether the condition (T′-T) ≤ ΔT holds or not, where T′ is the timestamp of receiving the login request message and ΔT is the legitimate time interval allowed for the transmission delay. If it is negative, the server rejects the request.
4. Checks the equation, $Y_i^e = ID_i \bullet X_i^{f(CID_i, T)} \bmod n$. If it holds, then the remote server accepts the login request and gives access to the U_i.
5. Computes $R = (f(CID_i, T''))^d \bmod n$ where, T″ is the current timestamp and returns $M' = \{R, T''\}$ to U_i.

When the user receives M', the verification of the server is performed by U_i as:

1. It Checks (T‴-T″) ≤ ΔT, where T‴ is the timestamp of receiving the message M'. If it is affirmative, it goes forward; otherwise, rejects the server message.
2. Calculates $R' = R^e \bmod n = (f(CID_i, T''))^{d})^e = f(CID_i, T'')$. If the condition, $R' = f(CID_i, T'')$ does not hold, then the remote server is rejected, otherwise the mutual verification is succeeded.

4. Cryptanalysis of Shen et al.'s Scheme

4.1 Attack Based on [6] and [9]

As the attacker could intercept the login request message $M = \{ID_i, CID_i, X_i, Y_i, n, e, g, T\}$, it can get the valid values of ID_i and CID_i. Using these values it could launch the impersonation attack as follows:

1. Let, $a = f(CID_i, T_c)$ where T_c is the current timestamp. Use the Extended Euclidean algorithm to compute $gcd(e, a) = 1$. Let, u and v be the coefficients computed by the Extended Euclidean algorithm such that, $e \bullet u - a \bullet v = 1$
2. Compute $X_f = ID_i^v \bmod n$
3. Compute $Y_f = ID_i^u \bmod n$
4. Send the forged login request message $M_f = \{ID_i, CID_i, X_f, Y_f, n, e, g, T_c\}$ and this request will eventually pass the authentication phase as,

$$Y_f^e = ID_i^{e \bullet u} \bmod n = ID_i^{1+a \bullet v} \bmod n$$
$$= ID_i \bullet ID_i^{a \bullet v} \bmod n = ID_i \bullet (X_f)^a \bmod n$$
$$= ID_i \bullet (X_f)^{f(CID_i, T_c)} \bmod n$$

In fact, this attack could be extended for $gcd(e,a)=2,3,\ldots$ instead of only $gcd(e, a) = 1$.

4.2 Yang et. al.'s Attack

The attacker intercepts the message, M and then:

1. Finds a value w such that it satisfies, $w \bullet f(CID_i, T_f) = f(CID_i, T)$, where T_f denotes the attacker's attack launching time.
2. Computes the equation, $X_f = X_i^w = g^{r_i \bullet PW_i \bullet w} \bmod n$
3. Now, the attacker constructs the forged login request message as, $M_f = \{ID_i, CID_i, X_f, Y_i, n, e, g, T_f\}$

This forged message eventually passes the authentication phase of [1] because:

$$\begin{aligned} Y_i^e &= (S_i \bullet h_i^{r_i \bullet f(CID_i, T)})^e \bmod n \\ &= (ID_i^d \bullet g^{PW_i \bullet d \bullet r_i \bullet f(CID_i, T)})^e \bmod n \\ &= ID_i \bullet g^{PW_i \bullet r_i \bullet f(CID_i, T)} \bmod n \end{aligned}$$

and,

$$\begin{aligned} ID_i \bullet X_f^{f(CID_i, T_f)} \bmod n &= ID_i \bullet g^{r_i \bullet PW_i \bullet w \bullet f(CID_i, T_f)} \bmod n \\ &= ID_i \bullet g^{PW_i \bullet r_i \bullet f(CID_i, T)} \bmod n \end{aligned}$$

4.3 Impersonation Attack Based on [8]

An attacker can impersonate a legitimate user U_i, with identity ID_i, following the procedure:

1. It Intercepts the login request message $M = \{ID_i, CID_i, X_i, Y_i, n, e, g, T\}$.
2. Computes the identity, $ID_f = ID_i^{-1} \bmod n$
3. Now, the attacker submits ID_f and a random value as his password to the KIC to obtain a valid smart card with information $\{n, e, g, ID_f, CID_f, S_k, h_k$ and $f(.)\}$.
4. Since, in the registration phase, $S_i = ID_i^d \bmod n$ and here, $S_k = ID_f^d \bmod n = ID_i^{-d} \bmod n$, the attacker can compute S_i as, $S_i = S_k^{-1} \bmod n$
5. Chooses a random integer y.
6. Sets, $X_f = y^e \bmod n$ and $Y_f = S_i \bullet y^{f(CID_i, T_f)} \bmod n$ where T_f is the timestamp for the login request from the attacker and sends the forged login message, $M_f = \{ID_i, CID_i, X_f, Y_f, n, e, g, T_f\}$. The request is validated as the login request from the user U_i because,

$$\begin{aligned} Y_f^e &= (S_i \bullet y^{f(CID_i, T_f)})^e \bmod n \quad = ID_i^{ed} \bullet y^{f(CID_i, T_f) \bullet e} \bmod n \\ &= ID_i \bullet (X_f)^{f(CID_i, T_f)} \bmod n \end{aligned}$$

4.4 Our Novel Attack

We have shown earlier that the attacker can get the values of ID_i and CID_i from the login request message, and $CID_i = f(ID_i \oplus d)$ is a fixed value for a particular login request from the user. In such a case, an attacker can launch an attack on the basis of the following theorem:

Theorem 1: Let, $a = f(CID_i, T_f)$ where T_f is the attacker's login timestamp. The attacker finds a value b such that, $a \bullet b \equiv 1 \bmod n$. This could be used for forgery attack against Shen et al.'s scheme.

Proof.

1. The adversary chooses a random integer k, computes, $Y_f = k^{f(CID_i, T_f)} \bmod n$ and sets $X_f = ID_i^{(-1) \bullet b} \bullet k^e \bmod n$.
2. Sends the forged login request message, $M_f = \{ID_i, CID_i, X_f, Y_f, n, e, g, T_f\}$
3. The attacker could pass the authentication phase as,

$$Y_f^e = k^{f(CID_i, T_f) \bullet e} \bmod n$$

and,

$$\begin{aligned} ID_i \bullet X_f^{f(CID_i, T_f)} \bmod n &= ID_i \bullet (ID_i^{(-1) \bullet b} \bullet k^e)^{f(CID_i, T_f)} \bmod n \\ &= ID_i \bullet ID_i^{-1} \bullet k^{f(CID_i, T_f) \bullet e} \bmod n \\ &= k^{f(CID_i, T_f) \bullet e} \bmod n \end{aligned}$$

5. Our Improved Scheme

Like the scheme [1], our improved scheme also has three distinct but interrelated phases namely, registration phase, login phase and mutual authentication phase. We keep the registration phase same as [1] and improve the other phases to surmount the drawbacks of the previously proposed schemes. After the registration phase, the smart card gets the values of n, e, g, ID_i, CID_i, S_i, h_i and $f(.)$.

Login Phase: In the login phase, U_i attaches the smart card with the reader device and keys in his ID_i and PW_i. Then the smart card performs the following operations:

1. Generates a random number r_i and computes X_i, Y_i and Z_i as follows:

$$\begin{aligned} X_i &= g^{r_i \bullet PW_i} \bmod n \\ Y_i &= S_i \bullet h_i^{r_i \bullet f(CID_i, T)} \bmod n \\ Z_i &= X_i \oplus CID_i \oplus f(CID_i, Y_i) \end{aligned}$$

Here, T is the current timestamp.

2. Sends the login request message, $M = \{ID_i, Y_i, Z_i, n, e, g, T\}$

Mutual Authentication Phase: When the server gets the login request message, it performs the operations:

1. Checks the validity of ID_i. If the format of the ID_i is incorrect, the server rejects the request.
2. Checks whether the condition $(T' - T) \leq \Delta T$ holds or not, where T' is the timestamp of receiving the login request message and ΔT is the legitimate time interval allowed for the transmission delay. If the condition does not hold, the server rejects the request.
3. Computes, $CID_i' = f(ID_i \oplus d)$ and $val = f(CID_i', Y_i)$. Then, computes, $Z_i \oplus CID_i' \oplus val$ which should generate the value of X_i as $CID_i' = f(ID_i \oplus d) = CID_i$ for the legitimate users.
4. Checks the equation, $Y_i^e = ID_i \bullet X_i^{f(CID_i, T)} \bmod n$. If it holds, then the remote server accepts the login request and gives access to U_i, otherwise rejects the request as it implies that the value of X_i that is generated in the previous step is not correct.
5. Once, the user U_i is authenticated by the server, to provide mutual authentication, the server now computes, $R = (f(CID_i', T''))^d \bmod n$ where, T'' is the

current timestamp and returns $M' = \{R, T''\}$ to the user U_i.

After receiving the message M', the user U_i authenticates it as follows:

1. Checks the legal time interval, $(T'''-T'') \leq \Delta T$, where T''' is the timestamp of receiving the message M'. If it is positive, it goes forward; otherwise rejects the server message.
2. Calculates $R' = R^e \bmod n = (f(CID_i, T'')^d)^e = f(CID_i, T'')$. If the condition, $R' = f(CID_i, T'')$ does not hold, then the remote server is rejected, otherwise the mutual authentication is succeeded.

Password Renewal. If U_i needs to change his password, he has to go through the registration phase where he submits his identity and the new password, and accordingly the KIC performs the steps 5 to 7.

6. Security Analysis of the Improved Scheme

r_i randomizes the outputs of the parameters from session to session for a particular user so that the outputs could not be same for each new login attempt. Z_i is basically used to hide the values of X_i and CID_i. As CID_i is fixed for a particular user, if it is sent in plain format, the attacker could employ some other techniques to deduce some important information. Now, considering some common attacks, we show how our scheme could perform well.

Replay Attack: Probability of this attack is negligible as repetition of old login request message will be detected by the server in step 2 of the mutual authentication phase.

Forged Login or Forged Server Attack: In our scheme, the values of X_i and CID_i are kept secret at the time of communication and are not available to the eavesdropper. So, forging or replacing other values will be detected in the mutual authentication phase. From the server side, message R could not be generated by attacker as d is not public and is kept secret only by the server.

Impersonation: The impersonation attacks mentioned in section 4.1, 4.2, and 4.4 are not applicable against our scheme. Let us consider the attack presented in section 4.3. The attacker: (1) Intercepts the login request message. In our scheme it is, $M = \{ID_i, Y_i, Z_i, n, e, g, T\}$. (2) Computes, $ID_f = ID_i^{-1} \bmod n$ (3) Now, the attacker submits the identity ID_f and a random value as his password to the KIC to obtain a valid smart card with information $\{n, e, g, ID_f, CID_f, S_k, h_k$ and $f(.)\}$. (4) Since, in the registration phase, $S_i = ID_i^d \bmod n$ and here, $S_k = ID_f^d \bmod n = ID_i^{-d} \bmod n$, the attacker can compute S_i as, $S_i = S_k^{-1} \bmod n$ (5) Chooses a random integer y. (6) Now, this step could not be performed as we do not expose the value of the parameter X_i. At this point, the adversary could at best replace the value of Y_i with, $Y_f = S_i \bullet y^{f(CID_i, T_f)} \bmod n$ but, that simply does not make any sense and even the first phase of authentication could not be passed in any way. The attacker is allowed even to replace the value of Z_i, but without the proper values, any of such attempts can never pass the authentication phase.

7. Conclusion

In this letter, we have shown the loopholes and different types of attacks against Shen et al. scheme including a new type of forgery attack. We have presented our improved scheme which could successfully defend all sorts of attacks mentioned in the article.

References

[1] Shen, J.-J., Lin, C.-W., and Hwang, M.-S., "Security Enhancement for the Timestamp-Based Password Authentication Schemes using Smart Cards," Computers & Security, Vol. 22, No 7, pp. 591–595, 2003.

[2] Yang, W.-H. and Shieh, S.-P., "Password Authentication Schemes with Smart Cards," Computers & Security, Vol. 18, No. 8, pp. 727-733, 1999.

[3] Chan, C.-K. and Cheng, L. M., "Cryptanalysis of a Timestamp-Based Password Authentication Scheme," Computers & Security, Vol. 21, No. 1, pp. 74-76, 2002.

[4] Fan, L., Li, J.-H., and Zhu, H.-W., "An Enhancement of Timestamp-Based Password Authentication Scheme," Computers & Security, Vol. 21, No. 7, pp. 665-667, 2002.

[5] Wang, B., Li, J.-H., and Tong, Z.-P., "Cryptanalysis of an Enhanced Timestamp-Based Password Authentication Scheme," Computers & Security, Vol. 22, No. 7, pp. 643-645, 2003.

[6] Chen, K.-F. and Zhong, S., "Attacks on the (Enhanced) Yang-Shieh Authentication," Computers & Security, Vol. 22, No. 8, pp. 725-727, 2003.

[7] Yang, C.-C., Yang, H.-W., and Wang, R. C., "Cryptanalysis of Security Enhancement for the Timestamp-Based Password Authentication Scheme using Smart Cards," IEEE Trans. on Cons. Elec., Vol. 50, No. 2, pp. 578-579, 2004.

[8] Yang, L. and Chen, K., "Cryptanalysis of a Timestamp-Based Password Authentication Scheme," (2004) available at: http://eprint.iacr.org/2004/040.pdf

[9] Sun, H.-M. and Yeh, H.-T., "Further Cryptanalysis of a Password Authentication Scheme with Smart Cards," IEICE Trans. on Comm., Vol. E86-B, No. 4, pp. 1412-1415, 2003.

[10] Wang, Y. and Li, J., "Security Improvement on a Timestamp-Based Password Authentication Scheme," IEEE Trans. on Cons. Elec., Vol. 50, No. 2, pp. 580-582, 2004.

[11] Gong, L., "A Security Risk of Depending on Synchronized Clocks," ACM SIGOPS Operating Systems Review, Volume 26 , Issue 1, January, pp. 49 – 53, 1992.

[12] Syverson, P., "A Taxonomy of Replay Attacks," Proc. Computer Security Foundations Workshop VII, 1994, CSFW 7, 14-16 June, pp. 187 – 191, 1994.

[13] Pathan, A. S. K. and Hong, C. S., "An Improved Timestamp-Based Password Authentication Scheme with Two-Party Verification using Smart Cards," Proc. of the 9th IEEE ICACT, Vol. I, pp. 804-809, 2007.