An Improved Timestamp-Based Password Remote User Authentication Scheme

Keerti Srivastava*, Amit K Awasthi* and R.C.Mittal**

*Group for Cryptology Reseach, Department of Applied Science Pranveer singh Institute of Technology, Kanpur, U.P INDIA

**Department of Mathematics Indian Institute Of Technology, Roorkee, U.A, INDIA

Abstract

In 2003, Shen et al [4] proposed a timestamp-based password authentication scheme in which remote server does not need to store the passwords or verification table for users authentication. Unfortunately Wang and Li[6], E.J.Yoon [8], Lieu et al.[3], analyzed independently the Shen Lin Scheme [4] and was found to be vulnerable to some deadly attacks. In continuation to it, this paper analyzes few attacks and finally proposes an improved Timestamp- based password remote user authentication scheme so that it can withstand the existing forged attacks.

Keywords: Authentication, personate attack, smart card, security improvement

1. Introdution

In 1999, Yang and Sheih [7] proposed a password remote authentication scheme to remove the need of password tables or verification tables at the end of server using smart card. In the scheme, users are permitted to choose and change their passwords freely. However, this scheme was later found to be vulnerable to the forged login attacks by Chang [1], Fan [2], Shen [4] . In 2003, Shen et al [4] proposed an improved scheme to resist the forged login attacks. and also provided mutual authentication. In [4] the attacker can intercept the legal user's login request and register the smart card to carry out the forged login attacks. In 2004 Wang and Li [6] proposed a new idea which offered a solution to overcome that perticular attack but carried some short-comings related to the remote server to store the different smart card marks of the users that made it open to new threats (authentication efficiency and other security problems [5]) .

In continuation process, Liu et al.[3] also pointed out that Shen et al scheme [4] is vulnerable to forged login attack. To overcoming this problem he proposed a new improved scheme based on nonce [3], But in absence of time-stamp this scheme is pron to certain attacks (Replay attack).

This paper analyzes the weakness of the Shen et al scheme [4], and presents an improved remote authentication scheme which still keeps the features of the non-storage data at server side. In this, remote server need not to store any verification information of the users.

2. Review of Shen et al's. scheme[4]

In this scheme, the key information center (KIC) is responsible for generating some related elements and providing smart cards to the new users. The authentication scheme is divided in to four phases: initialization, registration, login and authentication.

2.1. Initialization phase

In Shen's scheme Key informarmation center KIC is a trusted authority which generates global parameters. KIC also computes user's secret information and provides smart cards to users.KIC performs the following steps:

1. Genrate two large primes p and q and compute $n = pq$.
2. Choose a prime number e and an integer d such that
   $e.d \bmod (p-1)(q-1) = 1$
   where e is the system public key, d is the corresponding private key, which should be provided to the server in a safe way.
3. Find an integer g, which is a primitive element in both $GF(p)$ and $GF(q)$ and the public information in the system.

2.2. Registration phase

A new user U_i securely submits his identifier ID_i and password PW_i to the KIC. The KIC then performs the following steps:

1. Calculate the user's secret information $S_i : S_i = ID_i^d \bmod n$.
2. Generate the smart card's identifier CID_i of U_i and $h_i : CID = f(ID_i \oplus d)$
   $h_i = g^{pw_i.d} \bmod n$ where $f(x)$ is a one way function.
3. Write $n, e, g, ID_i, CID_i, S_i$ and h_i in to the smart card of U_i, and issue it through a secure channel.

2.3. Login phase

1. Generate a random number r_i and compute X_i and Y_i as follows:
   $X_i = g^{r_i \cdot pw_i} \bmod n$, $Y_i = S_i.h_i^{r_i.f(CID_i, T_c)} \bmod n$
   where T_c is the date and time on the login device and $f(x, y)$ is a one way function.
2. $U_i \xrightarrow{M} S$(the remote server):
   $M = ID_i, CID_i, X_i, Y_i, n, e, g, T_c$
   here M is a login request message of the user U_i

2.4. Authentication phase

After receiving the login request message M from U_i, the remote server will perform the following steps to verify the correctness of M.

1. Verify that ID_i is a valid user identifier. If not the login request is rejected.
2. Check the validity of T_c. If $(T_s - T_c) \succ \Delta T$, then the server rejects the login request, where T_s is the current data and time on the remote server; $\Delta T$is expected legitimate time interval for transmission delay.
3. Compute $CID'_i = f(ID_i \oplus d)$, $CID'_i \neq CID_i$, the login request is rejected.
4. Check the equation $Y_i^e = ID_i.X_i^{f(CID_i,T_C)} \bmod n$. If it holds, the login request is accepted;otherwise rejected.
5. $S \rightarrow U_i : M' = (R, T'_s)$ where $R = (f(CID_i, T'_s))^d \bmod n$ and T'_S is the timestamp showing the current date and time on the remote server. Upon receiving the message M' from the server, the user U_i verifies the server as follows.
6. Check the time interval between T'_s and T'_c where T'_c is the time and date when the user U_i receives the message M'. If $T'_c - T'_S \succ \Delta T$, then U_i rejects the remote server, where ΔT denotes the predetermined legitimate time interval of transmission delay.
7. Compute $R' = R^e \bmod n$. In fact, $R^e \bmod n = (f(CID_i, T'_s))^d)^e \bmod n = f(CID_i, T'_s)$

3. Forged login attack on the Shen et al [4]

3.1. By Liu, Zhou, Gao

In this section, we have depicted a forged login attack on the Timestamp-based password authentication scheme [4], which was earlier discovered by Lieu et al [3]. In this an attacker can pretend to be a legal user and login the remote server successfully by registering a legal smart card and intercepting valid login request sent by the legal user. Suppose an attacker U_f attempts to impersonate a legal user U_i with identity ID_i, attacker can login the remote server successfully by performing the following steps:

1. Intercepts a login request message of the user $U_i : ID_i$, CID_i, X_i, Y_i, n, e, g, T_c by monitoring the power consumption.
2. Computes $ID_f = ID_i^{-1} \bmod n$, $CID_f = f(ID_f \oplus d)$ $S_f = ID_f^d \bmod n$,$h_f = g^{PW_f.d} \bmod n$.where d is the secret information known to server. where ID_f as the identity PW_f as the password.
3. Compute $S_f = ID_f^d \bmod n = (ID_i^{-1})^d \bmod n = ID_i^{-d} \bmod n$, and because $S_i = ID_i^d \bmod n$ so $S_i.S_f = 1 \bmod n$ and then, the attacker can compute the secret information S_i of the user U_i by using the extended euclidean algorithm.
4. Generates a random number r_f, and computes X_f and Y_f.

$$X_f = g^{r_f.PW_f} \mod n, \quad Y_f = S_i.h_f^{r_f.f(CID,T_f)} \mod n$$

here T_f is the current timestamp.

5. $U_f \rightarrow S$: M=X_f, Y_f, ID_i, CID_i, n, e, g, T_f here M is the forged login request message of the user U_i. It is easy to verify that $M = X_f, Y_f, ID_i, CID_i, n, e, g, T_f$ is a valid login request.
   In fact, $Y_f^e = (S_i.h_f^{r_f.f(CID_i,T_f)})^e \bmod n = ID_i^{ed}.h_f^{r_f.f(CID_i,T_f).e} \bmod n = ID_i.g^{PW_f.d.r_f.f(CID_i,T_f).e} \bmod n = ID_i.X_f^{f(CID,T_c)} \bmod n$ by using Extended Euclidean algorithm.
   So an attacker can also forge valid login request of the user U_i.

3.2. Proposed attack

Suppose that the adversary has intercepted one of $U_i's$ previous login message $ID_i, CID_i, X_i, Y_i, S_i, n, e, g, T_c$ transmitted in login phase.So he or she could login the remote server successfully by performing the following steps:

1. Intercepts a login request message of the user $U_i : ID_i, CID_i, X_i, Y_i, n, e, g, T_c$.
2. Attacker sends X_i to the Remote server as his identifier and chosen password PW_i. Server compute $S_x = X_i^d \bmod n$ The attacker U_f can get the message (n, e, g, S_x) of the valid smart card through the registration phase.
3. An Attacker could extract S_i from stolen smart card. then the adversary can compute $Y_f = S_i.S_x^{f(CID,T_f)} \bmod n$ and $X_f = S_x$
4. $U_f \rightarrow S : M = X_f, Y_f, ID_i, CID_i, n, e, g, T_f$ here M is the forged login request message of the user U_f.
   It is easy to verify that $M = CID_i, ID_i, X_f, Y_f, n, e, g, T_f$ is a valid login request. In fact,

$$Y_f^e = S_i^e.S_x^{e.f(CID_i,T_f)} \bmod n, = ID_i.S_x^{e.f(CID_i,T_f)} \bmod n$$

   $= ID_i.X_i^{f(CID_i,T_f)} \bmod n$ by using Extended Euclidean algorithm. and from Shen et al Authentication phase 2.4(4) it shows that adversary U_f is succeeded to make server fool.

4. The Improved authentication scheme

4.1. Initialization phase

KIC performs the following steps:

1. Genrate two large primes p and q and compute $n = pq$.
2. Choose a prime number e and an integer d such that $e.d \bmod (p-1)(q-1) = 1$ where e is the system public key, d is the corresponding private key, which should be provided to the server in a safe way.
3. Find an integer g, which is a primitive element in both $GF(p)$ and $GF(q)$and the public information in the system.

4.2. Registration phase

A new user U_i securely submits his identifier ID_i and choosen password PW_i to the KIC. The KIC then performs the following steps:

1. Compute $CID = f(ID \oplus d)$
2. Calculate the user's secret information $S_i : S_i = CID_i^d \bmod n$.
3. Calculate $h_i = g^{pw_i.d} \bmod n$ where $f(x)$is a one way function.
4. Write n, e, g, ID_i, S_i and h_i in to the smart card of U_i, and issue it through a secure channel.

4.3. Login phase

1. Generate a random number r_i and compute X_i and Y_i as follows: $X_i = g^{r_i, pw_i} \bmod n$, $Y_i = S_i.h_i^{r_i.f(ID_i, T_c)} \bmod n$, where T_c is the date and time on the login device and $f(x, y)$ is a one way function.
2. $U_i \overset{M}{\rightarrow} S$

   $M = ID_i, X_i, Y_i, n, e, g, T_c$
   here M is a login request message of the user U_i

4.4. verification phase

1. verify ID_i and T_c and Compute $CID_i = f(ID_i \oplus d)$
2. Check $Y_i^e = CID_i.X_i^{f(ID_i, T_c)} \bmod n$
3. Compute $R = (f(CID_i, T_s))^d$ where T_s is current time stamp.
4. S (the remote server)$\overset{R, T_s}{\rightarrow} U_i$
5. verify $(T_s - T_c) \succ \Delta T$ and Check $R^e \bmod n = f(CID_i, T_s)$

5. Security Analysis of the Proposed Scheme

This section analyzes the security of Proposed Scheme.

- Resistence to Forged login attack
  The improved scheme is secure against the forged login attack by calculating different structure of secret information $S_i = CID^d \bmod n$, and still the security of the improved scheme is based on the security of one way function and the difficulty of computing the discrete logrithm and decomposition of large integral number. although an adversary can intercept the login message$ID_i, X_i, Y_i, S_i, e, g, T_c$ however, without knowing the secret information d he or she could not compute CID, and will be fail to forge the legal user.

6. Attributes of the Proposed Scheme

- Perfect Secrecy
  Suppose that the adversary has intercepted all $U's$ transmitting and receiving message$ID_i, X_i, Y_i, S_i, e, g, T_c$, the adversary can not compute $CID = f(ID \oplus d)$. since it is computationally infeasible for the adversary to obtain d by solving the discrete lograthim problem, so CID will still be secure. therfore, the improved scheme can provide perfect forward secrecy.

- Mutual Authentication
  The user and the server can authenticate each other. Not only can the server verify the legal users, but the users can also verify the legal server. Mutual authentication can help withstand the server spoofing attack where an attacker pretends to be the server to manipulate sensitive data of the legal users.

- Cost analysis
  In login phase of proposed scheme CID is not transmitted with Login message M,which saves transmission cost comparison to Shen et al scheme [4], and does not add additional computational cost to the smart card.

- Storing capacity
  Improved scheme still maintains the features of the non-storage data model scheme. The remote server does not need to store any authentication information of the user. In the whole process of the authentication, the server can carry out the authentication using the elements coming directly from the user's login, its own secure private key and the public information of the system.

7. Conclusion

The analysis above shows that Shen et al's scheme is vulnerable to forgery attack. The above analysis shows that Shen, Lin and Hwang's timestamp-based password remote authentication scheme [4] is still vulnerable to the forged login. To solve the problems of Shen's scheme in the registration and authentication, this paper proposed an improved scheme based specialised ID to prevent from forged attacks. The proposed scheme will not add additional computation cost to the smart card, and performs better than Shen's scheme in practical application.

References

[1] C. K. Chan and L. M. Cheng. Cryptanalysis of timestamp-based password authentication scheme. *Computers and Security*, 21(1):74–76, 2002.

[2] L. Fan, J. H. Li, and H. W. Zhu. An enhancement of timestamp-based password authentication scheme. *Computers and Security*, 21(7):665–667, 2002.

[3] Jia-Yong Liu, An-Min Zhou, and Min-Xu Gao. A new mutual authentication scheme based on nonce and smart cards. *Computer Communications*, 31:2205–2209, 2008.

[4] J. J. Shen, C. W. Lin, and M. S. Hwang. Security enhancement for the timestamp-based password authentication. *Computers and Security*, 22(7):591–595., 2003.

[5] M. Wang, J. Z. Lu, and X. F. Li. Remote password authentication scheme based on smartcards. *Computer Applications*, 25(10):2289–90, 2005.

[6] Y. J. Wang and J. H. Li. Security improvement on a timestamp-based password authentication scheme. *IEEE Transactiions on cnsumer Electronics*, 50(2):580–582, 2004.

[7] W. H. Yang and S. P. Shieh. Password authentication scheme with smard cards. *Computers and Security*, 18(8):727–733, 1999.

[8] E. J. Yoon, E. K. Ryu, and K. Y. Yoo. Attacks on the shen et al's timestamp-based password authentication scheme using smart cards. *IEICE Transactions on Fundamentals*, E88(A(1)):319–321, 2005.