New Time based User Security Scheme for Smart Cards

B.Srinivas
Department of Computer Science and Engineering, Christu Jyothi Institute of Technology and Science, Jangaon, Andhra Pradesh, India.

B.Upender
Department of Computer Science and Engineering, Christu Jyothi Institute of Technology and Science, Jangaon, Andhra Pradesh, India.

Abstract- **User Security is an important technology to guarantee that only the legal users can access resources from the remote server. The advantages of smart cards are storage and computation abilities. Recently, there are many remote user authentication protocols with smart card have been proposed to improve security, efficiency, and functionality extensively by many scholars. This article finds that R. C. Mittal *'s* scheme may suffer impersonate attack, and do not allow changing password freely for the user. Finally, we proposed an improved timestamp-based user authentication scheme. The modified method is more efficient and secure than R. C. Mittal scheme.**

Keywords: Authentication, password, security, smart card

I. INTRODUCTION

With rapid development of the network technology, we could access any service from any place and at any time. Password based authentication has been the essential security mechanism for the remote access control systems. In 1981, Lamport [6] proposed a password authentication scheme using a one-way hash function and a password table to achieve remote user authentication for insecure communication. Lamport's scheme is simple and efficient, but it suffers from the replay attack and the impersonation attacks caused by modifying or stealing the hashed password table maintained by the servers.

Smart card advantages are storage and compute abilities. There are many remote user authentication protocols with smart card have been proposed to improve security, efficiency, and functionality Step 2: Choose two *large numbers e and d , ed* □1mod □(*n*) , where □ However, those previous schemes are still vulnerable for some offline password guessing attack, replay attack and forgery attack [1]. Moreover, some scholars' schemes have to maintain a verified table of password and do not allow changing passwords freely .In 2003, Shen *et al.* [9] proposed a timestamp-based password authentication scheme with smart card in which the remote server does not

need to store the passwords or verification table for user authentication. Unfortunately, R. C. Mittal [1] showed that Shen *et al.*'s scheme is vulnerable to forged login attack, and presented an improved remote authentication scheme which still keeps the feature of the non-storage of data at server side. However, this paper finds that R. C. Mittal's scheme may suffer impersonate attack, and do not allow changing password freely for the user.

To overcome R. C. Mittal's weaknesses, we present an improved password authentication scheme. In the proposed scheme, the remote server does not require any verification information for the users.

The remainder of this paper is organized as follows. I give a brief review of R. C. Mittal.'s scheme in the next section. In Section 3, the security weakness of R. C. Mittal's given. In Section 4, we present the improved scheme and analyze its security. At last, some conclusions will be made in the last section.

II. REVIEW OF R. C. MITTAL'S SCHEME

In this section, I will review R. C. Mittal.'s scheme [1]. In their scheme, first, the KDC (Key Detail Center) is responsible for generating some related parameters. There are four phases in R. C. Mittal.'s scheme: initialization, registration, login, and authentication phases.

2.1 Initialization Phase :

The KIC performs the following steps.:

Step 1: Generate two large primes p and q and compute . n= p*q
Step 2: Choose two integers e and d such that , ed= 1mod ¥(n) ,where ¥(n)=(p-1)(q-1) ,where and e and d are the system's public key and private key, respectively.
Step 3: Find an integer g which is a primitive element of modulo n.

2.2 Registration Phase:

A new user Ux performs the following steps for the registration phase.
Step 1: Ux sends his/her identifier IDx and password PWx to KIC over a secure channel.
Step 2: KIC computes $CID_x=f(ID_x \otimes d), h_x=g^{pw}x^{*d}$ mod n and $S_x=CID_x^d$ mod n where f( ) is a one way fuction.
Step 3: KIC stores $\{n,e,g,ID_x,S_x,h_i\}$ into a smart card and then sends this smart card to user U_x through a secure channel.
2.3 Login Phase :
In this phase, the smart card will execute the following steps.
Step 4: First, U_x inputs his password PW_x and chooses a random number r_i and the current timestamp T_c , then computes $M_x=g^r{}_x{}^{pw}{}_x$ mod n and $N_x=S_x*h_x{}^{rxf(IDi*Tc)}$ mod n .
Step 5: U sends the login request messages $P=\{ID_x, M_x, N_x,, n, e, g, T_c\}$ to the server .

2.4 Authentication Phase
After receiving the login request message M at time T_s , S performs the following steps:
Step 1: Verify whether the ID_x is a legitimate user or not.
Step 2: Check timestamp T_s . If $(T_s-T_{c)<} \Delta T$ holds, S accepts the login request of U_x ; otherwise, rejects this request.
Step 3: S computes $CID_{x=} f(ID_x \otimes d)$.
Step 4: S checks the equation $Ni^e=CID_x*M_x{}^{f(CIDx*Tc)}$ mod n. If the equation is holds, then S accept the login request; otherwise, rejects it.
Step 5: Then S computes , $R=(f(ID_i,T_s^{'}))^d$ mod n and sends $P'=\{R,T'_s\}$ to U_x , where T'_s is the current timestamp on the server. After receiving the reply message P'at time T'_s, U_x performs the following steps:
Step 1: Check timestamp $T_s^{'}$. If $(T^{'}_c-T^{'}_{s)<} \Delta T$ holds, U_x accepts the login respond of S ; otherwise, stops this procedure.
Step 2: U_x computes $R^{'}=R^e$ mod n , and then checks If the equation $R^{'=} f(ID_i,T_s^{'}))$ holds. If it holds, U_x accepts the S ; otherwise, rejects S .

III. SECURITY ANALYSIS OF R. C. MITTAL'S SCHEME

In this section, we will point out that R. C. Mittal*'s.*' scheme may suffer impersonate attack. Moreover, in their scheme, user cannon easily change his/her password without the remote server joining this phase. The detail of the impersonation attack is given below:
1. Assume that an adversary U_A obtains 's U_x smart card, and logins request at time T_A .
2. U_A selects a random number $r_A=0$,then computes $M_{x=}g^r{}_A{}^{pw}{}_A=1$and $N_x=S_x*h_x{}^{rAf(IDi*TA)}=S_i$ mod n ,where PW_A is randomly selected by adversary U_A .
3. U_A sends the login request messages $P=\{ID_x, M_x, N_x,, n, e, g, T_A\}$ to server S .
4. S verifies whether the ID_x is a legitimate user or not.
5.S checks timestamp . If $(T_s-T_{A)<} \Delta T$ holds, accepts the login request of U_x , where T_s is the current timestamp on the server.
6. S computes $CID_x^{'}= f(ID_x \otimes d)$.
7. S checks the equation $Ni^e=CID^{'}_x*M_x{}^{f(CIDx*TA)}$ mod n , where $M_i=1$ and $N_i=S_i= f(ID_x \otimes d)^d$ In Step 7, it is obvious that $N_i^e = S_i^e = CID^{'}_x*1= CID^{'}_x$

After executing above steps, the adversary U_A can pretend as the legitimate user U_x and be successfully authenticated by the server S .

Moreover, in the registration phase, the KIC computes $h_x=g^{pw}x^{*d} \bmod n$ and stores it in U_x's smart card. If U_x wants to update his/her password, he/she should be to derive the new $h^*_x=h_x^{pw\text{-}1pw}i^* = h_x^{pwx*\times d} \bmod n$, where pw^*_x is a new password. However, without knowing the ¥(n) of the server, it is very hard for U_x to obtain PW^{-1} mod ¥(n) . Therefore, in R. C. Mittal*'s* scheme, the user cannot freely change his/ her password without the server S.

IV. THE IMPROVED SCHEME AND SECURITY ANALYSIS

In this section, we improve the R. C. Mittal*'s* scheme to remedy their weaknesses and enhance the security. To illustrate the protocol clearly, the notations used in the proposed protocol are the same as Awasthi *et al.*'s scheme. There are four phases in our scheme: initialization, registration, login and authentication, updated password phases. The details steps of the proposed protocol are described as follows:

4.1 Initialization Phase

First, the KIC performs the following steps

Step 1: Generate two large primes p and q and compute $n = p \times q$.

S**tep 2:** Choose two integers e and d such that , where $ed = 1 \bmod \phi(n)$, where $\phi(n) = (p-1)(q-1)$ and e and d are the system's public key and private key, respectively. □□

4.2 Registration Phase

A new user U_x carries out the following steps for the registration phase.

Step 1: U_x sends his/her identifier ID_x and password PW_x to KIC over a secure channel.

Step 2: KDC computes $CID_{x=} f(ID_x \otimes d)$ and $s=CID_x^d \bmod n \otimes f(Pw)$, where f( ) is a one way function.

Step 3: KIC stores $\{n, e, S_x, ID_x\}$ into a smart card and then sends this smart card to user through a secure channel.

4.3 Login And Authentication Phase

In this phase, the smart card will execute the following steps.

Step 1: First, U_x inputs his password PW_x and computes M_x and N_x as follows:

$M_x=S_x \otimes f(PW_x)$ and $N_x=M_x^{f(IDx \otimes Tc)} \bmod n$

and , where is the T_c current timestamp on the user U_x.

Step 2: U_x sends the login request messages $P=\{ ID_x, M_x, N_x, n, e, T_{c,,} N_x\}$ to the server .

Step 3: After receiving the login request message P at time T_s , S verifies whether the ID_x is a legitimate user or not. Next, S checks the current timestamp T_s . If $(T_s\text{-}T_{c)<} \Delta T$ holds, the login request is proceed; otherwise, rejects this request.

Step 4: S computes $CID_{x=} f(ID_x \otimes d)$ and checks the equation $N^e_{i.=} f(ID_x \otimes d)^{f(IDx \otimes Tc)} \bmod n$ if the equation is holds, S accepts the login request; otherwise, rejects it.

Step 5: Then S computes $R= (f(ID_x, T_s^{'})) \bmod n$, and sends $P^{'}=\{R, T^{'}_s\}$ to U_x , where $T^{'}_s$ is the current timestamp on the server.

Step 6: After receiving the reply message $P^{'}$ at time $T^{'}_c$, U_x checks the timestamp $T^{'}_s$. If $(T^{'}_c\text{-}T^{'}_{s)<} \Delta T$ holds, U_x accepts the login respond of S ; otherwise, stops this procedure.

Step 7: U_x computes $R^{'}=R^e \bmod n$, and then checks if the equation $R^{'=} f(ID_x, T_s^{'}))$ holds. If it holds, U_x accepts the server S ; otherwise, rejects S .

The above login and authentication process are briefly illustrated in Figure 1.

4.4 Updated Password Phase :

In our method, if a user wants to arbitrarily update his password PW_x , he does not need to register with the remote server. It is very convenient for the user to change his password. Now, suppose user U_X would like to change his password, he is only required to perform the following steps.

1. Choose a new password PW'_x
2. Compute $S'_X = S_X \otimes f(PW_x) \otimes f(PW'_x)$,and PW_x is an old password of user U_x .
3. Replace S_X with S'_X on the memory of the smart card. It is accepted because

$S'_X = S_X \otimes f(PW_x) \otimes PW'_x$

$= CID^d_i \otimes f(PW'_x)$

where $S_x = CID^d_i \otimes f(PW_x)$

The improvement protocol is based on the RSA cryptosystem [8]. That is n=p*q ,it is computationally intractable to factorize n when p and q are large enough. Given n, then determining ¥(n)=(p-1)(q-1) is equivalent to factoring n. It lies on the difficulty of the integer factoring problem. Moreover, giving n, e, C, and M, it is intractable to find d such that such that $C=P^d \bmod n$, where $e*d= 1 \bmod (p-1)(q-1)$. It is also equivalent to factoring n such that such that $e*d= 1 \bmod (p-1)(q-1)$ and $C=P^d \bmod n$.

Next, we analyze the security of the improvement method as follows. Based on R. C. Mittal*'s* scheme [1], our scheme can overcome the weaknesses indicated above of Section 3. In our improved method, in Steps 1 and 5, an adversary could use the eavesdropped the messages $P=\{ ID_x ,,N_x,,n,e,T_{c,,}\}$ and $R= (f(ID_x,T_s'')) \bmod n$ from the communication network, where $N_x= M_x^{f(IDx,Tc)} = (f(ID_x \otimes d)^{d) f(IDx \otimes Tc)} \bmod n$. Even if an adversary knows the messages n, R, and , it is exceedingly difficult for him to derive d, p, and q for n=p*q . Since d, p, and q are based on the difficulty of the integer factoring problem. Without having the value of p and q, it is not easy to guess the secret d of the server S. The probability of obtaining the exactly R and is equivalent to performing an exhaustive search on p and q. Hence, the off-line guessing attack is thwarted by the improved protocol. Moreover, without any password PW_x of the U_X in the transmitted messages R and N , it is very hard for the adversary to derive the password of U_X from the network.

With regard to efficiency and communications, for convenience, we define related notations to analyze the computational complexity. The notation means the time Te .for one modular exponentiation, denotes the time for m T one modular multiplication computation, and denotes h T

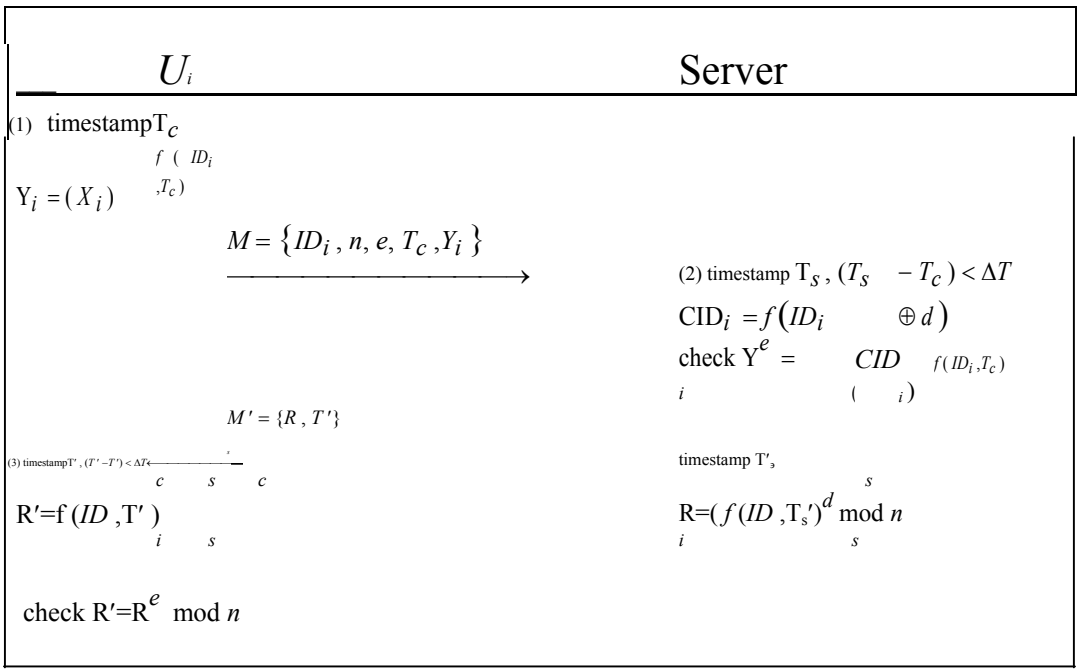

Figure 1: The proposed of login and authentication phase

Table 1: Comparisons of computation and transmission for two schemes

Schemes	R. C. Mittal's	The improved scheme
Computations for user to achieve authentication	3Te □+3T_m+2T_h	2T_e+2T_h □
Computations for server to achieve authentication	3Te □+1T_m+3T_h □□	3T_e+2T_h

the time for executing the adopted one-way hash function in one's scheme. Note that the times for computing modular addition is ignored, since they are much smaller than , , and . Te ,Tm and T_h.

We summarize the comparisons of the proposed scheme with R. C. Mittal*'s* in Table 1. As shown in Table 1, in R. C. Mittal*'s* scheme [8], each user needs to perform two hash function computation (2T_h), three modular multiplication computation (3Tm), and three modular exponentiations (3Te) for authentication. And it is required three hash function computation (3T_h), one modular multiplication computation (1Tm), and three modular exponentiations (3Te) for the server in R. C. Mittal*'s* authentication phase.

In the improved scheme, the computation time for each user to achieve mutual authentication is two hash function computations (2T_h) and two modular exponentiations (2Te).Consequently, the improved method needs two hash function computations (2T_h) and three modular exponentiations (3Te) to achieve mutual authentication for the server. Therefore, the improved method is more efficient than R. C. Mittal*'s* scheme.

V. CONCLUSIONS

In this paper, we have proposed an improvement to overcome the weaknesses of R. C. Mittal*'s*. The improved method can provide the following characters: (1) no password table is required for KIC and the designated servers; (2) users can freely choose their own passwords; (3) users may update their passwords after registration phase; (4) it supplies mutual authentication between the user and the designated server. In addition, the improved method is more efficient than Awasthi *et al.'s* scheme.

ACKNOWLEDGMENTS

This research was partially supported by the Christu Jyothi Inctitute of Technology and Science ,Jangaon,Andhra Pradesh,India under contract no: (08716202101).

REFERENCES

[1] K. Awasthi, K. S. Srivastava, and R. C. Mittal, "An improved timestamp-based remote user authentication scheme," *Computers and Electrical Engineering*, vol. 37, pp. 869-874, 2011.

[2] C. C. Chang and C. Y. Lee, "A smart card-based authentication scheme using user identify cryptography," *International Journal of Network Security*, vol. 15, no. 2, pp. 139-147, 2013.

[3] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication: Smart card," *Computer & Security*, vol. 21, pp. 372-375, 2002.

[4] S. T. Hsu, C. C. Yang, and M. S. Hwang, "A study of public key encryption with keyword search", *International Journal of Network Security*, vol. 15, no. 2, pp. 71-79, 2013.

[5] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," I*EEE Transactions on Consumer Electronics*, vol. 46, pp. 28-30, 2000.

[6] L. Lamport, "Password authentication with insecure communication," *Communication of ACM*, vol. 24, pp. 770-772, 1981.

[7] J. Y. Liu, A. M. Zhou, and M. X. Gao, "A new mutual authentication scheme based on nonce and smart cards," *Computer Communications,* vol. 31, pp. 2205–2209, June 2008.

[8] R. L. Rivest, A. Shamir, and L.M. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120-126, Feb. 1978.

[9] J. J. Shen, C. W. Lin, and M. S. Hwang, "A modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, pp. 414-416, 2003.

[10] H. M. Sun, "An efficient remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, pp. 958-961, 2000.