A Review and Cryptanalysis of Similar Timestamp-Based Password Authentication Schemes Using Smart Cards

Al-Sakib Khan Pathan

Department of Computer Science and Engineering, BRAC University
66 Mohakhali Dhaka 1212, Bangladesh
spathan@ieee.org, spathan@bracu.ac.bd

***Abstract*:** The intent of this paper is to review some timestamp-based password authentication schemes using smart cards which have similar working principles. Many of the proposed timestamp-based password authentication schemes were subsequently found to be insecure. Here, we investigate three schemes with similar working principles, show that they are vulnerable to tricky forgery attacks, and thus they fail to ensure the level of security that is needed for remote login procedure using smart cards. Though there are numerous works available in this field, to the best of our knowledge this is the first time we have found some critical flaws in these schemes that were not detected previously. Along with the proofs of their flaws and inefficiencies, we note down our solution which could surmount all sorts of known attacks and thus reduces the probability of intelligent forgery attacks. We provide a detailed literature review how the schemes have been developed and modified throughout years. We prove that some of the schemes which so far have been thought to be intractable are still flawed, in spite of their later improvements.

***Keywords*:** Authentication, Cryptanalysis, Forgery Attack, Secure, Smart Card**.**

1. Introduction

Remote server in a Client/Sever system requires password from the user to verify the legitimacy of *access-requesting* user. The password given by the user could not be transmitted to the server in plain text format because of security reasons. Usually, we consider the presence of insecure channels for the communications between remote server and user, where an eavesdropper could tap the transmitted messages and may try to forge false messages later at a suitable time. To secure the communications between remote server and user, several timestamp-based password authentication schemes have been proposed so far to protect users' passwords while transmitting those over insecure channels.

Starting from 1999, by this time a wide variety of timestamp-based password authentication schemes have been proposed, most of which fail to guarantee the level of security needed for remote password authentication procedure. Once one scheme had been proposed, for some time it was thought to be secure but later was found as faulty. Up to today, there are some schemes that have remained unchallenged and have been thought to be flawless. However, after detailed analysis of all those schemes, we have found the weaknesses for some of the unchallenged solutions. In this paper, we note down a brief history of timestamp-based password authentication schemes and show that many of them are inefficient as they cannot provide the required level of security that the authors claimed to achieve in their proposals. It should be noted that, in this paper we used the names of the authors to distinguish different schemes.

The major contributions of this paper are:

1. A detailed literature review of the timestamp-based password authentication schemes using smart cards.
2. Cryptanalysis and pointing out the inefficiencies of Wang-Li's [1] improved scheme.
3. Cryptanalysis of the password authentication scheme proposed by Yang, Wang, and Chang [2].
4. Cryptanalysis of Kim et al.'s [3] improved password authentication scheme.
5. Comments on the improved schemes, pointing out their weaknesses, and suggesting the feasible solution.

The rest of the paper is organized as follows; Section 2 presents the literature review and relevant works that motivated us to write this paper, Section 3 recaps the basic scheme proposed by Yang and Shieh, Section 4 presents the cryptanalysis of Wang-Li's scheme, Section 5 presents the cryptanalysis of Yang-Wang-Chang's scheme, Section 6 shows the flaws of Kim et al.'s improved scheme, Section 7 talks about the crucial points for the flaws in the schemes, Section 8 notes down our improved solution for the completeness of this paper, and Section 9 concludes the paper delineating the achievements from this work.

2. Literature Review and Motivation

In 1999, Yang and Shieh [4] proposed two password authentication schemes with smart cards one of which was the timestamp-based password authentication scheme. In 2002, Chan and Cheng [5] showed that [4] 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. [6] presented a cryptanalysis of [4] and showed a different type of attack than that of [5] and also proposed an enhanced scheme which they claimed to withstand Chan-Cheng attack and the attack that they demonstrated in their paper. But later, [7] showed that Fan et al.'s scheme was still insecure and vulnerable to forged login attack. Again, [8] showed two other attacks on Fan et al.'s enhanced scheme. Shen et al. [9] came up with one enhanced scheme based on [4] which they claimed to be efficient enough to protect the authentication process from forged login or forged server attacks. Unfortunately, later [10], [11], [12] and, [13] showed that the improved scheme proposed by Shen et al. was still vulnerable to the forgery attacks.

Wang and Li [1] proposed a separate improved scheme based on Yang-Shieh scheme [4] assuming that the remote host possesses extra storage facilities for storing some

information.

Again, Yang, Wang, and Chang [2] proposed an alternative improved solution considering the attacks showed in [5] and [10]. Later Kim et al. [3] showed two attacks on Yang-Wang-Chang's scheme. In addition to those two attacks, we have devised two more attacks that could be launched against [2].

So far Kim et al.'s scheme has remained unchallenged for timestamp-based authentication procedure. After analyzing their scheme we have again found that, even Kim et al.'s improved scheme is vulnerable. We prove in this paper that our recently proposed solution [13] has the least probability of such attacks.

The long sequence of all these works motivated us to review all of these so that a clear picture could be deduced for this research field. Hence with our work, we have investigated almost all the related schemes to analyze the weaknesses of various timestamp-based password authentication schemes.

3. Review of Basic Yang-Shieh Scheme

Before presenting the proofs of the vulnerabilities of various schemes, first we note down the basic timestamp-based password authentication scheme that was proposed by Yang and Shieh in 1999 [4].

3.1 Basic Terms and Preliminaries

U_i – The ith user seeking for authentication

KIC – The Key Information Center

ID_i – The chosen 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 Basic Timestamp-Based Password Authentication Scheme

This scheme has mainly three phases; registration, login, and verification phase. Here, we mention the steps of all the phases in detail.

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 arbitrarily chosen 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 $n = p \cdot q$

3. A prime number *e* and an integer *d* are chosen which satisfy, $e \cdot d \equiv 1 \bmod (p\text{-}1)(q\text{-}1)$, 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. A value h_i for U_i is computed such that, $h_i = g^{PW_i \cdot d} \bmod n$ and smart card's identifier CID_i is generated.

7. 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 by the user. After that, the smart card performs the following operations:

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

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

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 and CID_i. If the format of any of these is incorrect, the server rejects the request.

2. Checks whether the condition $(T' - T) \le \Delta T$ 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 this condition is violated, the server rejects the request.

4. Checks the equation, $Y_i^e = ID_i \cdot X_i^{f(CID_i, T)} \bmod n$. If it holds, then the remote server accepts the login request and gives access to U_i. Otherwise, it rejects the login request.

4. Cryptanalysis of Wang-Li's Improved Scheme

Wang and Li [1] noticed that the forged login attacks proposed by Chan-Cheng [5] and Fan et al. [6], would not work without the value of $f(CID_i, T_c)$, where T_c is the timestamp of the attacker's login request. To prevent the attacker from getting the value of CID_i in plaintext, they proposed a modification of approach that is, in the login phase $f(CID_i)$ should be computed in addition to X_i and Y_i, and instead of CID_i, the value of $f(CID_i)$ should be sent with the login request message for verification. To facilitate this modification, they assumed that, extra storage capabilities are available in the remote host for keeping the values of all CID_is. This requirement of extra storage surely makes this scheme inefficient compared to the other alternative solutions. Another drawback is that their scheme

provides only unilateral authentication, where the server messages are always thought to be fully secure. Moreover, we have found that their modified scheme could also be broken with two types of tricky forgery attacks. Here we mention the proofs of those attacks.

4.1 First Type of Forged Message Attack

1. The attacker intercepts the login request message from a valid user and gets it as, M = { ID_i, $f(CID_i)$, X_i, Y_i, n, e, g, T}.

2. It chooses two prime numbers p_f and q_f, and then computes a new composite number $n_f = p_f.q_f$.

3. Chooses a prime number e_f and d_f so that they satisfy, $e_f \cdot d_f \equiv 1 \bmod (p_f - 1)(q_f - 1)$.

4. Sets, $X_f = 1$ and $Y_f = ID_i^{d_f} \bmod n$.

5. Sends the forged login request message, M_f = { ID_i, $f(CID_i)$, X_f, Y_f, n_f, e_f, g, T_f}, where T_f is the attacker's attack launching timestamp.

6. This false message could pass the verification phase in the remote server because,

$$Y_f^{e_f} = ID_i^{d_f \cdot e_f} \bmod n = ID_i \bmod n$$

and,

$$ID_i \cdot (X_f)^{f(CID_i, T_f)} \bmod n = ID_i \cdot (1)^{f(CID_i, T_f)} \bmod n = ID_i \bmod n$$

4.2 Second Type of Forgery Attack

1. The attacker intercepts the login request message from a valid user and gets it as, M = { ID_i, $f(CID_i)$, X_i, Y_i, n, e, g, T}.

2. Sets e_f = 1, $X_f = 1$ and $Y_f = ID_i \bmod n$.

3. Sends the login request to the remote server, M_f = { ID_i, $f(CID_i)$, X_f, Y_f, n, e_f, g, T_f}, where T_f is the timestamp of attackers login request.

4. This trial succeeds as,

$$Y_f^{e_f} = (ID_i)^1 \bmod n = ID_i \bmod n$$

and,

$$ID_i \cdot (X_f)^{f(CID_i, T_f)} \bmod n = ID_i \cdot (1)^{f(CID_i, T_f)} \bmod n$$

$$= ID_i \bmod n$$

Both of these attacks could be launched because there is no step in their scheme which could verify the values of the parameters included in the login request message. Just by setting up the necessary values, an attacker can succeed to break Wang-Li's scheme. The first of these attacks could be launched because the parameter values are sent in open text and the attacker could replace the values for a forged message. The second attack could be resisted if there is another extra step to verify the value of e, X_f along with the values of ID_i and CID_i.

So in a nutshell, in this section we have pointed out that,

1. Wang-Li's scheme is inefficient because of the requirement for extra storage which could be huge for supporting a large number of users.

2. Their scheme is vulnerable to two types of simple forgery attacks as the parameters passed with the login request are open and could be replaced by an attacker according to its needs. As there is no checking step for validating the parameters or structures of parameters, the scheme could be broken.

5. Cryptanalysis of Yang-Wang-Chang's Improved Scheme

In this section, we mention four different types of forgery attacks on Yang-Wang-Chang password authentication scheme. Kim et al. [3] pointed out first two attacks which we mention here. In addition, we show two more novel attacks on Yang-Wang-Chang scheme to prove that, their scheme is fairly vulnerable in contrast of their claim of its intractable security [14].

5.1 Attack Based on [8] and [10]

As the attacker can 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 a forgery attack as follows:

1. Let T_a be the timestamp for the attacker's login request. Use the Extended Euclidean algorithm to compute gcd(e, T_a) = 1 that is, e and T_a are relatively prime. Let, u and v be the coefficients computed by the extended Euclidean algorithm such that, e.u – T_a.v = 1

2. Compute $X_f = ID_i^{CID_i \cdot v} \bmod n$

3. Compute $Y_f = ID_i^{CID_i \cdot u} \bmod n$

4. Send the forged login request message M_f = { ID_i, CID_i, X_f, Y_f, n, e, g, T_a} and this request will eventually pass the authentication phase as,

$$Y_f^e = (ID_i^{CID_i \cdot u})^e \bmod n$$

$$= (ID_i^{CID_i})^{eu} \bmod n$$

$$= (ID_i^{CID_i})^{1+T_a \cdot v} \bmod n$$

$$= ID_i^{CID_i} \cdot (ID_i^{CID_i})^{T_a \cdot v} \bmod n$$

$$= ID_i^{CID_i} \cdot (X_f)^{T_a} \bmod n$$

In fact, this attack could be extended for gcd(e,a)=2,3,….

instead of only gcd(e, a) = 1. Hence, the claim that their improved scheme is resistant to Sun et al.'s [10] attack or similar attacks is not correct.

5.2 Forgery Attack Based on Yang et al.'s [11] Attack

In this attack the attacker intercepts the message, $M = \{ID_i, CID_i, X_i, Y_i, n, e, g, T\}$ and then:

1. Finds a value w such that it satisfies, $w \cdot T_a = T$, where T_a denotes the attacker's attack launching time.

2. Computes the value, $X_f = X_i^w = g^{r_i \cdot PW_i \cdot w} \bmod n$

3. Now, the attacker constructs the forged login request message as, $M_f = \{ID_i, CID_i, X_f, Y_i, n, e, g, T_a\}$

This forged message eventually passes the authentication phase because:

$$Y_i^e = (S_i \cdot h_i^{r_i \cdot T})^e \bmod n$$

$$= (ID_i^{CID_i \cdot d} \cdot g^{PW_i \cdot d \cdot r_i \cdot T})^e \bmod n$$

$$= ID_i^{CID_i} \cdot g^{PW_i \cdot r_i \cdot T} \bmod n$$

and,

$$ID_i^{CID_i \cdot} \cdot (X_f)^{T_a} \bmod n = ID_i^{CID_i \cdot} \cdot g^{r_i \cdot PW_i \cdot w \cdot T_a} \bmod n$$

$$= ID_i^{CID_i \cdot} \cdot g^{PW_i \cdot r_i \cdot T} \bmod n$$

5.3 Our Novel Impersonation Attack

Based on the attacks shown in [13] and [14], an attacker can impersonate a legitimate user U_i, with identity ID_i, by using the following procedure:

1. It Intercepts the login request message $M = \{ID_i, CID_i, X_i, Y_i, n, e, g, T\}$.

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 in their scheme, $S_i = ID_i^{CID_i \cdot d} \bmod n$ and here, $S_k = ID_f^{CID_i \cdot d} \bmod n = ID_i^{-CID_i \cdot d} \bmod n$, the attacker can compute S_i as, $S_i = S_k^{-1} \bmod n$

5. Then, the attacker chooses a random integer y.

6. Sets, $X_f = y^e \bmod n$ and $Y_f = S_i \cdot y^{T_f} \bmod n$, 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,

$$Y_f^e = (S_i \cdot y^{T_f})^e \bmod n$$

$$= (S_k^{-1} \cdot y^{T_f})^e \bmod n$$

$$= ID_i^{CID_i \cdot d \cdot e} \cdot y^{T_f \cdot e} \bmod n$$

$$= ID_i^{CID_i} \cdot (X_f)^{T_f} \bmod n$$

5.4 Our Novel Forgery Attack

The attacker can get the values of ID_i and CID_i from the login request message from the valid user, and the smart card identifier CID_i is a fixed value for a particular login request from a user. The attacker could launch an attack using the following steps:

1. The attacker finds a value T_f such that, $T \cdot T_f \equiv 1 \bmod n$ where T_f is the attacker's login timestamp

2. It chooses a random integer *k* and computes, $Y_f = k^{T_f} \bmod n$ and sets $X_f = ID_i^{-CID_i \cdot T} \cdot k^e \bmod n$

3. Sends the forged login request message, $M_f = \{ID_i, CID_i, X_f, Y_f, n, e, g, T_f\}$

4. The attacker could pass the authentication phase as,

$$Y_f^e = k^{e \cdot T_f} \bmod n$$

and,

$$ID_i^{CID_i} \cdot (X_f)^{T_f} \bmod n$$

$$= ID_i^{CID_i} \cdot (ID_i^{-CID_i \cdot T} \cdot k^e)^{T_f} \bmod n$$

$$= ID_i^{CID_i} \cdot ID_i^{-CID_i \cdot T \cdot T_f} \cdot k^{e \cdot T_f} \bmod n$$

$$= ID_i^{CID_i} \cdot ID_i^{-CID_i} \cdot k^{e \cdot T_f} \bmod n$$

$$= k^{e \cdot T_f} \bmod n$$

6. Cryptanalysis of Kim et al.'s Improved Scheme

In 2005, Kim et al. [3] proposed an improvement on Yang-Wang-Chang's [2] timestamp-based password authentication scheme. In their proposal, they modified some of the calculations and checking steps keeping the basic working method same as the previous scheme. In their scheme, they kept the registration phase exactly similar as Yang-Wang-Chang scheme. In the login phase, X_i and Y_i are calculated differently as, $X_i = g^{PW_i \cdot r_i \cdot e} \bmod n$ and $Y_i = h_i^{r_i} \cdot S_i^T \bmod n$ where, T is the current timestamp. In

the verification phase, for the final checking step the equation was changed to, $Y_i^e = X_i^d \cdot ID_i^{CID_i \cdot T} \bmod n$. So far, Kim et al.'s scheme has not been challenged and has been thought to be fully secure. After analyzing their scheme, we have found that even it could be broken with a tricky forgery attack based on an attack presented in [13].

Our Novel Impersonation Attack on Kim et al. Scheme. An attacker can impersonate a legitimate user by using the following procedure:

1. It Intercepts the login request message $M = \{ID_i, CID_i, X_i, Y_i, n, e, g, T\}$.

2. Computes, $ID_f = ID_i^{-1} \bmod n$

3. Now, the attacker submits this identity ID_f and a chosen 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 in their scheme,

$$S_i = ID_i^{CID_i \cdot d} \bmod n$$

and here, $S_k = ID_f^{CID_i \cdot d} \bmod n = ID_i^{-cid_i \cdot d} \bmod n$, the attacker can compute S_i as, $S_i = S_k^{-1} \bmod n$.

5. Then, the attacker chooses a random integer *y*.

6. Sets, $X_f = 1$ and $Y_f = S_i^{T_f} \bmod n$, where T_f is the timestamp for the login request from the attacker and then 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,

$$Y_f^e = (S_i^{T_f})^e \bmod n$$

$$= S_k^{-T_f \cdot e} \bmod n$$

$$= ID_i^{CID_i \cdot d \cdot e \cdot T_f} \bmod n$$

$$= ID_i^{CID_i \cdot T_f} \bmod n$$

and,

$$X_i^d \cdot ID_i^{CID_i \cdot T_f} \bmod n = (1) \cdot ID_i^{CID_i \cdot T_f} \bmod n$$

$$= ID_i^{CID_i \cdot T_f} \bmod n$$

This attack could be resisted by imposing another extra step in the verification step to check the values of the parameters passed via the login request message.

7. Comments on the Improved Authentication Schemes

All the improved schemes mentioned here have a common drawback that is, none of them provides bilateral verification. All of the mentioned schemes, Wang-Li, Yang-Wang-Chang, and Kim et al. schemes consider that the server message is always secure. But, while using insecure channels, an ideal environment might not exist all the times. Hence, a bilateral verification mechanism is necessary where the user would also get the opportunity to verify the messages sent from the remote server. Most of these schemes are vulnerable because of the passing of the critical parameters with the login request message in plaintext. As there is no mechanism to conceal the actual values of ID_i, CID_i, X_i, Y_i, *n*, *e*, *g*, *T*, some attacks could be launched simply by replacing the values with necessary terms and conditions. To resolve the problems and inefficiency of all these schemes we have recently proposed our improved scheme and proved that it is not tractable by any of the known attacks.

8. Our Established Solution for Overcoming the Flaws

For the completeness of this paper, we present our scheme [13] here which so far has withstood all types of scrutiny and cryptanalysis. None of the above mentioned attacks or any other known attacks could be launched against our scheme. Also this scheme ensures bilateral verification. Hence, to the best of our knowledge, this is the best solution among all the alternate solutions (that use the similar working principles).

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 $n = p \cdot q$

3. A prime number *e* and an integer *d* are chosen which satisfy, $e.d \equiv 1 \bmod (p-1)(q-1)$, 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, $h_i = g^{PW_i \cdot d} \bmod n$.

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. 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:

$$X_i = g^{r_i \cdot PW_i} \bmod n$$

$$Y_i = S_i \cdot h_i^{r_i \cdot f(CID_i, T)} \bmod n$$

$$Z_i = X_i \oplus CID_i \oplus f(CID_i, Y_i)$$

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) ≤ 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 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, $Y_i^e = ID_i \cdot X_i^{f(CID_i, T)} \bmod n$. 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″) ≤ ΔT, 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.

The details of security analysis and strengths of our improved scheme are mentioned in [13]. Here, we mention our scheme as a reference.

9. Conclusion

In this paper, we have presented a detailed literature review of the timestamp-based password authentication schemes using smart cards. We have investigated a number of schemes, noted how they have been developed and proved some of their flaws and inefficiencies. For the completeness of the paper, we have also mentioned our recently proposed solution which to the best of our knowledge is the best solution up to this moment.

References

[1] Y. Wang, J. Li, "Security Improvement on a Timestamp-Based Password Authentication Scheme," IEEE Transactions on Consumer Electronics, Vol. 50, No. 2, pp. 580-582, 2004.

[2] C.C. Yang, R.-C. Wang, T.-Y. Chang, "An improvement of the Yang-Shieh password authentication schemes," Applied Mathematics and Computation, 162, Elsevier, pp. 1391-1396, 2005.

[3] K.-W. Kim, J.-C. Jeon, K.-Y. Yoo, "An improvement on Yang et al.'s password authentication schemes," Applied Mathematics and Computation, 170, Elsevier, pp. 207-215, 2005.

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

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

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

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

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

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

[10] H.-M. Sun, H.-T. Yeh, "Further Cryptanalysis of a Password Authentication Scheme with Smart Cards," IEICE Transactions on Communications, Vol. E86-B, No. 4, pp. 1212-1215, 2003.

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

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

[13] A.-S.K. Pathan, C.S. Hong, "A Security Enhanced Timestamp-Based Password Authentication Scheme Using Smart Cards," IEICE Transactions on Information and Systems, Vol. E90-D, No. 11, pp. 1885-1888, November, 2007.

[14] A.-S.K. Pathan, C.S. Hong, "Cryptanalysis of Yang-Wang-Chang's Password Authentication Scheme with Smart Cards," Proceedings of the 10th International Conference on Advanced Communication Technology (IEEE ICACT 2008), Volume III, Phoenix Park, Korea, pp. 1618-1620, February 17-20, 2008.