The International Journal Research Publication's
ISSN:2251 1563
Research Journal of Science & IT Management

An enhanced authentication scheme based remote user password using smart card

Ahmed Y.F. Alsahlani
School of Computer Science and Technology, Huazhong University of Science and Technology
Wuhan, China
&
Songfeng Lu
School of Computer Science and Technology, Huazhong University of Science and Technology
Wuhan, China

Abstract
Authentication using smart card is a mechanism to verify the legitimacy of the user over insecure communication. Recently, Chen et al. figured out some weaknesses in previously published schemes, they proposed a robust smart card based remote user password authentication scheme. They claimed that,their scheme is efficient and can ensure the session key forward secrecy. We analyzed their scheme, we found that, it cannot detect incorrect password within login phase. Furthermore, the user required to communicate with the server to change or update his/her password. Besides, it cannot securely forward the secrecy. In this paper, we propose a scheme to overcome the aforesaid weaknesses and produce an enhanced authentication scheme based remote user password using smart card. We use a TRPT (Temporary Registration Password Technique) within registration phase to secure user's password. Our proposed scheme can resist various malicious attacks, achieve mutual authentication, user can choose and change his/her password freely without need to communicates with the server, securely forward secrecy, and the login password never been exposed or transferred over channel. We show that, our proposed scheme achieved the goal, and it is more legible to practical use compared to the other related schemes.

Keywords: Authentication, Smart Card, Password, Temporary Password, key agreement, Security, Remote access

1. Introduction

Internet technology and online services become very important as human daily life needs. Online services such as online shopping, internet banking, online gaming, e-learning, e-health, etc, these services make human life more convenient. At the same time accessing these online services over insecure environments is a subject of security and privacy risks. Thus, Authentication protocols are deployed to verify the legitimacy of the remote user and ensure trustworthy of the communication. Authentication factors generally categorized as: (1). Something you know, like password. (2). Something you possess, like smart card. (3). Something you are, like finger print, iris scan, and voice print, etc.The major difficulties is to address the vast possibilities of an *Adv.* to gain information and compromising the services.In general, a strong authentication scheme using smart card based password should encompasses the security requirements and withstand a wide spectrum of attacks such as forgery attacks, password guessing attacks, replay attacks, parallel session attacks, impersonation attacks, etc. Whereas, the functional requirement of authentication scheme listed as:(1). Friendly change password, so the user can freely changes his/her password without need to communicate with the server; (2). Mutual authentication between both user and sever sides to verify the legality of each other; (3). Share a session key between the user and the server to ensure the secret communication; (4). User identity and password does not need to be stored in verification table, or embedded into the smart card; (5). Detect unauthorized access attempt at login phase.

In 1981, Lamport proposed well-known password based remote user authentication over insecure communication. Then, many researchers adopted the smart card in their schemes [2–10].

In 2009, Xu et al. [11] proposed two factors smart card based password scheme. They claimed that their scheme can withstand attacks while the content stored in the smart card is disclosed. However, in

2010 Sood et al. [12] pointed out that, the scheme of Xu et al. is vulnerable to offline password guessing and forgery attacks. Sood et al. summarized that, a good password based authentication scheme should protect the users from attacks such as (1) forgery attacks;(2) malicious user attacks; (3) stolen smart card attacks; (4) offline dictionary attacks; (5) denial of service attacks;(6) Replay attacks; (7) server spoofing attacks; (8) leak of verifier attacks; (9) online dictionary attacks; (10) man in the middle attacks. Then, an improved scheme proposed by Sood et al. [12], they claimed that, their scheme not only inherits the merits of the scheme of Xu et al., but also avoid its discovered security flaws.

In 2010 Song et al. [13], found that, in Xu et al.'s scheme an internal user can easily execute an impersonation attacks by retrieving data from his own smart card. Recently, Chen et al., in [14], found that the schemes presented by Song [13], Sood et al. [12] and Xu et al. [11] are insecure. In Song's scheme, the secret key of the symmetric encryption operation is composed of the user identity and the secret key of the server, both are permanent and no way to change them in the scheme, so the *Adv.* can execute an offline dictionary attack on the stolen smart card to guess the user password and by pass Song's scheme. Sood et al.'s scheme, does not provide mutual authentication between the user and the server, this means the user will not verify the validity of the server. Chen et al. in [14], proposed a robust smart card based remote user password authentication scheme. Li et. al [15], proposed their scheme over Chen et.al's scheme to overcome some flaws. In this paper ,we revisited Chen et al.'s scheme, we found that, their scheme cannot ensure forward secrecy, unnecessary computation and communication cost are wasted in case of incorrect password is entered. Since, the user's password verified at the server side. Furthermore, the password change phase in their scheme is inefficient because it requires to communicate with server. Besides, an *Adv.* can easily steal user identity then perform forgery attacks. To overcome aforementioned flaws in Chen et al.'s scheme, we propose an enhanced authentication scheme based remote user password using smart card with TRPT.
The rest of this paper is organized as follows: in Section 2, Cryptanalysis of Chen et al.'s scheme. In section 3, the proposed scheme. In Section 4, security analysis of the proposed scheme. In Section 5, the performance analysis of the proposed scheme. Finally, our conclusion in Section 6.

Table 1.The notations of this paper

Notation	Description	Notation	Description
U	The user	ΔT	The maximum transmission delay
S	The authentication server	p, q	Two large prime numbers
Adv.	An attacker	Z_q	The ring of integers modulo q
ID_u	The identity of U	Z_q^*	The multiplicative group of Z_q
TPW_u	Temporary password of U	$H(.)$	Cryptographic one way hash function
PW_u	The login password of U	$\|\|$	The message concatenation operation
x	The master secret key of S	- - - →	Secure channel
T	The timestamp	⟶	Public channel

2.Cryptanalysis of Chen et al.'s scheme
In this section, we will discuss the weaknesses and flaws of Chen et al.'s robust smart card based remote user password authentication scheme[14]. Their scheme consist of four phases: initialization, registration, login, authentication, and the password change activity. Figure 1. Shows the detailed steps of Chen et al.'s scheme phases.
The notation used through this paper are described in Table 1.

2.1 *Forwarding secrecy problem*
In Chen et al's scheme [14]. They claimed that, the *Adv.* cannot calculates any previous session key even if the master secret key of the server x is compromised. We analysis their scheme, we find that, their scheme cannot really ensure perfect forward secrecy. Assume that, an *Adv.* has obtained the

master secret key x from a compromised server, and previously transmitted message $\{ID_u, D_i, M_i, T_i\}$ has eavesdropped. So, an *Adv.* can simply computes the shared session key $Skey = H(H(ID_u)^x . D_i \ mod\ p) = h(C_i D_i \ mod\ p) = H(W_i)$. the *Adv.* performs this attack using $x, ID_u,$ and D_i , so there is no need to find the random number α from $D_i = H(ID_u)^{\alpha} \ mod\ p$ .Therefore, if the *Adv.* can eavesdrop the communication messages which are encrypted using session key $Skey$, so he can really access the content of the communication messages. Hence, Chen et al's scheme does not securely forward secrecy.

User	Channel	Server
Chooses ID_u , PW_u	*Registration request* $\{ID_u$, $PW_u\}$ ⇢	*Chooses* $\in Z_q^*$, $H(.)$. $B_i = H(ID_u)^{(x+PW_u)} \ mod\ p$
	Registration acknowledgement *Smart card* ⇠	*Smart card* ⇠ $\{ B_i, H(.), p, q \}$
Inputs ID_u , PW_u *Select* $\alpha \in_R Z_q^*$ $C_i = B_i / H(ID_u)^{PW_u} mod\ p$ $D_i = H(ID_u)^{\alpha} \ mod\ p$ $W_i = CiDi \ mod\ p$ $M_i = H(ID_u \| C_i \| D_i \| W_i \| T_i)$	*Login request* $\{ID_u$,$D_i, M_i, T_i\}$ ⇢	*Verify* ID_u *and* T_i $C_i' = H(ID_u)^x \ mod\ p$ $Wi' = Ci'Di \ mod\ p$ $M_i = H(ID_u \| C_i' \| D_i \| W_i' \| T_i)$?. $M_s = H(ID_u \| W_i' \| T_s)$
Check ID_u and T_s $M_s = H(ID_u \| W_i \| T_s)$?. *Session key* $Skey = H(W_i)$	*Mutual authentication* $\{ ID_u, M_s, T_s\}$ ⇠	*Session key* $Skey = H(W_i')$

Figure 1. Chen et. al's scheme

2.2 *Incorrect password detection*

In general, an authorized user may enters incorrect password, while he/she attempts to access a certain online resources. Such mistake cannot detected within login phase of Chen et al's scheme. This means that, the smart card performs login computation and create login request message which contain incorrect password and send it to the server, then the server will detect this wrong entered password after doing some computations within authentication phase. This can be considered as an inherent flaws in login and authentication phases of Chen et al's scheme .this flaw result waste in computation and communication cost. The details shown as follows:

Suppose that, the user U entered wrong password PW_u^* in the login phase, so the smart card chooses $\alpha \in_R Z_q^*$, then computes:

$C_i^* = B_i / H(ID_u)^{PW_u^*} mod\ p = H(ID_u)^{(x+PW_u-PW_u^*)} \ mod\ p$,

$D_i^* = H(ID_u)^{\alpha} mod\ p$,

$W_i^* = C_i^* D_i^* mod\ p = H(ID_u)^{(x+PW_u-PW_u^*+\alpha)} \ mod\ p$,

$M_i^* = H(ID_u \| C_i^* \| D_i^* \| W_i^* \| T_i)$. Where T_i is the current timestamp of U. The smart card sends the login message $\{ID_u, D_i^*, M_i^*, T_i\}$ to S. upon receiving login request , S checks both the format of identity ID_u and the validity of T_i compared to T_i' ,where T_i' is the current timestamp of S . Then, S computes $C_i' = H(ID_u)^x \ mod\ p$; $W_i' = C_i' D_i^* mod\ p = H(ID_u)^{(x+\alpha)} \ mod\ p$, and $M_i' = H(ID_u \| C_i' \| D_i \| W_i' \| T_i)$. Comparing these results show that, $M_i^* \neq M_i'$ since $C_i^* \neq C_i'$ and $Wi^* \neq Wi'$. Therefore, this login request will be rejected by S after all aforementioned computation and communication.

2.3. *Inefficient password change activity*

In Chen et al's scheme, the remote user U need to communicates with server every time he/she wants to change or update his/her password. Besides that, U may enters a wrong password as mentioned in section 2.2.in this case, U performs both login and authentication phases to check the password validity. Then, S keep rejecting login requests as wrong entered password, until U enters a valid password. Then login request is accepted, as a correct password entered. So, U inputs his/her new password. Then, the smart card replaces $B_i$with B_i^{new} . Such scheme cost unnecessary computations and communications. The aforementioned, obviously show the inefficient password change activites of Chen et al's scheme.

3. The proposed scheme

In this section, we propose an enhanced authentication scheme based remote user password using smart card to overcome the mentioned weaknesses of Chen et al.'s scheme. Figures 2,3 show the summary of registration, login and authentication phases respectively of our proposed scheme. Our enhanced scheme contain four phases as follows.

- registration phase
- login phase
- authentication phase
- password change/update phase

In the beginning, the server S chooses two large prime numbers p and q, where $p = 2q + 1$; S chooses *x* as a master security key where $\in Z_q$, x will be kept securely in S, finally S chooses a proper cryptographic one way hash function $H(.): \{0,1\}^* \rightarrow Z_p^*$. The details of our scheme is as follows:

User	Secure Channel	Server
Chooses ID_u,TPW_u , b $EID_u = H(ID_u \| \| b)$	*Registration request* $\{EID_u, TPW_u\}$	*Chooses* $x \in Z_q$, $H(.)$ $ID_s = H(EID_u \| \| x)$,*checks* ID_s $A_i = H(EID_u \| \| TPW_u)^{TPW_u} \bmod p B_i = H(EID_u)^{(x+TPW_u)} \bmod p$
$A_i^{'} = H(EID_u \| \| TPW_u)^{TPW_u} \bmod p =? A_i$ *Chooses* PW_u $A_i^{''} = H(EID_u \| \| PW_u)^{PW_u} \bmod p$ $B_i^{'} = \frac{B_i . H(EID_u)^{PW_u}}{H(EID_u)^{TPW_u}} \bmod p$ *Replaces* A_i, B_i *with* $A_i^{''}, B_i^{'}$ *Store b into smart-card*	*Registration Acknowledgement* *Smart card* ← - - - - - - -	*Smart card* ——— $\{A_i, B_i, H(.), p, q\}$

Figure 2. Registration phase of proposed scheme

3.1 Registration Phase

Step 1. U chooses his/her identity ID_u, random number b, andTPW_u , where TPW_u is a temporary password used only at registration phase.

Step 2. U computes:$EID_u = H(ID_u \| \| b)$ then submits both EID_u , andTPW_u to S via secure channel.

Step 3. S computes: $ID_s = H(EID_u \| \| x)$, then check ID_s whether it is already registered so, S requests U to submit a new identity.

Step 4. S computes: $A_i = H(EID_u \| \| TPW_u)^{TPW_u} \bmod p$, $B_i = H(EID_u)^{(x+TPW_u)} \bmod p$.

Step 5. S stores $\{A_i, B_i, H(.), p, q\}$ into the smart card and issues it to U.

Step 6 U Inserts his/her smart card into the card reader, and inputs his/her ID_u and TPW_u . the smart card computes:

$A_i^{'} = H(EID_u||TPW_u)^{TPW_u} \ mod\ p$, then compare $A_i^{'}$ with A_i .if they are not match, the smart card terminates this session. Otherwise, Uchooses fresh login password PW_u. Then the smart card computes:
$A_i^{''} = H(EID_u||PW_u)^{PW_u} \ mod\ p$,
$B_i^{'} = \frac{B_i .H(EID_u)^{PW\,u}}{H(EID_u)^{TPW\,u}} \ mod\ p$.
Step 7. The smart card replaces A_i, B_i with $A_i^{''}, B_i^{'}$ respectively .Then the number b stored in the smart card.

3.2 Login Phase

Step 1. U inserts his/her smart card into the smart card reader. Then inputs his/her ID_u,and PW_u . The smart card computes: $EID_u = H(ID_u||b)$; $A_i^{'} = H(EID_u||PW_u)^{PW_u} \ mod\ p$, and verifies $A_i^{'} =? A_i$, if not equal ,the smart card terminates the session.
Step 2. The Smart card chooses $\alpha \in_R Z_q^*$ and computes: $C_i = \frac{B_i}{H(EID_u)^{PW\,u}} \ mod\ p$,$D_i = h(EID_u)^{\alpha} \ mod\ p$,
$M_i = H(EID_u||C_i||D_i||T_i)$, where T_i is the current time of U.
Step 3. The smart card create a login request message $\{EID_u, D_i, M_i, T_i\}$ and sends it to S.

User	Public Channel	Server
Inputs ID_u , PW_u $A_i^{'} = H(H(ID_u\|\|b)\|\|PW_u)^{PW_u} \ mod\ p$ $=? A_i$ *Chooses* $\alpha \in_R Z_q^*$ $C_i = \frac{B_i}{H(EID_u)^{PW_u}} \ mod\ p$ $D_i = H(EID_u)^{\alpha} \ mod\ p$ $M_i = H(EID_u\|\|C_i\|\|D_i\|\|T_i)$	*Login request* $\{EID_u, D_i, M_i, T_i\}$ →	*Verifies* T_i , $ID_s = H(EID_u\|\|x)$ $C_i^{'} = H(EID_u)^x \ mod\ p$ $M_i^{'} = H(EID_u\|\|C_i^{'}\|\|D_i\|\|T_i) =? M_i$ *chooses* $\beta \in_R Z_q^*$ $V_i = H(EID_u)^{\beta} \ mod\ p$, $Skey = D_i^{\beta} mod\ p$, $M_s = H(EID_u\|\|C_i^{'}\|\|V_i\|\|Skey\|\|T_s)$
Verifies EID_u ,T_s $Skey^{'} = V_i^{\alpha} mod\ p$ $M_s^{'} = H\left(EID_u\|\|C_i\|\|V_i\left\|\|Skey^{'}\right\|T_s\right) =? M_s$ *Shared session key* $Skey^{'} = Skey = H(EID_u)^{\alpha\beta} \ mod\ p$	*Mutual authentication* ← $\{EID_u, V_i, M_s, T_s\}$	*Shared session key* $Skey^{'} = Skey$ $= H(EID_u)^{\alpha\beta} \ mod\ p$

Figure 3. Login and authentication phases of proposed scheme

3.3 Authentication phase

Step1. Upon receiving login request message $\{EID_u, D_i, M_i, T_i\}$ at time $T_i^{'}$, S validates T_i ,$T_i^{'} - T_i \leq \Delta T$. If T_i is not valid, S terminates the session. Otherwise, S computes $ID_s = H(EID_u||x)$ and checks whether ID_s is already registered. If ID_s is not exist, S terminates the session. Otherwise, S computes: $C_i^{'} = H(EID_u)^x \ mod\ p$,
$M_i^{'} = H(EID_u||C_i^{'}||D_i||T_i)$, and verifies $M_i^{'} \neq? M_i$,if not equal, S terminates login attempt. Otherwise, U is authenticated by S.
Step 2. S chooses $\beta \in_R Z_q^*$ and computes: $V_i = H(EID_u)^{\beta} \ mod\ p, Skey = D_i^{\beta} mod\ p$,
$M_s = H(EID_u||C_i^{'}||V_i||Skey||T_s)$, where T_s is S's current time. S creates mutual authentication message $\{EID_u, V_i, M_s, T_s\}$ and sends it to U.
Step 3.upon receiving the message , smart card validate the EID_u and T_s , $T_s^{'} - T_s \leq \Delta T$, where $T_s^{'}$is the time of receiving mutual authentication message at U side .if any or both EID_u and T_s are not valid so, the smart card terminates the session.

Step 4. The Smart card computes: $Skey' = V_i^{\alpha} mod\ p$, $M_s' = H(EID_u||C_i||V_i||Skey'||T_s)$ .compare M_s'andM_s . If they are not equal, S terminates the session. On the contrary, if $M_s' = M_s$, S is authenticated by U. Furthermore, both S and U shared an agreed session key $Skey = Skey' = H(EID_u)^{\alpha\beta}\ mod\ p$.

3.4. Password Change /Update phase

This phase is invoked on U requests to change his/her password PW_u with a new password PW_{u-new} , it can be performed without need to communicate with S.

Step 1. U inserts his/her smart card into the card reader and submits ID_u, PW_u, then requests to change password

Step 2. The smart card computes: $EID_u = H(ID_u||b)$, $A_i' = H(EID_u||PW_u)^{PW_u}\ mod\ p$. U verifies $A_i' =? A_i$, where A_i is stored in the smart card, if they are not equal, the request is rejected. On contrary, U inputs his/her new password PW_{u-new}

Step 3. The smart card computes:

$$A_{i-new} = H(EID_u||PW_{u-new})^{PW_{u-new}}\ mod\ p$$

$$B_{i-new} = \frac{B_i \,.\, H(EID_u)^{PW_{u-new}}}{H(EID_u)^{PW_u}}\ mod\ p$$

Step 4. The smart card replaces A_i, B_i withA_{i-new} , B_{i-new} respectively, which finishes the password change.

4.Security analysis and discussion

In this section, we analyze the security of the proposed scheme. We show that, our proposed scheme can withstand various attacks, and can overcome aforementioned weaknesses of Chen et al' scheme.

4.1. Protects users anonymity

In our proposed scheme, the login request message $\{EID_u, D_i, M_i, T_i\}$ and the mutual authentication message $\{EID_u, V_i, M_s, T_s\}$ do not include the user identityID_u. Instead, hashed identity EID_u used, where $EID_u = H(ID_u||b)$. So, an adversary cannot map user ID_u to server communications. this shows that, the proposed scheme can protect the user anonymity

4.2. Perfect forward secrecy

We suppose that, U's previous login request message $\{EID_u, D_i, M_i, T_i\}$ and mutual authentication message $\{EID_u, V_i, M_s, T_s\}$ were eavesdropped by an adversary, who attempts to get previous session key $Skey = H(EID_u)^{\alpha\beta}\ mod\ p = D_i^{\beta} mod\ p = V_i^{\alpha} mod\ p$. an adversary either can resolve Diffie-Hellman problem, or has to get randomly choose integers α and β. In fact, to compute α from $D_i = h(EID_u)^{\alpha}\ mod\ p$ and β from $V_i = H(EID_u)^{\beta}\ mod\ p$ are equal to resolving the discrete logarithm problem. Furthermore, if an adversary knows both of the master secret key *x* of the server S, and the password PW_u of the user U, an adversary cannot derive the previous session key $Skey = H(EID_u)^{\alpha\beta}\ mod\ p$. Since, there are no relation between them. So, this analysis can show that, an adversary has no way to get previous session key $Skey$ even when login request message, mutual authentication message ,and the master secret key *x* have been obtained by an adversary. Hence, our proposed scheme can ensure perfect forward secrecy.

4.3. Resist smart card stolen attacks

In our proposed scheme, assume that, an adversary can achieve the smart card's stored parameters $\{A_i, B_i, H(.), p, q\}$, and he can intercept the login request message $\{EID_u, D_i, M_i, T_i\}$. However, an adversary cannot generates a valid faked login message $\{EID_u, D_i, M_i^*, T_i\}$. Because, there is no way to compute secret parameter C_i by using the achieved parameters. Since, it required to know the master secret key *x* of the server, as follow.

$$C_i = \frac{B_i}{H(EID_u)^{PW_u}}\ mod\ p$$

$$= \frac{H(EID_u)^{(x+PW_u)}}{H(EID_u)^{PW_u}} \ mod\ p$$
$$= H(EID_u)^x \ mod\ p \ .$$

Our proposed scheme ensure that, only authorized user with valid identity and login password can create a valid login request message.

4.4. Efficient password change

In our proposed scheme, the user can updates his/her password efficiently after checking the validity of the current password PW_u if the validity of the PW_u is true, the user inputs his/her new passwordPW_{u-new} . Then, the smart card computes A_{i-new} ,B_{i-new} using PW_{u-new} .At the end of these computations the smart card replaces A_i ,B_i with A_{i-new} ,B_{i-new} , respectively. We can see that, password change activity completed at user side without need to communicate with server. Therefore, our proposed scheme produce an efficient password change activity.

4.5. Known key security

In our proposed scheme, if the session key $Skey$ is compromised, it will not be useful to compute other session key $Skey'$ since α and β are random variables and their values are different each new session. Hence, our proposed scheme can provide known key security.

4.6.Forgery attacks

In our proposed scheme, an adversary cannot perform the forgery attacks, because an adversary has to forge a login request message$\{EID_u, D_i, M_i, T_i\}$, which can successfully pass authentication. However, an adversary has no way to computes C_i since both password $PW_u$and parameter $B_i$are not obtained by an adversary. Besides, the secret key x of the server is only known to the server and it is already protected using discrete logarithm problem. Therefore, our proposed scheme can resist forgery attacks.

4.7.Key agreement

In our proposed scheme at authentication phase, both of the user and the server shared a session key $Skey = H(EID_u)^{\alpha\beta} \ mod\ p$, where α and β have variable values in each session. $Skey$used to secure transmitted data between the user and the server.

5. Performance and security requirement analysis

In this section, we evaluate the proposed scheme and compare it to the related schemes, Xu et al [11]; Sood et al [12]; Song[13]; and Chen et al [14]. The comparison of computation cost based on the time complexity of hash function, exponential operation, and multiplication/division operation. Since the login phase and authentication phase are required phases in each user's login attempt, we only focus on these two phases. Table 2. Shows the comparison results.

Table 2. Performance comparisons.

Scheme	Login phase	Authentication phase	Total
Xu et al	$3T_h + 2T_e$	$4T_h + 2T_e$	$7T_h + 4T_e$
Sood et al	$3T_h + 3T_e + 2T_m$	$3T_h + 2T_e + 1T_m$	$6T_h + 5T_e + 3T_m$
Song	$2T_h + 1T_S$	$6T_h + 1T_e + 1T_S$	$8T_h + 1T_e + 2T_S$
Chen et al	$2T_h + 2T_e + 2T_m$	$6T_h + 1T_e + 1T_m$	$8T_h + 3T_e + 3T_m$
Our scheme	$4T_h + 3T_e + 1T_m$	$6T_h + 4T_e$	$10T_h + 7T_e + 1T_m$

T_h : complexity of hash function
T_e : complexity of exponential operation
T_m : complexity of multiplication/division operation
T_S : complexity of symmetric encryption-decryption operation

These results show that, our proposed scheme, needs additional computation cost compared to the mentioned schemes. However, our proposed scheme, achieve perfect forward secrecy, quickly detect wrong entered password within login phase. Besides, login password never been exposed or transmitted over channel. The proposed scheme can resist various attacks. Table 3. Illustrates the functionality and the security attributes of our proposed scheme compared to the related schemes.

Table 3.Functionality and security attributes comparisons of proposed and other related schemes

attributes	Xu et al	Song	Sood et al	Chen et al	The proposed
Smart-card stolen attacks	Yes	No	Yes	Yes	Yes
Insider attacks	No	Yes	No	Yes	Yes
Forgery attacks	No	Yes	Yes	Yes	Yes
Server spoofing attacks	Yes	Yes	No	Yes	Yes
Impersonation attacks	No	No	No	No	Yes
Mutual authentication	No	Yes	No	Yes	Yes
Session-key agreement	Yes	Yes	No	Yes	Yes
Perfect forward secrecy	No	No	No	No	Yes
Quickly detect wrong password	No	No	No	No	Yes
User-side change password	No	No	No	No	Yes
Temporary registration password	No	No	No	No	Yes

6. Conclusion

In this paper, we present an enhanced authentication scheme based remote user password using smart card. We use TRPT (Temporary Registration Password Technique) within registration phase.The temporary password is required to initiate registration request. Then, the user uses a fresh login password which is neither been stored in smart cardnor transmitted over channel, to accomplish the registration phase. In our proposed scheme, the user can change his/her login password freely without need to communicate with server, forthwith detect wrong entered password, achieve mutual authentication, and other security attributes are achieved as mentioned in Section 5. Moreover, our proposed scheme overcome the weaknesses of Chen et al.'s and others related schemes, and resist various malicious attacks. Therefore, our proposed scheme is more secure, efficient, and suitable for practical use compared to the related schemes.

References

[1] L. Lamport. Password authentication with insecure communication. Communications of the ACM, 1981, 24(11): 770-772.
[2] H.M. Sun. An efficient remote use authentication scheme using smart cards, IEEE Transactions on Consumer Electronics, 2000, 46, 958-961.
[3] W.C. Ku, S.M. Chen, Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics, 2004, 50, 204-207.
[4] C.K. Chan, L.M. Cheng. Cryptanalysis of a remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, 2000, 46(4): 992-993.
[5] H.Y. Chien, J.Y. Jan, Y.M. Tseng. An efficient and practical solution to remote authentication: smart card. Computers & Security, 2002, 21(4): 372-375.
[6] C.L. Hsu. Security of Chien et al.'s remote user authentication scheme using smart cards. Computer Standards & Interfaces, 2004, 26(3): 167-169.
[7] M.S. Hwang, L.H. Li, A new remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics, 2000, 46(1): 28-30.

[8] K.U. Wei-Chi, S.T. Chang. Impersonation attack on a dynamic ID-based remote user authentication scheme using smart cards. IEICE Transactions on Communications, 2005, 88(5): 2165-2167.
[9] S,-J. Wang, and Jin-Fu Chang, "Smart card based secure password authentication scheme," Computers &Security,Vol. 15, No. 3, pp. 231-237, 1996.
[10] Chun-I Fan Robust remote authentication scheme with smart cards. Computers & Security, 2005, Vol. 24, Issue 8, 619-628
[11] J. Xu, W.T. Zhu, D.G. Feng. An improved smart card based password authentication scheme with provable security. Computer Standards& Interfaces, 2009, 31(4): 723-728.
[12] S.K. Sood, A.K. Sarje, K. Singh. An improvement of Xu et al.'s authentication scheme using smart cards. in: Proceedings of The Third Annual ACM Bangalore Conference, Bangalore, Karnataka, India, 2010; 15.
[13] R. Song. Advanced smart card based password authentication protocol. Computer Standards & Interfaces 2010; 32(5): 321-325.
[14] B.L. Chen, W.C. Kuo, L.C. Wuu. Robust smart-card-based remote user password authentication scheme. International Journal of Communication Systems, 2014, 27(2): 377-389.
[15] Li X, Niu J, Khurram Khan M, Liao J. An enhanced smart cardbased remote user password authentication scheme. J NetwComputAppl 2013;36(5):1365e71.