Cryptanalysis of Two Efficient Password-based Authentication Schemes Using Smart Cards

Ying Wang and Xinguang Peng
(Corresponding author: Xinguang Peng)

Department of computer science and technology, Taiyuan University of Technology, Taiyuan 030024, China
(Email: sxgrant@126.com)
(Received May. 31, 2013; revised and accepted Jan. 28 & Mar. 14, 2014)

Abstract

In 2011, Kumar *et al.* proposed an efficient password authentication scheme using smart cards to overcome the security flaws in Liao *et al.* scheme. However, in this paper, we point out that Kumar *et al.*'s scheme actually has various defects been overlooked, such as no provision of forward secrecy, poor repairability and practicality. More recently, Ramasamy and Muniyandi presented an efficient two-factor scheme based on RSA and this scheme is claimed to have a number of merits over existing schemes. Notwithstanding their ambitions, Ramasamy-Muniyandi's scheme is vulnerable to user impersonation attack, and it actually is equivalent to a verifier-table-based scheme, which discourages any use of the scheme for practical applications.

Keywords: Authentication protocol, cryptanalysis, impersonation attack, RSA, smart card

1 Introduction

With the increasing need of accessing remote digital services and protecting electronic transactions, password-based authentication that enable two or more parties sharing memorable passwords to securely communicate over an open channel are gaining popularity due in large part to its practical significance. Its feasibility was investigated as early as the work of Lamport [21], and this initial study has been followed by various proposals, including ones employing multi-application smart cards, [4, 6, 7, 10, 16, 18, 24, 26, 36, 37, 42, 46, 47, 55].

In such schemes, two participants, i.e. a server S and a user U, are involved. In the beginning, U submits her identity ID and password PW to S over a secure channel, and upon receiving the registration request, S issues a smart card to U with the smart card being personalized with some initial security parameters [15, 32]. This phase is called the registration phase and is carried out only once for each client. With the smart card obtained, U can get access to S by employing the login-and-authentication phase. This phase can be carried out as many times as demanded. Besides registration phase and login-and-authentication phase, there may be additional phases, such as the password change phase used when U wants to change her password, and the user eviction phase is used to delete an expired or malicious account.

In 2000, Peyravian and Zunic [34] proposed two user authentication schemes which only employ lightweight hash functions, and thus these two schemes are simple and efficient to be implemented on resource-constrained smart cards. Unfortunately, Peyravian-Zunic's schemes are found vulnerable to various attacks, such as offline password guessing attack, stolen-verifier attack and denial-of-service attack, by Hwang and Yeh in 2002 [14]. To overcome the defects in Peyravian-Zunic's schemes, a number of enhanced versions [3, 30] are subsequently put forward. One common feature among these schemes is that, a password-verifier table is stored on the authentication server. As stated by Chen and Lee [5], these schemes in [3, 14, 30, 34] invariably suffer from the risk of modified-verifier-table attack and the cost of protecting and maintaining the verifier table on remote server. If this password-verifier table is stolen by the adversary or leaked by accident, the entire system will be completely broken. Accordingly, intensive research has been made to cope with this problem [12, 18, 22, 28, 48, 50], yet most of the previous schemes are found prone to various issues on both security and performance aspects [13, 23, 25, 27, 31, 32, 40, 41, 45].

As stated by a comprehensive work [44], an important reason for the failure of previous schemes is that, in most of these previous studies, the authors demonstrate attacks on problematic schemes and advance new proposals with claims of the superior aspects of their schemes, and ignore benefits that their schemes fail to provide. Accordingly, a comprehensive and reasonable evaluation metric is of particular importance. In 2006 Liao *et al.* [29] first proposed ten requirements for evaluating a password authentication, and then presented a new scheme using smart cards for password authentication over insecure networks. Liao *et al.* argued that their scheme can satisfy all the ten requirements and thus is immune to various attacks. Although this scheme possesses many admired features, particularly, no verifier table is needed on the server and a user can freely change her password without interaction with the remote server. However, some security loopholes of this scheme are shortly pointed out by Xiang *et al.* [52].

To remedy the defects identified in Liao *et al.*'s scheme, Kumar *et al.* [20] further put forward an improved scheme in 2011. This scheme is claimed to have enhanced security and could maintain all the advantages of the original scheme and be free from the attacks pointed out by Xiang *et al.* [52]. Notwithstanding their claims, we will report that this scheme still has serval serious defects: (1) it cannot preserve forward secrecy; (2) it has poor repairability; (3) it is not user friendly.

In 2012, Ramasamy and Muniyandi [35] also reported that previous two-factor authentications are far from practicality, and accordingly they put forward an efficient RSA-based password authentication scheme with smart card, which is claimed to be well-suited for practical applications. Their schemes are not only very efficient, but also can withstand various sophisticated attacks such as parallel session attack, denial of service attack and smart card loss attack, and the server has no need to maintain a sensitive password table for authenticating users. However, in this short paper, we will show that Ramasamy-Muniyandi's protocol cannot even attain the basic goal of user authentication by demonstrating its vulnerability to user impersonation attack, in which an adversary does not need any credentials of the legitimate user but just a protocol transcript. Moreover, we reveal that this scheme actually is equal to a password-table-based scheme by presenting a reduction to absurdity.

The rest of this paper is organized as follows: in Section 2, we review Kumar *et al.*'s scheme. Section 3 describes the defects of Kumar *et al.*'s scheme. Then, we turn to review and analyze masamy-Muniyandi's scheme in Section 4 and Section 5, respectively. Finally, the conclusion is drawn in Section 6.

2 Review of Kumar et al.'s Scheme

In this Section, we briefly review the remote user authentication scheme proposed by Kumar *et al.* [20]. Their scheme is composed of four phases: registration, login, authentication, and password change. The notations and descriptions used throughout this paper are summarized in Table 1 and we will follow the notations in Kumar *et al.*'s scheme as closely as possible.

2.1 Initialization Phase

In this phase, AS first selects a large prime number p. Without loss of generality, p is large enough, e.g., at least 1024 bits. Besides, AS selects a secure one-way hash function $h(\cdot)$ and a long secret key x. The details of this phase are described in the following.

Table 1: Notations and abbreviations

Symbol	Description
U_i	i^{th} user
AS	remote authentication server
$\mathcal{M}$	malicious attacker
ID_i	identity of user U_i
PW_i	password of user U_i
x	the secret key of remote server AS
S_{key}	the session key
$h(\cdot)$	collision free one-way hash function
$\oplus$	the bitwise XOR operation
$\|$	the string concatenation operation
$\rightarrow$	a common (insecure) channel
$\Rightarrow$	a secure channel

2.2 Registration Phase

The registration phase involves the following operations:

1) U_i chooses her ID_i and PW_i, generates a random number b and computes $h(b\|PW_i)$.

2) $U_i \Rightarrow AS$: $\{ID_i, h(b\|PW_i)\}$.

3) AS checks the format of ID_i and computes $A_1 = h(ID_i)^{h(b\|PW_i)} \bmod p$, $A_2 = (A_1)^{K(x)} \bmod p$, $EA_2 = A_2 \oplus h(b\|PW_i)$, $B = (h(ID_i))^x \bmod p$, $B_K = K(B)$ and $EB_K = B_K \oplus h(b\|PW_i)$.

4) $AS \Rightarrow U_i : SC$ containing $\{A_1, EA_2, EB_K, p, h(\cdot)\}$.

2.3 Login Phase

When U_i wants to login to AS, the following operations will be performed:

1) U_i inserts her smart card into a card reader and submits her identity ID_i, password PW_i and the random number b^*;

2) SC computes $A_1^* = h(ID_i^*)^{h(b^*\|PW_i^*)} \bmod p$ and checks if $A_1^* \neq A_1$. If the equality does not hold, the login request is rejected by the smart card. Otherwise, SC proceeds to the next step.

3) SC computes $A_2 = EA_2 \oplus h(b\|PW_i)$, $B_K = EB_K \oplus h(b\|PW_i)$, $A_3 = A_2 \oplus h(B_K\|T_{U1})$, $C_1 = R \oplus h(B_K \|T_{U1})$, $C2 = (A_2, B_K)^R \bmod p$ and $C_3 = h(C_2\|T_{U1})$, where R is a random number.

4) $U_i \rightarrow AS$: Login request $\{ID_i, A_3, C_1, C_3, T_{U1}\}$.

It should be noted that, as with many commercial cards, if U_i fails to enter the correct triple $\{ID_i, PW_i, b\}$ and the number of failed attempts exceeds a predefined value, then SC denies to work further and displays need for re-registration.

2.4 Authentication Phase

After receiving the login request from user U_i, S performs the following operations:

1) S checks the validity of ID_i and that $T_{AS1} - T_{U1} \leq \Delta T$, where T_{AS1} is the time when the login request was received. If either is invalid, the login request is rejected. Otherwise, S performs the following operations.

2) Computes $B_K = K(B) = K[(h(ID_i))^x \bmod p]$, $A_2^* = A_3 \| h(B_K \| T_{U1})$ and $R^* = C_1 \oplus h(B_K \| T_{U1})$.

3) Computes $C_2^* = (A_2^* \| B_K)^{R^*} \bmod p$ and $C_3^* = h(C_2^* \| T_{U1})$. If $C_3^* \neq C_3$ then rejects the login request.

4) Computes $D_1 = S \oplus h(A_2 \| T_{AS2})$, $D_2 = (C_2)^S \bmod p$ and $D_3 = h(D_2 \| T_{AS2})$, where S is a random number chosen by AS from Z_p^*.

5) $AS \rightarrow U_i : \{D_1, D_3, T_{AS2}\}$. On receiving the response from AS, SC performs as follows:

   a. Checks whether $T_{U2} - T_{AS2} \leq \Delta T$, where T_{U2} is the time when the response was received. If so, then extracts $S^* = D_1 \oplus h(A_2 \| T_{AS2})$.

   b. Computes $D_2^* = (C2)^{S^*} \bmod p$ and $D_3^* = h(D_2^* \| \ T_{AS2})$. If $D_3^* = D_3$, then the legality of AS is confirmed.

6) After authenticating each other, U_i and AS use the same session key $S_{key} = h(D_2 \| A_2 \ \| BK \ \| R \ \| S \ \| T_{U1} \ \| T_{AS2})$ for further communications.

2.5 Password Change Activity

When U_i wants to change the old password PW_i to a new one, this phase will be involved and U_i does not need to interact with AS.

1) U inserts her SC into the smart card device and then keys her identity ID_i^*, password PW_i^*, and random number b^*; and requests SC to change the password.

2) Computes $A_1^* = h(ID_i^*)^{h(b^* \| PW_i^*)} \bmod p$. If $A_1^* = A_1$, then U is allowed to enter the new password PW_i^{**};

3) Extracts $A_2 = EA_2 \oplus h(b^* \| PW_i^*)$, $B_K = EB_K \oplus h(b^* \| PW_i^*)$ and $A_1^{**} = h(ID^*)^{h(b^* \| PW_i^{**})}$;

4) Computes $A_2^{**} = A_2^{(h^{-1}(b^* \| PW_i^*))(h(b^* \| PW_i^{**}))} \bmod p$, $EA_2^{**} = A_2^{**} \oplus h(b^* \| PW_i^{**})$ and $EB_K^{**} = B_K \oplus h(b^* \| PW_i^{**})$;

5) Replaces A_1, EA_2 and EB_K with A_1^{**}, EA_2^{**}, and BK^{**} respectively.

3 Cryptanalysis of Kumar et al.'s Scheme

In this Section we will show that Kumar et al.'s scheme [20] fails to provide forward secrecy, has poor repairability and is not user-friendly, which make this scheme unpractical. There are three assumptions of the adversary's capabilities clearly made in Kumar et al.'s scheme, and we summarize them as follows:

Assumption 1. *The malicious attacker $\mathcal{M}$ can eavesdrop, insert, delete, alter, intercept or block any messages transmitted in the channel. In other words, $\mathcal{M}$ has total control over the communication channel between the user U and the remote server S, this is consistent with the Dolev-Yao standard distributed computing adversary model [9];*

Assumption 2. *The malicious attacker $\mathcal{M}$ is able to extract the secret security parameters stored in the smart card when the user's smart card is in $\mathcal{M}$'s possession. This assumption is reasonable according to the recent research results on side-channel attack techniques [1, 2, 17, 33].*

Assumption 3. *The malicious attacker $\mathcal{M}$ can offline enumerate the password space. For user-friendliness, most schemes (e.g., the schemes in [11, 23, 27, 31]) facilitate the users to select their own password at will during the password change phase and registration phase and the users often choose passwords which are easily remembered for their convenience, and these easily-remembered passwords are weak and fall into a small dictionary [8, 51].*

It is worth noting that the above three assumptions are also explicitly made in most of the latest works [13, 27, 32, 38, 39, 40, 41, 45], and indeed reasonable as justified in [46, 54]. Based on the above assumptions, in the following discussions of the security flaws of Kumar et al.'s scheme, we assume that an attacker can extract the secret values $\{A_1, EA_2, EB_k, p\}$ stored in the legitimate user's smart card, and the attacker can also intercept or block the login request $\{ID_i, A_3, C_1, C_3, T_{U1}\}$ sent out by U_i and the reply message $\{D_1, D_3, T_{AS2}\}$ sent out by the server AS.

3.1 Failure to Achieve Forward Secrecy

As noted in [43, 53], forward secrecy is an important property of remote user authentication schemes for limiting the effects of eventual failure of the entire system in case the long-term private key(s) of the authentication server is compromised (leaked or stolen). A scheme with perfect forward secrecy assures that, even if the server's long-term key is compromised, the previously established session keys will not be compromised.

When analyzing their scheme, Kumar *et al.* argued that "if the secret key x of AS is revealed accidentally, even in possession of U_i's smart card, $\mathcal{M}$ can neither behave like legal AS nor like a legal U_i", and hence this scheme is claimed to provide forward secrecy. Firstly, we have to say that Kumar et al. have misunderstood the meaning of forward secrecy. Actually, as stated in [19, 43], forward secrecy has nothing to do with impersonation but relates to session keys. With this notion misunderstood, their scheme, of course, cannot achieve this important property.

Supposing an attacker $\mathcal{M}$ has obtained the master secret key x from the compromised server and eavesdropped the transcripts $\{ID_i, A_3, C_1, C_3, T_{U1}, D_1, D_3, T_{AS2}\}$ during U_i and AS's jth authentication process from the open channel. $\mathcal{M}$ can compute the session key of U_i and AS's jth encrypted communication as follows:

Step 1. Computes $B_K = K(B) = K[(h(ID_i))^x \bmod p]$, where ID_i is previously obtained by eavesdropping on the public channel.

Step 2. Computes $A_2 = A_3 \| h(B_K \| T_{U1})$, $R = C_1 \oplus h(B_K \| T_{U1})$, where A_3 and T_{U1} is previously obtained by eavesdropping on the public channel;

Step 3. Computes $C_2 = (A_2 \| B_K)^R \bmod p$;

Step 4. Computes $S = D_1 \oplus h(A_2 \| T_{AS2})$, where T_{AS2} is previously obtained by eavesdropping on the public channel;

Step 5. Computes $D_2 = (C_2)^S \bmod p$;

Step 6. Computes the jth session key $S^j_{key} = h(D_2 \| A_2 \| BK \| R \| S \| T_{U1} \| T_{AS2})$.

Once the session key SK^j is obtained, the whole jth session will be completely exposed to $\mathcal{M}$. Therefore, as opposed to Kumar et al.'s claim, forward secrecy is not provided in their scheme.

3.2 Poor Practicality

In Kumar *et al.*'s scheme, the user has to input three items, i.e. ID_i, PW_i and b when login. As stated in [20], b is a random number generated by U_i when registration. If it is large (and really random), it will be very hard for the user to remember and it is most likely that U_i may forget this long and random number if she does not frequently use the system, which will render the scheme completely unusable. However, if it is not large enough (i.e. not of high entropy and drawn from a small dictionary $\mathcal{D}_b$), it can be easily guessed as with guessing the password, and this scheme will be vulnerable to offline password guessing attack. In case an attacker $\mathcal{M}$ gets access to U_i's smart card for a period of time, according Assumption 2, $\mathcal{M}$ can extract the secret values $\{A_1, EA_2, EB_k, p\}$ stored in the legitimate user's smart card. Then, an offline password guessing attack can be launched as follows:

Step 1. Guesses the value of PW_i to be PW_i^* from a dictionary space $\mathcal{D}_{pw}$, the value of b to be b_i^* from a dictionary space $\mathcal{D}_b$;

Step 2. Computes $A_1^* = h(ID_i)^{b^* \| PW_i^*}$;

Step 3. Verifies the correctness of PW_i^* and b^* by checking if the computed A_1^* is equal to the revealed A_1, where A_1 is extracted from U_i's smart card;

Step 4. Repeats the above steps until the correct value of PW_i is found.

Let $|\mathcal{D}_{pw}|$ denote the number of passwords in the password space $\mathcal{D}_{pw}$, $|\mathcal{D}_b|$ denote the number of items in $\mathcal{D}_b$. The running time of the above attack procedure is $\mathcal{O}(|\mathcal{D}_{pw}| * |\mathcal{D}_{pw}| * T_H)$, where T_H is the running time for hash operation. As $|\mathcal{D}_{pw}|$ and $|\mathcal{D}_b|$ are very limited in practice [8, 51], the above attack can be completed in polynomial time.

3.3 Poor Repairability

In Kumar *et al.*'s scheme, when a user suspects (or realizes) that she has been impersonated by an attacker, however, even if U_i changes her password to a new one, such a fraud can not be prohibited. Since A_1 is uniquely determined by U_i's identity ID_i and AS's permanent secret key x, AS can not change A_1 for U_i unless either ID_i or x is changed. Unfortunately, since ID_i is tied to U_i uniquely in most application systems and it is not reasonable to change ID_i. Furthermore, it is also impractical and inefficient to change x to recover the security for U_i, since x is commonly used for all users rather than specifically used for only one user.

4 A Brief Review of Ramasamy-Muniyandi's Scheme

In this Section, we briefly review the remote user authentication scheme proposed by Ramasamy and Muniyandi [35] in 2012. Their scheme is based on RSA and involves three parties, i.e. the user U_i, the server S and the key information center (KIC). KIC is responsible for registration only and does not participate in the authentication process. Their scheme consists of three phases: the registration phase, the login phase and the authentication phase. In the following, we employ the notations listed in Table 1 and follow the original notations in [35] as closely as possible.

4.1 Registration Phase

User U_i chooses her identity ID_i and password PW_i, and submits them to KIC. For issuing a smart card to user U_i, KIC performs the registration steps:

1) Generates an RSA key pair, namely a private key d and a public key (e, n), $ed = 1 \texttt{mod} \psi(n)$, $n = pq$, where p and q are two large primes of nearly the same length. KIC publishes (e, n) and keeps d secret.

2) Determines an integer g, which g is a primitive in both GF_p and GF_q.

3) Generates the smart card identifier CID_i of U_i and calculates security parameter $W_i = ID_i^{CID_i \times d} \bmod n$.

4) Computes $V_i = g^{PW_i \times d \times T_R} \bmod n$, where T_R is the user's registration time. This value is unique for every user and maintained by the server AS. In other words, AS keeps an entry $\{ID_i, T_R\}$ for each registered user U_i.

5) $AS \Rightarrow U_i$: A smart card containing security parameters $\{n, e, CID_i, W_i, V_i, h(\cdot)\}$.

4.2 Login Phase

When U_i wants to login to S, she inserts her smart card into a card reader and keys ID_i and PW_i. Then the smart card will perform the following steps:

1) Generates a random number r and calculate $X_i = g^{PW_i \times r} \bmod n$ and $Y_i = W_i \times V_i^{r \times T} \bmod n$.

2) $U_i \rightarrow S$: $\{(ID_i, CID_i, X_i, Y_i, n, e, g, T_u)\}$.

4.3 Authentication Phase

On receiving the login request, the server S performs the following steps:

1) Checks whether ID_i is a valid user identity and CID_i is a legal smart card identity. If either is not valid, AS rejects the login request.

2) Checks whether $T_s - T_u \leq \Delta T$, where T_s is the time when the login request is received and ΔT is the legal time interval due to transmission delay, if not, then AS rejects the login request.

3) Evaluates the equation $Y_i^e = ID_i^{CID_i} \times X_i^{T_u \times T_R} \bmod n$, where T_u is the login request time and T_R is the registration time of U_i.

4) If any one of the above results is negative, then login request is rejected. Otherwise, the login request is accepted.

5) If the login request is rejected three times then the user account will be automatically locked and she has to contact the server to unlock the account.

5 Cryptanalysis of Ramasamy-Muniyandi's Scheme

In this Section, we will discuss the flaws of Ramasamy-Muniyandi's scheme. Note that the three assumptions listed in Section 3 are also clearly made in [35]. This scheme is simple and elegant, however, after careful examination, we find it cannot achieve the basic goal of user authentication. Besides, their scheme has an inherent design flaw in the registration phase and it actually is equal to a verifier-table-based scheme. The identified defects discourage any use of the scheme for practical applications.

5.1 User Impersonation Attack

In the following, we will show how an attacker $\mathcal{M}$ without any credentials (i.e., the password and the smart card) of U_i can successfully impersonate U_i to login to SA and freely enjoy the services.

Step 1. Intercepts and block a login request $\{(ID_i, CID_i, X_i, Y_i, n, e, g, T_u)\}$ of the user U_i from the public communication channel;

Step 2. Computes $T'_u = \varepsilon T_u$, where ε is a small real number chosen by $\mathcal{M}$ in such a way that T'_u is a valid timestamp in the near future;

Step 3. $\mathcal{M} \rightarrow AS$: $\{(ID_i, CID_i, X_i^{\varepsilon}, Y_i, n, e, g, T'_u)\}$.

Step 4. The server AS checks the validity of the timestamp T'_u by checking $T_s - T'_u \leq \Delta T$, where T_s denotes the server's current timestamp. Then the server AS checks $Y_i^e \stackrel{?}{=} ID_i^{CID_i} \times (X_i^{\varepsilon})^{T_u \times T_R} \bmod n$.

Now we show that in Step 4, AS will find no abnormality, because

$$
\begin{aligned}
Y_i^e &= (W_i \times V_i^{r \times T'_u}) \bmod n \\
&= ID_i^{CID_i} \times g^{PW_i \times r \times T_R \times T'_u} \bmod n \\
&= ID_i^{CID_i} \times g^{PW_i \times r \times T_R \times \varepsilon \times T_u} \bmod n \\
&= ID_i^{CID_i} \times g^{(PW_i \times r)^{T_R \times \varepsilon \times T_u}} \bmod n \\
&= ID_i^{CID_i} \times (X_i^{\varepsilon})^{T_R \times T_u} \bmod n.
\end{aligned}
$$

On successful verification, the server AS accepts the forged login authentication request. Therefore, the attacker $\mathcal{M}$ can impersonate as the legitimate user without any cryptographic credentials, which breaches the soundness of the underlying authentication scheme.

5.2 The Problem of Storing Parameter T_R

In this Section, we demonstrate another serious defect in Ramasamy-Muniyandi's scheme. In the registration phase, AS keeps an entry $\{ID_i, T_R\}$ for each registered user U_i. At first glance, T_R is not the user's password and the store of such an entry does not violate the basic goal of no password-verifier table. However, T_R actually is as critical as the password, and Ramasamy-Muniyandi's scheme equals to a scheme with password-verifier table. We prove this by contradiction.

If Ramasamy-Muniyandi's scheme is a scheme with no "password-verifier table", then the disclosure of T_R alone (i.e., U_i's smart card and password, server's private key x are still secure) will pose no threat to the security of the scheme. Now we assume U_i's entry on the server has disclosed and been obtained by the attacker $\mathcal{M}$.

If $\texttt{gcd}\ (T_R, e) = 1$, $\mathcal{M}$ can impersonate as U_i by performing the following steps:

Step 1. Intercepts and blocks a login request $\{ID_i, CID_i, X_i, Y_i, n, e, g, T_u\}$ of the user U_i from the public communication channel.

Step 2. Reads the current timestamp T_u and checks if $\texttt{gcd}\ (T_R \times T_u, e) = 1$. If it holds, proceeds to the next step. Otherwise, $\mathcal{M}$ repeats this step.

Step 3. Runs the Extended Euclidean algorithm to compute two integers a and b such that $a \times e + b \times T_u \times T_R = 1(\text{in } \mathbb{Z})$.

Step 4. Computes $X_i' = (ID_i^{CID_i})^{-b} \bmod n$ and $Y_i' = (ID_i^{CID_i})^{a} \bmod n$.

Step 5. $\mathcal{M} \rightarrow AS$: $\{(ID_i, CID_i, X_i', Y_i', n, e, g, T_u)\}$.

Step 6. The server AS checks the validity of the timestamp T_u by checking $T_s - T_u \leq \Delta T$, where T_s denotes the server's current timestamp. Then the server AS checks $(Y_i')^e \stackrel{?}{=} ID_i^{CID_i} \times (X_i')^{T_u \times T_R} \bmod n$.

We give a few remarks on the above attack. Firstly, in Step 3, $\mathcal{M}$ can definitely find a and b, for the value of T_u is chosen in such a way that $\texttt{gcd}\ (T_R \times T_u, e) = 1$. Secondly, in Step 6, the server AS will accept, which is justified by the following equalities:

$$\begin{aligned}(Y_i')^e &= (ID_i^{CID_i})^{ae} \bmod n\\ &= (ID_i^{CID_i})^{(-b)\times T_u \times T_R} \bmod n\\ &= ID_i^{CID_i} \times (ID_i^{CID_i})^{-b\times T_u \times T_R} \bmod n\\ &= ID_i^{CID_i} \times (ID_i^{CID_i \times (-b)})^{T_u \times T_R} \bmod n\\ &= ID_i^{CID_i} \times X_i^{T_u \times T_R} \bmod n.\end{aligned}$$

The above attack procedure has shown that if $\texttt{gcd}\ (T_R, e) = 1$, $\mathcal{M}$ can impersonate as U_i with the help of the leaked T_R. We now show that, the above attack has a success rate about 60% due to the following two facts: (1) The probability of $\texttt{gcd}\ (T_R, e) = 1$ is about $6/\pi^2 \approx 0.6$ [49]; (2) T_R and e are chosen by different parties, and thus they are independent.

The above analysis demonstrates that $\mathcal{M}$ can impersonate as U_i with remarkably high probability (i.e., a success rate about 60%) in case T_R is leaked. Consequently, the leakage of the $\{ID_i, T_R\}$ table does endanger the security of the scheme and it should be well kept secret, which invalidates the claim of a "no verifier table" scheme. As stated in the introduction, it is greatly undesirable for the server to maintain and protect a verifier table.

6 Conclusion

Two-factor authentication is an important mechanism for remote login systems that enables the server and its users to authenticate each other. In this paper, we first pointed out that Kumar *et al.*'s scheme is really impractical by demonstrating three serious defects. Then, we illustrated that Ramasamy-Muniyandi's RSA-based authentication scheme is prone to a user impersonation attack and equal to a verifier-based scheme. In our security analysis, we employed the number theory that two random (or independently chosen) numbers are relatively prime with a probability about $6/\pi^2 \approx 0.6$. As for future work, we are considering to design two-factor authentication schemes with formal security.

Acknowledgments

The authors would like to thank the anonymous reviewers for their valuable comments and constructive suggestions. This research was in part supported by the Natural Science Foundation for Young Scientists of Shanxi Province under Grant No. 2012021011-3, National Natural Science Foundation of Shanxi Province under Grant No. 2009011022-2 and Shanxi Scholarship Council of China under Grant No. 2009-28.

References

[1] F. Amiel, B. Feix, and K. Villegas, "Power analysis for secret recovering and reverse engineering of public key algorithms," in *Proceedings of SAC'07*, LNCS 4876, pp. 110–125, Springer, 2007.

[2] J. Balasch, B. Gierlichs, R. Verdult, L. Batina, and I. Verbauwhede, "Power analysis of atmel crypto Memory–Recovering keys from secure EEPROMs," in *Topics in Cryptology (CT-RSA'12)*, pp. 19–34, Springer, 2012.

[3] Y. F. Chang, C. C. Chang, and L. I. U. Yi-Long, "Password authentication without the server public key," *IEICE Transactions on Communications*, vol. 87, no. 10, pp. 3088–3091, 2004.

[4] T. H. Chen, H. C. Hsiang, and W. K. Shih, "Security enhancement on an improvement on two remote user authentication schemes using smart cards," *Future Generation Computer Systems*, vol. 27, no. 4, pp. 377–380, 2011.

[5] T. H. Chen and W. B. Lee, "A new method for using hash functions to solve remote user authentication," *Computers & Electrical Engineering*, vol. 34, no. 1, pp. 53–62, 2008.

[6] H. R. Chung, W. C. Ku, and M. J. Tsaur, "Weaknesses and improvement of wang et al.'s remote user password authentication scheme for resource-limited environments," *Computer Standards & Interfaces*, vol. 31, no. 4, pp. 863–868, 2009.

[7] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 629–631, 2004.

[8] M. Dell'Amico, P. Michiardi, and Y. Roudier, "Password strength: An empirical analysis," in *Proceedings of Infocom'10*, pp. 1–9, Mar. 2010.

[9] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[10] D. He, J. Chen, and J. Hu, "An ID-based client authentication with key agreement protocol for mobile client-server environment on ECC with provable security," *Information Fusion*, vol. 13, no. 3, pp. 223–230, 2012.

[11] D. He, J. Chen, and J. Hu, "Improvement on a smart card based password authentication scheme," *Journal of Internet Technology*, vol. 13, no. 3, pp. 38–42, 2012.

[12] D. He, J. Chen, and R. Zhang, "Weaknesses of a dynamic ID-based remote user authentication scheme," *International Journal of Electronic Security and Digital Forensics*, vol. 3, no. 4, pp. 355–362, 2010.

[13] D. He and S. Wu, "Security flaws in a smart card based authentication scheme for multi-server environment," *Wireless Personal Communications*, vol. 70, no. 1, pp. 323–329, 2013.

[14] J. J. Hwang and Y. E. H. Tzu-Chang, "Improvement on Peyravian-Zunic's password authentication schemes," *IEICE Transactions on Communications*, vol. 85, no. 4, pp. 823–825, 2002.

[15] M. S. Hwang, S. K. Chong, and T. Y. Chen, "DoS-resistant ID-based password authentication scheme using smart cards," *Journal of Systems and Software*, vol. 83, no. 1, pp. 163–172, 2010.

[16] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28–30, 2000.

[17] T. Kasper, D. Oswald, and C. Paar, "Side-channel analysis of cryptographic RFIDs with analog demodulation," in *Proceedings of RFIDSec'12*, LNCS 7055, pp. 61–77, Springer, 2012.

[18] M. K. Khan, S. K. Kim, and K. Alghathbar, "Cryptanalysis and security enhancement of a more efficient & secure dynamic ID-based remote user authentication scheme'," *Computer Communications*, vol. 34, no. 3, pp. 305–309, 2011.

[19] H. Krawczyk, "HMQV: A High-Performance secure Diffie-Hellman protocol," in *Advances in Cryptology (Crypto'05)*, LNCS 3621, pp. 546–566, 2005.

[20] M. Kumar, M. K. Gupta, and S. Kumari, "An improved efficient remote password authentication scheme with smart card over insecure networks," *International Journal of Network Security*, vol. 13, no. 3, pp. 167–177, 2011.

[21] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[22] C. C. Lee, M. S. Hwang, and I. E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Industrial Electronics*, vol. 53, no. 5, pp. 1683–1687, 2006.

[23] C. C. Lee, C. T. Li, and R. X. Chang, "A simple and efficient authentication scheme for mobile satellite communication systems," *International Journal of Satellite Communications Networking*, vol. 30, no. 1, pp. 29–38, 2012.

[24] C. C. Lee, T. H. Lin, and R. X. Chang, "A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards," *Expert Systems with Applications*, vol. 38, no. 11, pp. 13863–13870, 2011.

[25] C. C. Lee, C. H. Liu, and M. S. Hwang, "Guessing attacks on strong-password authentication protocol," *International Journal of Network Security*, vol. 15, no. 1, pp. 64–67, 2013.

[26] C. T. Li and C. C. Lee, "A robust remote user authentication scheme using smart card," *Information Technology and Control*, vol. 40, no. 3, pp. 236–245, 2011.

[27] C. T. Li and C. C. Lee, "A novel user authentication and privacy preserving scheme with smart cards for wireless communications," *Mathematical and Computer Modelling*, vol. 55, no. 1, pp. 35–44, 2012.

[28] C. T. Li, C. C. Lee, C. J. Liu, and C. W. Lee, "A robust remote user authentication scheme against smart card security breach," in *Proceedings of 25th Annual IFIP Conference on Data and Applications Security and Privacy (DBSec '11)*, LNCS 6818, pp. 231–238, 2011.

[29] I. E. Liao, C. C. Lee, and M. S. Hwang, "A password authentication scheme over insecure networks," *Journal of Computer and System Sciences*, vol. 72, no. 4, pp. 727–740, 2006.

[30] C. L. Lin and T. Hwang, "A password authentication scheme with secure password updating," *Computers & Security*, vol. 22, no. 1, pp. 68–72, 2003.

[31] C. G. Ma, D. Wang, and Q. M. Zhang, "Cryptanalysis and improvement of sood et al.s dynamic ID-Based authentication scheme," in *Proceedings of International Conference on Distributed Computing and Internet Technology (ICDCIT'12)*, LNCS 7154, pp. 141–152, 2012.

[32] C. G. Ma, D. Wang, and S. D. Zhao, "Security flaws in two improved remote user authentication schemes using smart cards," *International Journal of Communication Systems*, vol. 27, no. 10, pp. 2215–2227, 2014.

[33] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.

[34] M. Peyravian and N. Zunic, "Methods for protecting password transmission," *Computers & Security*, vol. 19, no. 5, pp. 466–469, 2000.

[35] R. Ramasamy and A. P. Muniyandi, "An efficient password authentication scheme for smart card," *International Journal of Network Security*, vol. 14, no. 3, pp. 180–186, 2012.

[36] 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, no. 2, pp. 414–416, 2003.

[37] J. J. Shen, C. W. Lin, and M. S. Hwang, "Security enhancement for the timestamp-based password authentication scheme using smart cards," *Computers & Security*, vol. 22, no. 7, pp. 591–595, 2003.

[38] K. A. Shim, "Security flaws in three Password-Based remote user authentication schemes with smart cards," *Cryptologia*, vol. 36, no. 1, pp. 62–69, 2012.

[39] R. Song, "Advanced smart card based password authentication protocol," *Computer Standards & Interfaces*, vol. 32, no. 5, pp. 321–325, 2010.

[40] S. K. Sood, "An improved and secure smart card based dynamic identity authentication protocol," *International Journal of Network Security*, vol. 14, no. 1, pp. 39–46, 2012.

[41] H. B. Tang, X. S. Liu, and L. Jiang, "A robust and efficient timestamp-based remote user authentication scheme with smart card lost attack resistance," *International Journal of Network Security*, vol. 15, no. 6, pp. 360–368, 2013.

[42] X. Tian, R. W. Zhu, and D. S. Wong, "Improved efficient remote user authentication schemes," *International Journal of Network Security*, vol. 4, no. 2, pp. 149–154, 2007.

[43] D. Wang and C. G. Ma, "Cryptanalysis and security enhancement of a remote user authentication scheme using smart cards," *The Journal of China Universities of Posts and Telecommunications*, vol. 19, no. 5, pp. 104–114, 2012.

[44] D. Wang and C. G. Ma, "Robust smart card based password authentication scheme against smart card loss problem," Cryptology ePrint Archive, Report 2012/439, 2012. (`http://eprint.iacr.org/2012/439.pdf`)

[45] D. Wang, C. G. Ma, and P. Wu, "Secure Password-Based remote user authentication scheme with Non-tamper resistant smart cards," in *Data and Applications Security and Privacy*, LNCS 7371, pp. 114–121, 2012.

[46] D. Wang and P. Wang, "Offline dictionary attack on password authentication schemes using smart cards," in *Proceedings of the 16th Information Security Conference (ISC'13)*, pp. 1–16, 2013.

[47] X. M. Wang, W. F. Zhang, J. S. Zhang, and M. K. Khan, "Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards," *Computer Standards & Interfaces*, vol. 29, no. 5, pp. 507–512, 2007.

[48] Y. Wang, J. Liu, F. Xiao, and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme," *Computer Communications*, vol. 32, no. 4, pp. 583–585, 2009.

[49] E. Weisstein, "Relatively prime," 2013. (`http://mathworld.wolfram.com/RelativelyPrime.html`)

[50] F. Wen and X. Li, "An improved dynamic ID-based remote user authentication with key agreement scheme," *Computers & Electrical Engineering*, vol. 38, no. 2, pp. 381–387, 2012.

[51] T. Wu, "A real-world analysis of kerberos password security," in *Proceedings of the 1999 ISOC Network and Distributed System Security Symposium*, pp. 1–14, 1999.

[52] T. Xiang, K. Wong, and X. Liao, "Cryptanalysis of a password authentication scheme over insecure networks," *Journal of Computer and System Sciences*, vol. 74, no. 5, pp. 657–661, 2008.

[53] L. Xiong, N. Jianwei, K. Muhammad Khurram, and L. Junguo, "An enhanced smart card based remote user password authentication scheme," *Journal of Network and Computer Applications*, vol. 36, no. 5, pp. 1365–1371, 2013.

[54] J. Xu, W. T. Zhu, and D. G. Feng, "An improved smart card based password authentication scheme with provable security," *Computer Standards & Interfaces*, vol. 31, no. 4, pp. 723–728, 2009.

[55] K. H. Yeh, C. Su, N. W. Lo, Y. Li, and Y. X. Hung, "Two robust remote user authentication protocols using smart cards," *Journal of Systems and Software*, vol. 83, no. 12, pp. 2556–2565, 2010.

Ying Wang received her MS degree in the department of computer science and technology in 2006 from Taiyuan University of Technology, China. She is currently a Ph.D. candidate and lecturer in the department of computer science and technology of Taiyuan University of Technology, China. Her research interests include computer network and security, trusted computing and cryptography.

Xin-Guang Peng received his Ph.D. in computer application technology from the Beijing Institute of Technology, China in 2004. He is a professor in the department of computer science and technology of Taiyuan University of Technology, China. His research interests include computer network and security, trusted computing.