Security Improvement of Two Dynamic ID-based Authentication Schemes by Sood-Sarje-Singh

R. Martínez-Peláez[*1], F. Rico-Novella[2], J. Forné[2], P. Velarde-Alvarado[3]

[1] Institute of Informatics
University of Sierra Sur
Oaxaca, Miahuatlán de Porfirio Díaz, Mexico
*rpelaez@unsis.edu.mx
[2] Department of Telematics Engineering
Universitat Politécnica de Catalunya
Barcelona, Spain
[3] Area of Basic Sciences and Engineering
Autonomous University of Nayarit
Nayarit, Tepic, Mexico

ABSTRACT
In 2010, Sood-Sarje-Singh proposed two dynamic ID-based remote user authentication schemes. The first scheme is a security improvement of Liao et al.'s scheme and the second scheme is a security improvement of Wang et al.'s scheme. In both cases, the authors claimed that their schemes can resist many attacks. However, we find that both schemes have security flaws. In addition, their schemes require a verification table and time-synchronization, making the schemes unfeasible and unsecured for electronic services. In order to remedy the security flaws of Sood et al.'s schemes, we propose a robust scheme which resists the well-known attacks and achieves all the desirable security goals.

Keywords: cryptanalysis, mutual authentication, network security, smart cards.

RESUMEN
En el año 2010, Sood-Sarje-Singh propusieron dos esquemas de autenticación de usuario remoto. El primer esquema presenta una mejora de seguridad sobre el esquema propuesto por Liao-Lee-Hwang en el año 2005, y el segundo esquema presenta una mejora de seguridad sobre el esquema propuesto por Wang-Liu-Xiao-Dan en el año 2009. En ambos casos, los autores claman que sus esquemas pueden resistir varios ataques. Sin embargo, nosotros hemos encontrado que ambos esquemas tienen deficiencias de seguridad. Además, los esquemas propuestos requieren de una tabla de verificación y sincronización de tiempo, haciendo a los esquemas imprácticos e inseguros para servicios electrónicos. Para remediar las deficiencias de seguridad presentadas en los esquemas propuestos por Sood-Sarje-Singh, nosotros proponemos un esquema robusto de seguridad que resiste los ataques más populares y consigue todas las metas de seguridad deseadas.

1. Introduction

Remote user authentication is a key security component for electronic services, such as e-banking and e-payments, in order to verify the real identity of each user. The most popular mechanism to carry out the authentication process is by means of password-based authentication protocols. However, the server must store and maintain the identities and password of each user in a database, making possible the insider attack [1], threats of revealing passwords in the directory [2] or modifying the verification table [3].

Although, many approaches have been proposed [4, 5] to overcome the weakness of storing users' identity and password in a database, using cryptography or one-way hash function, the security of the whole system can be broken if an attacker steals or modifies the information stored in the database. For this reason, Chan and Wu [6] proposed a remote user authentication scheme without a verification table, in 1990. The next year, Chang and Wu [2] introduced the concept of timestamp in the login request message to prevent the replay attack.

In 2002, Chien et al. [7] proposed a remote user authentication scheme which requires low-computational cost. However, Hsu [8] demonstrated that Chien et al.'s scheme is vulnerable to parallel session attack. Moreover, Ku et al. [1] demonstrated that Chien et al.'s scheme is vulnerable to insider attack and guessing attack.

Das et al. introduced the concept of dynamic ID-based [9] remote user authentication scheme using smart cards in 2004. Their scheme prevents the possibilities of an attacker knowing user's identity. However, the scheme is susceptible to insider attack, masquerade attack, and server spoofing attack [10, 11, 12, 13]. Moreover, the scheme does not provide mutual authentication and does not establish a session key. Then, Liao et al. [12] and Wang et al. [10] proposed different schemes which resolve the security flaws of Das et al.'s scheme. However, Sood et al. [14, 15] demonstrated that Liao et al.'s and Wang et al.'s schemes are vulnerable to malicious user attack, impersonation attack, stolen smart card attack, and off-line password guessing attack. In both cases, authors claimed that their schemes are more secure than previous one.

In this paper, we demonstrate that Sood et al.'s schemes [14, 15] have security drawbacks. We show that their schemes are still vulnerable to malicious user attack, stolen smart card attack, off-line ID guessing attack, impersonation attack, and server spoofing attack. In addition, their schemes are based on time-synchronization which it is still a problem [16, 17, 18] in existing networks environments because the data transmission and processing delay is uncertain. Moreover, the server maintains a verification table giving the opportunity an adversary to steal information from database. In order to remedy these security drawbacks, we propose an improvement on both schemes with more security. As a result, our scheme can withstand well-known attacks. Furthermore, the proposed scheme achieves the following security goals [19, 20]: 1) no verification table; 2) users choose password freely; 3) no password reveal; 4) mutual authentication; 5) session key agreement; 6) user anonymity; and 7) efficiency for wrong password login.

The rest of the paper is organized as follows: In Section 2, we review the schemes proposed by Sood-Sarje-Singh. Section 3 describes the cryptanalysis of Sood et al.'s schemes. In Section 4, we show the details of the proposed scheme. In section 5, we carry out the security analysis of the proposed scheme. In section 6, we compare our scheme with Sood et al.'s schemes demonstrating the enhanced security. Finally, we present the conclusions in Section 7.

2. Review of Sood-Sarje-Singh's schemes

In this section, we review the dynamic ID-based remote user authentication schemes [14, 15] proposed by Sood-Sarje-Singh. Each scheme is based on one-way hash function and it is composed of four phases – registration, login, verification, and password change. The notations used throughout this paper are summarized as follows:

U:	User
ID:	Identity of *U*
PW:	Password of *U*
S:	Server
x, z:	Secret keys of *S*
b:	Nonce
$h(\ )$*:*	One-way hash function
SK:	Session key between *U* and *S*
$E_{SK}(\ )$*:*	Symmetric encryption using *SK*
$D_{SK}(\ )$*:*	Symmetric decryption using *SK*
$\oplus$*:*	Exclusive-OR operation
$\|\|$*:*	Concatenation operation
$\rightarrow$*:*	Represents a secure channel
$\rightarrow$*:*	Represents an open channel

2.1 First scheme

Sood et al. proposed an improvement scheme [15] of Liao et la.'s scheme [12].

Registration phase: This phase is invoked when *U* wants to access *S*. The process is as follows:

- *U chooses her ID and PW*
- *U* $\rightarrow$ *S: ID*, *PW*
- *S chooses a random value y*
- *S computes:*
  $N = h(PW) \oplus h(y \,||\, ID) \oplus h(x)$
  $B = y \oplus h(PW)$
  $V = h(ID \,||\, PW) \oplus PW$
  $D = h(y \,||\, ID)$
- *S stores* $y \oplus x$ *and* $ID \oplus h(x)$ *corresponding to D in a database*
- *U* $\rightarrow$ *S: smart card containing N, B, V,* $h(\ )$

Login phase: When *U* wants to login the remote *S*, she inserts her smart card into the smart card reader and keys her *ID´* and *PW´*. Then, the smart card performs the following steps:

- *Computes:*
  $V´ = h(ID´ \| PW´) \oplus PW´$
- *Compares:*
  $V´ ?= V$ *if holds, the identity of U is assured*
- *After verification, the smart card computes:*
  $y = B \oplus h(PW)$
  $h(x) = N \oplus h(PW) \oplus h(y \| ID)$
  $CID = h(y \| ID) \oplus h(h(x) \| T)$
  $M = h(h(x) \| h(y) \| T)$
- $U \rightarrow S$: *CID*, *M*, *T*

Verification and session key agreement phase: When *S* receives the login request message (*CID*, *M*, *T*) at time *T'*, *S* carries out the following steps:

- *Checks the validity of time interval, if* $(T' - T) \leq \Delta T$, *S accepts the login request of U, otherwise the login request is rejected, where* ΔT *is expected time interval for a transmission delay.*
- *Computes:*
  $D´ = h(y \| ID)´ = CID \oplus h(h(x) \| T)$
- *Finds:*
  D´ in its database
- *Extracts:*
  $y \oplus x$ *and* $ID \oplus h(x)$ *corresponding to D´ from its database*
- *Recovers:*
  y from $y \oplus x$
  ID from $ID \oplus h(x)$
- *Computes:*
  $M´ = h(h(x) \| h(y) \| T)$
- *Compares:*
  $M´ ?= M$
  Finally, U and S computes the session key $SK = h(ID \| y \| h(x) \| T)$

Password change phase: When *U* wants to change the password, she inserts the smart card into the smart card reader, keys her *ID´* and *PW´*, and requests to change the password to new one, and then the smart card carries out the following operations:

- *Computes:*
  $V´ = h(ID´ \| PW´) \oplus PW´$
- *Compares:*
  $V´ ?= V$
- *Requests to U a new password* PW_{new}
- *Computes:*
  $N_{new} = N \oplus h(PW) \oplus h(PW_{new})$
  $B_{new} = B \oplus h(PW) \oplus h(PW_{new})$
  $V_{new} = h(ID \| PW_{new}) \oplus PW_{new}$

and updates the values N, B, and V stored in its memory with N_{new}, B_{new}, *and* V_{new}

2.2 Second scheme

Sood et al. proposed an improvement scheme [14] of Wang et la.'s scheme [10].

Registration phase: This phase is invoked when *U* wants to access *S*. The process is as follows:

- *U chooses her ID and PW*
- $U \rightarrow$ *S: ID*, *PW*
- *S chooses random value y*
- *S computes:*
  $N = h(ID \| PW) \oplus h(x)$
  $A = h(ID \| PW) \oplus PW \oplus h(y)$
  $B = y \oplus ID \oplus PW$
  $D = h(ID \| y)$
- *S stores* $y \oplus x$ *and* $ID \oplus h(x)$ *corresponding to D in a database*
- $S \rightarrow$ *U: smart containing N, A, B, h( )*

Login phase: When *U* wants to login the remote server *S*, she inserts her smart card into the smart card reader and keys her *ID** and *PW**. Then, the smart card performs the following steps:

- *Computes:*
  $y´ = B \oplus ID´ \oplus PW´$
  $A´ = h(ID´ \| PW´) \oplus PW´ \oplus h(y´)$
- *Compares:*
  $A´ ?= A$
- *After verification, the smart card computes:*
  $h(x) = h(\mathrm{ID} \| PW) \oplus \mathrm{N}$
  $CID = h(ID \| y) \oplus h(h(x) \| T)$
  $M = h(ID \| h(x) \| y \| T)$
- $U \rightarrow S$: *CID*, *M*, *T*

Verification and session key agreement phase:

When S receives the request (CID, M, T) at time T', S carries out the following steps:

- *Checks the validity of time interval, if* $(T' - T) \leq \Delta T$*, S accepts the login request of U, otherwise the login request is rejected, where* ΔT *is expected time interval for a transmission delay.*
- *Computes:*
  $D' = h(y \| ID)' = CID \oplus h(h(x) \| T)$
- *Finds:*
  D' *in its database*
- *Recovers:*
  $y \oplus x$ *and* $ID \oplus h(x)$ *corresponding to* D' *from its database*
- *Extracts:*
  y *from* $y \oplus x$
  ID *from* $ID \oplus h(x)$
- *Computes:*
  $M' = h(ID \| h(x) \| y \| T)$
- *Compares:*
  $M' ?= M$ *if holds, the legality of U is assured*
  Finally, U and S computes the session key $SK = h(h(x) \| ID \| T \| y)$

Password change phase: When U wants to change the password, she inserts the smart card into the smart card reader, keys her ID' and PW', and requests to change the password to new one, and then the smart card carries out the following operations:

- *Computes:*
  $y' = B \oplus ID' \oplus PW'$
  $A' = h(ID' \| PW') \oplus PW' \oplus h(y')$
- *Compares:*
  $A' ?= A$
- *Request to U a new password* PW_{new}
- *Computes:*
  $N_{new} = h(\text{ID} \| PW_{new}) \oplus h(x)$
  $A_{new} = h(\text{ID} \| PW_{new}) \oplus PW_{new} \oplus h(y)$
  $B_{new} = y \oplus \text{ID} \oplus PW_{new}$
  and updates the values N, A, and B stored in its memory with N_{new}, A_{new}, *and* B_{new}

3. Cryptanalysis of Sood-Sarje-Singh's schemes

In this section, we demonstrate that Sood et al.'s schemes have security vulnerabilities which make both schemes unfeasible and unsecured for electronic services. We assume that a legal user but malicious user is the adversary and she can extract security parameters stored in her smart card by means of different methods [21, 22].

3.1 First scheme

In this sub-section, we evaluate the security of the scheme proposed by Sood-Sarje-Singh in [15].

3.1.1 Malicious user attack

A legal but malicious user can know $h(x)$ as follows:

- *Keys her* ID' *and* PW'
- *Computes:*
  $y' = B \oplus h(PW)$
  $h(x) = h(PW) \oplus h(y' \| ID) \oplus N$

Here, $h(x)$ is the same value for each legal user. It is obvious that $h(x)$ is not well-protected

3.1.2 Man-in-the-middle attack

The legal but malicious user can intercept the login request message (CID, M, T) transmitted between U and S. At this moment, she knows CID, M, T, and $h(x)$; for that reason, she can recover $D = h(y \| ID)$ from CID as follows:

- *Computes:*
  $D' = h(y \| ID) = CID \oplus h(h(x) \| T)$

3.1.3 Stolen smart card attack

Suppose that the legal but malicious user can obtain security parameters (N, B, V) from a legal U's smart card. Now, she knows the following security parameters: $h(x)$, $D = h(y \| ID)$, $N = h(PW) \oplus h(y \| ID) \oplus h(x)$, $B = y \oplus h(PW)$, $V = h(ID \| PW) \oplus PW$. Then, she can recover y from B as follows:

- *Computes:*
  $h(PW)' = N \oplus D \oplus h(x)$
  $y' = B \oplus h(PW)$

The attacker knows y without known user's PW

3.1.4 Off-line ID guessing attack

The *ID* guessing attack is similar to password guessing attack described in [15], where the legal but malicious user attacks the password by picking random passwords. In this case, the attacker knows y and $D = h(y \| ID)$, so she needs to find the correct *ID* for *D*. The complexity of this attack depends on the length of *ID*.

3.1.5 Impersonation attack

The legal but malicious user can forge a login request message that can pass the verification process of *S* because she knows *D*, $h(x)$, and y. The attacker performs the following process:

- *Computes:*
  $h(y)$
  $CID = D \oplus h(h(x) \| T)$
  $M = h(h(x) \| h(y) \| T)$
- *Sends an imitative login request message* (*CID*, *M*, *T*) *to S*

After *S* receives the login request message, *S* carries out the verification process and *S* will accept the login request because CID and M are equals to the valid login request message. Moreover, the attacker can compute the secret key $SK = h(ID \| y \| h(x) \| T)$

3.1.6 Server spoofing attack

Because the legal but malicious user knows *ID*, y, and $h(x)$, she can establish a secure communication with *U* as *S*.

3.2 Second scheme

In this sub-section, we evaluate the security of the scheme proposed by Sood-Sarje-Singh in [14].

3.2.1 Malicious user attack

A legal but malicious user can extract $h(x)$ from *N* as follows:

- *Keys her ID´ and PW´*
- *Computes:*
  $h(x) = h(ID´ \| PW´) \oplus N$

Here, $h(x)$ is the same value for each legal user. It is obvious that $h(x)$ is not well-protected

3.2.2 Man-in-the-middle attack

The legal but malicious user can intercept the login request message (*CID*, *M*, *T*) transmitted between a legal user *U* and *S*. At this moment, she knows *CID*, *M*, *T*, and $h(x)$; for that reason, she can recover $D = h(y \| ID)$ from *CID* as follows:

- *Computes:*
  $D´ = h(ID \| y) = CID \oplus h(h(x) \| T)$

3.2.3 Steal information from a database attack

Suppose that the adversary can get access to the server and can copy the entire database to an external hard disk. Then, she can find *D* corresponding to *D´* and extracts *ID* from $ID \oplus h(x)$. The whole scheme has been broken down in terms of security.

4. Proposed scheme

Based on Sood et al.'s schemes, we propose an improved scheme. The scheme is based on nonce instead of time-synchronization. Moreover, the server does not need to maintain a verification table. The scheme is composed of the following phases: registration, login, verification and session key agreement, and password change.

4.1 Registration phase

This phase is invoked when *U* wants to access *S*. The process is as follows:

- *U chooses her ID, PW and b*
- *U computes* $h(ID \| PW \| b)$
- *U* ➔ *S: ID*, $h(ID \| PW \| b)$
- *S chooses random value y*
- *S computes:*
  $N = h(ID \| h(x \| z) \| y) \oplus h(ID \| PW \| b) \oplus h(ID \| y)$
  $A = h(h(ID \| h(x \| z) \| y))$
  $B = h(x \| z) \oplus h(h(x \| z) \| y) \oplus ID$
- *S* ➔ *U: smart containing N, A, B, y,* $h(\ )$
  Finally, *U* enters *b* into her smart card [23]. Note that *U*'s smart card contains *N, A, B, y, b,* $h(\ )$.

4.2 Login phase

When *U* wants to login the remote server *S*, she inserts her smart card into the smart card reader and keys her *ID´* and *PW´*. Then, the smart card performs the following steps:

- *Computes:*
  $h(ID \| h(x \| z) \| y)´ = N \oplus h(ID´ \| PW´ \| b) \oplus h(ID´ \| y)$
  $A´ = h(h(ID \| h(x \| z) \| y)´)$
- *Compares:*
  A´ ?= A if holds, the identity of U is assured; otherwise, the process finalized
- *After verification, the smart card carries out the following operations:*
- *Generates* b_{new} *as random number*
- *Computes:*
  $CID = h(ID \| h(x \| z) \| y)^* \oplus h(ID \| y) \oplus b_{new}$
  $SK = h(h(ID \| y \| b_{new}))$
  $M = E_{SK}(h(ID \| b_{new}))$
- $U \rightarrow S$: *y, B, CID, M*

4.3 Verification and session key agreement phase

When *S* receives the request (*y*, *B*, *CID*, *M*), *S* carries out the following steps:

- *Computes:*
  $ID´ = h(x \| z) \oplus h(h(x \| z) \| y) \oplus B$
- *Verifies the format of ID´ if it is not correct the request is rejected; otherwise, the process continues*
  $b_{new}´ = h(ID´ \| h(x \| z) \| y) \oplus h(ID´ \| y) \oplus CID$
  $h(ID´ \| b_{new}´)´$
  $SK = h(h(ID \| y \| b_{new}))$
  $h(ID \| b_{new}) = D_{SK}(M)$
- *Compares:*
  $h(ID \| b_{new})´ ?= h(ID \| b_{new})$ *if it holds, the identity of U is assured; otherwise, the process finalized*
- *Generates* y_{new}
- *Computes:*
  $N_{new} = h(ID \| h(x \| z) \| y_{new}) \oplus h(ID \| PW \| b_{new}) \oplus h(ID \| y_{new})$
  $A_{new} = h(h(ID \| h(x \| z) \| y_{new}))$
  $B_{new} = h(x \| z) \oplus h(h(x \| z) \| y_{new}) \oplus ID$
  $C = h(N_{new} \| A_{new} \| B_{new} \| y_{new} \| b_{new})$
  $O = E_{SK}(N_{new} \| A_{new} \| B_{new} \| y_{new})$
- $S \rightarrow U$: *O, C*

Upon receiving the login response message (*O, C*), *U*'s smart card performs the following operations:

  $(N_{new} \| A_{new} \| B_{new} \| y_{new}) = D_{SK}(O)$
  $C´ = h(N_{new} \| A_{new} \| B_{new} \| y_{new} \| b_{new})$
- *Compares:*
  C´ ?= C if holds, the identity of S is assured; otherwise, the process finalized
- *Replaces N, A, B, y, and b by* N_{new}, A_{new}, B_{new}, y_{new}, *and* b_{new}, *respectively*

After successful mutual authentication process, *U* and *S* have the same session key $SK = h(h(ID \| y \| b_{new}))$.

4.4 Password change phase

This phase is invoked whenever *U* wants to change her *PW* with a new one (PW_{new}). She inserts her smart card into the smart card reader and keys her *ID* and *PW*, and requests to change password. Then, her smart card carries out the following process:

- *Computes:*
  $h(ID \| h(x \| z) \| y)^* = N \oplus h(ID \| PW \| b) \oplus h(ID \| y)$
  $A^* = h(h(ID \| h(x \| z) \| y)^*)$
- *Compares:*
  A^* *?= A if holds, the identity of U is assured and U can key a new password* (PW_{new})*; otherwise, the smart card rejects the password change request*
- *Computes:*
  $N_{new} = h(ID \| h(x \| z) \| y) \oplus h(ID \| PW_{new} \| b) \oplus h(ID \| y)$

The value of N_{new} is stored in the smart card to replace *N*.

5. Security analysis

In this section, we demonstrate that our proposed scheme can resist very well-known attacks and achieves the desirable security goals described in [19, 20]. Table 1 shows the security comparison between our proposed scheme and Sood et al.'s schemes.

5.1 Denial of service attack

Suppose that the adversary can get access to the victim's smart card and she wants to change the password. However, the adversary will fail in this attack because the smart card verifies the identity of the owner before updates or modifies the password for another one.

5.2 Impersonation attack

If an adversary wants to impersonate *U*, she must be able to forge a valid login message (*y, B, CID*, *M*). Suppose that the adversary has intercepted one of the victim's login request message (*y, B, CID*, *M*) and she knows the security information (*N, A, B, y, b, h*( )) stored in victim's smart card. However, she cannot compute a valid session key $SK = h(h(ID \| y \| b_{new}))$ without the knowledge of *U*'s *ID* and b_{new} because she cannot extract the correct *ID* from $B = h(x \| z) \oplus h(h(x \| z) \| y) \oplus ID$ or b_{new} from $CID = h(ID \| h(x \| z) \| y) \oplus h(ID \| y) \oplus b_{new}$.

5.3 Malicious user attack

A legal but malicious user can attempt to extract the server secret keys *x* and *z* from $N = h(ID \| h(x \| z) \| y) \oplus h(ID \| PW \| b) \oplus h(ID \| y)$ or $B = h(x \| z) \oplus h(h(x \| z) \| y) \oplus ID$. However, this attempt will fail because it is computationally infeasible to invert the one-way hash function *h*( ).

5.4 Off-line ID guessing attack

If the adversary tries to obtains *U*'s *ID* from $N = h(ID \| h(x \| z) \| y) \oplus h(ID \| PW \| b) \oplus h(ID \| y)$, $A = h(h(ID \| h(x \| z) \| y))$ or $B = h(x \| z) \oplus h(h(x \| z) \| y) \oplus ID$, she needs to guess three security parameters *ID*, *x* and *z* correctly at the same time which represents a higher challenge than just one security parameter. Moreover, the value of *x* and *z* are hidden by a one-way hash function.

5.5 Parallel session attack

If the adversary has intercepted the victim's login request message (*y, B, CID*, *M*) and the login response message (*O, C*), she cannot compute a valid login request message by any combination of (*y, B, CID*, *M*) and (*O, C*). Moreover, the adversary cannot extract the *U*'s *ID*, y_{new} and b_{new} from $C = h(N_{new} \| A_{new} \| B_{new} \| y_{new} \| b_{new})$ or $O = E_{SK}(N_{new} \| A_{new} \| B_{new} \| y_{new})$. Furthermore, the adversary cannot compute the session key $SK = h(h(ID \| y \| b_{new}))$ because she does not *ID* and b_{new}.

5.6 Replay attack

If the adversary has intercepted the victim's login request message (*y, B, CID*, *M*) and the login response message (*O, C*), she cannot compute a valid login request message by any combination of (*y, B, CID*, *M*) and (*O, C*). Moreover, the adversary cannot extract the *U*'s *ID*, y_{new} and b_{new} from $C = h(N_{new} \| A_{new} \| B_{new} \| y_{new} \| b_{new})$ or $O = E_{SK}(N_{new} \| A_{new} \| B_{new} \| y_{new})$. Furthermore, the adversary cannot know the session key $SK = h(h(ID \| y \| b_{new}))$ because she does not *ID* and b_{new}.

5.7 Server spoofing attack

Suppose that the adversary wants to impersonate *S*, she must be able to forge a valid login response message (*O, C*). However, this attempt will fail because the adversary cannot compute a valid $SK = h(h(ID \| y \| b_{new}))$ without the knowledge of *x* and *z*. Moreover, the adversary cannot compute a valid *C* or *O* without the correct *U*'s *ID*.

5.8 Stolen smart card attack

Suppose that the adversary has stolen victim's smart card and she can access to the security information (*N, A, B, y, b, h*( )) stored in victim's smart card. However, the adversary cannot obtain information for creating a valid login request message (*y, B, CID*, *M*) without the knowledge of *ID* and *PW*.

6. Comparison

Table 1 shows that our proposed scheme does not need a verification table for carrying out the verification phase. On the other hand, the schemes proposed by Sood et al. require that the server maintains a verification table which represents security vulnerability for the entire system. Moreover, the schemes proposed by Sood et al. require that each user reveals her password to *S*, during the registration phase, while our scheme keeps the privacy of *U*'s password. Furthermore, the proposed scheme uses nonce instead of time-stamping, avoiding the time-synchronization problem between *U* and *S*. In fact, the proposed scheme is more secure than Sood et al.'s schemes.

Security goal	[15]	[14]	Our scheme
No verification table	No	No	Yes
Users choose password freely	Yes	Yes	Yes
No password reveal	No	No	Yes
Mutual authentication	Yes	Yes	Yes
Session key agreement	Yes	Yes	Yes
User anonymity	Yes	Yes	Yes
No time-synchronization	No	No	Yes
Efficiency for wrong password login	Yes	Yes	Yes

Table 1. Comparison between our scheme and Sood et al.'s schemes.

7. Conclusions

In this paper, we analyzed two schemes by Sood-Sarje-Singh and found that both schemes are unsecured. We proposed an improvement of Sood et al.'s schemes to overcome the security flaws without damage their merits. Moreover, Table 1 demonstrates that the improved scheme can achieve all the desirable security goals, such as without maintain a verification table and no time-synchronization.

Acknowledgements

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions. This research was supported by The Mexican Teacher Improvement Program (PROMEP), under the project number PROMEP/103.5/12/4525.

References

[1] Ku W.-C. & Chen S.-M., Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, 2004, pp. 204-207.

[2] Chang C.-C. & Wu T.-C., Remote password authentication with smart cards, IEE Proceedings-E, Vol. 138, No. 3, 1991, pp. 165-168.

[3] Hwang M. S. & Li L. H., A new remote user authentication scheme using smart card, IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, 2000, pp. 28-30.

[4] Evans A.-J., Kantrowitz W. & Weiss E., A user authentication scheme not requiring secrecy in the computer, Communications of the ACM, Vol. 17, No. 8, 1974, pp. 437-442.

[5] Feistel H., Notz W.-A. & Smith J.-L., Some cryptographic techniques for machine to machine data communications, Proccedings of the IEEE, Vol. 63, No. 11, 1975, pp. 1545-1554.

[6] Chang C.-C. & Wu T.-C., A password authentication scheme without verification tables, 8th IASTED International Simposium of Applied Informatics, 1990, pp. 202-204.

[7] Chien H. Y., Jan J. K. & Tseng Y. M., An Efficient and practical solution to remote authentication: smart card, Computers & Security, Vol. 21, No. 4, 2002, pp. 372-375.

[8] Hsu C.-L., Security of two remote user authentication schemes using smart cards, IEEE Transaction on Consumer Electronics, Vol. 49, No. 4, 2003, pp. 1196-1198.

[9] Das M.-L., Saxena A. & Gulati V.-P., A Dynamic ID-based remote user authentication scheme, IEEE Transactions on Consumer Electronics, Vol. 50, No. 2, 2004, pp. 629-631.

[10] Wang Y.-Y., Liu J.-Y., Xiao F. X., & Dan J., A more efficient and secure dynamic ID-based remote user authentication scheme, Computer Communications, Vol. 32, No. 2, 2009, pp. 583-585.

[11] Goriparthi T., Das M.-L. & Saxena A., An improved bilinear pairing based remote user authentication scheme, Computer Standards & Interfaces, Vol. 31, No. 1, 2009, pp. 181-185.

[12] Liao I.-E., Lee C.-C. & Hwang M.-S., Security enhancement for a dynamic ID-based remote user authentication Scheme, International Conference on Next Generation Web Services Practices, 2005, pp. 437-440.

[13] Liou Y.-P., Lin J. & Wang S.-S., A New Dynamic ID-Based Remote User Authentication Scheme using Smart Cards, 16th Information Security Conference, 2006, pp. 198-205.

[14] Sood S.-K., Sarje A.-K. & Singh K., An improvement of Wang et al.'s authentication scheme using smart cards, National Conference on Communications, 2010, pp. 29-31.

[15] Sood S.-K., Sarje A.-K. & Singh K., An Improvement of Liao et al.'s Authentication Scheme using Smart Cards, IEEE 2nd International Advance Computing Conference, 2010, pp. 240-245.

[16] Juang W.-S., Efficient password authenticated key agreement using smart cards, Computers & Security, Vol. 23, No. 2, 2004, pp. 167-173.

[17] Lee S.-W., Kim H.-S. & Yoo K.-Y., Efficient nonce-based remote user authentication scheme using smart cards, Applied Mathematics and Computation, Vol. 167, No. 1, 2005, pp. 355-361.

[18] Liaw H.-T., Lin J.-F. & Wu W.-C., An efficient and complete remote user authentication scheme using smart cards, Mathematical and Computer Modelling, Vol. 44, No. 1-2, 2006, pp. 223–228.

[19] Madhusudhan R. & Mittal R.-C., Dynamic ID-based remote user password authentication schemes using smart cards: A review, Journal of Network and Computer Applications, Vol. 35, No. 4, 2012, pp. 1235-1248.

[20] Li C.-T., Secure smart card based password authentication scheme with user anonymity, Information Technology and Control, Vol. 40, No. 2, 2011, pp. 157-162.

[21] Kocher P., Jaffe J. & Jun B., Differential power analysis, Advances in Cryptology - Crypto'99, vol. LNCS 1666, 1999, pp. 388-397.

[22] Messerges T.-S., Dabbish E.-A. & Sloan R.-H., Examining smart-card security under the threat of power analysis attacks, IEEE Transactions on Computers, Vol. 51, No. 5, 2002, pp. 541-552.

[23] Hsiang H. C. & Shih W. K., Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment, Computer Standards & Interfaces, Vol. 31, No. 6, 2009, pp. 1118-1123.