# Analysis and Improvement of an Authentication Scheme Using Smart Cards

Sonam Devgan Kaul and Amit K. Awasthi

Department of Applied Mathematics,
Gautam Buddha University, Greater Noida,201308, UP, India
{sonamdevgan11,awasthi.amitk}@gmail.com

**Abstract.** In 2010, Sood et al [16] proposed a secure dynamic identity based authentication scheme using smart cards. They claimed that their scheme is secure against various attacks. In this paper, we demonstrate that their scheme is completely insecure and vulnerable to outsider attack as well as insider attack. An outsider attacker can obtain the common session key between the user and the server, while an insider attacker can get not only the session key but also the secret key of the server. Therefore, the entire system collapses. To remedy these security flaws, an improved scheme is proposed to withstand these attacks.

**Keywords:** cryptanalysis, authentication protocol, smart cards, dynamic identity, password.

## 1 Introduction

With the rapid increasing need of remote digital services and electronic transactions; authentication schemes that ensure secure communication through an insecure channel are gaining popularity and have been studied widely in recent years. In 1981, Lamport [9] proposed first remote user password based authentication scheme by employing a one way hash chain, in an insecure and untrusted network, but this scheme has a major drawback of its dependency on verification table. Smart cards implementation solved this problem of dependency on verification tables and ensures secure communication. That is why, Smart cards based authentication schemes are becoming day by day more popular. In 2001, Hwang et al [6] proposed first smart cards based authentication scheme. As Security and efficiency are the main factors for any authentication scheme from the user's perspective. In view of the fact, several smart cards based remote user authentication schemes [1,2,3,5,8,11,12,15] have been proposed.

In 2004, Das et al [4] proposed a dynamic identity based remote user authentication scheme using smart cards that preserves user's anonymity. However, their scheme is vulnerable to various attacks. In 2005, Liao et al [10] proposed an improved scheme that achieves mutual authentication. In 2006, Yoon and Yoo [17] cryptanlyse the mutual authentication of Liao et al's scheme. In the same direction in 2010, Sood et al [16] proposed an improved protocol of Liao

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 719–728, 2013.

et al's scheme and demonstrated that improved protocol is secure against various attacks like malicious user attack, impersonation attack, offline and online dictionary attack, denial of service attack and so on.

Recently, Pelaez and Novella [14] demonstrated that Sood et al's scheme is vulnerable to malicious user attack, man-in-the-middle attack, stolen smart card attack, off-line ID guessing attack, impersonation attack and server spoofing attack. In this paper, we also pointed out few weaknesses of the scheme. This paper shows that an insider attacker who has access to server can obtain the secret key of the server, which makes this scheme totally insecure. To remedy these security flaws, we proposed an upgraded authentication scheme, that preserves some properties of Sood et al's scheme, resolves all the identified weaknesses of their scheme and makes it more secure and efficient for practical applications.

The rest of the paper is organized as follows: Section 2 briefly reviews Sood et al's authentication scheme. Section 3 describes the weaknesses of Sood et al's scheme. Our proposed scheme is presented in Section 4, followed by security analysis in Section 5. Finally, we conclude the paper in Section 6.

## 2 Review of Sood et al's Scheme

In this section, we examine the dynamic identity based authentication scheme proposed by Sood et al in 2010. This scheme consists of four phases: registration phase, login phase, verification and session key agreement phase and password changing phase. The notations used throughout the paper are summarized in table 1.

**Table 1.** Notations and Symbols used in paper

| | |
|---|---|
| $U_i$ | Legitimate $i^{th}$ user |
| $ID_i$ | Identifier of $U_i$ |
| $PW_i$ | Password of $U_i$ |
| $S$ | The Server |
| $x$ | Secret key of the server $S$ |
| $y_i$ | Server's random value |
| $sk_i$ | Session Key |
| $T$ | Current date and time of input device |
| $T'$ | Current date and time of the server $S$ |
| $\delta T$ | Expected time interval for a transmission delay |
| $H(.)$ | Secure one way Hash Function |
| $\oplus$ | Bitwise Exclusively or (XOR) operation |
| $\|$ | Bitwise concatenation operation |

### 2.1 Registration Phase

To register itself to the server $S$, the user $U_i$ chooses his identity $ID_i$ and password $PW_i$ and sends it to server $S$ via a secure communication channel. Then the server $S$ chooses random value $y_i$ for $i^{th}$ user and computes:

$N_i = H(PW_i) \oplus H(y_i \| ID_i) \oplus H(x)$,
$B_i = y_i \oplus H(PW_i)$,
$V_i = H(ID_i \| PW_i) \oplus PW_i$,
$D_i = H(y_i \| ID_i)$

The server $S$ stores $y_i \oplus x$ and $ID_i \oplus H(x)$ corresponding to $D_i$ in its database. Then $S$ stores $(N_i, B_i, V_i, H(.))$ into smart card and sends it to $U_i$ via a secure communication channel.

### 2.2 Login Phase

When the user $U_i$ wants to login, he simply inserts the smart card into the card reader and keys in $ID_i^*$ and $PW_i^*$. The smart card computes
$V_i^* = H(ID_i^* \| PW_i^*) \oplus PW_i^*$
and verifies it with the stored $V_i$. After verifying the legality of the user, the smart card computes:
$y_i = B_i \oplus H(PW_i)$,
$H(x) = N_i \oplus H(PW_i) \oplus H(y_i \| ID_i)$,
$CID_i = H(y_i \| ID_i) \oplus H(H(x) \| T)$,
$M_i = H(H(x) \| H(y_i) \| T)$
and sends the login request message $(CID_i, M_i, T)$ to the server $S$.

### 2.3 Verification and Session Key Agreement Phase

Upon receiving the login request, $S$ first check the validity of time stamp $T$ by checking $(T' - T) \leq \delta T$ to accept/reject the login request. If login request is accepted, the server $S$ computes $D_i^* = CID_i \oplus H(H(x) \| T)$ and extract $y_i \oplus x$ and $ID_i \oplus H(x)$ corresponding to $D_i^*$ from its database to obtain $y_i$ and $ID_i$. Then the server computes $M_i^* = H(H(x) \| H(y_i) \| T)$ and verifies it with the received $M_i$ . If it finds true, then $U_i$ is authenticated. Finally, $S$ and $U_i$ computes common session key $sk_i = H(ID_i \| y_i \| H(x) \| T)$ for further communication.

### 2.4 Password Change Phase

Whenever $U_i$ wants to update his password, he inserts his smart card into card reader and presents the credentials such as identifier $ID_i$ and password $PW_i$. After verifying the legality of the user by verifying $V_i$, the smart card ask $U_i$ to input the new password $PW_i^{new}$ to replace the value of $N_i, B_i$ and $V_i$ with the $N_i^{new}, B_i^{new}$ and $V_i^{new}$ where $N_i^{new} = N_i \oplus H(PW_i) \oplus H(PW_i^{new})$, $B_i^{new} = B_i \oplus H(PW_i) \oplus H(PW_i^{new})$ and $V_i^{new} = H(ID_i \| PW_i^{new}) \oplus PW_i^{new}$.

## 3 Security Flaws in Sood et al's Scheme

Here, we consider an outside attacker is one who has no direct access to the server. An user with valid identity and password also comes in outside attacker

category. On the other side, Insider attacker is one who is having administrative access of the server. It is the basic requirement of the authentication scheme that any insider can not get the secret key of the server or any attacker can not compute the common session key between the user and the server. Sood et al's scheme is highly insecure as the basic requirement is not fulfilled. In this section, we demonstrate that Sood et al's scheme is vulnerable to outsider attack and insider attack.

### 3.1 Outsider Attack

The secret information stored in the smart card can be extracted by some means, such as monitoring the power consumption [7] or analyzing the leaked information [13]. So, any outsider $U_a$, who is the legal user and owns a smart card, can get information $(N_a, B_a, V_a, H(.))$, that is stored on his smart card, where

$N_a = H(PW_a) \oplus H(y_a \| ID_a) \oplus H(x)$,
$B_a = y_a \oplus H(PW_a)$,
$V_a = H(ID_a \| PW_a) \oplus PW_a$,

then he compute: $y_a = B_a \oplus H(PW_a)$ and $H(x) = N_a \oplus H(PW_a) \oplus H(y_a \| ID_a)$. Thus, an outsider can get $H(x)$ which is same for each legal user and is very sensitive information, the hash value of secret key of the server.

An the attacker extracts security parameters $(N_i, B_i, V_i, H(.))$ from other legitimate user $U_i's$ smart card. During the login transaction between $U_i$ and the server, the attacker intercepts login request message $(CID_i, M_i, T)$ that the user $U_i$ sends to the server $S$. The attacker uses his knowledge of $H(x)$ and computes the following

$$y_i = CID_i \oplus N_i \oplus B_i \oplus H(H(x) \| T) \oplus H(x)$$

In such a way an outsider $U_a$ obtains $H(x)$ as well as $y_i$, just by using his own smart card and the legitimate user's smart card. Then, an outsider attacker (the user $U_a$) can easily compute the session key for the transmission between server and the user $U_i$, as,

$$sk_i = H(ID_i \| y_i \| H(x) \| T)$$

and thus, he can get the unauthorized access to the services provided by the server to the user $U_i$.

### 3.2 Insider Attack

The system manager or a privileged insider user, who has direct access to the server, simply apply for registration and gets a valid smart card. Now he may adopt the procedure like outsider attacker to get $H(x)$ as well as $y_i$. He computes $D_i = H(y_i \| ID_i)$ and extracts the information $y_i \oplus x$ and $ID_i \oplus H(x)$ from server's database. With this information he can easily compute the secret key of the server as

$$x = y_i \oplus (y_i \oplus x)$$

Thus any privileged insider user of the system, after getting the secret key of the server can purposely leak the information or impersonate the legitimate user or

may modify the information. He can also issue an illegal smart card to some fake user. Thus, Sood et al's proposed scheme is insecure and vulnerable to various attacks and is not secure and efficient for practical applications.

## 4 Our Proposed Scheme

In this section, we propose an upgraded authentication scheme, that preserves the properties of Sood et al's scheme and resolves all the identified weaknesses of their scheme and make it secure and efficient for practical applications. The scheme consists of four phases: registration phase, login phase, verification & session key agreement phase and password changing phase.

### 4.1 Registration Phase

When the user $U_i$ wants to register, he chooses his identity $ID_i$ and password $PW_i$, and send it to the server $S$ via a secure communication channel. Then, the server $S$ chooses random value $y_i$ for $i^{th}$ user and computes:

$N_i = H(y_i \| PW_i) \oplus H(y_i \| ID_i) \oplus H(x)$,
$B_i = y_i \oplus H(PW_i)$,
$V_i = H(ID_i \| PW_i) \oplus PW_i$,
$D_i = H(y_i \| ID_i)$

$S$ chooses the value of $y_i$ in such a way that the value of $D_i$ must be unique for each user. The server $S$ stores $y_i \oplus H(x||ID_i)$ and $ID_i \oplus H(x)$ corresponding to $D_i$ in its database. Then, $S$ stores $(N_i, B_i, V_i, H(.))$ into smart card and sends it to $U_i$ via a secure channel.

### 4.2 Login Phase

The user $U_i$ inserts the smart card in to the card reader and keys in $ID_i^*$ and $PW_i^*$, then the smart card computes

$V_i^* = H(ID_i^* \| PW_i^*) \oplus PW_i^*$

and checks whether computed $V_i^*$ is equal to the stored $V_i$ or not. If they are equal, the requested user is the legitimate bearer of the smart card otherwise rejects the login request. To resist offline password guessing attack, the card reader locks the card if $U_i$ enters either wrong identifier or wrong password more than limited number of times. After verifying the legality of the user, the smart card computes:

$y_i = B_i \oplus H(PW_i)$,
$H(x) = N_i \oplus H(y_i \| PW_i) \oplus H(y_i \| ID_i)$,
$CID_i = H(y_i \| ID_i) \oplus H(H(x) \| T)$,
$M_i = H(H(x) \| H(y_i) \| T)$

and sends the login request message $(CID_i, M_i, T)$ to the server $S$.

**Table 2.** Registration Phase

| $U_i$ | | $S$ |
|---|---|---|
| Choose $ID_i$ and $PW_i$ | $\xrightarrow[Secure]{ID_i,\ PW_i}$ | |
| | | Choose random value $y_i$ |
| | | $N_i = H(y_i \| PW_i) \oplus H(y_i \| ID_i) \oplus H(x)$ |
| | | $B_i = y_i \oplus H(PW_i)$ |
| | | $V_i = H(ID_i \| PW_i) \oplus PW_i$ |
| | | $D_i = H(y_i \| ID_i)$ |
| | | Store $y_i \oplus H(x \| ID_i)$ and $ID_i \oplus H(x)$ for each $D_i$ |
| | | Store $(N_i, B_i, V_i, H(.))$ into smart card |
| | $\xleftarrow[SmartCard]{(N_i,B_i,V_i,H(.))}$ | |

**Table 3.** Login Phase

| $U_i$ | **Smart card** | **S** |
|---|---|---|
| Input $ID_i^*$ and $PW_i^*$ | | |
| | Compute $V_i^* = H(ID_i^* \| PW_i^*) \oplus PW_i^*$ | |
| | Verifies $V_i^* \ ? = \ V_i$ | |
| | Compute $y_i = B_i \oplus H(PW_i)$ | |
| | $H(x) = N_i \oplus H(y_i \| PW_i) \oplus H(y_i \| ID_i)$ | |
| | $CID_i = H(y_i \| ID_i) \oplus H(H(x) \| T)$ | |
| | $M_i = H(H(x) \| H(y_i) \| T)$ | |
| | $\xrightarrow{(CID_i, M_i, T)}$ | |

### 4.3 Verification and Session Key Agreement Phase

Upon receiving the login request, $S$ first check the validity of time stamp $T$ by checking $(T' - T) \leq \delta T$ to accept/reject the login request. If it finds incorrect, the login request is rejected else the server $S$ computes

$D_i^* = CID_i \oplus H(H(x) \| T)$

and extract $y_i \oplus H(x \| ID_i)$ and $ID_i \oplus H(x)$ corresponding to $D_i^*$ from its database and recompute $ID_i$ and $y_i$ using its secret information $x$. Then the server computes

$M_i^* = H(H(x) \| H(y_i) \| T)$

and verifies computed $M_i^*$ with the received $M_i$. If it finds true, then $U_i$ is authenticated and the login request is accepted else the connection is interrupted. Finally, $S$ and $U_i$ computes the common session key $sk_i = H(ID_i \| y_i \| H(x) \| T)$ of the transmission.

### 4.4 Password Change Phase

Whenever $U_i$ wants to update his password, he inserts his smart card into the card reader and presents the credentials such as identifier $ID_i$ and current password $PW_i$. After verifying the legality of the user by verifying $V_i$, the smart card

**Table 4.** Verification and Session Key Agreement Phase

| $U_i$ | | **S** |
|---|---|---|
| | $\xrightarrow{(CID_i, M_i, T)}$ | |
| | | Verifies $(T' - T) \leq \delta T$ |
| | | Compute $D_i^* = CID_i \oplus H(H(x)\|\|T)$ |
| | | Extract $D_i^*$, $y_i \oplus H(x\|\|ID_i)$ and $ID_i \oplus H(x)$ |
| | | Obtain $ID_i$ and $y_i$ |
| | | Compute $M_i^* = H(H(x)\|\|H(y_i)\|\|T)$ |
| | | Verifies $M_i^* \stackrel{?}{=} M_i$ |
| | | Session Key $sk_i = H(ID_i\|\|y_i\|\|H(x)\|\|T)$ |
| Session Key | | |
| $sk_i = H(ID_i\|\|y_i\|\|H(x)\|\|T)$ | | |

ask $U_i$ to input the new password $PW_i^{new}$ to replace the value of $N_i, B_i$ and $V_i$ with the $N_i^{new}, B_i^{new}$ and $V_i^{new}$ where $N_i^{new} = N_i \oplus H(y_i\|PW_i) \oplus H(y_i\|PW_i^{new})$, $B_i^{new} = B_i \oplus H(PW_i) \oplus H(PW_i^{new})$ and $V_i^{new} = H(ID_i\|PW_i^{new}) \oplus PW_i^{new}$. To resist offline password guessing attack, the card reader locks the card if $U_i$ enters either wrong identifier or wrong password more than limited number of times.

## 5 Security Analysis

In this section, we analyze the security of our scheme under the assumption that the secret information stored in the smart card could be extracted by some means, such as monitoring the power consumption [7] or analyzing the leaked information [13].

### 5.1 Denial of Service Attack

To resist password guessing attack, the card reader locks the card if someone enters either wrong identifier or wrong password more than limited number of times, So even if an adversary got the legitimate user smart card, but he is unable to create valid login request by guessing identity $ID_i$ and password $PW_i$ correctly at the same time. Thus, the proposed protocol is secure against denial of service attack.

### 5.2 Malicious User Attack

A legal but malicious user $U_a$ can get the value of $H(x)$ from his own card, which is same for each user. But from $H(x)$, $U_a$ may not be able to compute $y_i$, which makes the proposed protocol secure against malicious user attack.

### 5.3 Impersonation Attack

As both $CID_i$ and $M_i$ are protected by secure one way hash function, any modification in login request message $(CID_i, M_i, T)$ will be detected by the server by verifying $M_i$. So, because the attacker has no way to find $PW_i$ and $y_i$ of the legitimate user $U_i$, he can not modify login request message, which makes this protocol secure against impersonation attack.

### 5.4 Offline Password Guessing Attack

After gathering the information on legitimate user $U_i$'s smart card, an attacker can intercept the login request message $(CID_i, M_i, T)$ during the login transaction, and try to guess out $ID_i$, $PW_i$, $y_i$ and $x$, but it is not possible to guess out all the parameters correctly at the same time, which makes this protocol secure against offline guessing attacks.

### 5.5 Stolen Smart Card Attack

An attacker can extract security parameters $(N_i, B_i, V_i, H(.))$ from legitimate user $U_i$'s smart card. But, this information does not help him to find out the value of server's secret $x$, or user's secret parameter $y_i$ corresponding to the $i^{th}$ legitimate user. He can not use this information to generate fake login request. He is also not able to play as man in middle by using any information on card. Thus, the proposed protocol is secure against stolen smart card attack.

### 5.6 Insider Attack

Any privileged insider user (a system manager as an attacker) can obtain $H(x)$ from his registered legal smart card, but without knowing the password of $i^{th}$ user, he cannot compute $y_i$ and secret key $x$ of the server and can not use the secret information for personal benefit. Thus, this protocol is secure against an insider attack.

### 5.7 Online Password Guessing Attack

As the card reader locks the card after limited number of wrong login attempts, So it is impossible for an attacker, to pretend to be the legitimate user $U_i$ and try to login the server by online guessing different words as identity $ID_i$ and password $PW_i$ of the user $U_i$.

### 5.8 Server Spoofing Attack

An adversary may not be able to masquerade server by modifying login transaction message because of verification of $M_i$. So, he may not be able to compute the common session key $sk_i = H(ID_i \| y_i \| H(x) \| T)$. Moreover, the session key is session variant for the same user. Thus, the proposed protocol is secure against server spoofing or masquerading attack.

### 5.9 Stolen Verifier Attack

If an attacker may be able to steal the verification table from the server, then he can obtain $y_i \oplus H(x\|ID_i)$ and $ID_i \oplus H(x)$ corresponding to $D_i$ from its database but from this, he is unable to compute the secret key $x$ and $y_i$ of the legitimate user.

### 5.10 Replay Attack and Parallel Session Attack

Our proposed protocol, can withstand Replay attack and Parallel Session Attack because replaying a login request message $(CID_i, M_i, T)$ of one session into another session is useless as the authenticity of the login request is verified by checking the freshness of the time stamp $T$ and also by replaying a login request message within the valid time frame window, can not give an attacker, the common session key between the user $U_i$ and the server $S$.

### 5.11 Man-in-the-Middle Attack

Even if an adversary can intercept the session, get the login request message $(CID_i, M_i, T)$ and authenticate himself to the server $S$, but he can not compute the session key $sk_i = H(ID_i\|y_i\|H(x)\|T)$ between the user and the server as there are two secret parameters $H(x)$ and $y_i$ are included in the session key. Only registered users are able to compute $H(x)$, but they can not compute $y_i$ for any other user until they know the password of the user $U_i$. Thus, either the valid user who initiated the session or the server can retrieve the original message during transmission.

## 6 Conclusion

In this paper, we analysed Sood et al's dynamic identity based authentication scheme using smart cards and its immunity against various attacks. We got that their scheme is insecure for practical applications and vulnerable to outsider and insider attacks. To remedy these security flaws, we proposed an upgraded protocol for authentication scheme that preserves the similar properties of their scheme and resolves all the identified weaknesses of their scheme and make it more secure and efficient for practical purpose.

## References

1. Awasthi, A.K.: Comment on a dynamic id-based remote user authentication scheme. Transaction on Cryptology 1(2), 15–16 (2004)
2. Chien, H.-Y., Chen, C.H.: A remote authentication scheme preserving user anonymity. Proc. Advanced Information Networking and Applications 2, 245–248 (2005)
3. Chien, H.-Y., Jan, J.-K., Tseng, Y.-M.: An efficient and practical solution to remote authentication: smart card. Computers and Security 21(4), 372–375 (2002)

4. Das, M.L., Saxena, A., Gulati, V.P.: A dynamic id-based remote user authentication scheme. IEEE Transactions on Consumer Electronics 50(2), 629–631 (2004)
5. He, D., Wu, S.: Security flaws in smart card based authentication scheme for multi server environment. Wireless Personal Communications (2012) (0929-6212)
6. Hwang, M.-S., Li, L.H.: A new remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics 46(1), 28–30 (2000)
7. Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)
8. Ku, W.-C., Chang, S.-T.: Impersonation attack on dynamic id-based remote user authentication scheme using smart cards. IEICE, Transactions on Communications E88-B(5), 2165–2167 (2005)
9. Lamport, L.: Password authentication with insecure communication. Communication of the ACM 24(11), 770–772 (1981)
10. Liao, I.-E., Lee, C.-C., Hwang, M.-S.: Security enhancement for a dynamic id-based remote user authentication scheme. Proc. Conference on Next Generation Web Services Practice, 437–440 (2005)
11. Liou, Y., Lin, J., Wang, S.: A new dynamic id-based remote user authentication scheme using smart cards. In: Proc. 16th Information Security Conference, Taiwan, pp. 198–205 (July 2006)
12. Liu, J., Zhong, S.: Analysis of kim-jeon-yoo password authentication scheme. Cryptologia 33(2), 183–187 (2009)
13. Messerges, T.S., Dabbish, E.A., Sloan, R.H.: Examining smart card security under the threat of power analysis attacks. IEEE Transactions on Computers 51(5), 541–552 (2002)
14. Pelaez, R.M., Novella, F.R.: Cryptanalysis of sood et al's authentication scheme using smart cards. IACR Cryptology ePrint Archive (386) (July 2012)
15. Snih, H.C.: Cryptanalysis on two password authentication schemes. In: Labortary of Cryptography and Information Security. National Central University, Taiwan (2008)
16. Sood, S.K., Sarje, A.K., Singh, K.: An improvement of liao et al's authentication scheme using smard cards. In: Proc. IEEE 2nd International Advance Computing Conference, pp. 240–245 (February 2010)
17. Yoon, E.-J., Yoo, K.-Y.: Improving the dynamic ID-based remote mutual authentication scheme. In: Meersman, R., Tari, Z., Herrero, P. (eds.) OTM 2006 Workshops. LNCS, vol. 4277, pp. 499–507. Springer, Heidelberg (2006)