Cryptanalysis of Sood et al.'s Authentication Scheme using Smart Cards

Rafael Martínez-Peláez [a,*] and Francisco Rico-Novella [b]

[a,*] *Universidad de la Sierra Sur, Instituto de Informática, Guillermo Rojas Mijangos S/N. 70800 Miahuatlán de Porfirio Díaz, Mexico*
rpelaez@unsis.edu.mx

[b] *Technical University of Catalonia, Department of Telematics Engineering, Jordi Girona 31. 08034 Barcelona, Spain*
f.rico@entel.upc.edu

Abstract: In 2010, Sood-Sarje-Singh proposed a dynamic ID-based remote user authentication scheme and claimed that their scheme is more secure than Das et al.'s scheme and Liao et al.'s scheme. However, we show that Sood et al.'s scheme is still 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, making the scheme unfeasible for practical implementation.

Keywords: Authentication; ID-based; Cryptanalysis; Network Security; Smart Cards

1. Introduction

The most popular mechanism to carry out the user authentication 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 (Ku and Chen, 2004).

Although, many approaches have been proposed (Evans et al., 1974; Feistel et al., 1975) to overcome the weakness of storing users' identity and password in a database, using cryptography or one-way hash functions, 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 (Chang and Wu, 1990) proposed a remote user authentication scheme without a verification table, in 1990. In 1991, Chang and Wu (Chang and Wu, 1991) introduced the concept of timestamp in the login request message to prevent the replay attack. In 2002, Chien et al. (Chien et al., 2002) proposed a remote user authentication scheme which requires low-computational cost. However, Hsu (Hsu, 2003) demonstrated that Chien et al.'s scheme is vulnerable to parallel session attack. Moreover, Ku et al. (Ku and Chen, 2004) demonstrated that Chien et al.'s scheme is vulnerable to insider attack and guessing attack.

In 2004, Das et al. (Das et al., 2004) introduced the concept of dynamic ID-based remote user authentication scheme using smart cards. Their scheme prevents that an attacker can know the user's identity. However, the scheme is susceptible to insider attack, masquerade attack, and server spoofing attack (Goriparthi et al., 2009; Liao and Wang, 2009; Wang et al., 2009). Liao et al. (Liou et al., 2006) proposed a new scheme which resolves the security vulnerabilities of Das et al.'s scheme, in 2005. However, Sood et al. (Sood et al., 2010) demonstrated that Liao et al.'s scheme is vulnerable to malicious user attack, impersonation attack, stolen smart card attack, and off-line password guessing attack.

In this paper, we demonstrate that Sood et al.' 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.

2. Review of Sood et al.'s scheme

In this section, we briefly review Sood et al.'s scheme (Sood et al., 2010). The scheme consists of four phases (registration, login, verification and session key agreement, and password change). The notations used throughout this paper are summarized in Table 1.

Table 1. Notations

U	User
ID	User's identity
PW	User's password
S	Server
x	Server's secret key
$H(\cdot)$	One-way hash function
T	Timestamp
$\|\|$	Concatenation operation
$\oplus$	Exclusive-or operation

2.1. Registration phase

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

1. U chooses her ID and PW
2. U sends (ID, PW) to S via a secure communication channel
3. S chooses random value y
4. S computes:
   $N = \mathrm{h}(PW) \oplus \mathrm{h}(y \,||\, ID) \oplus \mathrm{h}(x)$
   $B = y \oplus \mathrm{h}(PW)$
   $V = \mathrm{h}(ID \,||\, PW) \oplus PW$
   $D = \mathrm{h}(y \,||\, ID)$
5. S stores $y \oplus x$ and $ID \oplus \mathrm{h}(x)$ corresponding to D in a database
6. S issues the smart card to U, through a secure communication channel. The smart card contains the following security parameters: N, B, V, h( )

2.2. Login phase

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

1. Computes:
   $V^* = \mathrm{h}(ID^* \,||\, PW^*) \oplus PW^*$
2. Compares:
   $V^* \stackrel{?}{=} V$
3. After verification, the smart card computes:
   $y = B \oplus \mathrm{h}(PW)$
   $\mathrm{h}(x) = N \oplus \mathrm{h}(PW) \oplus \mathrm{h}(y \,||\, ID)$
   $CID = \mathrm{h}(y \,||\, ID) \oplus \mathrm{h}(\mathrm{h}(x) \,||\, T)$
   $M = \mathrm{h}(\mathrm{h}(x) \,||\, \mathrm{h}(y) \,||\, T)$
4. Smart card sends (CID, M, T) to S

2.3. Verification and session key agreement phase

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

1. 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.
2. Computes:
   $D^* = h(y \| ID)^* = CID \oplus h(h(x) \| T)$
3. Recovers:
   $y \oplus x$ and $ID \oplus h(x)$ corresponding to D^* from its database
4. Extracts:
   y from $y \oplus x$
   ID from $ID \oplus h(x)$
5. Computes:
   $M^* = h(h(x) \| h(y) \| T)$
6. Compares:
   $M^* \stackrel{?}{=} M$
   Finally, U and S computes the session key $SK = h(ID \| y \| h(x) \| T)$

2.4. 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 request to change the password to new one, then the smart card carries out the following operations:

1. Computes:
   $V^* = h(ID^* \| PW^*) \oplus PW^*$
2. Compares:
   $V^* \stackrel{?}{=} V$
3. Request to U a new password PW_{new}
4. 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}

3. Cryptanalysis of Sood et al.'s scheme

In this section, we demonstrate 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. Although the smart card is a tamper resistant device some researchers have shown that security parameters stored in a smart card can be recover by different methods (Kocher et al., 1999; Messerges et al., 2002).

3.1. Malicious user attack

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

1. Keys her ID^* and PW^*
2. 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

3.2. 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:

1. Computes:
   $D^* = h(y \| ID) = CID \oplus h(h(x)^* \| T)$

This attack is possible because S uses the same hash value of x for each user

3.3. 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, and 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:

1. Computes:
   $h(PW)^* = N \oplus D^* \oplus h(x)^*$
   $y^* = B \oplus h(PW)^*$

The attacker knows y without U's PW

3.4. Off-line ID guessing attack

The ID guessing attack is similar to password guessing attack described in (Sood et al., 2010), 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 the ID.

3.5. Impersonation attack

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

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

When S receives the login request message, S carries out the verification process as follows:

3. 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.
4. Computes:
   $D^* = h(y \| ID)^* = CID \oplus h(h(x) \| T)$
5. Recovers:

$y \oplus x$ and $ID \oplus h(x)$ corresponding to D^* from its database

6. Extracts:
   y from $y \oplus x$
   ID from $ID \oplus h(x)$
7. Computes:
   $M^* = h(h(x) \| h(y) \| T)$
8. Compares:
   $M^* ?= M$
   S accepts the login request

Moreover, the attacker can compute the secret key $SK^* = h(ID \| y \| h(x) \| T)$

3.6. Server spoofing attack

Because the legal but malicious user can know ID^*, y^*, and $h(x)^*$, and intercepts the login request message (CID, M, T) from the victim, the attacker computes:

1. the session key $SK^* = h(ID^* \| y^* \| h(x)^* \| T^*)$
   This attack is possible because the server does not send a confirmation message

4. Conclusions

In this paper, we briefly reviewed Sood et al.'s scheme and demonstrated that their 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. The security of the proposed scheme depends on the server's secret key which it is used to register each user, making possible that a legal but malicious user can recover it. Moreover, the server must store and maintain a directory with security parameters of each user.

Acknowledgments

This research was supported by The Mexican Teacher-Improvement Program (PROMEP)

References

Chang C.-C., Wu T.-C. A password authentication scheme without verification tables. Proceedings of the 8th IASTED International Symposium of Applied Informatics. (1990): 202-204.

Chang C.-C., Wu T.-C. Remote password authentication with smart cards. IEE Proceedings-E 1991; 138(3): 165-168.

Chien H.-Y., Jan J.-K., Tseng Y.-M. An Efficient and practical solution to remote authentication: smart card. Computers & Security 2002; 21(4): 372-375.

Das M.-L., Saxena A., Gulati V.-P. A Dynamic ID-based remote user authentication scheme. IEEE Transactions on Consumer Electronics 2004; 50(2): 629-631.

Evans A.-J., Kantrowitz W., Weiss E. A user authentication scheme not requiring secrecy in the computer. Communications of the ACM 1974; 17(8): 437-442.

Feistel H., Notz W.-A., Smith J.-L. Some cryptographic techniques for machine to machine data communications. Proceedings of the IEEE. (1975): 1545-1554.

Goriparthi T., Das M.-L., Saxena A. An improved bilinear pairing based remote user authentication scheme. Computer Standards & Interfaces 2009; 31(181-185).

Hsu C.-L. Security of two remote user authentication schemes using smart cards. IEEE Transaction on Consumer Electronics 2003; 49(4): 1196-1198.

Kocher P., Jaffe J., Jun B. Differential power analysis. Advances in Cryptology - Crypto'99. (1999), LNCS 1666: 388-397.

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 2004; 50(1): 204-207.

Liao Y.-P., Wang S.-S. A Secure Dynamic ID Based Remote User Authentication Scheme for Multi-server environment. Computer Standards & Interfaces 2009; 31(1): 24-29.

Liou Y.-P., Lin J., Wang S.-S. A New Dynamic ID-Based Remote User Authentication Scheme using Smart Cards. Proceedings of the 16th Information Security Conference. (2006): 198-205.

Messerges T.-S., Dabbish E.-A., Sloan R.-H. Examining smart-card security under the threat of power analysis attacks. IEEE Transactions on Computers 2002; 51(5): 541-552.

Sood S.-K., Sarje A.-K., Singh K. An Improvement of Liao et al.'s Authentication Scheme using Smart Cards. Proceedings of the IEEE 2nd International Advance Computing Conference. (2010): 240-245.

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 2009; 32(2): 583-585.