Weaknesses of an Improvement 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: Recently, Sood-Sarje-Singh proposed an improvement to Liou et al.'s dynamic ID-based remote user authentication scheme using smart cards to prevent impersonation attack, malicious user attack, off-line password guessing attack, and man-in-the-middle attack. However, we demonstrate that Sood et al.'s scheme is still vulnerable to malicious user attack, impersonation attack and steal information from a database attack.

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

1. Introduction

In 2004, Das et al. (Das, Saxena and Gulati, 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 (Awasthi, 2004, Goriparthi, Das and Saxena, 2009, Liao and Wang, 2009, Liou, Lin and Wang, 2006, Wang et al., 2009). Liou et al. (Liou, Lin and Wang, 2006) proposed a new scheme which resolves the security vulnerabilities of Das et al.'s scheme, in 2006. However, Sood et al. (Sood, Sarje and Singh, 2010) demonstrated that Liou et al.'s scheme is vulnerable to impersonation attack, malicious user attack, off-line password guessing attack, and man-in-the-middle attack.

In this paper, we demonstrate that Sood et al.' scheme is still vulnerable to malicious user attack, impersonation attack and steal information from a database attack.

The rest of this paper is organized as follows. In Section 2, we describe the scheme proposed by Sood-Sarje-Singh. Section 3 presents the security drawbacks of Sood et al.'s scheme. Finally, conclusions are given in Section 4.

2. Review of Sood et al.'s scheme

In this section, we briefly review Sood et al.'s scheme (Sood, Sarje and Singh, 2010). The scheme consists of the following phases: 1) registration, when a user wants to become a legal member of the system; 2) login, when a user wants to initialize a communication with the server; 3) authentication, when the server and the user verify the authenticity of each other and establish a session key; 4) password change, when a user wants to update her password. 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
y	Random number selected by S
h(·)	One-way hash function
||	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 a random value y
4. S computes:
   $A = h(x \| y)$
   $B = h(ID \| PW) \oplus PW \oplus h(x \| y)$
   $C = h(x \| y) \oplus h(PW)$
   $D = h(ID \| PW) \oplus h(x)$
5. S stores $y \oplus x$ and $ID \oplus h(x)$ *corresponding to A in a database*
6. S issues the smart card to U *through a secure communication channel*.
   The smart card contains the following security parameters: B, C, D, 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:
   $h(x \| y)^* = h(ID^* \| PW^*) \oplus PW^* \oplus B$
   $C^* = h(x \| y)^* \oplus h(PW^*)$
2. Compares:
   $C^* \stackrel{?}{=} C$
3. After verification, the smart card computes:
   $h(x) = h(ID \| PW) \oplus D$
   $CID = h(x \| y) \oplus h(h(x) \| T)$ *where T is the current date and time of U*
   $M = h(h(x) \| h(x \| y) \| T)$
4. U's smart card sends (CID, M, T) to S

2.3. Authentication 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:
   $A^* = h(x \| y) = CID \oplus h(h(x) \| T)$
3. Recovers:
   $y \oplus x$ and $ID \oplus h(x)$ *corresponding to* A^* *from its database*
4. Extracts:
   y from $y \oplus x$
   ID from $ID \oplus h(x)$
5. Computes:
   $M^* = h(h(x) \| h(x \| y) \| T)$
6. Compares:
   $M^* ?= M$ *if the verification is correct the authenticity of U is assured*
7. Computes:
   $V = h(A \| h(x) \| T \| T_S)$ *where* T_S *is the current date and time of S*
8. S sends (V, T_S) to U's smart card

Upon receiving the login response message (V, T_S), U's smart card carries out the following operations:

9. Checks the validity of T_S.
10. Computes:
    $V^* = h(h(x \| y) \| h(x) \| T \| T_S)$
11. Compares:
    $V^* ?= V$ *if the verification is correct the authenticity of S is assured*

Finally, U and S computes the session key $SK = h(ID \| h(x \| y) \| h(x) \| T \| T_S)$

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:
   $h(x \| y)^* = h(ID^* \| PW^*) \oplus PW^* \oplus B$
   $C^* = h(x \| y)^* \oplus h(PW^*)$
2. Compares:
   $C^* ?= C$
3. Request to U a new password PW_{new}
4. Computes:
   $B_{new} = h(ID \| PW_{new}) \oplus PW_{new} \oplus h(x \| y)$
   $C_{new} = h(x \| y) \oplus h(PW_{new})$
   $D_{new} = h(ID \| PW_{new}) \oplus h(x)$

and updates the values B, C, and D stored in its memory with B_{new}, C_{new}, and D_{new}

3. Weaknesses of Sood et al.'s scheme

In this section, we demonstrate that Sood et al.'s scheme is vulnerable to impersonation attack, malicious user attack and steal information from a database attack.

3.1. Malicious user attack

Sood et al. demonstrated that Liou et al.'s scheme is vulnerable to an off-line password guessing attack under the assumption that an adversary can extract the secret information stored in her smart card by monitoring the power consumption (Kocher, Jaffe and Jun, 1999) or by analyzing

the leaked information (Messerges, Dabbish and Sloan, 2002). However, Sood et al.'s scheme is still vulnerable to this attack.

Suppose a legal but malicious user, she can extract the secret information (B, C and D) stored in her smart card. Then, she can extract $h(x)$ from $D = h(ID \| PW) \oplus h(x)$ because she knows ID and PW. Moreover, the adversary can try to guess the different values of x and check its correctness by verifying it with the value of $h(x)$. Thus, Sood et al.'s scheme cannot resist the off-line password guessing attack.

3.2. Impersonation attack

If the adversary has intercepted one of U's previous login request message (CID, M, T) and she has extracted $h(x)$, she can perform the impersonation attack as follows:

1. Computes:
   $h(x \| y)^* = CID \oplus h(h(x) \| T)$ *because she knows h(x) and T*
   $CID_{false} = h(x \| y)^* \oplus h(h(x) \| T_{false})$ *where* T_{false} *is the current date and time of the adversary*
   $M_{false} = h(h(x) \| h(x \| y) \| T_{false})$
2. Adversary sends (CID_{false}, M_{false}, T_{false}) to S

In this case, T_{false} is valid because was computed by the adversary with the current time and date.

Upon receiving the login request message from the adversary, S will carry out the verification process:

3. Checks: the freshness of T_{false} by means of $T' - T_{false} <= \Delta T$, where T' is the S's current date and time.
4. Computes:
   $A^* = h(x \| y) = CID \oplus h(h(x) \| T_{false})$
5. Recovers:
   $y \oplus x$ and $ID \oplus h(x)$ corresponding to A^* from its database
6. Extracts:
   y from $y \oplus x$
   ID from $ID \oplus h(x)$
7. Computes:
   $M^* = h(h(x) \| h(x \| y) \| T)$
8. Compares:
   $M^* ?= M_{false}$ *it is obvious that S will accept the login request message*

It is obvious that Sood et al.'s scheme cannot resist the impersonation attack. Although the session key computed by S is unknown by the adversary, the attack reveals a weakness in Sood et al.'s scheme.

3.3. Steal information from a database attack

In Sood et al.'s scheme, S maintains a verification table where security information is stored. If the adversary can obtain the database, she can recover y from $y \oplus x$ and ID from $ID \oplus h(x)$ of each user. The scheme proposed by Sood et al. cannot resist the steal information from a database attack.

4. Conclusions

In this paper, we demonstrate that the improvement authentication scheme proposed by Sood-Sarje-Singh is still vulnerable to malicious user attack, impersonation attack and steal information from a database attack, making the scheme unsecured for electronic services.

Acknowledgments

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

References

Awasthi A.-K. Comment on A Dynamic ID-based remote user authentication scheme. Transaction on Cryptology 2004; 1(2): 15-16.

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.

Goriparthi T., Das M.-L., Saxena A. An improved bilinear pairing based remote user authentication scheme. Computer Standards & Interfaces 2009; 31(1): 181-185.

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

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 Liou et al.'s authentication scheme using smart cards. International Journal of Computer Applications 2010; 1(8): 16-23.

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.