Cryptanalysis Of Dynamic ID Based Remote User Authentication Scheme With Key Agreement

Sonam Devgan Kaul, Amit K. Awasthi

School of Applied Sciences, Gautam Buddha University, Greater Noida, India
sonamdevgan11@gmail.com, amitkawasthi@gbu.ac.in

Summary. In 2012, Wen and Li proposed a secure and robust dynamic identity based remote user authentication scheme with key agreement using smart cards. They claimed that their scheme is efficient and secure. But in this paper, we demonstrate that their scheme is completely insecure and vulnerable to various known attacks like offline and online password guessing attack, impersonation attack, server masquerading attack, denial of service attack and an insider attack. Also we point out that there are loopholes in password change phase and online secret renew phase which leads to the desynchronization between user and the server and even the legitimate user is rejected by the server. In addition, an adversary can easily generate the common session key of further transmission between user and the server. Thus the entire system collapses and authors claims are proven to be wrong and their scheme will not be secure and efficient for practical purpose.

Key words: Cryptanalysis; Remote User Authentication; Key Agreement; Hash function

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 smart card based remote user authentication protocols, the server verifies the authenticity of the legitimate user over an insecure communication channel so that the user will be granted to access resources at remote systems.

In a real world scenario, like in e-banking, e-commerce, etc., the consequence of an adversary interpretation will be expensive as well as unsafe for society. As an adversary has full control of the communication channel between the communicating parties and he can extract the secret information of the card. Thus any authentication protocol inspite of low storage capacity and limited computation and communication cost, must be secure against several known attacks like stolen smart card attack, denial of service attack, impersonation attack, replay attack, online and offline password guessing attack, insider attack, server masquerading attack, etc. and achieves mutual authentication and user anonymity.

In 1981, Lamport [2] proposed first remote user password based authentication scheme in an insecure network, but his scheme has a major drawback of its dependency on verification table. Smart cards based authentication schemes are becoming day by day more popular as implementation of smart cards reduce the dependency on verification tables and ensures secure communication. In 2001, Hwang et al [3] 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 [4, 5, 6, 7, 8] have been proposed.

In 2004, Das et al [9] 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 [11] cryptanlyse the mutual authentication of Liao et al's scheme. In the same direction in 2009, Wang et al. [12] proposed an improved protocol of Das et al's scheme [9] and demonstrated that an enhanced password authentication scheme will still keeps the merits of the original scheme [9] and withstands all their weaknesses. Recently, Wen and Li [1] claimed that Wang et al. [12] scheme is not secure against impersonation attack and leak secret information of the user when an adversary launch offline password guessing attack. In addition their scheme does not provide users anonymity and lacks smart card revocation,

key exchange and secret renew phases between users and servers. Furthermore an insider can get the secret parameters by analyzing the parameters on smart cards. Thus collapses the system and proposed an upgraded secure and robust authentication protocol to remedy these security flaws. In this paper, we have pointed out that even their scheme will not be secure and efficient and vulnerable to various known attacks.

The rest of the paper is organized as follows: Section 2 briefly reviews Wen and Li authentication protocol. Section 3 describes the weaknesses of Wen and Li's scheme. Finally, we conclude the paper in Section 4.

2 Review of Wen and Li Protocol

In this section, we examine the dynamic identity based remote user authentication scheme with key agreemet proposed by Wen and Li [1] in 2012. Their scheme consists of seven phases: Registration phase, Login phase, Authentication and key exchange phase, Mutual authentication and key confirmation phase, Revocation phase, Offline password change phase, Online secret renew phase. The notations used throughout the paper are summarized in table 1.

Table 1. Notations and Symbols

U_i	Legitimate i^{th} user
ID_i	Identifier of U_i
PW_i	Password of U_i
S	Server
x	Secret key of the server S
SK	Session Key
T, T''	Current date and time of input device
T_s	Current date and time of the server S
δT	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

User U_i performs the following steps to register into to the remote server S:

1. Foremost U_i chooses his identity and password parameters ID_i, PW_i respectively and sends it to the server S via a secure communication channel.
2. Then server S computes:
$$\begin{aligned} n_i &= h(ID_i \| PW_i) \\ m_i &= n_i \oplus x \\ N_i &= h(ID_i) \oplus h(PW_i) \oplus h(x) \oplus h(m_i) \end{aligned}$$
where x is the server's secret key. Server S stores the list of unique numbers n_i for i^{th} user to check the validity of smart card in its database while does not keep any identity or password table.
3. Finally server S personalized the smart card with the parameters $(h(.), N_i, n_i)$ and sends it to the user U_i via a secure communication channel.

2.2 Login Phase

User U_i and smart card reader performs the following steps when U_i wants to login into the system:

1. U_i simply inserts the smart card into the card reader and keys in ID_i and PW_i.

2. Card reader computes the following parameters:

$$\begin{aligned} A_i &= h(ID_i) \oplus h(PW_i) \\ B_i &= N_i \oplus h(ID_i) \oplus h(PW_i) \\ &= h(x) \oplus h(m_i) \\ CID_i &= h(A_i) \oplus h(h(n_i) \oplus B_i \oplus h(N_i) \oplus T) \end{aligned}$$

   where T is the current time stamp of smart card.
3. Eventually reader sends the login request message $\{CID_i, n_i, N_i, T\}$ to the remote server S.

2.3 Authentication and Key Exchange Phase

Upon receiving the login request $\{CID_i, n_i, N_i, T\}$ at time T, server computes the following steps to authenticate the legitimate user:

1. Firstly server S checks the validity of time stamp T by verifying $(T' - T) \leq \delta T$ to accept or reject the login request message.
2. Also server checks the parameter n_i from the database to verify whether the request send by registered user or not.
3. Server computes:

$$\begin{aligned} m_i &= n_i \oplus x \\ B_i &= h(x) \oplus h(m_i) \\ A_i &= N_i \oplus B_i \\ &= h(ID_i) \oplus h(PW_i) \end{aligned}$$

4. Server further computes:

$$CID_i = h(A_i) \oplus h(h(n_i) \oplus B_i \oplus h(N_i) \oplus T)$$

   and verify the legality of the user U_i by verifying the computed CID_i with the received CID_i. If it finds true, then U_i is authenticated otherwise session is terminate immediately.
5. If login request is accepted, the server S computes

$$C_i = h(A_i \oplus T_s \oplus h(n_i))$$

   where T_s is the current time stamp of the server.
6. Now server can generate the session key for further communication by computing:

$$SK = h(A_i \| T \| B_i \| T_s)$$

   and the session key confirmation message by computing:

$$KC = h(B_i \| SK \| T_s)$$

7. Finally server responds the authentication message $\{C_i, KC, T_s\}$.

2.4 Mutual Authentication and Key Confirmation Phase

User's smart card do the following procedures to authenticate the server S and to confirm the session key message:

1. Foremost checks the validity of time stamp T_s by verifying $(T_s' - T_s) \leq \delta T_s$.
2. Smart card computes

$$C_i = h(A_i \oplus T_s \oplus h(n_i))$$

   and verify it with the received C_i to authenticate the server.

3. After mutually authentication user also generate the session key for further communication by computing:
$$SK = h(A_i \| T \| B_i \| T_s)$$
and to verify whether the server generate the correct session key smart card computes:
$$KC = h(B_i \| SK \| T_s)$$
and verify it with received KC
4. Finally the confirmation message $\{KC', T''\}$ is send to the server where
$$KC' = h(B_i \| SK \| T'')$$
and T'' is the current time stamp.
5. At the last server verifies the key confirmation message $\{KC', T''\}$.

2.5 Revocation Phase

When user's smart card is lost or stolen then server S performs as follows to do the revocation:

1. Server verifies the i^{th} user's credentials by checking whether the corresponding $n_i = h(ID_i \| PW_i)$ is in the server's database or not.
2. If so, then server's delete n_i from the database. Now user has to re-register the remote user system with the change credentials.

2.6 Offline Password Change Phase

Whenever U_i wants to update his password, he inserts his credentials such as identifier ID_i, password PW_i and new password PW_i^*, the smart card performs as follows to change the password locally:

1. Smart card computes:
$$\begin{aligned} N_i^* &= N_i \oplus h(PW_i) \oplus h(PW_i^*) \\ &= h(ID_i) \oplus h(PW_i) \oplus h(x) \oplus h(m_i) \oplus h(PW_i) \oplus h(PW_i^*) \\ &= h(ID_i) \oplus h(x) \oplus h(m_i) \oplus h(PW_i^*) \end{aligned}$$
2. Smart card update the parameter N_i with the N_i^*.

2.7 Online Secret Renew Phase

When the remote server wants to update its secret key x with the new secret key x^* to enhance its security then S interacts with its users and performs as follows:

1. After establishing the session key SK with the user U_i, server computes:
$$n_i = m_i \oplus x$$
$$m_i^* = n_i \oplus x^*$$
$$N_i^* = N_i \oplus h(x) \oplus h(m_i) \oplus h(x^*) \oplus h(m_i^*)$$
2. Server sends N_i^* to the user via a secure communication channel. Eventually smart card update the parameter N_i with the N_i^*.

3 Cryptanalysis of Wen and Li Scheme

In this section we describe the security flaws in Wen and Li [1] remote user mutual authentication protocol on the assumption that an adversary has full control over the communication channel. An adversary can intercept the transaction messages or can modify or delete the messages. Also the secret information stored in the smart card could be extracted by some means, such as monitoring the power consumption [13] or analyzing the leaked information [14]. Security flaws in their scheme are described as follows:

3.1 Loopholes in password change phase

Wen and Li give the provision to the user U_i to update his password offline but his method is inconvenient and has following loopholes:

1. An adversary can easily update the password PW_i by arbitrary password PW_a by replacing N_i with the N_a on the smart card, where
$$N_a = N_i \oplus h(PW_i) \oplus h(PW_a)$$
as there is no verification of the old password locally by the smart card.
2. When the user wants to update the password PW_i by PW_i^*, then smart card only updates the parameter N_i with the N_i^* on the smart card, but there is no updation on the parameter $n_i = h(ID_i \| PW_i)$, which leads to the desynchronization. Even the legitimate user is rejected by the server, as the computed B_i and CID_i of the server is not same as the computed B_i and CID_i of the smart card.

3.2 Loophole in online secret renew phase

Wen and Li give the provision to the server to update his secret key but his method is inconvenient as the registered user will not be able to login into the system after doing this updation. When the server wants to update the password x by x^*, then server sends only the parameter N_i^* to the user via a secure channel. Thus smart card only updates the parameter N_i with the N_i^* on the smart card, but there is no updation on the parameter $n_i = h(ID_i \| PW_i)$, which leads to the desynchronization. Then even the legitimate user is rejected by the server, as the computed B_i and CID_i of the server is not same as the computed B_i and CID_i of the smart card.

3.3 Offline password guessing attack

An adversary can easily guess the password offline in either of the following ways:

1. Either an adversary get the user's smart card and extract the stored parameters N_i and n_i on the smart card by monitoring the power consumption or she can get the parameter n_i by intercepting the login message where $n_i = h(ID_i \| PW_i)$. Now she guess the possible password PW_i^* of user U_i and verify it with comparing n_i^* is equal to n_i or not where $n_i^* = h(ID_i \| PW_i^*)$. If $n_i^* = n_i$, then an adversary success probability to guess the password offline is 1.
2. An adversary can intercept the login transaction message and get the parameters $\{CID_i, n_i, N_i, T\}$, where
$$\begin{aligned} CID_i &= h(A_i) \oplus h(h(n_i) \oplus B_i \oplus h(N_i) \oplus T \\ &= h(h(ID_i) \oplus h(PW_i)) \oplus h(h(n_i) \oplus (N_i \oplus h(ID_i) \oplus h(PW_i)) \\ &\quad \oplus h(N_i) \oplus T) \end{aligned}$$
An adversary can get the value of n_i, N_i and T from the login message. Now the parameter CID_i depends directly only upon the parameter PW_i. Now she guess the possible password PW_i^* of user U_i and verify it with comparing CID_i^* is equal to CID_i or not. If $CID_i^* = CID_i$, then an adversary success probability to guess the password offline is 1.

3.4 Online password guessing attack

In Wen and Li protocol, it is possible 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. As there is no verification mechanism of password on smart card side and server will not locks the card after limited number of wrong login attampts, thus an adversary, to guess the password correctly, sends the guessed password online a number of times till she will not succeed.

3.5 Impersonation attack

As discussed in section 3.1, an adversary successfully get the password PW_i offline. Now she can impersonate the user any time in the following manner:

1. An adversary intercepts the login transaction message $\{CID_i, n_i, N_i, T\}$ and gets the current time stamp T_a.
2. An adversary computes:

$$CID_a = h(h(ID_i) \oplus h(PW_i)) \oplus h(h(n_i) \oplus (N_i \oplus h(ID_i) \oplus h(PW_i)) \oplus h(N_i) \oplus T_a)$$

3. She transmits the login message $\{CID_a, n_i, N_i, T_a\}$ to the server.
4. Server S checks the validity of time stamp T_a and accepts it as T_a is fresh time stamp.
5. Also for registered user U_i, server finds the parameter n_i in its database.
6. Server computes $m_i = n_i \oplus x$, $B_i = h(x) \oplus h(m_i)$, $A_i = N_i \oplus B_i = h(ID_i) \oplus h(PW_i)$ and $CID_i = h(A_i) \oplus h(h(n_i) \oplus B_i \oplus h(N_i) \oplus T_a)$
7. Server accepts the login request as the computed CID_i and the received CID_a are same by the virtue of correctly guessed password PW_i.

Thus an adversary can successfully impersonate the legitimate user of the server.

3.6 Server masquerading attack

As discussed in section 3.1, an adversary successfully get the password PW_i offline. Now she can also impersonate the legal server in the following manner:

1. An adversary intercepts the login transaction message $\{CID_i, n_i, N_i, T\}$ and blocks the message from reaching to the server.
2. She gets the current time stamp T_a and sends the message $\{C_a, KC_a, T_a\}$, where

$$C_a = h((h(ID_i) \oplus h(PW_i)) \oplus T_a \oplus h(n_i))$$

$$SK_a = h((h(ID_i) \oplus h(PW_i))\|T\|(N_i \oplus h(ID_i) \oplus h(PW_i))\|T_a)$$

$$KC_a = h((N_i \oplus h(ID_i) \oplus h(PW_i))\|SK\|T_a)$$

3. Smart card accepts the message as T_a is fresh. Also smart card obviously accepts the message $\{C_a, KC_a, T_a\}$ by the virtue of correctly guessed password PW_i.

In this manner, an adversary make fool of the user by imitating the legal server.

3.7 Computation of session key by an adversary

It is the basic requirement of the authentication scheme that any attacker can not compute the common session key between the user and the server but in Wen and Li protocol an adversary can compute the session key for further transmission in the following manner:

1. An adversary successfully get the password PW_i offline as discussed in section 3.1.
2. An adversary can intercept the login transaction message and get the parameters $\{CID_i, n_i, N_i, T\}$.
3. An adversary can also intercept the authentication message and get the parameters $\{C_i, KC, T_s\}$.
4. An adversary can now easily compute:

$$A_i = h(ID_i) \oplus h(PW_i)$$
$$B_i = N_i \oplus (h(ID_i) \oplus h(PW_i)$$

5. Eventually an adversary generate session key just by computing:

$$SK = h(A_i\|T\|B_i\|T_s)$$

3.8 Denial of service attack

Wen and Li protocol is not secure against computation exhaustive attacks like denial of service attack as there is no verification of password on the smart card side. Thus an adversary sends a number of fake login request messages to the server which leads to the excessive computation on the server side. Similarly to guess the password correctly, an adversary sends the guessed password online a number of times till she will not succeed which leads to excessive computation on server as smart card lacks any verification mechanism. Thus protocol is not secure against denial of service attack.

3.9 Insider attack

Insider attacker is one who is having administrative access of the server. At the time of registration user sends his identity ID_i and password PW_i in the plain text to the server. The system manager or a privileged insider user, who has direct access to the server, can get these parameters and use the secret information for personal benefit. Having user's password, insider can impersonate legal user of the system at other servers. After getting the password of the user, insider can purposely leak the information or impersonate the legitimate user or may modify the information. Also he can also issue an illegal smart card to some fake user. Thus submission of password in plaintext format during registration has many serious consequences.

4 Conclusion

In this paper, we have analyzed Wen and Li dynamic identity based remote user authentication scheme with key agreement using smart cards. We demonstrate that their scheme is insecure for practical applications as there are loopholes in password change phase and online secret renew phase which leads to the desynchronization between user and the server and even the legitimate user is rejected by the server. Also their scheme is vulnerable to offline and online password guessing attack, impersonation attack, server masquerading attack, denial of service attack and an insider attack. In addition, even an adversary can generate the common session key between user and the server. Thus authors claims are proven to be wrong and their scheme will not be secure and efficient for practical purpose.

References

1. Fengtong Wen and Xuelei Li. An improved dynamic id-based remote user authentication with key agreement scheme. *Computers & Electrical Engineering*, 38(2):381–387, 2012.
2. Leslie Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24(11):770–772, Nov 1981.
3. Min Shiang Hwang and Li Hua Li. A new remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, 46(1):28–30, Feb 2000.
4. Amit K Awasthi. Comment on a dynamic id-based remote user authentication scheme. *Transaction on Cryptology*, 1(2):15–16, May 2004.
5. Hung Yu Chien and Che Hao Chen. A remote authentication scheme preserving user anonymity. *Proc. Advanced Information Networking and Applications*, 2:245–248, March 2005.
6. Debiao He and Shuhua Wu. Security flaws in smart card based authentication scheme for multi server environment. *Wireless Personal Communications*, (0929-6212), June 2012.
7. Wei Chi Ku and Shen Tien Chang. Impersonation attack on dynamic id-based remote user authentication scheme using smart cards. *IEICE Transactions on Communications*, E88-B(5):2165–2167, May 2005.
8. Jiqiang Liu and Sheng Zhong. Analysis of kim-jeon-yoo password authentication scheme. *Cryptologia*, 33(2):183–187, July 2009.
9. Manik Lal Das, Ashutosh Saxena, and Ved P. Gulati. A dynamic id-based remote user authentication scheme. *IEEE Transactions on Consumer Electronics*, 50(2):629–631, May 2004.

10. I En Liao, Chenge Chi Lee, and Min Shiang Hwang. Security enhancement for a dynamic id-based remote user authentication scheme. *Proc. Conference on Next Generation Web Services Practice*, pages 437–440, Aug 2005.
11. Eun Jun Yoon and Key Young Yoo. Improving the dynamic id-based remote mutual authentication scheme. *Proc. OTM Workshops 2006*, 4277:499–507, July 2006.
12. Yan-yan Wang, Jia-yong Liu, Feng-xia Xiao, and Jing Dan. A more efficient and secure dynamic id-based remote user authentication scheme. *Computer communications*, 32(4):583–585, 2009.
13. Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. *Advances in Cryptology - CRYPTO'99*, LNCS1666:388–397, Aug 1999.
14. Thomas S. Messerges, Ezzat A. Dabbish, and Robert H. Sloan. Examining smart card security under the threat of power analysis attacks. *IEEE Transactions on Computers*, 51(5):541–552, May 2002.