Contemporary Engineering Sciences, Vol. 8, 2015, no. 35, 1651 - 1658
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2015.510284

Cryptanalysis of ID-based User Off-line Password Authentication for Mobile Memory Cards

Hae-Jung Kim

College of Liberal Education, Keimyung University
Daegu 704-701, Republic of Korea

Eun-Jun Yoon[1]

Department of Computer Engineering, Kyungil University
Kyungsangpuk-Do 712-701, Republic of Korea

Abstract

In 2015, Li et al. proposed an ID-based user off-line password authentication scheme for mobile memory cards. Li et al. claimed that their proposed scheme is secure to an off-line password guessing attack. However, this paper points out that Li et al.'s scheme is still vulnerable to the off-line password guessing attack unlike their claims. For this reason, Li et al.'s scheme is insecure for practical application.

Keywords: Cryptography; Off-line password authentication; Mobile memory cards; Cryptanalysis; Password guessing attack

1 Introduction

The user authentication method for mobile memory cards is one of big security issues because people can get data in memory cards nearly arbitrarily. In 2015, Li et al.[1] proposed an ID-based user off-line password authentication scheme for mobile memory cards. The scheme uses off-line authentication

[1]Corresponding author: Eun-Jun Yoon. Tel.: +82-53-600-5623; Fax: +82-53-600-5639

mode to achieve the management of memory cards and the user groups, completes the user off-line authentication, and achieves the off-line update of user passwords[2, 3, 4, 5, 6, 7, 8, 9, 10]. Li et al. claimed that their proposed scheme is secure to an off-line password guessing attack[2, 3, 10].

However, this paper points out that Li et al.'s scheme is still vulnerable to the off-line password guessing attack unlike their claims. In Li et al.'s scheme, an attacker can use a guessed password to verify the correctness of the password in an off-line manner and then can freely guess a password without limitation in the number of guesses. For this reason, Li et al.'s scheme is insecure for practical application.

This paper is organized as follows: Section 2 briefly reviews the Li et al.'s ID-based user off-line password authentication scheme for mobile memory cards. The security flaws of Li et al.'s scheme are shown in Section 3. Finally, conclusions are given in Section 4.

2 Review of Li et al.'s ID-based User Off-line Password Authentication Scheme

This section briefly reviews Li et al.'s ID-based user off-line password authentication scheme for mobile memory cards[1]. The authentication system is composed of remote server, users, and mobile memory cards. It is mainly based on elliptic bilinear pairing theory[4, 9].

Bilinear Pairing[1, 4, 9] Let G_1 be a cyclic additive group generated by P and G_2 be a cyclic multiplicative group. G_1 and G_2 have the same prime order q. Let $G_1 \times G_1 \rightarrow G_2$ be a computable bilinear map, which satisfies the following properties:

1. Bilinear: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$, where $P, Q \in G_1$ and $a, b \in Z_q$.
2. Non-degenerate: P is a generator of G_1, then $\hat{e}(P, P)$ is a generator of G_2.
3. Computable: There exists an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P, Q \in G_1$.

Such a bilinear map $\hat{e}$ is called an admissible pairing, and the modified Weil or Tate pairing on elliptic curves gives a good implementation of such an admissible bilinear pairing[1, 4, 9].

There are four phases in the Li et al.'s scheme: user registration, user login authentication, user password update and delegation update of mobile cards. We outlined some notations used in this research paper.

- ID_i : user identity
- PW : user password
- ID_{card} : the identity of mobile memory card
- x : the group key of server
- T : timestamp
- $H_1(\cdot)$: secure one-way hash function $H_1 : \{0,1\}^* \to G_1$
- $H_2(\cdot)$: secure one-way hash function $H_2 : \{0,1\}^* \to Z_q$
- $\oplus$: exclusive operation

2.1 User Registration Phase

Remote server selects different keys for different groups, and selects different passwords for different users. The user registration phase performs as follows:

1. The remote server computes (Y_1, Y_2, RID, J, L) as follows:

$$Y_1 = x \cdot H_1(ID_i) \cdot H_2(PW) \tag{1}$$

$$Y_2 = x \cdot H_1(ID_{card}) \tag{2}$$

$$RID = H_2(ID_i) \tag{3}$$

$$J = x \oplus H_2(PW) \tag{4}$$

$$\begin{aligned} L &= J \oplus RID \\ &= x \oplus H_2(PW) \oplus H_2(ID_i) \end{aligned} \tag{5}$$

2. The remote server stores the parameters (Y_1, Y_2, J, L, T) in the binding card with ID_i, where T is the time stamp for the group of users delegated by the server.

3. The remote server only stores the group keys, user ID_i and the binding card ID_{card}.

2.2 User Login Phase

Assume that a user wants to login and authenticate to the mobile card. Fig. 1 depicts the Li et al.'s user login phase. The user login phase performs as follows:

1. When user logins, the user inserts the card to a PC or a card reader, then keys ID^* and PW^*.

2. The card judges whether the time stamp T is expired. If so, the authentication is denied, otherwise it takes the following two steps to authenticate:

   (a) User ID authentication: The card calculates the followings:

   $$\begin{aligned} J^* &= L \oplus H_2(ID^*) \\ &= x \oplus H_2(PW) \oplus H_2(ID_i) \oplus H_2(ID^*) \end{aligned} \tag{6}$$

   If J^* is equal to J stored in the card, it continues to the next step, otherwise, exits the authentication.

   (b) User password authentication: The card takes the followings bilinear pairing calculation:

   $$\begin{aligned} \hat{e}[Y_1, H(ID_{card})] &= \hat{e}[x \cdot H_1(ID_i) \cdot H_2(PW), H(ID_{card})] \\ &= \hat{e}[x \cdot H(ID_{card}), H_1(ID_i) \cdot H_2(PW)] \\ &= \hat{e}[Y_2, H_1(ID^*) \cdot H_2(PW^*)] \end{aligned} \tag{7}$$

   If the equation holds, the user's password is correct, and the user is matched with the card. Otherwise the authentication is exited.

3. After above two steps, the legitimacy is determined in three aspects of user identity, user password and mobile card identity. Then the card can be read normally.

User	Mobile memory card
(ID^*, PW^*)	(Y_1, Y_2, J, L, T)
Key ID^* and PW^*	
Verify time stamp T	
$\xrightarrow{\{ID^*, PW^*\}}$	
	Compute $J^* = L \oplus H_2(ID^*)$
Verify $\hat{e}[Y_1, H(ID_{card})] \stackrel{?}{=} \hat{e}[x \cdot H_1(ID_i) \cdot H_2(PW), H(ID_{card})]$	

Figure 1: User Login Phase

2.3 User Password Update Phase

Legitimate users can freely update password without helping of a remote server. And the parameters needed to be updated at the same time are (Y_1, J, L). Y_2 does not update. User do not have the permission to update T. The user password update phase performs as follows:

$$P = H_2(PW_{new}) \tag{8}$$

$$Q = H_2^{-1}(PW) \tag{9}$$

$$\begin{aligned} Y_{1new} &= Y_1 \cdot P \cdot Q \\ &= x \cdot H_1(ID_i) \cdot H_2(PW) \cdot H_2(PW_{new}) \cdot H_2^{-1}(PW) \\ &= x \cdot H_1(ID_i) \cdot H_2(PW_{new}) \end{aligned} \tag{10}$$

$$\begin{aligned} J_{new} &= J \oplus H_2(PW) \oplus P \\ &= x \oplus H_2(PW) \oplus H_2(PW) \oplus H_2(PW_{new}) \\ &= x \oplus H_2(PW_{new}) \end{aligned} \tag{11}$$

$$\begin{aligned} L_{new} &= J_{new} \oplus H_2(ID_i) \\ &= x \oplus H_2(PW_{new}) \oplus H_2(ID_i) \end{aligned} \tag{12}$$

After the update, the storage parameters are $(Y_{1new}, Y_2, J_{new}, L_{new}, T)$.

2.4 Delegation Update Phase of Mobile Cards

When the card is lost, the legitimate user should provide an effective identification to the server.

1. With the legitimate ID, the server will cancel the identity of the old card based on the relation of the user ID_i and the card ID_{new} and stop the delegation update to the old card.

2. When the time expires, the old card cannot be used.

3. If the time stamp of the legitimate user's card expires, the user will report the server to extend the time.

4. The user logins, if it is passed, the card reader will send the user's ID and the parameter Y_2 to the server. The server verifies the legitimacy of the card ID_{new}.

5. At the same time if $Y_2^* = x \cdot H_1(ID_{card})$ is equal to the received Y_2, the server updates the time stamp of the card. Otherwise, the server refuses to provide services.

3 Off-line Password Guessing Attack on Li et al.'s Scheme

This section demonstrates that Li et al.'s ID-based user off-line password authentication scheme for mobile memory cards[1] cannot withstand an off-line password guessing attack. An off-line password guessing attack is the most powerful attack to the password-based authentication schemes. In the off-line password guessing attack, an attacker uses a guessed password to verify the correctness of the password in an off-line manner. The attacker can freely guess a password and then check if it is correct without limitation in the number of guesses[2, 3, 5, 6, 7, 8, 10].

Suppose that the attacker steals the parameters (Y_1, Y_2, J, L, T) from a lost card and knows the user's ID. Then the attacker can perform an off-line password guessing attack to obtain the password PW of the user as follows:

1. The attacker selects a candidate password PW^*.
2. The attacker checks if the following equation holds or not

$$Y_1 \stackrel{?}{=} (J \oplus H_2(PW^*)) \cdot H_1(ID_i) \cdot H_2(PW^*) \tag{13}$$

   If the check passes, then the attacker confirms that the guessed password PW^* is the correct one.
3. If it is not correct, the attacker chooses another password PW^{**} and repeatedly performs above step (2) until

$$Y_1 \stackrel{?}{=} (J \oplus H_2(PW^{**})) \cdot H_1(ID_i) \cdot H_2(PW^{**}) \tag{14}$$

It is clear that if $PW^* = PW$, then

$$\begin{aligned} &(J \oplus H_2(PW^*)) \cdot H_1(ID_i) \cdot H_2(PW^*) \\ &\quad = (x \oplus H_2(PW) \oplus H_2(PW^*)) \cdot H_1(ID_i) \cdot H_2(PW^*) \\ &\quad = x \cdot H_1(ID_i) \cdot H_2(PW^*) \\ &\quad = Y_1 \end{aligned} \tag{15}$$

Therefore, Li et al.'s scheme is vulnerable to the off-line password guessing attack. The algorithm of the off-line password guessing attack for getting the password PW^* is as follows:

Password Guessing Attack$(Y_1, J, ID_i, \mathbb{D}_{PW}))$
{
  for $i := 0$ to $|\mathbb{D}_{PW}|$

```
    {
        PW* ← D_PW;
        Y_1* = (J ⊕ H_2(PW*)) · H_1(ID_i) · H_2(PW*);
        if Y_1 ?= Y_1* then
                    return PW*
    }
}
```

The running time of the above off-line password guessing attack is $(O(|\mathbb{D}_{PW}|) \times 2T_M \times 1T_X \times 3T_H)$, where T_M, T_X and T_H represent the execution time of multiplications, bit-wise XOR operations, and hash operations respectively. The search spaces $\mathbb{D}_{PW}$ is unlikely to be large enough (for example, $|\mathbb{D}_{PW}| \leq 10^6$), and the time complexities T_M, T_X and T_H all can be executed with negligible amount of time, thus the polynomial time-bounded attacker can find the exact password PW of the user easily[2, 3, 10].

4 Conclusions

This paper reviewed Li et al.'s ID-based user off-line password authentication scheme for mobile memory cards and then pointed out that Li et al.'s scheme is still vulnerable to off-line password guessing attack using stolen smart card unlike their claims. For this reason, Li et al.'s scheme is insecure for practical application. Further works will be focused on improving the Li et al.'s scheme which can be able to provide greater security and to be more efficient than the existing mobile memory card-based user off-line password authentication schemes by an accurate performance analysis.

Acknowledgements. This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP)(No. 2015R1A2A2A01006824).

References

[1] N. Li, J. Duan, and Z. Deng, ID-based user off-line password authentication for mobile memory cards, *Multimedia, Communication and Computing Application*, **1** (2015), 23-27. http://dx.doi.org/10.1201/b18512-7

[2] E. Yoon, E. Ryu, and K. Yoo, An improvement of HwangLeeTang's simple remote user authentication scheme, *Computers & Security*, **24** (2005), no. 1, 50-56. http://dx.doi.org/10.1016/j.cose.2004.06.004

[3] E. Yoon and K. Yoo, SAKAwp: Simple Authenticated Key Agreement Protocol Based on Weil Pairing, *International Conference on Convergence*

Information Technology, **1** (2007), 2096-2101.
http://dx.doi.org/10.1109/iccit.2007.370

[4] D. He and J. Chen, Cryptanalysis of a three-party password-based authenticated key exchange protocol using Weil pairing, *Int. J. of Electronic Security and Digital Forensics*, **4** (2012), no. 4, 244-251.
http://dx.doi.org/10.1504/ijesdf.2012.049754

[5] X. Zhuang, C. Chang, Z. Wang, and Y. Zhu, A simple password authentication scheme based on geometric hashing function, *International Journal of Network Security*, **16** (2014), no. 4, 237-243.

[6] T. Feng, C. Ling, and M.Hwang, Cryptanalysis of Tan's improvement on a password authentication scheme for multi-server environments, *International Journal of Network Security*, **16** (2014), no. 4, 318-321.

[7] M. Hwang, S. Hsiao, and W. Yang, Security on improvement of modified authenticated key agreement protocol, *Information-An International Interdisciplinary Journal*, **17** (2014), no. 4, 1173-1178.

[8] R. Amin and G. Biswas, Design and analysis of bilinear pairing based mutual authentication and key agreement protocol usable in multi-server environment, *Wireless Personal Communications*, **84** (2015), no. 1, 439-462. http://dx.doi.org/10.1007/s11277-015-2616-7

[9] C. Wang and Y. Zhang, New authentication scheme for wireless body area networks using the bilinear pairing, *Journal of Medical Systems*, **39** (2015), no. 11, 1-8. http://dx.doi.org/10.1007/s10916-015-0331-2

[10] S. Choi and E. Yoon, Cryptanalysis of Tso et al.'s password authentication scheme based on smart card, *Applied Mathematical Sciences*, **9** (2015), no. 101, 5027-5034. http://dx.doi.org/10.12988/ams.2015.56420

Received: October 22, 2015; Published: December 12, 2015