Applied Mathematical Sciences, vol. 8, 2014, no. 148, 7367 - 7374
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ams.2014.49731

Cryptanalysis of Qu's Improved Smart Card-based Remote User Authentication Scheme

Eun-Jun Yoon [1]

Department of Cyber Security, Kyungil University
Kyungsangpuk-Do 712-701, Republic of Korea

Abstract

In 2013, Qu demonstrated that Awasthi et al.'s remote user authentication scheme is vulnerable to smart card loss attack, off-line password guessing attack and does not preserve anonymity of user. However, this paper points out that Qu's scheme is still vulnerable to off-line password guessing attack and smart card loss attack, and also does not preserve anonymity of a user unlike its claim. For this reason, Qu's scheme is insecure for practical application.

Keywords: Smart card; Authentication; Cryptanalysis; Off-line password guessing attack; Stolen smart card attack; User anonymity

1 Introduction

Smart card-based remote user authentication is a mechanism which allows the user and the server to mutually authenticate the legitimacy of each other over public network. In 1999, Yang and Shieh [1] proposed two password authentication schemes with smart cards. In 2002, Fan [2] proposed an enhancement of Yang and Shieh's scheme to improve the security. In 2003, Wang et al. [3] pointed out that an intruder can construct a forged login request message from the intercepted legitimate login requests. However, Shen et al. [4] proposed a modified scheme of the Yang-Shieh's scheme to withstand the forged login

[1]Corresponding author: Eun-Jun Yoon

attack and provide secure mutual authentication. However, Awasthi et al. [5] pointed out that Shen et al.'s scheme is still vulnerable to the forged login attack and then proposed another improved scheme.

In 2013, Qu [6] showed that Awasthi et al.'s scheme is also vulnerable to smart card loss attack, off-line password guessing attack and does not preserve anonymity of user. However, this paper points out that Qu's remote user authentication scheme is still vulnerable to off-line password guessing attack and smart card loss attack, and also does not preserve anonymity of a user unlike its claim. For this reason, Qu's scheme is insecure for practical application.

The remainder of this paper is organized as follows. We review Qu's remote user authentication scheme in Section 2. The attacks on the Qu's scheme are presented in Section 3. Finally, we draw some conclusions in Section 4.

2 Review of Qu's Authentication Scheme

In 2013, Qu [6] analyzed the weaknesses of the Awasthi et al.'s scheme, and then presented an improved remote authentication scheme. The improved scheme is composed for four phase: Registration phase, Login phase, Verification phase and Password change phase.

2.1 Registration phase

Suppose x is the secret key of Key information Center(KIC), and KIC computes $Q = xP$, where P is an ECC point $\in E_p(a, b)$ and the elliptic curve equation is defined as the form of $E_p(a, b) : y^2 = x^3 + ax + b(\mathrm{mod}p)$. Keeps secret x and publishes the public parameters P, Q, $h(\cdot) : \{0, 1\}^* \rightarrow Z_n^*$, where $h(\cdot)$ is a secure one way hash function. The registration phase performs the following steps:

1. A new user U_i chooses his/her real identity ID_i, password pw_i and then computes pw_iP.

2. U_i submits his/her ID_i and pw_iP to KIC via a secure channel.

3. KIC computes
$$h_i = xpw_iP \tag{1}$$
$$S_i = h(x||ID_i)P \tag{2}$$
$$T_i = h(ID_i||pw_iP) \tag{3}$$

4. KIC issues smart card to U_i which contains values of h_i, S_i, T_i, and P via a secure channel.

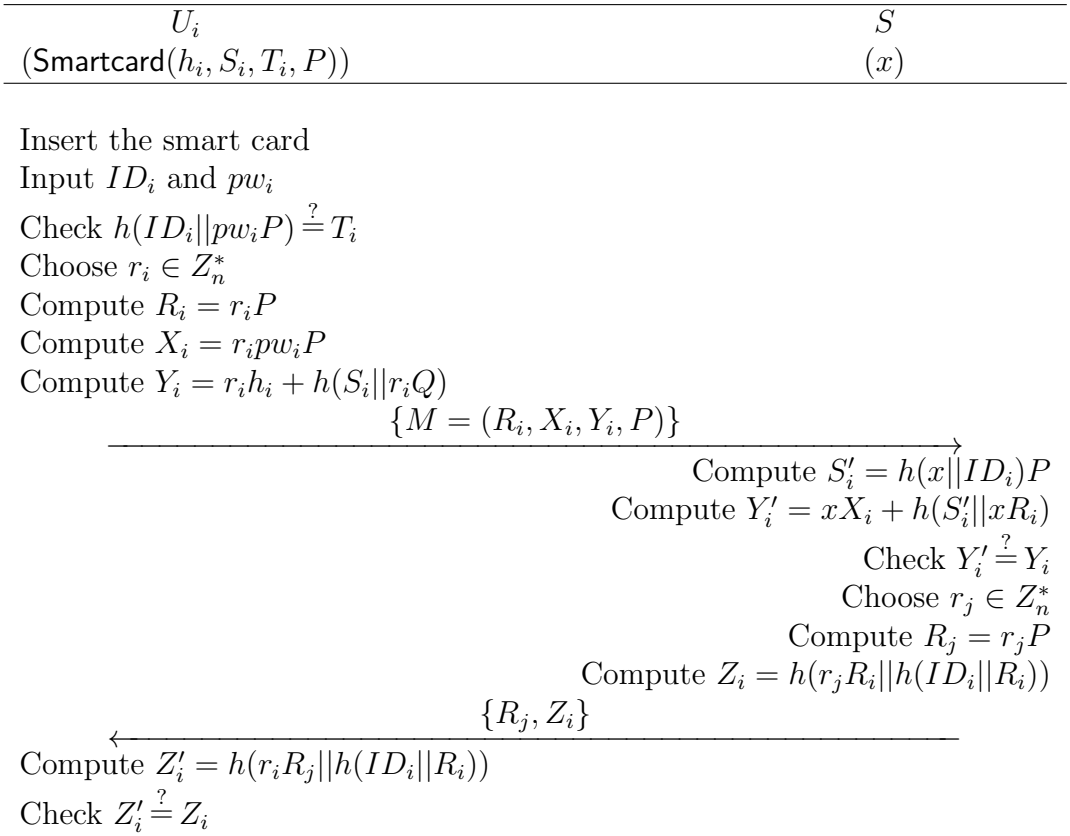

Figure 1: Login and verification phases

2.2 Login phase

If U_i wants to access the server, he/she inserts smart card into the terminal, keys ID_i with pw_i, then the smart card verifies the equation

$$h(ID_i||pw_iP) \stackrel{?}{=} T_i \tag{4}$$

holds or not. If it holds, U_i performs the following steps:

1. Choose a random number $r_i \in Z_n^*$ and computes

$$R_i = r_iP \tag{5}$$

$$X_i = r_ipw_iP \tag{6}$$

$$Y_i = r_ih_i + h(S_i||r_iQ) \tag{7}$$

2. Send $M = (R_i, X_i, Y_i, P)$ to the remote server S, where M is a login request message of the user U_i.

2.3 Verification phase

After receiving the login request message M from U_i, the remote server S and the user U_i will perform the following steps to authenticate each other and agree the common session key sk for their subsequent communications.

1. S computes
$$S_i' = h(x||ID_i)P \tag{8}$$
$$Y_i' = xX_i + h(S_i'||xR_i) \tag{9}$$
S checks whether
$$Y_i' \stackrel{?}{=} Y_i \tag{10}$$
If this holds, S authenticates U_i otherwise login request is rejected.

2. For mutual authentication, S selects a random number $r_j \in Z_n^*$ and computes
$$R_j = r_j P \tag{11}$$
$$Z_i = h(r_j R_i||h(ID_i||R_i)) \tag{12}$$
and then sends the mutual authentication message (R_j, Z_i) to U_i.

3. Upon receiving the mutual authentication message, U_i computes
$$Z_i' = h(r_i R_j||h(ID_i||R_i)) \tag{13}$$
and then verifies
$$Z_i' \stackrel{?}{=} Z_i \tag{14}$$
If this holds, U_i authenticates S otherwise login request is give up by U_i.

4. U_i and S share the symmetric session key $sk = h(r_i r_j P||S_i)$ for performing further operations during a session.

2.4 Password change phase

In the password-change phase, when a user wants to change his/her password pw_i with a new password pw_i^{new}, he/she inserts his/her smart card into smart card reader and enters his/her ID_i and password pw_i. The smart card performs the following operations without interacting with KIC:

1. Computes
$$T_i^* = h(ID_i||pw_iP) \tag{15}$$
If $T_i^* = T_i$, then U_i is allowed to change the password, otherwise password-change phase is terminated.

2. Computes
$$h_i^{new} = pw_i^{new}Q \tag{16}$$
and replaces the old value of h_i with the new value h_i^{new}. Now, the new password is successfully changed and this phase is terminated.

3 Cryptanalysis of Qu's Authentication Scheme

This section demonstrates that Qu's scheme [6] is still vulnerable to off-line password guessing attack, smart card loss attack, and does not preserve anonymity of user unlike its claims. The details of these flaws are described as follows.

3.1 Off-line password guessing attack

An attacker can perform the following off-line password guessing attack. Let us assume that an attacker *Eve* has intercepted one of the U_i's past login request messages, i.e., $M = (R_i, X_i, Y_i, P)$. Then *Eve* can perform an off-line password guessing attack to obtain the password pw_i of U_i as follows:

1. *Eve* selects a candidate password pw_i^*

2. *Eve* checks if the following equation holds or not
$$X_i \stackrel{?}{=} pw_i^* R_i \tag{17}$$
If the check passes, then *Eve* confirms that the guessed password pw_i^* is the correct one.

3. If it is not correct, *Eve* chooses another password pw_i^{**} and repeatedly performs above step (2) until
$$X_i \stackrel{?}{=} pw_i^{**} R_i \tag{18}$$

It is clear that if $pw_i^* = pw_i$, then
$$pw_i^* R_i = pw_i^* r_i P = r_i pw_i^* P = X_i \tag{19}$$

Therefore, Qu's authentication scheme is vulnerable to off-line password guessing attack. The algorithm of the off-line password guessing attack for getting

the password pw_i^* is as follows:

Off-line Password Guessing Attack(X_i, R_i, D)
{
  for $i := 0$ to $|D|$
  {
    $pw_i^* \leftarrow D$;
    if $X_i \stackrel{?}{=} pw_i^* R_i$ **then**
      return pw_i^*
  }
}

3.2 Smart card loss attack

The attacker *Eve* can perform the smart card loss attack by using the guessed password pw_i^* in the proposed off-line password guessing attack. Suppose that the user U_i's smart card is lost or stolen, then the attacker *Eve* can extract the stored secret information (h_i, S_i, T_i, P) stored in the smart card. Then *Eve* can perform the smart card loss attack to impersonate U_i as follows:

1. *Eve* chooses a random number $r_e \in Z_n^*$ and computes

$$R_e = r_e P \tag{20}$$

$$X_e = r_e pw_i^* P \tag{21}$$

$$Y_e = r_e h_i + h(S_i || r_e Q) \tag{22}$$

2. *Eve* sends $M_e = (R_e, X_e, Y_e, P)$ to the remote server S.

3. After receiving M_e, the remote server S will compute

$$S_i' = h(x||ID_i)P \tag{23}$$

$$Y_e' = xX_e + h(S_i' || xR_e) \tag{24}$$

4. Finally, S will check whether

$$Y_e' \stackrel{?}{=} Y_e \tag{25}$$

It is obvious that

$$\begin{aligned} Y_e' &= xX_e + h(S_i' || xR_e) \\ &= xr_e pw_i^* P + h(S_i' || xr_e P) \\ &= r_e xpw_i^* P + h(S_i' || r_e xP) \\ &= r_e h_i + h(S_i || r_e Q) \\ &= Y_e \end{aligned} \tag{26}$$

Therefore, S will accept the login request of Eve. Hence, Qu's scheme cannot resist the smart card loss attack.

3.3 User anonymity problem

User anonymity is an important feature that a practical authentication scheme should achieve. In the Qu's scheme, Qu claimed that its proposed scheme preserves user anonymity because a user's real identity ID_i is concealed in the Y_i. However, we can easily see that the remote server cannot compute

$$S_i' = h(x||ID_i)P \tag{27}$$

without knowing the user's real identity ID_i in step (1) of the verification phase. Moreover, the user U_i do not send his/her real identity ID_i to S to protect his/her identity. Qu do not proof clearly how the proposed scheme can provide user anonymity. As a result, Qu's scheme cannot archive the user anonymity property unlike its claim.

4 Conclusions

This paper reviewed Qu's remote user authentication scheme and then pointed out that Qu's scheme is still vulnerable to off-line password guessing attack and smart card loss attack, and also does not preserve anonymity of a user unlike its claim. For this reason, Qu's scheme is insecure for practical application. Further works will be focused on improving the Qu's scheme which can be able to provide greater security and to be more efficient than the existing smart card-based remote user authentication schemes by an accurate performance analysis.

Acknowledgements

This work was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(No. 2010-0010106).

References

[1] W.H. Yang, S.P. Shieh, Password authentication schemes with smart cards, *Computer & Security*, **18(8)** (1999), 27-733.

[2] L. Fan, J.H. Li, H.W. Zhu, An enhancement of timestamp-based password authentication scheme, *Computer & Security*, **21(7)** (2002), 665-667.

[3] B. Wang, J.H. Li, Z.P. Tong, Cryptanalysis of an enhanced timestamp-based password authentication scheme, *Computer & Security*, **22(7)** (2003), 643-645.

[4] J.J. Shen, C.W. Lin, M.S. Hwang, Security enhancement for the timestamp-based password authentication scheme using smart cards, *Computer & Security*, **22(7)** (2003), 591-595.

[5] A.K. Awasthi, K. Srivastava, R.C. Mittal, An improved timestamp-based remote user authentication scheme, *Computers and Electrical Engineering*, **37(6)** (2011), 869-874.

[6] J. Qu, Security flaws in an improved timestamp-based remote user authentication scheme, *Journal of Mathematical and Computational Science*, **3(3)** (2013), 799-807.

Received: September 16, 2014; Published: October 22, 2014