Contemporary Engineering Sciences, Vol. 7, 2014, no. 26, 1475 - 1482
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2014.49186

Security Vulnerabilities of an Enhanced Remote User Authentication Scheme

Hae-Soon Ahn

Faculty of Liberal Education, Daegu University
Kyungsangpuk-Do 712-830, Republic of Korea

Eun-Jun Yoon[1]

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

Abstract

In 2014, Yang et al. proposed a new dynamic ID-based user authentication scheme based on smart card which is believed to have many abilities to resist a range of network attacks. However, this paper analyzes the security of Yang et al.'s scheme and then shows that the scheme not only is still vulnerable to off-line password guessing attack, but also does not provide the unlinkability property and user anonymity because of the identity guessing attack unlike their claims.

Keywords: User authentication; Dynamic identity; Cryptanalysis; Password; Unlinkability

1 Introduction

Remote user authentication schemes are used to verify the legitimacy of remote users' login request. In verifier-free authentication scheme, the user's login identity ID is always static [1]. It means that it can be leak partial information

[1] Corresponding author: Eun-Jun Yoon, Fax: +82-53-600-5579

related with the user's login messages. Furthermore, an adversary can use the information to forge the user's login messages by some subtle means. One of the solutions to eliminate this security problem is to employ dynamic identity ID in different login session [1, 2, 3, 4].

In 2004, Das et al. [1] first proposed a dynamic ID-based remote user authentication scheme which can resist replay, masquerade, and insider attacks. In 2007, Wang et al. [2], however, pointed out that Das et al.'s scheme is susceptible to smart card attack and does not provide mutual authentication. Then they proposed a more efficient and secure dynamic ID-based remote user authentication scheme. In 2011, Khan et al. [3], however, pointed out that Wang et al.'s scheme still is susceptible to insider attack and does not provide user's anonymity and session key agreement. They also proposed a new dynamic ID-based remote user authentication scheme. In 2014, Yang et al. [4] pointed out that previously proposed schemes have weaknesses because of using timestamps and lead to serious clock synchronization problems and then proposed an enhanced dynamic ID-based remote user authentication (in short, ERUA) scheme. Yang et al. claimed that the proposed ERUA scheme provides mutual authentication using a challenge-response handshake and user's anonymity.

This paper researches Yang et al.'s ERUA scheme and then shows that the ERUA scheme not only is still vulnerable to off-line password guessing attack, but also does not provide the unlinkability property [5] and user anonymity because of the identity guessing attack [6, 7] unlike their claims. For this reason, Yang et al.'s ERUA scheme is insecure for practical application.

The remainder of this paper is organized as follows. We review Yang et al.'s ERUA scheme in Section 2. The security flaws of Yang et al.'s ERUA scheme are presented in Section 3. Finally, we draw some conclusions in Section 4.

2 Review of Yang et al.'s ERUA Scheme

This section reviews the Yang et al.'s ERUA scheme [4]. Throughout the paper, notations are employed in Table 1. The ERUA scheme is divided into four phase: registration phase, login phase, authentication phase, and password change phase.

2.1 Registration phase

A user U_i with identifier ID_i should first carry out this phase once before he/she can use any of the services provided by the server S. In this phase, U_i and S need to perform the following steps:

R1. $U_i \rightarrow S$: $\{ID_i, h(ID_i||PW_i)\}$

Table 1: Notations used in ERUA scheme

U_i	A remote user i.
S	A trusted server.
ID_i	An identity of the user U_i.
PW_i	A password of the user U_i.
$h(\cdot)$	A secure one-way hash function.
x	A secret key of server S.
$\oplus$	A bitwise eXclusie-OR (XOR) operation.
$\|\|$	A concatenation operation.

User U_i keys his/her identity ID_i and password PW_i, and his/her smart card computes and submits $\{ID_i, h(ID_i||PW_i)\}$ to S through a secure channel.

R2. $S \rightarrow U_i$: $\{h(\cdot), B_i, C_i\}$

After receiving the request, S computes $A_i = h(h(ID_i) \oplus x)$, $B_i = h(ID_i||PW_i) \oplus A_i$ and $C_i = h(A_i)$, where x is the permanent secret key of S. Then, S sends $\{h(\cdot), B_i, C_i\}$ to U_i through a secure channel.

2.2 Login phase

Whenever U_i wants to login a server S, he/she must perform the following steps:

L1. After inserting his/her smart card into the card reader, U_i inputs the identity ID_i and password PW_i. Then, the smart card computes $D_i = B_i \oplus h(ID_i||PW_i)$ and $E_i = h(D_i)$.

L2. The smart card checks whether or not E_i and C_i are equal. If yes, U_i passes the legitimate verification and performs the following steps; otherwise, U_i is rejected.

L3. The smart card randomly chooses a nonce R_1 and computes $F_i = D_i \oplus R_1$.

L4. $U_i \rightarrow S$: $\{h(ID_i), F_i\}$

U_i sends the login request message $\{h(ID_i), F_i\}$ to the remote server S.

2.3 Authentication phase

A user performs the remote authentication phase based on the login message for authentication as long as it visits the server. U_i and S perform the following steps to achieve mutual authentication and to establish a session key:

A1. After receiving the login message $\{h(ID_i), F_i\}$, S computes $G_i = h(h(ID_i) \oplus x)$ and $R'_1 = F_i \oplus G_i$. Then, S chooses a nonce R_2 and computes $H_i = G_i \oplus R_2$.

A2. $S \rightarrow U_i$: $\{H_i, h(R'_1)\}$

The server S sends the mutual authentication message $\{H_i, h(R'_1)\}$ to the user U_i.

A3. $U_i \rightarrow S$: $\{h(R'_2)\}$

After receiving the mutual authentication message $\{H_i, h(R'_1)\}$ from the server S, the user U_i checks whether or not $h(R'_1)$ and $h(R_1)$ are equal. If no, U_i rejects this message and terminates the operation; otherwise, U_i authenticates S successfully and computes $R'_2 = H_i \oplus D_i$. Then, U_i sends $\{h(R'_2)\}$ to S.

A4. When the server S receives $\{h(R'_2)\}$, S checks whether or not $h(R'_2)$ and $h(R_2)$ are equal. If no, S sends reject message to the U_i; otherwise, S authenticates U_i.

After finishing mutual authentication phase, the user U_i and the server S each can compute a common session key $SK = h(R_1||R_2)$ for the next data transmission.

2.4 Password change phase

The user U_i can change his/her password without the help of the server S, and the details of the password change procedures are as follows:

C1. U_i inserts the smart card, and input his/her old password PW_i and the identity ID_i.

C2. The smart card computes $A'_i = B_i \oplus h(ID_i||PW_i)$, $C'_i = h(A'_i)$, and checks whether or not C'_i and C_i are equal. If the verification process is correct, the smart card asks the cardholder to resubmit a new password PW_i^{new}.

C3. The smart card computes $B_i^{new} = h(ID_i||PW_i^{new}) \oplus A_i$.

C4. The smart card replaces the values of B_i stored in its memory with B_i^{new} to finish the password change phase.

3 Security Vulnerabilities of ERUA Scheme

This section demonstrates that Yang et al.'s ERUA scheme [4] is still vulnerable to off-line password guessing attack and does not provide the unlinkability property and user anonymity because of the identity guessing attack unlike their claims. The details of these flaws are described as follows:

3.1 User anonymity problem

Users' anonymity is an important security requirement that a practical dynamic identity-based remote authentication scheme should achieve [7]. In the Yang et al.s ERUA scheme, they claimed that their proposed scheme preserves user anonymity because a user's real identity ID_i is concealed in the $h(ID_i)$. However, we show that Yang et al.s ERUA scheme [4] still fails to achieve the anonymity as follows:

1. *Eve* intercepts a login message $\{h(ID_i), F_i\}$ of U_i of a previous session.
2. *Eve* guesses an identity ID_i^* and then computes $h(ID_i^*)$.
3. *Eve* verifies the correctness of ID_i by checking whether the $h(ID_i^*)$ and the intercepted $h(ID_i)$ are equal. If the check passes, then *Eve* confirms that the guessed password ID_i^* is the correct one.
4. If it is not correct, *Eve* chooses another identity ID_i^{**} and repeatedly performs above steps (2) and (3) until it finds the exact identity ID_i of U_i.

The adversary *Eve* can easily guess the identity ID_i of U_i by checking all possible identities from the search space $|\mathbb{D}_{ID}|$, where $|\cdot|$ indicates the cardinality of $\mathbb{D}_{ID}$. The running time of the aforementioned procedure is $O(|\mathbb{D}_{ID}|) \times T_h$, where T_h represents the execution time of hash operation. It can be noted that for easy memorization, user generally chooses his/her identity with low intensity value from the set $\mathbb{D}_{ID}$ having small number of elements. Since $\mathbb{D}_{ID}$ is not large enough in practice, for example, $|\mathbb{D}_{ID}| \leq 10^6$ and the time complexities T_h are also negligible, thus *Eve* can complete the above procedure in polynomial time [6, 7].

3.2 Linkability attack

Unlinkability is a property which means an adversary cannot recognize whether outputs are from the same user, and this property is important with respect to the privacy problem in the anonymous user identification [5]. However, Yang et al.'s ERUA scheme cannot provide unlinkability property. That is, an adversary *Eve* can eavesdrop the user U_i's login request message $\{h(ID_i), F_i\}$ between the user U_i and the server S from the public channel; $h(ID_i)$ in the login request message $\{h(ID_i), F_i\}$ is kept the same in every login session. In other words, a malicious adversary *Eve* is capable of tracing out the user U_i according to $h(ID_i)$ which is in the U_i's login request message. For example, *Eve* can perform the following attack to break user privacy and anonymity.

1. In any session, *Eve* intercepts user's login request message $\{h(ID'_i), F'_i\}$.

2. *Eve* checks whether both $h(ID'_i)$ is equal to $h(ID_i)$. If this condition is true, it means that $ID'_i \equiv ID_i$. So, the attacker can know this login request message $\{h(ID'_i), F'_i\}$ is sent from the same user U_i.

As a result, anyone can decide whether two transactions $\{h(ID_i), F_i\}$ and $\{h(ID'_i), F'_i\}$ are of the same user U_i or not by checking if the following equation holds: $h(ID'_i) \overset{?}{=} h(ID_i)$. The above linkability security problem in the ERUA scheme happens because anyone can easily check whether the intercepted two transactions are from the same user or not. Therefore, Yang et al.'s ERUA scheme fails in unlinkability property of U_i during the login phase.

3.3 Off-line password guessing attack

Moreover, *Eve* can obtain the password PW_i of U_i by using the ID_i^*. Suppose that the user U_i's smart card is lost or stolen, then the attacker *Eve* can extract the stored secret information $\{h(\cdot), B_i, C_i\}$ stored in the smart card. *Eve* cam extract the stored secret information by monitoring their timing information, power consumption and reverse engineering techniques. Then, *Eve* can perform the off-line password guessing attack as follows:

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

2. *Eve* checks if the following equation holds or not

$$C_i \overset{?}{=} h(B_i \oplus h(ID_i^*||PW_i^*)) \tag{1}$$

   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

$$C_i \overset{?}{=} h(B_i \oplus h(ID_i^*||PW_i^{**})) \tag{2}$$

It is clear that if $PW_i^* \equiv PW_i$, then

$$\begin{aligned} & h(B_i \oplus h(ID_i^*||PW_i^*)) \\ & \qquad = h(h(ID_i||PW_i) \oplus A_i \oplus h(ID_i^*||PW_i^*)) \\ & \qquad = h(A_i) \\ & \qquad = C_i \end{aligned} \tag{3}$$

Therefore, Yang et al.s ERUA 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**$(B_i, C_i, ID_i^*, h(\cdot), \mathbb{D}_{PW})$
{
    **for** $i := 0$ to $|\mathbb{D}_{PW}|$
    {
        $PW_i^* \leftarrow \mathbb{D}_{PW}$;
        $A_i^* = B_i \oplus h(ID_i^*||PW_i^*)$;
        **if** $C_i \overset{?}{=} h(A_i^*)$ **then**
                **return** $PW_i^*$
    }
}
```

The running time of the above password guessing attack is $(O(|\mathbb{D}_{ID}|) \times T_h) + (O(|\mathbb{D}_{PW}|) \times T_c \times T_x \times T_h)$, where T_c and T_x represent the execution time of concatenation and bit-wise XOR operations, respectively. The search spaces $\mathbb{D}_{ID}$ and $\mathbb{D}_{PW}$ are unlikely to be large enough (for example, $|\mathbb{D}_{ID}| \leq 10^6$ and $|\mathbb{D}_{PW}| \leq 10^6$), and the time complexities T_c, T_h and T_x all can be executed with negligible amount of time, thus the polynomial time-bounded adversary *Eve* can find the exact password PW_i of U_i easily [6, 7].

4 Conclusions

This paper reviewed Yang et al.'s ERUA scheme and then pointed out that the ERUA scheme scheme is still vulnerable to off-line password guessing attack and does not provide the unlinkability property and user anonymity because of the identity guessing attack unlike their claims. Consequently Yang et al.'s ERUA scheme is insecure for practical application. Further works will be focused on improving the ERUA's scheme which can be able to provide greater security and to be more efficient than the existing dynamic ID-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] M. Das, A. Saxena, P. Gulati, A dynamic ID-based remote user authentication scheme, *IEEE Trans actions on Consumer Electronics*, **50** (2004), 629-631.

[2] Y. Wang, J. Liu, F. Xiao, J. Dan, A more efficient and secure dynamic ID-based remote user authentication scheme, *Computer Communications*, **32** (2009), 583-585.

[3] M. Khan, K. Kim, K. Alghathbar, Cryptanalysis and security enhancement of a more efficient & secure dynamic ID-based remote user authentication scheme, *Computer Communications*, **34** (2011), 305-309.

[4] X. Yang, X. Cui, Z. Cao, Z. Hu, An enhanced remote user authentication scheme, *Engineering*, **6(1)** (2014), 261-267.

[5] E.Y. Yoon, K.Y. Yoo, An improvement of the user identification and key agreement protocol with user anonymity, *Informatica*, **23(1)** (2012), 155172.

[6] D. Florencio, C. Herley, A large-scale study of web password habits, *In Proceedings of the 16th International Conference on World Wide Web*, (2007), 657-666.

[7] S. Islam, G. Biswas, K. Choo, Cryptanalysis of an improved smartcard-based remote password authentication scheme, *Information Sciences Letters*, **3(1)** (2014), 35-40.

Received: October 4, 2014; Published: October 28, 2014