LETTER

On the Security of an Efficient and Secure Dynamic ID-Based Remote User Authentication Scheme

Eun-Jun YOON[†a)] ***and*** **Kee-Young YOO**[††b)], ***Members***

SUMMARY In 2009, Wang et al. proposed an efficient and secure dynamic ID-based remote user authentication scheme based on the one-way secure hash function. This letter demonstrates that Wang et al.'s scheme is still vulnerable to impersonation attacks.

key words: *authentication, password, cryptanalysis, hash function, smartcard*

1. Introduction

A remote user authentication scheme [1] is used to verify the legitimacy of remote users' login requests through an insecure channel. Password-based authentication scheme is the most common method to check the validity of the login message and authenticate the user. Recently, many authentication schemes [1]–[12] have been proposed to improve the security and practicability of authentication.

Quite recently, Wang et al. [12] proposed an efficient and secure dynamic ID-based remote user authentication scheme based on the one-way secure hash function. Wang et al. claimed that their scheme has the following merits: 1) it allows users to change and choose passwords freely; 2) server does not maintain any verifier tables because it uses a smartcard to store a secret key; 3) it provides mutual authentication between user and remote server; 4) it overcomes the fatal drawback that user's authentication is independent of the password; 5) it is secure to against ID-theft [9]–[11], replay attacks and insider attacks, etc.

Unfortunately, we find that Wang et al.'s scheme [12] is still vulnerable to impersonation attacks. Accordingly, this letter demonstrates that Wang et al.'s scheme is vulnerable to impersonation attacks, in which an attacker can easily impersonate any legal user.

2. Review of Wang et al.'s Scheme

We briefly recall Wang et al.'s scheme in [12]. The notations used in the scheme are shown as follows:

- U: The user
- pw: The password of U
- ID: The identity of U
- S: The remote server
- x: The secret key of S
- $h(\cdot)$: A one-way hash function
- $\oplus$: Bitwise XOR operation
- $\Rightarrow$: A secure channel
- $\rightarrow$: A common channel

Wang et al.'s scheme is composed of four phases; the registration phase, the login phase, the verification phase and the password change phase.

2.1 Registration Phase

The user U_i sends the registration request to the remote server S:

1. $U_i \Rightarrow S$: ID_i.
   U_i submits ID_i to S.
2. S computes
   $$N_i = h(pw_i) \oplus h(x) \oplus ID_i \tag{1}$$
   where x is the secret key of the remote server, and pw_i is the password of U_i chosen by S.
3. S personalizes the smartcard with the parameters $[h(\cdot), N_i, y]$, where y is the remote server's secret number stored in each registered user's smartcard.
4. $S \Rightarrow U_i$: pw_i and smartcard.

2.2 Login Phase

When a user wants to login to the remote server, he/she inserts the smartcard into the terminal and keys the identity ID_i and the password pw_i, then the smartcard will perform the following steps:

1. Computes dynamic ID
   $$CID_i = h(pw_i) \oplus h(N_i \oplus y \oplus T) \oplus ID_i \tag{2}$$
   where T is the current date and time.
2. $U_i \rightarrow S$: ID_i, CID_i, N_i, T.

2.3 Verification Phase

When the remote server S receives the login request (ID_i, CID_i, N_i, T) at time T', S verifies as:

Manuscript received June 10, 2011.

[†]The author is with the Department of Cyber Security, Kyungil University, 33 Buho-Ri, Hayang-Ub, Kyungsan-Si, Kyungsangpuk-Do 712–701, South Korea.

[††]The author is with the School of Electrical Engineering and Computer Science, Kyungpook National University, 1370 Sankyuk-Dong, Buk-Gu, Daegu 702–701, South Korea

a) E-mail: ejyoon@kiu.ac.kr

b) E-mail: yook@knu.ac.kr (Corresponding author)

DOI: 10.1587/transinf.E95.D.1684

1. Check the validity of the time interval, if $T' - T \leqslant \Delta T$ hold, S accepts the login request of U_i, otherwise, the login request will be refused.
2. Compute
$$h'(pw_i) = CID_i \oplus h(N_i \oplus y \oplus T) \oplus ID_i \tag{3}$$
3. Compute
$$ID'_i = N_i \oplus h(x) \oplus h'(pw_i) \tag{4}$$
and verifies whether it is equal to ID_i in the login request. If it does not holds, S rejects the login request of U_i, otherwise, accepts it. Then, S computes
$$a' = h(h'(pw_i) \oplus y \oplus T') \tag{5}$$
using the results of Step 2.
4. $S \rightarrow U_i$: (a', T').

Upon receiving the reply message (a', T') at time T^*, U_i verifies as:

1. Check whether $T^* - T \geqslant \Delta T$.
2. If not, U_i computes
$$a = h(h(pw_i) \oplus y \oplus T') \tag{6}$$
and compares it with the received a'. If it holds, U_i confirms that S is valid.

Figure 1 illustrates the login and verification phases of Wang et al.'s scheme.

2.4 Password Change Phase

When user wants to change the password, he/she inserts smartcard into the terminal device, keys the password pw_i and requests to change the password to new one pw_{new}, then the smartcard computes

$$N_i^* = N_i \oplus h(pw_i) \oplus h(pw_{new}) \tag{7}$$

and replaces the N_i with new N_i^*, password gets changed.

Shared Information: $h(\cdot)$
Information held by U_i: ID_i, pw_i, smartcard(N_i, y)
where $N_i = h(pw_i) \oplus h(x) \oplus ID_i$
Information held by S: x

User U_i | **Server** S

Input ID_i and pw_i
$CID_i = h(pw_i) \oplus h(N_i \oplus y \oplus T) \oplus ID_i$
$\xrightarrow{ID_i, CID_i, N_i, T}$
Verify $T' - T \leqslant \Delta T$
$h'(pw_i) = CID_i \oplus h(N_i \oplus y \oplus T) \oplus ID_i$
$ID'_i = N_i \oplus h(x) \oplus h'(pw_i)$
Verify $ID'_i \stackrel{?}{=} ID_i$
$a' = h(h'(pw_i) \oplus y \oplus T')$
$\xleftarrow{a', T'}$
Verify $T^* - T \leqslant \Delta T$
$a = h(h(pw_i) \oplus y \oplus T')$
Verify $a \stackrel{?}{=} a'$

Fig. 1 Login and verification phases of Wang et al.'s scheme.

3. Security Analysis of Wang et al.'s Scheme

3.1 User Impersonation Attack by an Attacker E

Suppose an attacker E wants to impersonate a legal user U_k ($k \neq i$). To succeed in the impersonation attack, E first obtains the identity ID_k of U_k. E can easily obtain all legal users' identities from the login phase because these values are transmitted on open network. When U_i sends a login request message (ID_i, CID_i, N_i, T) to S in Step 2 of the login phase, E intercepts it and then replaces ID_i with ID_k. Finally, E sends a forged login request message (ID_k, CID_i, N_i, T) to S.

Upon receiving the forged login request message (ID_k, CID_i, N_i, T), S will perform the following:

1. S will check the validity of the time interval. Since $T' - T \leqslant \Delta T$ always holds, S will accept the forged login request of E.
2. S then will compute
$$\begin{aligned} h'(pw_i) &= CID_i \oplus h(N_i \oplus y \oplus T) \oplus ID_k \\ &= h(pw_i) \oplus h(N_i \oplus y \oplus T) \oplus ID_i \oplus \\ &\quad h(N_i \oplus y \oplus T) \oplus ID_k \\ &= h(pw_i) \oplus ID_i \oplus ID_k \end{aligned} \tag{8}$$
3. S will compute
$$\begin{aligned} ID'_k &= N_i \oplus h(x) \oplus h'(pw_i) \\ &= h(pw_i) \oplus h(x) \oplus ID_i \oplus h(x) \oplus \\ &\quad h(pw_i) \oplus ID_i \oplus ID_k \\ &= ID_k \end{aligned} \tag{9}$$
4. S finally will verify whether ID'_k is equal to ID_k in the login request. Since it always holds (see the Eqs. (3) and (4)), S will accept the forged login request of E and believe that the request party is a user U_k (not U_i).

Consequently, E can freely impersonate any legal user without being detected by the server S by using the above impersonation attack.

The proposed user impersonation attack by an attacker E can succeed only during the valid time period $T' - T \leqslant \Delta T$. However, the success probability of the proposed attack is very high. That is, an attacker E can simply replace ID_i with ID_k within valid time period ΔT of S because it does not require any computation time. As a result, Wang et al.'s scheme is vulnerable to the above user impersonation attack by an attacker E.

3.2 User Impersonation Attack by a Legal User U_i

Moreover, a legal user U_i also can easily impersonate other legal users U_k ($k \neq i$) by using an identity ID_k ($k \neq i$) of the target user. For example, U_i first finds a value δ in advance which satisfies the following equation:

$$ID_k \equiv ID_i \oplus \delta \tag{10}$$

Then, U_i computes the followings:

$$\begin{aligned} CID_k^* &= CID_i \oplus \delta \\ &= h(pw_i) \oplus h(N_i \oplus y \oplus T) \oplus ID_i \oplus \delta \end{aligned} \tag{11}$$

$$\begin{aligned} N_k^* &= N_i \oplus \delta \\ &= h(pw_i) \oplus h(x) \oplus ID_i \oplus \delta \end{aligned} \tag{12}$$

Finally, U_i sends a forged login request message $(ID_k, CID_k^*, N_k^*, T)$ to S. Then, S will believe that the request party is a user U_k (not U_i) because $ID_i \oplus \delta$ is equal to ID_k.

The proposed user impersonation attack by a legal user U_i can succeed only during the valid time period $T' - T \leqslant \Delta T$. However, the success probability of the proposed attack is very high. That is, the illegal user U_i can simply modify CID_i and N_i with CID_k^* and N_k^* within valid time period ΔT of S because it needs to compute two XOR operations. As a result, Wang et al.'s scheme is vulnerable to the above user impersonation attack by a legal user U_i.

4. Conclusion

User authentication scheme technology has been widely deployed in various kinds of applications. Quite recently, Wang et al. proposed an efficient and secure dynamic ID-based remote user authentication scheme based on the one-way secure hash function. However, this letter demonstrated that Wang et al.'s scheme is still vulnerable to impersonation attacks. For this reason, Wang et al.'s scheme is insecure for practical application.

Acknowledgements

This research 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) and partially supported by the MKE (The Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2012-H0301-12-2004) supervised by the NIPA (National IT Industry Promotion Agency).

References

[1] L. Lamport, "Password authentication with insecure communication," Commun. ACM, vol.24, no.11, pp.70–772, 1981.
[2] M.S. Hwang and L.H. Li, "A new remote user authentication scheme using smart cards," IEEE Trans. Consum. Electron., vol.46, no.1, pp.28–30, 2000.
[3] H.M. Sun, "An efficient remote user authentication scheme using smart cards," IEEE Trans. Consum. Electron., vol.46, no.4, pp.958–961, 2000.
[4] Y.L. Tang, M.S. Hwang, and C.C. Lee, "A simple remote user authentication scheme," Mathematical and Computer Modeling, vol.36, pp.103–107, 2002.
[5] C.C. Lee, L.H. Li, and M.S. Hwang, "A remote user authentication scheme using hash functions," ACM Operating Systems Review, vol.36, no.4, pp.23–29, 2002.
[6] M.S. Hwang, C.C. Lee, and Y.L. Tang, "A simple remote user authentication scheme," Math. Comput. Model., vol.36, no.1-2, pp.103–107, 2002.
[7] C. Lee, M.S. Hwang, and W.P. Yang, "A flexible remote user authentication scheme using smart cards," ACM Oper. Syst. Rev., vol.36, no.3, pp.46–52, 2002.
[8] W.C. Ku and S.M. Chen, "Weaknesses and improvements of an efficient password base remote user authentication scheme using smartcards," IEEE Trans. Consum. Electron., vol.50, no.1, pp.204–206, 2004.
[9] H.C. Hsiang and W.K. Shih, "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment," Computer Standards & Interfaces, vol.31, pp.1118–1123, 2009.
[10] M.L. Das, A. Saxena, and V.P. Gulati, "A dynamic ID-based remote user authentication scheme," IEEE Trans. Consum. Electron., vol.50, no.2, pp.629–631, 2004.
[11] K. Amit, Awasthi, and S. Lal, "Security analysis of a dynamic ID-based remote user authentication scheme," Available from: <http:\\eprint.iacr.org/2004/238>, 2005.
[12] Y.Y. Wang, J.Y. Liu, F.X. Xiao, and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme," Comput. Commun., vol.32, pp.583–585, 2009.