Cryptanalysis of a More Secure Remote User Authentication Scheme

Wen-Bing Horng, Cheng-Ping Lee
Dept. Computer Science & Information Engineering
Tamkang University
Taipei, Taiwan, R.O.C.
Email: horng@mail.tku.edu.tw
selrahc.charles@msa.hinet.net

Jian-Wen Peng
Dept. Commerce Technology and Management
Chihlee Institute of Technology
Taipei, Taiwan, R.O.C.
Email: pchw8598@mail.chihlee.edu.tw

***Abstract*—Recently, Kim and Chung proposed a more secure remote user authentication scheme, which is an improvement over Yoon-Yoo's scheme to remedy their security flaws, such as leak of password and vulnerabilities to the masquerading user attack, the masquerading server attack, and the stolen-verifier attack. In this paper, we will show that Kim-Chung's improved scheme is vulnerable to the offline password guessing attack. In addition, the scheme does not possess the feature of secret key forward secrecy as they claimed. Hence, Kim-Chung's scheme is also subject to the masquerading user attack and the masquerading server attack as well. Moreover, their scheme does not generate session keys for secure communications.**

***Keywords*-authentication; network security; smart card;**

I. Introduction

With the prevalence of computer networks all over the world, many network services are provided by remote servers. However, for a secure network system, it needs a remote authentication mechanism to validate the legitimacy of communicating parties. Since Lamport [1] proposed his prominent work in 1981, many researchers have proposed new schemes to improve the efficiency and security of remote authentication.

In 2002, Chien et al. [2] proposed a very efficient remote mutual authentication scheme. However, as demonstrated by Hsu [3], [4], Chien et al.'s scheme is susceptible to the parallel session attack. Later, Lee et al. [5], [6] improved Chien et al.'s scheme to get rid of this drawback. Shortly, Yoon and Yoo [7] pointed out that Lee et al.'s scheme is vulnerable to the masquerading server attack and is insecure in changing passwords. They then proposed an enhancement to cope with these weaknesses. Recently, Kim and Chung [8] discovered that Yoon-Yoo's scheme is vulnerable to the masquerading server attack, the masquerading user attack, and the stolen verifier attack, and it is easy to leak passwords. Besides, they also improved Yoon-Yoo's scheme to eliminate these security flaws.

In this paper, we will show that Kim-Chung's improved scheme is vulnerable to the offline password guessing attack. In addition, their scheme fails to achieve the property of secret key forward secrecy as they claimed. Therefore, their scheme is also subject to both the masquerading server attack and the masquerading user attack.

The rest of the paper is organized as follows. In Section 2, we briefly review Kim-Chung's authentication scheme. In Section 3, we show the security weaknesses of Kim-Chung's scheme. Finally, we conclude this paper in the last section.

II. Review of Kim-Chung's Scheme

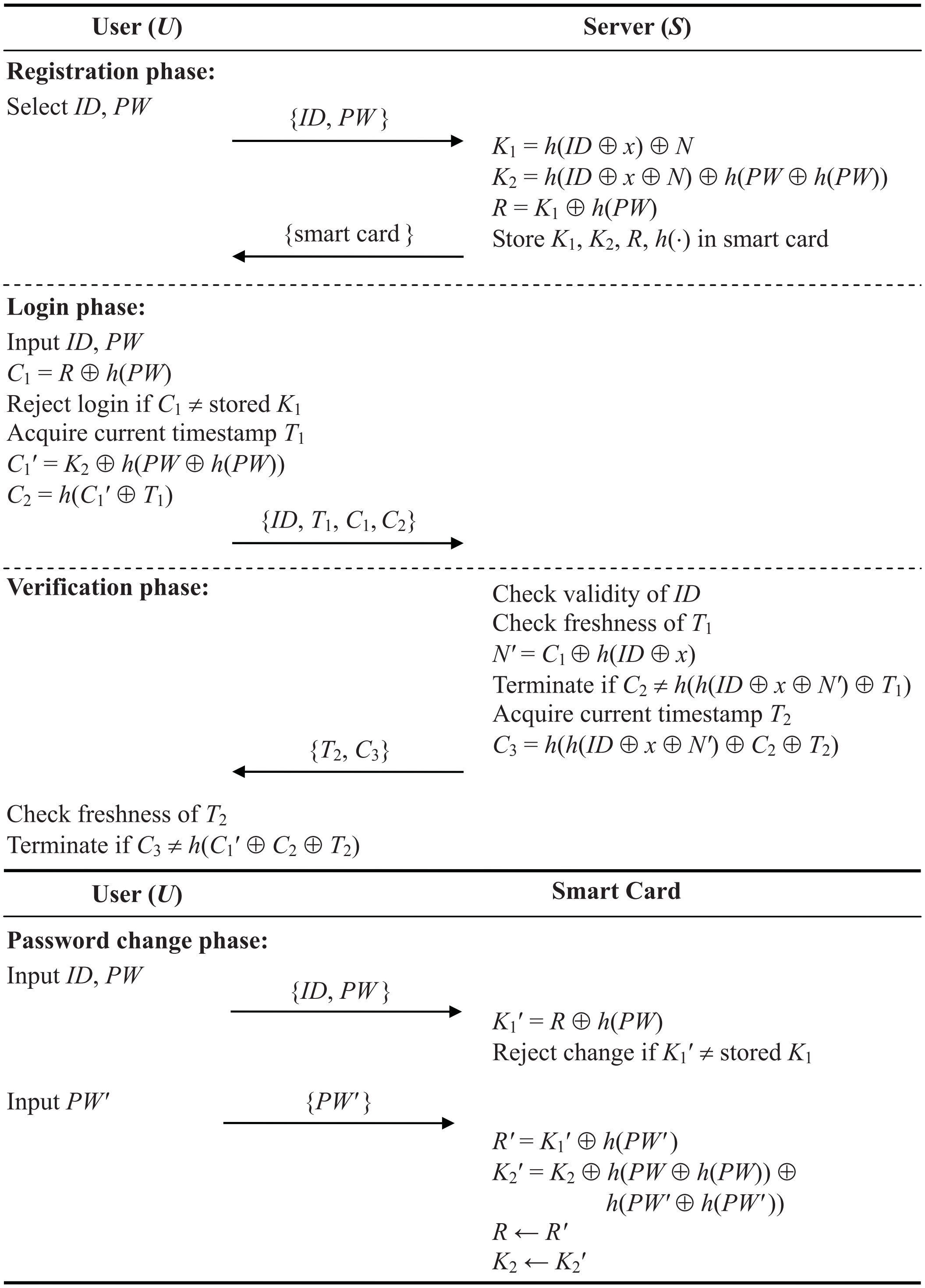
In this section, we briefly review the remote user authentication scheme proposed by Kim and Chung in 2009 [8]. Kim-Chung's scheme, summarized in Fig. 1, consists of four phases: registration, login, verification, and password change phases. For convenience, the notation used is listed below.

- U: a user (client)
- ID: U's identity
- PW: U's password
- S: a remote server
- x: the secret key of S
- $h()$: a hash function
- $\oplus$: bitwise XOR operation
- $\rightarrow$: a common (insecure) communication channel
- $\Rightarrow$: a secure communication channel
- $X \rightarrow Y : \{M\}$: X sends a message M to Y over a common communication channel

A. Registration Phase

In this phase, the user U initially registers with the server S by performing the following steps.

(1) $U \Rightarrow S : \{ID, PW\}$. U selects his ID and PW and sends them to S over a secure channel.
(2) After receiving ID and PW, S computes $K_1 = h(ID \oplus x) \oplus N$ and $K_2 = h(ID \oplus x \oplus N) \oplus h(PW \oplus h(PW))$, where N is a random number unique to the user U. Then, S computes $R = K_1 \oplus h(PW)$.
(3) S stores the secure information K_1, K_2, R, and $h()$ into U's smart card $CARD$.
(4) $S \Rightarrow U : \{CARD\}$. S delivers the smart card $CARD$ over a secure channel to U to complete the registration procedure.



User (U)		Server (S)
Registration phase:		
Select ID, PW	$\{ID, PW\}$ →	$K_1 = h(ID \oplus x) \oplus N$ $K_2 = h(ID \oplus x \oplus N) \oplus h(PW \oplus h(PW))$ $R = K_1 \oplus h(PW)$
	← $\{\text{smart card}\}$	Store K_1, K_2, R, $h(\cdot)$ in smart card
Login phase:		
Input ID, PW $C_1 = R \oplus h(PW)$ Reject login if $C_1 \neq$ stored K_1 Acquire current timestamp T_1 $C_1' = K_2 \oplus h(PW \oplus h(PW))$ $C_2 = h(C_1' \oplus T_1)$	$\{ID, T_1, C_1, C_2\}$ →	
Verification phase:		Check validity of ID Check freshness of T_1 $N' = C_1 \oplus h(ID \oplus x)$ Terminate if $C_2 \neq h(h(ID \oplus x \oplus N') \oplus T_1)$ Acquire current timestamp T_2 $C_3 = h(h(ID \oplus x \oplus N') \oplus C_2 \oplus T_2)$
	← $\{T_2, C_3\}$	
Check freshness of T_2 Terminate if $C_3 \neq h(C_1' \oplus C_2 \oplus T_2)$		

User (U)		Smart Card
Password change phase:		
Input ID, PW	$\{ID, PW\}$ →	$K_1' = R \oplus h(PW)$ Reject change if $K_1' \neq$ stored K_1
Input PW'	$\{PW'\}$ →	$R' = K_1' \oplus h(PW')$ $K_2' = K_2 \oplus h(PW \oplus h(PW)) \oplus h(PW' \oplus h(PW'))$ $R \leftarrow R'$ $K_2 \leftarrow K_2'$

Figure 1. Kim-Chung's remote user authentication scheme

B. Login Phase

In this phase, the user U sends a login request message to the server S to access the services provided by S.

(1) U inserts his smart card, $CARD$, into a card reader and inputs his ID and PW.

(2) The smart card first computes $C_1 = R \oplus h(PW)$. If C_1 is not equal to the stored K_1, then the smart card rejects the login request. Otherwise, it computes $C_1' = K_2 \oplus h(PW \oplus h(PW))$ and $C_2 = h(C_1' \oplus T_1)$, where T_1 is the current timestamp.

(3) $U \rightarrow S : \{ID, T_1, C_1, C_2\}$.

C. Verification Phase

In this phase, the server S verifies the authenticity of the login request sent by U, and finally U will in turn verify S as well to achieve mutual authentication.

(1) Upon receiving the login message $\{ID, T_1, C_1, C_2\}$ at timestamp T_1', S first checks the validity of ID and the freshness of T_1, where the freshness of T_1 is checked by verifying whether $T_1' - T_1 \leq \Delta T$ and ΔT is a valid time interval.

(2) If ID is not valid or T_1 is not fresh, S terminates the current session. Otherwise, S computes $N' = C_1 \oplus h(ID \oplus x)$ and checks if $h(h(ID \oplus x \oplus N') \oplus T_1)$ is equal to the received C_2. If it is not, S terminates the current session. Otherwise, S successfully authenticates U and computes $C_3 = h(h(ID \oplus x \oplus N') \oplus C_2 \oplus T_2)$, where T_2 is the current timestamp.

(3) $S \rightarrow U : \{T_2, C_3\}$.

(4) On the receipt of the message $\{T_2, C_3\}$ from S at timestamp T_2', U first checks the freshness of T_2 in the same way as above. If T_2 is not fresh, U terminates the current session. Otherwise, U checks if $h(C_1' \oplus C_2 \oplus T_2)$ is equal to the received C_3. It it is not, U terminates the current session. Otherwise, U now has successfully authenticated S.

D. Password Change Phase

In this phase, if the user U wants to change his password, he performs the following steps.

(1) U inserts his smart card, $CARD$, into a card reader and then inputs his ID and PW.

(2) The smart card computes $K_1' = R \oplus h(PW)$ and compares K_1' with the stored K_1. If they are not equal, the smart card rejects the password change request. Otherwise, U inputs a new password PW'.

(3) The smart card then computes $R' = K_1' \oplus h(PW')$ and $K_2' = K_2 \oplus h(PW \oplus h(PW)) \oplus h(PW' \oplus h(PW'))$. Then, it replaces R and K_2 with R' and K_2', respectively.

III. Security Weaknesses

There are two assumptions made by Kim-Chung's scheme [8]:

- It is assumed that an attacker has total control over the communication channel between the user U and the remote server S. In other words, the attacker can insert, delete, alter, or intercept any messages transmitted in the channel.
- As reported in [9], [10], the values stored in a smart card could be extracted by monitoring its power consumption. Thus, it is also assumed that the attacker can steal the user's smart card to extract the secret values stored in the smart card.

In the following discussions of the security flaws of Kim-Chung's remote user authentication scheme, based on the above two assumptions, we assume that an attacker U_a can extract the secret values $\{K_1, K_2, R\}$ stored in the user U's smart card, and he can intercept the login request message $\{ID, T_1, C_1, C_2\}$ from the user U and the reply message $\{T_2, C_3\}$ from the server S.

A. Offline Password Guessing Attack

A remote user authentication scheme which is vulnerable to the offline password guessing attack must satisfy the following two conditions: (1) the user's password is weak, and (2) there exists a piece of password-related information used as a comparison target for password guessing.

In Kim-Chung's scheme, a user is allowed to choose his own password at will during the registration phase; the user usually tends to select a password that is easily remembered for his convenience. Hence, these easy-to-remember passwords, which are called weak passwords, are potentially vulnerable to the password guessing attack, in which an adversary can try to guess the user's password from a dictionary of all possible weak passwords and then verify his guess.

Besides, since the secret values stored in the smart card are assumed to be able to be extracted, an attacker U_a can steal the user U's smart card to obtain the stored secret values K_1, K_2, and R. Then, the attacker U_a can guess the value of PW by verifying his guess using the equation $h(PW) = R \oplus K_1$.

On the other hands, the user U's password can be guessed by the useful features provided by Kim-Chung's scheme, such as early detection of incorrect password or secure password change. In Kim-Chung's scheme, an incorrect password PW^* can be detected earlier by the smart card in the login phase by checking whether C_1 is equal to the stored K_1, without resorting to the checking of the remote server, where $C_1 = R \oplus h(PW^*)$. If they are not equal, the smart card will reject the login request. Therefore, the attacker U_a can steal the user U's smart card and then launch the offline password guessing attack by providing guessed passwords. If the smart card accepts the login request, then the current guessed-password is the correct one. In a similar way, the feature of secure password change provided in Kim-Chung's scheme is also vulnerable to the offline password guessing attack.

Once the password PW is known to the attacker, Kim-Chung's scheme is subject to the masquerading server attack and the masquerading user attack, as shown in Subsections III-C and III-D, respectively.

B. Secret Key Forward Secrecy

Kim and Chung claimed that their scheme provides the security feature of secret key forward secrecy; that is, even if the secret key x of the server S happens to be revealed, an attacker cannot impersonate other users by using the revealed key x. However, this claim is not true. If x is revealed, an attacker can derive the random number N unique to the user U by computing $N = C_1 \oplus h(ID \oplus x)$, where ID and C_1 can be obtained from the intercepted login request message over the communication channel. Once, N is known, the attacker can impersonate the server S (masquerading server attack) as well as impersonate the user U (masquerading user attack) as shown in the following subsections.

C. Masquerading Server Attack

If an attacker knows PW or N, he can impersonate the server S in the following two ways. If the attacker only obtains PW, he can first compute $K = K_2 \oplus h(PW \oplus h(PW))$, which is equal to $h(ID \oplus x \oplus N)$. If he only knows N, he can direct compute $K = h(ID \oplus x \oplus N)$. Then, the attacker computes a fake $C_3^* = h(K \oplus C_2 \oplus T_2^*)$, where T_2^* is the current timestamp and C_2 is obtained from the intercepted login message. Finally, the attacker sends a forged reply message $\{T_2^*, C_3^*\}$ to the user U to impersonate the server S.

D. Masquerading User Attack

Similarly, an attacker can impersonate U if he obtains PW or N by the following two methods. He can compute $K = K_2 \oplus h(PW \oplus h(PW))$ by using PW only or $K = h(ID \oplus x \oplus N)$ by using N only. Then, the attacker computes a bogus $C_2^* = h(K \oplus T_1^*)$, where T_1^* is the current timestamp. Finally, the attacker transmits the forged login request message $\{ID, T_1^*, C_1, C_2^*\}$ to the remote server S to pretend to be the user U.

Note that once the attacker can impersonate both the server S and the user U, Kim-Chung's scheme is also vulnerable to the man-in-the-middle attack.

IV. Conclusion

In recent years, Yoon and Yoo proposed a remote user authentication scheme with some good features such as providing mutual authentication, secret key forward secrecy, and fast detection of wrong password. However, Kim and Chung pointed out that Yoon-Yoo's scheme is vulnerable to the masquerading user attack, the masquerading server attack, the stolen verifier attack, and leak of password. They then presented an improvement to remove these security flaws while preserving all the merits of Yoon-Yoo's scheme.

In this paper, we have shown that Kim-Chung's improved scheme is vulnerable to the offline password guessing attack. In addition, the scheme does not possess the feature of secret key forward secrecy as claimed. Therefore, their scheme is also susceptible to the masquerading server attack and the masquerading user attack as well. Furthermore, their scheme does not provide session key exchanges for secure communications.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable comments and constructive suggestions. This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC 98-2631-S-032-003.

References

[1] L. Lamport, "Password authentication with insecure communication," Commun. ACM, vol. 24, no. 11, pp. 770–772, 1981.

[2] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card," Comput. Secur., vol. 21, no. 4, pp. 372–375, 2002.

[3] C. L. Hsu, "Security of two remote user authentication schemes using smart cards," IEEE Trans. Consum. Electron., vol. 49, no. 4, pp. 1196-1198, 2003.

[4] C. L. Hsu, "Security of Chien et al.'s remote user authentication scheme using smart cards," Comput. Stand. Interfaces, vol. 26, no. 3, pp. 167-169, 2004.

[5] S. W. Lee, H. S. Kim, and K. Y. Yoo, "Improved efficient remote user authentication scheme using smart cards," IEEE Trans. Consum. Electron., vol. 50, no. 2, pp. 565–567, 2004.

[6] S. W. Lee, H. S. Kim, and K. Y. Yoo, "Improvement of Chien et al.'s remote user authentication scheme using smart cards," Comput. Stand. Interfaces, vol. 27, no. 2, pp. 181–183, 2005.

[7] E. J. Yoon and K. Y. Yoo, "More efficient and secure remote user authentication scheme using smart cards," Proc. 11th International Conference on Parallel and Distributed Systems, Vol. 2, 2005, pp. 73–77.

[8] S. K. Kim and M. G. Chung, "More secure remote user authentication scheme," Comput. Commun., vol. 32, no. 6, pp. 1018–1021, 2009.

[9] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," Proc. Advances in Cryptology (LNCS 1666), 1999, pp. 388–397.

[10] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," IEEE Trans. Comput., vol. 51, no. 5, pp. 541–552, 2002.