# A modified user-friendly remote authentication scheme with smart cards

Yi-Hwa Chen[1], Jinn-Ke Jan[2]
[1]*Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan 402*
[2]*Institute of Computer Science, National Chung Hsing University,Taichung, Taiwan 402*
*Corresponding E-mail: jkjan@cs.nchu.edu.tw*

***Abstract****-Wu and Chieu proposed a user-friendly remote authentication scheme with smart cards. Their scheme allows the users to freely choose a variable-length password to achieve the aim of user friendliness. However, Liu et al. showed that it is insecure. In this paper, we provide another attack and propose an improved scheme to overcome the weaknesses.*

**Keywords:** Authentication, Smart Card, Password, Password guessing Attack

## 1. Introduction

A remote password authentication scheme is used for authenticating the legitimacy of the remote users over an insecure channel.

In 1981, Lamport [1] proposed a scheme with password table stored in authentication server (AS), which could prevent the replaying attack. However, the password table storing in system's storage is vulnerable to the stolen-verifier attack. Therefore, many researchers [2-4] have proposed a variety of schemes to overcome this problem.

Recently, using smart cards, Hwang and Li [5] proposed a remote user authentication scheme without password table. Soon, Sun [6] further proposed a more efficient and practical remote user authentication scheme with less communication and computation costs. However, both schemes exist a disadvantage that is the users cannot freely choose passwords themselves. Therefore, Wu and Chieu [7] proposed a new scheme to achieve the aim of user-friendliness which meaning is that their scheme allows the users to freely choose a variable-length password. However, Liu et al. [8] showed that their scheme is insecure since any adversary can easily forge a valid message to pass the authentication phase. In this paper, we propose another attack to extract the user's password.

In Section 2, a brief review of Wu and Chieu's scheme is given. Section 3 provides Liu et al.'s attack and our attack. In Section 4, we propose a modified scheme to overcome these flaws. Section 5 discusses the security of the modified scheme. Finally, a brief conclusion is given.

## 2. Brief Review of the Wu and Chieu's scheme

We first describe some parameters in this paper as follows:

$x$: the secret key of AS
$h(\ )$: one-way hash function
$P$: a large modulus prime number
$g$: a primitive element in $GF(P)$

Let $h(\ )$, $P$ and $g$ be public. Their scheme is composed of three phases: the registration, login and authentication phases.

In the registration phase, each new user $U_i$ should submit his identity $ID_i$ and a freely choosing password $PW_i$ to AS over a secure channel. After authenticating $U_i$'s identity, AS computes two values $A_i = h(ID_i, x)$ and $B_i = g^{A_i \cdot h(PW_i)} \bmod P$. AS then stores the message $\{ID_i, A_i, B_i, h(\ ), P, g\}$ to the smart card and sends the card to $U_i$ securely.

In the login phase, $U_i$ first attaches his smart card to the card reader, then inputs $ID_i$ and $PW_i'$ to the terminal. The smart card computes two integer $B_i' = g^{A_i \cdot h(PW_i')} \bmod P$ and $C_1 = h(T \oplus B_i)$, where $T$ is the current date and time of the input device. The terminal then sends the message $m = \{ID_i, B_i', C_1, T\}$ to AS.

In the authentication phase, upon receiving the message $m$ at time $T'$ from $U_i$, AS performs the following steps:

1. Check the validity of the format of $ID_i$. If it is invalid, then the request is rejected.
2. Check whether it is a reasonable time interval between $T$ and $T'$ in order to resist replay attack. If $(T' - T) \geq \Delta T$, where $\Delta T$ denotes a reasonable time interval for transmission delay.
3. Compute $C_1^* = h(T \oplus B_i')$ then check if the equation $C_1^* = C_1$ holds. If it is true, then the login request is accepted. Otherwise, the request will be rejected.

## 3. Some Attacks

### 3.1 Liu et al.'s attack

An adversary $E$ can first collect some identities with valid format by forging or intercepting method. Then, he forges a message $m' = (ID_i, B, C, T_t)$ to perform the impersonation attack, where $B$ is a value randomly chosen by $E$, and $C = h(B \oplus T_t)$ is computed by $E$ and $T_t$ is the time when the adversary sends the message $m'$ to AS for attacking. This attack will succeed obviously since the verification equation in step 3 of the authentication phase in Wu and Chieu's scheme holds.

The verification equation uses $B$ and $T_t$ to deduce $C^*$, then checks if the equation $C^* = C$ holds. However, the three values $\{B, T_t, C\}$ are all in the message $m'$. Therefore, anyone can randomly choose $B$ and $T_t$ to calculate a value of $C$ to pass the verification. That is the weak point in Wu and Chieu's scheme.

### 3.2 Our attack

Excepting the previous attack, Wu and Chieu's scheme is vulnerable to the offline password guessing attack. If any cardholder loses his smart card by accident, he must worry about this kind of attack since there is not any verifying mechanism in login phase. Therefore, an adversary who wants to impersonate the user $U_i$ can firstly collect the message $m = \{ID_i, B_i, C_1, T\}$ by eavesdropping from the channel whenever the user $U_i$ logs in. After obtaining the smart card by any condition, he can perform the following offline password guessing attack.

***A1)*** The adversary first attaches a smart card obtained by evil to the card reader, then inputs $ID_i$ and a randomly chosen password $PW_i'$ to the terminal.

***A2)*** The smart card computes two integers $B_i' = g^{A_i \cdot h(PW_i')} \bmod P$ and $C_1 = h(T \oplus B_i)$, then outputs a message $m' = \{ID_i, B_i', C_1, T\}$.

***A3)*** By comparing if $B_i$ of $m$ is equal to $B_i'$ of $m'$, the adversary can justify whether a chosen password is correct or not.

Thus, we provide an improved scheme to mend the previous weaknesses and disadvantages.

## 4. Our modified scheme

In this section, we describe a modified scheme as follows:

***I1).*** **Registration phase:**

After receiving $ID_i$ and $PW_i$ submitted from requester $U_i$, AS performs the following steps:

Step1: Compute $A_i = h(ID_i, x)$

Step2: Compute $B_i = g^{A_i \cdot h(h(PW_i) \oplus A_i)} \bmod P$

Step3: Issue a smart card containing $\{ID_i, A_i, B_i, h(), P, g\}$ to the requester $U_i$

***I2).*** **Login phase:**

User $U_i$ inserts his smart card and keys in his identity $ID_i$ and password $PW_i^*$ to the terminal. The smart card performs the following steps:

Step1: Compute $L = g^{h(h(PW_i^*) \oplus A_i)} \bmod P$

Step2: Check whether the equation $B_i = L^{A_i} \bmod P$ holds. If it is not, the login request stops.

Step3: Compute $C = h(T \oplus B_i)$

Step4: Send the message $M = (ID_i, L, C, T)$ to AS

***I3).*** **Authentication phase:**

Upon receiving $M$ from $U_i$, AS performs the following steps:

Step1: Check the validity of $ID_i$

Step2: Check whether $T$ is valid or not

Step3: Compute $A_i = h(ID_i, x)$ with its secret key $x$

Step4: Compute $C^* = h(T \oplus L^{A_i})$

Step5: Compare $C^*$ with $C$. If they are equal, the login request is accepted. Otherwise, it is rejected.

## 5. Security analyses of our scheme

The security of our modified scheme is based on one-way hash function, discrete logarithm problem (DLP) and the property of tamper-proof of smart card. We discuss some attacks in the following:

***S1).*** **Replay attack:**

Without changing $T$, the replay attack will fail in Step2 of the authentication phase.

***S2).*** **Forgery attack:**

Adversary may want to change $T$ into $T^*$ in order to make the equation $C = h(T^* \oplus L^{A_i})$ holds. However, he will face the difficulties of one-way hash function and DLP.

***S3).*** **Password guessing attack:**

Adversary may try to guess a correct password from $L$. Let $L = g^{h(h(PW_i^*) \oplus A_i)} \bmod P$ be able to prevent this attack since the input value of hash function in our scheme is changed into $h(PW_i^*) \oplus A_i$. However, $A_i$ is unknown to the adversary. In addition, the adversary must face a DLP problem if he wants to get the value $h(h(PW_i^*) \oplus A_i)$ on exponent part of $g$.

***S4).*** **Offline password guessing attack:**

By establishing a verification mechanism in Step2 of the login phase, adversary cannot make the offline password guessing attack as we provide in section 3.2. If the equation $B_i = g^{A_i \cdot h(h(PW_i) \oplus A_i)} \bmod P$ doesn't hold, the login request will stop. Therefore, any adversary who obtains the smart card will be useless if he doesn't know a correct password.

## 6. Conclusion

In this paper, a modified scheme is provided to overcome the various attacks and mend the original disadvantages of Wu and Chieu's scheme. The provided properties of original scheme are still retained in the modified scheme such as the user can freely choose his password and so on. In addition, the modified scheme is still secure even a legitimate user loses his smart card by accident. Since a verification mechanism is included into our scheme, the offline password guessing attack will not be successful anymore.

## References

[1] L. Lamport, "Password authentication with insecure communication," *Communications of ACM*, Vol. 24, pp. 770-772, 1981.

[2] H.Y. Chien, J.K. Jan, and Y.M. Tseng, "A modified remote login authentication scheme based on geometric approach," *The Journal of System and Software*, Vol. 55, pp. 287-290, 2001.

[3] G. Horng, "Password authentication without using password table," *Information Processing Letters*, Vol. 55, pp. 247-250, 1995.

[4] J.K. Jan, and Y.Y. Chen, "Paramita wisdom' password authentication scheme without verification tables," *The Journal of Systems and Software*, Vol. 42, pp. 45-57, 1998.

[5] M.S. Hwang, and L.H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transaction on Consumer Electronics*, Vol. 46, No. 1, pp. 28-30, February, 2000.

[6] H.M. Sun, "An efficient remote user authentication scheme using smart cards," *IEEE Transaction on Consumer Electronics*, Vol. 46, No. 4, pp. 958-961, November, 2000.

[7] S.T. Wu, and B.C. Chieu, "A user friendly remote authentication scheme with smart cards," *Computer & Security*, Vol. 22, No. 6, pp. 547-550, 2003

[8] C.Y. Liu, M.S. Hwang, J.W. Lo, and S.C. Lin, "Cryptanalysis of A user friendly remote authentication scheme with smart cards," *Information Security Conference*, pp. 256-259, 2004.