# Cryptanalysis of a DoS-resistant ID-based password authentication scheme using smart cards

He Debiao*, Chen Jianhua, Hu Jin

School of Mathematics and Statistics, Wuhan University, Wuhan, Hubei 430072, China

**Abstract*:*** Remote authentication is a method to authenticate remote users over insecure communication channel. Password-based authentication schemes have been widely deployed to verify the legitimacy of remote users. Very recently, Hwang et al. proposed a DoS-resistant ID-based password authentication scheme using smart cards. In the current work, we are concerned with the password security of the Hwang et al.'s scheme. We first show that their scheme is vulnerable to a password guessing attack in which an attacker exhaustively enumerates all possible passwords in an off-line manner to determine the correct one. We then figure out how to eliminate the security vulnerability of their scheme.

**Key words**: Authentication; Security; Cryptanalysis; Smart card; Attacks.

# 1. Introduction

Remote authentication is a method to authenticate remote users over insecure communication channel. Password-based authentication schemes have been widely deployed to verify the legitimacy of remote users. In 1981, Lamport [1] proposed a password-based authentication scheme using password tables to authenticate remote users over insecure network. Since then,

*Corresponding author.: Email: hedebiao@163.com, School of Mathematics and Statistics, Wuhan University, Wuhan, Hubei 430072, China

many schemes were proposed to improve security, efficiency and cost [2-6].

Recently, Hwang et al. [7] provided a defense mechanism to Kim et al.'s ID-based password authentication scheme [2], which is vulnerable to impersonation attacks and resource exhaustion attacks. They claimed that their scheme is not only accomplishes the mutual authentication and the session key establishment, but also is secure against password guessing attacks, message replay attacks et al. Unfortunately, we find that their scheme is still vulnerable to password guessing attacks attack. So their scheme is insecure for practical application.

The rest of the paper is organized as follows: Section 2 briefly reviews Hwang et al.'s scheme. Section 3 elaborates the cryptanalysis of their scheme. Section 3 elaborates countermeasure to eliminate the security vulnerability of their scheme. At the end, Section 5 concludes this paper.

## 2. Review of Hwang et al.'s scheme

The notations used throughout this paper are described as in the following.

- $U$ : a user.
- $ID_U, PW_U$ : $U$ 's identifier and password, respectively.
- $S$ : a remote server.
- $h(\cdot)$ : a secure hash function.
- $\oplus$ : bitwise XOR operation.
- $n$ : a large prime number.
- $g$ : a generator of $Z_n^*$.
- $SK$ : $S$ 's secret key.
- $v_S$ : a solutions of the puzzle, decided by $S$ .

- $N_S$ : the nonce generated by $S$ .
- $N_U$ : the nonce generated by $U$ .
- $sk_S$ : the secret key of $S$ , used for puzzle verification.
- $token_U$ : the message authentication code issued from $S$ to $U$ .
- $puzzle(p, x_1, x_2, \cdots, x_n)$ : Given $p, x_1, x_2, \cdots, x_n$, find $v$ such that $h(x_1, x_2, \cdots, x_n, v) = p$ .

Hwang et al.'s scheme involves three phases, the registration phase, the login phase and the verification phase, which can be described as in the following.

When the system is setup, $S$ generate a large prime number $n$ , $Z_n^*$'s generator $g$ . Then $S$ chooses a random number $SK$ as its secret key and a secure hash function $h(\cdot)$. At last, $S$ publishes $n$ , $g$ and $h(\cdot)$.

**Registration phas**e. In this phase, the user $U$ initially registers with the server $S$ .

1) $U$ chooses his $ID_U$ and $PW_U$ , and sends them over a secure communication channel to $S$ .
2) Upon receiving $ID_U$ and $PW_U$ , $S$ computes $S_U = ID_U^{SK}$ , $h_U = g^{PW_U \cdot SK}$ , $W_U = h(ID_U, SK)$ and generates smart card's identifier $CID_U$ .
3) $S$ stores the secure information $CID_U, S_U, h_U, W_U, n, g$ and $h(\cdot)$ into $U$ 's smart card.
4) Now $S$ finishes the registration procedure by delivering the completed smart card to $U$ .
5) Upon receiving the smart card, the user $U$ enrolls his/her fingerprint which is written to the smart card as a template by a fingerprint input device.

**Login phase**. In this phase, the user $U$ sends a login request message to the server $S$ whenever $U$ wants to access some resources upon $S$.

1) $U$ inserts his smart card into a smart card reader and then inputs his $ID_U$, $PW_U$ and fingerprint.

2) $U$ 's smart card verify the fingerprint. If the fingerprint is wrong, the smart reject the request.

3) $U$ 's smart card generates nonce $N_U$, and sends the message $M_1 = \{ID_U, CID_U, N_U\}$ to $S$.

4) Upon receiving the message $M_1$, $S$ checks $ID_U, CID_U, N_U$. If $N_U$ has beeb already used, then $S$ rejects the session. Otherwise, $S$ determines $v_S$ based on its loading, then generates nonce $N_S$, computes $p = h(ID_U, N_U, N_S, v_S)$ and $token_U = h(p, ID_U, N_U, N_S, v_S, sk_S)$. Then $S$ sends $M_2 = \{p, N_S, token_U\}$ to $U$.

5) Upon receiving the message $M_2$, $U$ 's smart card tries to seek out the solution $v_S'$ of $puzzle(p, ID_U, N_U, N_S)$ through a brute-force method. Then, $U$ 's smart card generates random numbers $r_U, q_U$, computes $X_U = g^{r_U \cdot PW_U} \bmod n$, $Y_U = S_U \cdot h_U^{r_U \cdot token_U} \bmod n$, $Z_U = W_U \oplus q_U$ and $T_U = h(X_U, Y_U, token_U, q_U)$. At last, $U$ 's smart card sends $M_3 = \{ID_U, X_U, Y_U, Z_U, T_U, v_S', N_U, N_S\}$ to $S$.

**Verification phase**. In this phase, the server S verifies the authenticity of the login message requested by the user U.

1) Upon receiving the message $M_3$, $S$ checks the value $N_S$. If $N_S$ is not fresh, $S$ stops the session. $S$ checks if $token_U$ equals $h(p, ID_U, N_U, N_S, v_S', sk_S)$. If not

$S$ stops the session.

2) $S$ extracts the random number $q_U' = Z_U \oplus h(ID_U, SK)$, and checks if $T_U$ equals $h(X_U, Y_U, token_U, q_U')$.

3) $S$ checks if the equation $Y_U^{SK^{-1}} \equiv ID_U \cdot X_U^{token_U}$ holds. If not $S$ stops the session. Otherwise, $S$ computes $M_4 = \{h(q_U')\}$ and sends it to $U$ 's smart card.

4) Upon receiving the message $M_4$, $U$ 's smart card checks if $h(q_U)$ equals received $h(q_U')$. If not, $U$ 's smart card stops the session.

# 3. Security analysis of Hwang et al.'s scheme

In password authentication schemes that the user is allowed to choose his password, the user tends to choose a password that can be easily remembered for his convenience. However, these easy-to-remember passwords are potentially vulnerable to password guessing attack, in which an adversary can try to guess the user's password and then verify his guess. In general, the password guessing attack can be classified into online password guessing attack and offline password guessing attack. The adversary tries to use guessed passwords iteratively to pass the verification of the server in an online manner in online password guessing attack. While in off-line password guessing attack, the adversary intercepts some password-related messages exchanged between the user and the server, and then iteratively guesses the user's password and verifies whether his guess is correct or not in an offline manner. Online password guessing attacks can be easily thwarted by limiting the number of continuous login attempts within a short period. In an offline password guessing attack, since there is no need for the server to participate in the verification, the server cannot easily notice the attack. While in password authentication scheme using smart cards, two

points should be noticed to resist this kind of attack. One is that the password should not be transmitted between the client and the server during the authentication; otherwise it has the risk of being intercepted and recovered. The other is that the sensitive data stored in smart cards should be well protected so that the password would not be leaked even if smart cards are lost and all the data inside are disclosed. Although Hwang et al. claim that their scheme is secure even when the client's smart card is lost [7], an off-line password guessing attack method will be given here as a counter example.

Suppose the client's smart card is lost, an attacker $A$ can read all the data, including $CID_U$, $S_U$, $h_U$, $W_U$, $n$, $g$, from the smart card via physically access to the storage medium [8, 9]. Sometimes, $A$ may get more than one smart card. In fact, $A$ may be a legal user, he/she has a legal smart card consequently. Then $A$ can get the data in two different smart cards. Suppose $A$ get the data $\{CID_i, S_i, h_i, W_i\}$ and $\{CID_j, S_j, h_j, W_j\}$ in two smart cards. Then $A$ can carry out the password guessing attack as follows.

1) $A$ selects two passwords $PW_i'$ and $PW_j'$ from a uniformly distributed dictionary $D$.

2) $A$ computes $PW_i'^{-1}$ and $PW_j'^{-1}$ such that $PW_i' \cdot PW_i'^{-1} \equiv 1 \bmod n$ and $PW_j' \cdot PW_j'^{-1} \equiv 1 \bmod n$.

3) $A$ computes $t_i = h_i^{PW_i'^{-1}}$ and $t_j = h_j^{PW_j'^{-1}}$.

4) $A$ then verify the correctness of $PW_i'$ and $PW_j'$ by checking that $t_i$ equals $t_j$. If $t_i$ equals $t_j$, then $A$ find the correct passwords $PW_i$ and $PW_j$.

5) $A$ repeats steps 1, 2, 3 and 4 of until the correct password if found.

If $A$ is the legal user $i$ (or $j$), he/she just needs to guess the password $PW_j$ (or $PW_i$),

and get the correct value much easier. In addition, the attack can be used to other schemes [2, 10], which like Hwang et al.'s scheme.

# 4. Countermeasure

The vulnerability of Hwang et al.'s scheme to the password guessing attack above is attributed to the fact that the secret key $SK$ is used directly as the exponent of $g^{PW_U}$ in the computations of $h_U = g^{PW_U \cdot SK}$. This fact gives the attacker the idea of guessing the password and deriving the value $g^{SK}$. Fortunately, it appears that a slight modification of how $h_U$ and $S_U$ are computed can prevent the attack. We recommend the following changes to Hwang et al.'s scheme:

- Let $S_U = ID_U^{h(ID_U \oplus SK)}$, $h_U = g^{PW_U \cdot h(ID_U \oplus SK)}$, and $W_U = h(ID_U, SK)$ in registration phase.
- Accordingly, the way $S$ checks if the equation $Y_U^{h(ID_U \oplus SK)^{-1}} \equiv ID_U \cdot X_U^{token_U}$ holds.

With this modification applied, the value of $h_U$ is no longer useful in verifying password guesses.

# 5. Conclusion

In [7], Hwang et al. proposed a password authentication scheme using smart cards and demonstrated its immunity against various attacks. However, after review of their scheme and analysis of its security, we find their scheme is vulnerable to the password guessing attack. The analyses show that the scheme is insecure for practical application.

# Reference

[1]. Lamport L., Password authentication with insecure communication, Communications of ACM 24 (1981) 770 – 772.

[2]. Kim, H.S., Lee, S.W., Yoo, K.Y.. Id-based password authentication scheme using smart cards and fingerprints. ACM SIGOPS Operating Systems Review 37 (4), (2003) 32 – 41.

[3]. Ku, W.C., Chang, S.T., Chiang, M.H.. Further cryptanalysis of fingerprint-based remote user authentication scheme using smartcards. Electronics Letters 41 (5), (2005) 240 – 241.

[4]. Mangipudi, K.V., Katti, R.S.. A hash-based strong password authentication protocol with user anonymity. International Journal of Network Security 2 (3), (2006) 205 – 209.

[5]. Kumar, M.. An enhanced remote user authentication scheme with smart card. International Journal of Network Security 10 (3), (2010) 175 – 184.

[6]. Yong, Z., Jianfeng, M., Moon, S., An improvement on a three-party password based key exchange protocol using weil pairing. International Journal of Network Security 10 (3), (2010) 188 – 193.

[7]. Hwang M.-S., Chong S.-K., Chen T.-Y., DoS-resistant ID-based password authentication scheme using smart cards, The Journal of Systems and Software 83 (2010) 163 – 172.

[8]. P. Kocher, J. Jaffe, B. Jun, Differential power analysis, Proc. Advances in Cryptology (CRYPTO'99), (1999) 388 – 397.

[9]. T.S. Messerges, E.A. Dabbish, R.H. Sloan, Examining smart card security under the threat of power analysis attacks, IEEE Transactions on Computers 51 (5) (2002) 541–552.

[10]. Kim, K. W., Jeon J. C., and Yoo K. Y.., An Improvement on Yang et al.’ s Password Authentication Schemes, Applied Mathematics and Computation, 170(1) (2005) 207 – 215.