Security Analysis and Improvement of Authentication Scheme Based on a One-way Hash Function and Diffie-Hellman Key Exchange Using Smart Card

Kang-seok CHAE, Dai-hoon KIM, Jae-duck CHOI, Souh-wan JUNG
(*School of Electronic Engineering*, *Soongsil University*, *Seoul* 156-743, *Korea*)

Abstract – A new authentication scheme based on a one-way hash function and Diffie-Hellman key exchange using smart card was proposed by Yoon et al. in 2005. They claimed that the proposed protocol is against password guessing attack. In this paper, the author demonstrate that Yoon's scheme is vulnerable to the off-line password guessing attack by using a stolen smart card and the DoS attack by computational load at the remote system. An improvement of Yoon's scheme to resist the above attacks is also proposed.

Key words – *authentication*; *guessing attack*; *Diffie-Hellman*; *smart card*

Manuscript Number: 1674-8042(2010)04-0360-04

dio: 10.3969/j.issn.1674-8042.2010.04.13

1 Introduction

A number of studies for smart card authentication without storing password verification tables in the remote system have been proposed. In 2000, Hwang and Li proposed a new remote user authentication scheme that does not store the password or verification tables in the remote system[1]. Sun proposed an efficient and practical remote user authentication scheme to reduce communication and computation costs using a hash function[2]. Compared with Hwang's scheme requiring exponent operations, Sun's scheme is much more practical and efficient. Wu and Chieu proposed a modified version of Sun's scheme that required the assignment of un-human lengthy password[3-4]. However, Ku et al.[5] and Yoon et al.[6] showed that Wu's scheme has security flaws: an off-line password guessing attack, an impersonation attack using stolen smart card, forgery attack, and privileged insider's attack. In addition, Sun et al.[7] showed that Wu's scheme is not secure under the smart card loss assumption.

These schemes do not satisfy some requirements[8] for password authentication using smart card: mutual authentication and session key agreement. Recently, since computing resources have grown extremely, several authentication schemes based on Diffie-Hellman[9] providing mutual authentication and session key agreement have been proposed in Ref.[6], Ref.[8], and Ref.[10]. In 2005, Yoon et al. proposed a new authentication scheme based on a one-way hash function and Diffie-Hellman key exchange to provide mutual authentication between the user and the remote system[6]. In 2006, Liao et al.[8] and Liaw et al.[10] proposed a user authentication scheme using Diffie-Hellman key exchange protocol. Unfortunately, we point out that Yoon's scheme is vulnerable to the off-line password guessing attack by the use of a stolen smart card and the DoS attack by computational load at the remote system. The attacker can obtain sensitive information in smart card by power analysis attack[11].

In this paper, we will first review Yoon's scheme, and then demonstrate its security flaws. Furthermore, we propose our improved scheme of Yoon's scheme and analyze the security of our improved scheme.

2 Review of Yoon-Yoo's scheme

In this section, we briefly review Yoon's scheme. Like other authentication schemes using smart card, there are three phases: a registration phase, a login phase, and a session key agreement phase.

2.1 Registration phase

The user U_i submits his identifier ID_i and chosen password PW_i to the remote system. These private data must be sent off-line or over a secure channel. Upon receiving the registration request, the remote system performs the following steps:

Setp R1

Compute $A_i = h(ID_i, x)$, where $h()$ is a one-way hash function.

* **Received**: 2010-09-21
Corresponding author: Kang-seok CHAE(chaekhan@cns.ssu.ac.kr)

Step R2

Compute $B_i = A_i \oplus PW_i$, where $\oplus$ is a bit-wise XOR operation.

Step R3

Issue the smart card with secure information $\{ID_i, B_i, h(), p, g\}$ to the user U_i.

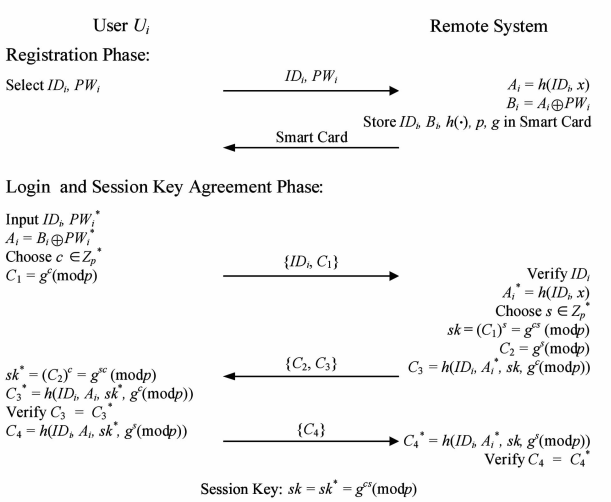

Fig.1 Yoon-Yoo's authentication scheme

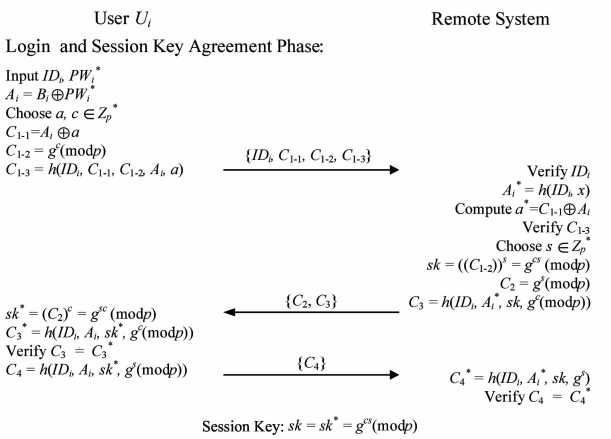

Fig.2 Proposed authentication scheme

2.2 Login phase

When the user U_i wants to log on the remote system, the user attaches the smart card to the card reader and enters his identity ID_i and password PW_i. Then the smart card performs the following steps:

Step L1

Extract $A_i = h(ID_i, x)$ from the smart card by computing $B_i \oplus PW_i^*$.

Step L2

Choose a fresh random value $c \in Z_p^*$ and compute $C_1 = g^c \pmod p$.

Step L3

Send a message $m = \{ID_i, C_1\}$ to the remote system.

2.3 Session key agreement phase

The remote system and the smart card execute the following steps for mutual authentication and session key agreement between the user U_i and the remote system.

Step S1

The remote system computes $A_i^* = h(ID_i, x)$, chooses a fresh random value $s \in Z_p^*$, and then computes $sk = (C_1)^s = g^{cs} \pmod p$, $C_2 = g^s \pmod p$, and $C_3 = h(ID_i, A_i^*, sk, g^c \pmod p)$. The remote system sends the message (C_2, C_3) to the smart card.

Step S2

The smart card computes $sk^* = (C_2)^c = g^{sc} \pmod p$ and $C_3^* = h(ID_i, A_i, sk^*, g^c \pmod p))$ and compares C_3 with C_3^*. Finally, the smart card computes $C_4 = h(ID_i, A_i, sk^*, g^s \pmod p))$ and sends this authentication token to the remote system.

Step S3

The remote system computes $C_4^* = h(ID_i, A_i^*, sk, g^s \pmod p))$ and compares C_4 with C_4^*.

3 Cryptanalysis of Yoon-Yoo's scheme

This section demonstrates that Yoon-Yoo's scheme is vulnerable to two attacks: an off-line password guessing attack by the use of a stolen smart card and a DoS attack by computational load at the remote system. We omit $(\bmod p)$ to simply represent.

3.1 Off-line Password Guessing Attack

Since user's password is the value of low entropy, authentication schemes based on password should be against various password guessing attacks. Unfortunately, Yoon's scheme is vulnerable to off-line password guessing attack by using stolen smart card. Suppose that an attacker has stolen a smart card with information $\{ID_i, B_i, h(\cdot), p, g\}$ and known these values. This sensitive information in smart card can be leaked by power analysis attack[11]. In addition, the attacker already has obtained the user ID_i during $U_i's$ previous login process from an open network. In order to obtain the legitimate password PW_i, the attacker makes a temporary password PW_i^{attacker}, and then performs step L1: $A_i^{\text{attacker}} = B_i \oplus PW_i^{\text{attacker}}$ and $C_1 = g^c$, where c is a new random number generated by the attacker. The remote system may perform step L2: $A_i^* = h(ID_i, x)$, $sk = (C_1)^s = g^{cs}$, $C_2 = g^s$, and $C_3 = h(ID_i, A_i^*, sk, g^c)$, where s is a new random number generated by the remote system. Note that the remote system does not verify the attacker having the temporary password PW_i^{attacker} since the remote system only receives ID_i and C_1. When the attacker receives the C_2 and C_3 from the remote system, the attacker can guess the legitimate password

PW_i by the following steps.

Step OA1

The attacker computes $sk^* = (C_2)^c = g^{sc}$, and then computes $C_3^{\text{attacker}} = h(ID_i, A_i^{\text{attacker}}, sk^*, g^c)$.

Step OA2

If the computed value C_3^{attacker} is the same as C_3, the password PW_i^{attacker} is the legitimate password PW_i of the legitimate user. Otherwise, the attacker makes other password $PW_i^{\text{attacker}'}$, computes $A_i^{\text{attacker}'} = B_i \oplus PW_i^{\text{attacker}'}$, and compares $C_3^{\text{attacker}'}$ with C_3. The attacker repeatedly performs it until $C_3^{\text{attacker}'} = C_3$.

This off-line password guessing attack is possible by following reasons. A attacker who picks up a lost smart card can know $B_i, h(), p$, and g by power analysis attacks. Also, the attacker can compute $A_i^{\text{attacker}} = B_i \oplus PW_i^{\text{attacker}}$. Therefore, the attacker who does not know the only legitimate password PW_i can guess the PW_i.

3.2 Denial of service attack

DoS attack for exhausting server's resource has become a major security threat. Remote systems should protect themselves from malicious users who will try to exhaust their computing power. Yoon's scheme based on Diffie-Hellman requires two exponent operations at the remote system. DoS attacks considered on this scheme are CPU exhaustion attacks when the remote system receives the message $\{ID_i, C_1\}$ from the attackers. This DoS attack can be done as follows.

Step DA1

Collect many ID_is from on open network and generate many fresh random number $c \in Z_p^*$.

Step DA2

Make login request messages (ID_i, C_1) s, and then send messages to the remote system.

Step DA3

The remote system performs exponent operations for login messages (ID_i, C_1) s: $sk = (C_1)^s = g^{cs}$ and $C_2 = g^s$, and then responses $\{C_2, C_3\}$ s for all requests. The remote system may have heavy computational load.

Step DA4

The attackers ignore response messages.

In Yoon's scheme, the weak point is that the remote system performs exponent operations after the remote system verifies the only user ID_i. The remote system performs meaningless computation exhausting CPU resource. However, these security flaws can be modified at the next section.

4 The improvement of Yoon-Yoo´s scheme

This section proposes improvement of Yoon's scheme so that they can withstand the above mentioned attacks. We modify Yoon's scheme as follows.

In the registration phase, the operations are same as the registration phase of Yoon's scheme.

In the login phase, the user chooses two fresh random values $a, c \in Z_p^*$, computes $C_{1\text{-}1} = A_i \oplus a$ and $C_{1\text{-}2} = g^c$, makes the message $C_{1\text{-}3} = h(ID_i, C_{1\text{-}1}, C_{1\text{-}2}, A_i, a)$, and then sends $\{ID_i, C_{1\text{-}1}, C_{1\text{-}2}, C_{1\text{-}3}\}$ to the remote system.

In the session key agreement phase, the remote system verifies ID_i, computes $A_i^* = h(ID_i, x)$ and $a^* = C_{1\text{-}1} \oplus A_i^*$, and then verifies the $C_{1\text{-}3}$ containing the user password information. If the value $C_{1\text{-}3}$ is incorrect, the remote system rejects the login request. Otherwise, the remote system computes $sk = (C_{1\text{-}2})^s = g^{cs}, C_2 = g^s$, and $C_3 = h(ID_i, A_i^*, sk, g^c)$. The remote system sends a message $\{C_2, C_3\}$ to the smart card. Upon receiving the message $\{C_2, C_3\}$, the smart card computes $sk^* = (C_2)^c = g^{sc}$. In order to verify the remote system, the smart card computes C_3^* and compares C_3^* with C_3. The other operations are same as the session key agreement phase of the original scheme.

Also, our improved scheme satisfies a total of four exponent operations that is same as the exponent computation costs of Yoon et al.´s scheme.

5 Security analysis of our improved scheme

Here, we analyze the security of our improved scheme: the off-line password guessing attack and the DoS attack.

5.1 Off-line password guessing attack

5.1.1 Under an adversary without U_i´s smart card

The attacker who does not have U_i´s smart card cannot guess the legitimate password PW_i since the values in the login message $\{ID_i, C_{1\text{-}1}, C_{1\text{-}2}, C_{1\text{-}3}\}$ are all independent of PW_i. Although the attacker exactly guesses and enuers the legitimate password, the attacker cannot judge whether the password is right or wrong due to the unknown value B_i stored in the smart card and a sandom value a. In case of knowing all messages in login and session key agreement phase, the attacker is not feasible to guess the password PW_i because the long term key x and a discrete logarithm problem.

5.1.2 Under an adversary with U_i´s smart card

In our improved scheme, it is impossible for an attacker to guess the legitimate password PW_i by receiving the value C_2 and C_3 from the remote system. The attacker who knows B_i from the smart card repeatedly wants to compute $A_i^{*\,\text{attacker}} = B_i \oplus PW_i^{*\,\text{attacker}}$ and compares C_3 with $C_3^{*\,\text{attacker}}$. However, our improved scheme rejects the login message $\{ID_i, C_{1\text{-}1}, C_{1\text{-}2}, C_{1\text{-}3}\}$ if the remote system fails to

verify the $C_{1\text{-}3}$. Therefore, the attacker is not able to guess the legitimate password PW_i without getting the C_2, and C_3.

Although the attacker obtains the $C_{1\text{-}1}, C_{1\text{-}2}, C_{1\text{-}3}$, C_2, and C_3 from the previous session and has user's smart card, the attacker cannot derive PW_i because x is the long secret key, a is a random value, and c in the C_1 is a private key in Diffie-Hellman algorithm.

5.2 Denial of service attack

Our improved scheme prevents DoS attack by computational load at the remote system. Upon receiving the login request message $\{ID_i, C_{1\text{-}1}^{\text{attacker}}, C_{1\text{-}2}, C_{1\text{-}3}^{\text{attacker}}\}$ generated using a false password PW_i^{attacker} by the attacker, the remote system should fail to verify $C_{1\text{-}3}^{\text{attacker}}$. The remote system performs the session key agreement phase no longer. Therefore, the remote system should be against DoS attack by checking and dropping malicious requests.

6 Conclusion

In this paper, we demonstrated that Yoon's scheme is vulnerable to the off-line password guessing attack and the DoS attack. An improved scheme is proposed to resist these security flaws. Our improved scheme is secure against these attacks and the same as the exponent computation costs of Yoon's scheme.

References

[1] M. S. Hwang, L. H Li, 2000. A new remote user authentication scheme using smart cards. *IEEE Trans. Consum. Electron.*,46(1): 28-30.

[2] H. M. Sun, 2000. An efficient remote user authentication scheme using smart cards. *IEEE Trans. Consum. Electron.*, 46(4): 958-961.

[3] S. T. Wu, B. C. Chieu, 2003. A user friendly remote authentication with smart cards. *Comput. Secur.*, 22(6): 547-550.

[4] S. T. Wu, B. C. Chieu, 2004. A note on a user friendly remote authentication scheme with smart cards. *IEICE Trans. Fund.*, E87-A(8): 2180-2181.

[5] W. C. Ku, H. M. Chuang, M. J. Tsaur, 2005. Vulnerabilities of Wu-Chieu's improved password authentication scheme using smart cards. *IEICE Trans. Fundamentals*, E88-A(11): 3241-3243.

[6] E. J. Yoon, K. Y. Yoo, 2005. New authentication scheme based on a one-way hash function and diffie-hellman key exchange. CANS 2005, LNCS, p. 147-160.

[7] D. Z. Sun, J. D. Zhong, Y. Sun, 2005. Weakness and improvement of Wang-Li-Tie's user-friendly remote authentication scheme. *Appl. Math. Comput.*, 170: 1185-1193.

[8] I. E. Liao, C. C. Lee, M. S. Hwang, 2006. A password authentication scheme over insecure networks. *J. Comput. Syst. Sci.*, 72(4): 727-740.

[9] W. Diffie, M. Hellman, 1976. New directions in cryptography. *IEEE Trans. Inf. Theory*, 22(6): 644-654.

[10] H. T. Liaw, J. F. Lin, W. C. Wu, 2006. An efficient and complete remote user authentication scheme using smart cards. *Math. Comput. Model.*, 44(1-2): 223-228.

[11] T. S. Messerges, E. A. Dabbish, R. H. Sloan, 2002. Examining smart-card security under the threat of power analysis attacks. *IEEE Trans. Commun.*, 51(5): 541-552.