一個植基於智慧卡的遠端使用者認證系統之安全分析

Cryptanalysis of A Remote User Authentication Scheme Based on Smart Cards

洪國寶* 劉兆樑** 周伯錕***

Gwoboa Horng Chao-Liang Liu Po-Kun Chou

國立中興大學 資訊科學研究所

Institute of Computer Science, National Chung Hsing University

E-mail : {gbhorng*, s9056001**, s9056022***}@cs.nchu.edu.tw

摘要

在這篇文章中，我們指出 Lee 等人的遠端認證系統中存有潛在的問題。明確地說，一個惡意的使用者可以使用自己的帳號及密碼，產生出系統未曾核准的帳號及密碼，並以此潛入系統而不被發現。

關鍵詞： 安全分析、密碼認證、遠端登入及智慧卡

Abstract

In this paper, we point out that there is a potential weakness in the remote user authentication scheme proposed by Lee, Ryu and Yoo. We show that a legitimate user can produce valid login messages using a pair of identification and password that are not issued by the server.

Keywords: cryptanalysis, password authentication, remote login and smart card

1. Introduction

Smart cards are often used in non-interactive remote user authentication schemes where the remote servers do not maintain password tables [2, 5, 7, 8]. Recently, Hwang and Li [4] constructed a remote user authentication scheme based on ElGamal's public key cryptosystem [3]. However, their scheme has a potential weakness [1], where a legitimate user can easily construct other pairs of (ID_f, PW_f), which can be accepted by the system. In other words, legitimate users might provide other illegitimate users with the right to access resources of the remote system.

In 2002, Lee et al. [6] proposed a fingerprint-based scheme, where the remote system uses two secret keys. They claimed to have improved the weakness in [4]. In this letter, we bring up a special trick to forge the login message, which can use n valid login messages to generate a $O(n^2)$ candidate list of fake ID. If n is big enough, then the animus user can choose valid ID form the list, which satisfies the ID format. That is, Lee et al.'s improved scheme is still vulnerable to the ID forge attack as the system without strict ID format.

2. Brief description of Lee et al.'s scheme

The scheme is divided into three phases, the registration phase, the login phase, and the authentication phase.

In the registration phase, a user U_i will submit his identity ID_i to the system for registration. The system will then utilize ID_i to calculate user's password PW_i as bellow:

$$ID_i' = (ID_i)^{SK_1} \mod p, \tag{2.1}$$
$$PW_i = (ID_i')^{SK_2} \mod p. \tag{2.2}$$

Where SK_1 and SK_2 are secret keys of the system and p is a large prime. Afterward, the system will deliver PW_i to U_i through secure channel. Furthermore, the system will store (f, p) in the smart card, where f is a one-way function. Finally, the system will issue this card to U_i.

During the login phase, the user U_i must attaches smart card to the terminal, keys in his

ID_i and PW_i, and imprints his fingerprint on the fingerprint device. Afterward, the smart card will perform the following steps:

1. Generate a random number r by making use of co-ordinates of minutia of input fingerprint.
2. Compute $C_1 = (ID_i')^r \bmod p$. (2.3)
3. Compute $t = f(T \oplus PW_i) \bmod (p-1)$ (2.4)
   T is the current time of the input device and $\oplus$ denotes an exclusive-or operation.
4. Compute $M = (ID_i')^t \bmod p$. (2.5)
5. Compute $C_2 = M(PW_i)^r \bmod p$. (2.6)
6. Send the request message $C = (ID_i, C_1, C_2, T)$ to the remote system.

In the authentication phase, if the system receives the authentication message C at time T'. It will perform the following three operations:

1. Test the validity of ID_i. If the format of ID_i is incorrect, the system will reject U_i's login request.
2. Check to see if $T'-T \geq \Delta T$. If it is true, then the system will reject U_i's login request, where ΔT is the legal transmission delay time.
3. Check to see if
   $C_2(C_1^{SK2})^{-1} \bmod P = (ID_i^{SK1})^{f(T \oplus PW_i)}$. (2.7)
   If it is true, then the system will accept U_i's login request, else the system will reject U_i's login request.

3. Cryptanalysis

Similar to the Chan-Cheng's attack, we have found a potential weakness in Lee et al.'s scheme. An attacker U_i can generate the login message C_f which can be accepted by the remote system without using the smart card. We will construct C_f by the following steps.

1. The animus user U_i generates n different legitimate login messages from her/his smart card, and put these login messages in a set LM.
2. U_i acquires two legitimate login messages C and C' from LM, where $C = (ID_i, C_1, C_2, T)$ and $C' = (ID_i, C_1', C_2', T')$.
3. U_i computes t and t' by the public elements (f, p) and her/his password PW_i.

$$t = f(T \oplus PW_i) \quad \bmod (p-1), \quad (3.1)$$
$$t' = f(T' \oplus PW_i) \quad \bmod (p-1). \quad (3.2)$$

4. U_i computes

$$ID_f = (ID_i)^{(t-t')} \quad \bmod p. \quad (3.3)$$
$$\text{or } ID_f = (ID_i)^{(t+t')} \quad \bmod p \quad (3.3')$$

5. If ID_f does not satisfy the ID format of this system than go to step *2*.

(We describe it in the subtraction operator *(t-t')* only to simplify the procedure.)

6. U_i computes

$$PW_f = (PW_i)^{(t-t')} \quad \bmod p, \quad (3.4)$$

$$\alpha = C_1(C_1')^{-1} \quad \bmod p, \quad (3.5)$$

$$\text{and } \beta = C_2(C_2')^{-1} \quad \bmod p. \quad (3.6)$$

From now on, U_i can impersonate another user U_f at time T_f by sending the forge login message $C_f = (ID_f, f_1, f_2, T_f)$ to the remote system, where t_f, f_1, and f_2 are calculated by the following:

$$t_f = f(T_f \oplus PW_f) \quad \bmod (p-1), \quad (3.7)$$

$$f_1 = \alpha^{tf} \quad \bmod p, \quad (3.8)$$

$$\text{and} \quad f_2 = \beta^{tf} \quad \bmod p. \quad (3.9)$$

Now, we show that the login message $C_f(ID_f, f_1, f_2, T_f)$ can be accepted by the remote system.

Since

$$PW_i^r = (ID_i^{SK1 * SK2})^r = C_1^{SK2} \quad \bmod p, \quad (3.10)$$

$$PW_i^{r'} = (ID_i^{SK1 * SK2})^{r'} = C_1'^{SK2} \quad \bmod p, \quad (3.11)$$

$$\begin{aligned} PW_f &= (PW_i)^{(t-t')} \\ &= (ID_i^{SK1 * SK2})^{(t-t')} \\ &= (ID_f)^{SK1 * SK2} \quad \bmod p, \end{aligned} \quad (3.12)$$

$$\alpha = C_1(C_1')^{-1} = (ID_i')^{(r-r')} \quad \bmod p, \quad (3.13)$$

$$\begin{aligned} \beta &= C_2(C_2')^{-1} \\ &= (ID_i')^{(t-t')} * (PW_i)^{(r-r')} \\ &= (ID_i^{SK1})^{(t-t')} * (ID_i')^{SK2 * (r-r')} \\ &= (ID_i^{SK1})^{(t-t')} * \alpha^{SK2} \quad \bmod p. \end{aligned} \quad (3.14)$$

Moreover,

$$f_2 = \beta^{tf} = [(ID_i^{SK1})^{(t-t')} * \alpha^{SK2}]^{tf}, \quad (3.15)$$

and

$$(f_1^{SK2})^{-1} = [\alpha^{tf}]^{-SK2} = [\alpha^{-SK2}]^{tf} \quad \bmod p. \quad (3.16)$$

Therefore,

$$\begin{aligned} f_2 * (f_1^{SK2})^{-1} &= [(ID_i^{SK1})^{(t-t')} * \alpha^{SK2}]^{tf} * [\alpha^{-SK2}]^{tf} \\ &= (ID_i^{SK1})^{(t-t')tf} \\ &= (ID_f^{SK1})^{f(Tf \oplus PWf)} \quad \bmod p. \end{aligned} \quad (3.17)$$

If the attacker has n different valid login messages, then he has $2(n^2-n)$'s chances to get a valid identities.

4. Concluding Remarks

In this letter, we have shown a potential weakness of Lee et al.'s scheme. More precisely, an attacker can produce valid login messages using forged (ID_f, PW_f) if the format of ID_f is correct. Similarly, the attack of Chan and Cheng to Hwang-Li can succeed only if they can produce correct *ID* format. Therefore, checking the correctness of the *ID* format is very important in these schemes.

Acknowledgement

This research was supported by the Communication Software Technology project of Institute for Information Industry and sponsored by MOEA, R.O.C

5. References

[1] C. K. Chan and L. M. Cheng "Cryptanalysis of a remote user authentication scheme using smart card," *IEEE Trans. Consum. Electron.*, 2000, 46, pp. 992-993

[2] C. C. Chang and S. J. Hwang, "Using Smart Cards to Authentication Remote Passwords," *Computer Mathematics with Applications*, vol. 26, no. 7, pp. 19-27, 1993.

[3] T. ElGamal "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, 1985, 31, pp. 469-472

[4] M. S. Hwang and L. H. Li "A new remote user authentication scheme using smart cards," *IEEE Trans. Consum. Electron.*, 2000, 46, pp. 28-30

[5] T. Hwang, Y. Chen and C. S. Laih, 1990, "Non-Interactive Password Authentication without Password Tables," *1990 IEEE Region 10 Conference on Computer and Communication Systems*, Hong Kong, pp. 429-431, September 1990.

[6] J. K. Lee, S. R. Ryu and K. Y. Yoo "Fingerprint-based remote user authentication scheme using smart cards," *Electron. Lett.*, 2002, 38, (12), pp. 554-555

[7] S. J. Wang and J. F. Chang, 1996, "Smart Card Based Secure Password Authentication Scheme," *Computers and Security*, vol. 15, no. 3, pp. 231-237, 1996.

[8] W. H. Yang and S. P. Shieh, 1999, "Password Authentication Schemes with Smart Cards," *Computers and Security*, vol. 18, no. 8, pp. 727-733, 1999.