Cryptanalysis of a timestamp-based password authentication scheme [1]

Lizhen Yang [a] Kefei Chen [a]

[a] *Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200030, P.R.China*

Abstract

Recently, J.-J. Shen, C.-W. Lin and M.-S. Hwang (Computers & Security, Vol 22, No 7, pp 591-595, 2003) proposed a modified Yang-Shieh scheme to enhance security. They claimed that their modified scheme can withstand the forged login attack and also provide a mutual authentication method to prevent the forged server attack. In this paper, we show that the Shen-Lin-Hwang scheme cannot resist the forged login attack either. The intruder is able to forge a valid forge request of a legitimate user U_i and then successfully impersonate him by intercepting a login request sent by U_i and registering a smart card.

Key words: Cryptanalysis, authentication, cryptography, password, smart card

1 Introduction

Password Authentication was proposed by L.Lamport [10] in 1981, and then developed by many authors since, such as [1] [2] [4] [5] [6] [7] [8]. In 2002, Hwang and Li [5] proposed a new remote user authentication scheme using a smart card based on ElGamals cryptosystem. However, this scheme has a drawback: the users cannot freely choose their passwords. Then Yang and Shieh [8] presented a timestamp-based password authentication that can allow the user freely choose their passwords and the remote server does not need to store the passwords or verification tables for authenticating the users. But their scheme can suffer the forged login attack [1], that is an intruder could

Email addresses: yang-lz@cs.sjtu.edu.cn (Lizhen Yang), chen-kf@cs.sjtu.edu.cn (Kefei Chen).

[1] This work has been supported by NFSE under grants 90104005 and Nation 863 program of China under grants 2001AA144060.

impersonate the legitimate users to login and accesses the remote server on their scheme. In 2002, Fan, Li and Zhu [3] also showed that Yang-Shieh scheme could not withstand the forge login attack and proposed a slight modification to resist this attack. However, the Fan-Li-Zhu scheme is inefficient and impracticality because it limits the user ID_i with a strict form. The length of ID_i should be 1024 bits at least in the Fan-Li-Zhu scheme. So in 2003, Shen, Lin and Hwang [9] proposed a modified Yang-Shieh scheme which has no striction on the form of the user ID_i. They also claimed that their enhance scheme withstands the forged login attack and also provides a mutual authentication method to prevent the forged server attack. In this paper, we show that the Shen-Lin-Hwang scheme cannot resist the forged login attack either. The intruder is able to forge a valid forge request of a legitimate user U_i and then successfully impersonate him by intercepting a login request sent by U_i and registering a smart card.

2 Review of the Shen-Lin-Hwang Scheme

In the Shen-Lin-Hwang scheme, each new user should submit his identity to the key information center (KIC) in the registration phase for registration. The KIC will issue a smart card for the new user. In the login phase, a user attaches his smart card to the input device and keys in his identifier ID_i and password PW_i. Then the device sends a login request message to the remote server. In the authentication phase, the remote server verifies the correctness of the submitted message and decides whether accept the login request or not. If the remote server accepts the login request, then sends a authentication message to the user. The user checks the correctness of the authentication message to decide whether login in the remote server or break the connect.

Parameters in the system: p and q are two large prime integers which are only known by the KIC, $n = pq$. e is the public key of the PIC which is an prime number chosen random and is relative prime to $(p-1)(q-1)$, the corresponding secret key d is an integer which satisfies $ed \equiv 1 \pmod{(p-1)(q-1)}$. g is an integer that is a primitive element in both $GF(p)$ and $GF(q)$. Moreover, g is public. $f(\cdot)$ is a one-way hash function.

Registration Phase: The User U_i submits his identity ID_i and a password to the KIC by a security method, then the KIC computes:

$$\begin{aligned} S_i &= ID_i^d \pmod{n} \\ h_i &= g^{PW_i \cdot d} \pmod{n} \\ CID_i &= f(ID_i \oplus d) \end{aligned} \tag{1}$$

Next, KIC stores $(n, e, g, ID_i, CID_i, S_i, h_i)$ into the smart card and sends it to U_i.

Login Phase: User U_i chooses a random integer r_i and computes:

$$X_i = g^{r_i \cdot PW_i}$$
$$Y_i = S_i \cdot h_i^{r_i \cdot f(CID_i, T)} \pmod{n}$$

where T is the current date and time. Next, U_i sends the login request $M = (ID_i, CID_i, X_i, Y_i, n, e, g, T)$ to the sever.

Authentication Phase: When the sever receives the login message sent from U_i, it implements the following steps

Step 1: Check the valid of ID_i, if it is invalid then reject the login request.
Step 2: Check the valid of T. If $T' - T \geq \triangle T$ then reject the login request, where T' is the current date and time of the server and $\triangle T$ is the expected legitimate time interval for transmission delay.
Step 3: Compute $CID_i' = h(ID_i \oplus d)$. If $CID_i' \neq CID_i$, then reject the login request.
Step 4: If the equation

$$Y_i^e \equiv ID_i \cdot X_i^{f(ID_i, T)} \pmod{n} \tag{2}$$

is not hold then reject the login request, otherwise accept the login request and send a message

$$M' = (R = (f(CID_i, T_2))^d \bmod n, T_2)$$

to the user U_i, where T_2 is the current date and time of the sever.

When U_i receives the message sent from the server, he checks

$$R^e = ? f(CID_i, T_2).$$

If it does not hold, U_i then rejects the remote server and breaks the connection.

3 Cryptanalysis of the Shen-Lin-Hwang Scheme

In this section, we will show that an intruder can forge a login request of a legitimate user U_i and then impersonate him by intercepting a login request sent by U_i and registering a legitimage smart card.

Suppose an intruder want to impersonate a legimate user U_i with identity ID_i. He first intercepts a login request $(ID_i, CID_i, X_i, Y_i, n, e, g, T_i)$ sent by U_i. Next, he computes

$$ID = ID_i^{-1} \bmod n. \tag{3}$$

Then he submits ID as his identity and a random value as his password to obtain a valid smart card (n, e, ID, CID, S, h). Then he forge a login request of user U_i for a choosing current date and time T as follows:

(1) Since $S_i = ID_i^d \pmod n$ and $S = ID^d = ID_i^{-d} \pmod n$, he can computes S_i as follows

$$S_i = S^{-1} \bmod n. \tag{4}$$

(2) Choose a random integer z.
(3) Set

$$X_i' \equiv z^e \pmod n \tag{5}$$
$$Y_i' \equiv S_i z^{f(CID_i, T)} \pmod n. \tag{6}$$

Combing eq. (4) and eq. (5), it has

$$(Y_i')^e \equiv (S_i z^{\cdot f(CID_i,T)})^e \equiv ID_i^{ed} z^{e \cdot f(CID_i,T)} \equiv ID_i \cdot (X_i')^{f(CID_i,T)} \pmod n$$

It can easy verify that $M' = (ID_i, CID_i, X_i', Y_i', n, e, g, T)$ is a a valid login request for date and time T. Hence he can successfully logins in the system and then impersonates user U_i.

4 Conclusion

In this paper, we show that the modified scheme presented by Shen, Lin and Hwang is insecure either. The intruder can forge a valid login request of a legitimate user U_i and then impersonate him by intercepting a login request sent by U_i and registering a legitimate smart card.

References

[1] C.K.Chan and L.M.Cheng,"Cryptanalysis of timestamp-based password authentication scheme," Computer & Security, vol.21, no.1, pp.74-76, 2002.

[2] C.C.Chang and W.Y.Liao, "A remote password authentication scheme based upon ElGamal's signature scheme," Computer & Security, vol.13, no.2, pp.137-144, 1994.

[3] L.Fan, J.H.Li, and H.W.Zhu,"An enhancement of timestamp-based password authentication scheme," Computers & Security, vol.21, no.7, pp.665-667, 2002.

[4] M.S.Hwang,"A remote password authentication scheme based on the digital signature method," International Journal of Computer Mathematics, vol.70, pp.657-666, 1999.

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

[6] C.C.Lee, M.S.Hwang, and W.P.Yang, "A flexible remote user authentication scheme using smart cards," ACM operating Systems Review, vol.36, no.3, pp.46-52, 2002.

[7] C.W.Lin, J.J.Shen, and M.S.Hwang, "Security enhancement for optimal strong-password authentication protocol," ACM Operating Systems Review, vol.37, no.2, pp.7-12,2003.

[8] W.H.Yang and S.P.Shieh, "Password authentication schemes with smart cards," Computers & Security, vol.18, no.8, pp.727-733, 1999.

[9] Jau-Ji Shen, Chih-Wei Lin and Min-Shiang Hwang, "Security enhancement for the timestamp-based password authentication scheme using smart cards", Computers & Security, Vol 22, No 7, pp 591-595, 2003.

[10] Lamport, L., Password authentication with insecure communication, Communication of ACM, Vol. 24, 1981, pp. 770-772.