Cryptanalysis of the Yang -Wang's password authentication schemes

Jue-Sam Chou[1], Ming-De Yang[2], Guey-Chuen Lee[3]

[1]Department of Information Management, Nanhua University
Chiayi 622 Taiwan, R.O.C
jschou@mail.nhu.edu.tw

[2]Department of Information Management, Nanhua University
Chiayi, 622 Taiwan, R.O.C
g3141012@mail2.nhu.edu.tw

[3]Department of Information Management, Central Taiwan University of Science and Technology
Taichung, 406 Taiwan, R.O.C
gclee@ctust.edu.tw

Abstract

In 1999, Yang and shieh proposed two password authentication schemes using smart cards. But in 2003, Sun and Yeh indicated that their schemes are subject to the forgery attack. So in 2005, Yang and Wang proposed an improvement of Yang and Shieh's schemes to resist against Sun and Yeh's attack. However in this paper, we will point out that Yang and Wang's schemes still suffer from the forgery attack. Because in their schemes, one can masquerade as a legal user and cheat the remote server successfully in the authentication phase.

Keywords: password authentication scheme, smart card, forgery attack, remote server

1. Introduction

Because of the open environment of Internet, people usually take actions to prevent any possible information destructions or eavesdropping over the network. One of the protection techniques for the security of information is the password authentication scheme. It requires a system to verify the legality of a user to prevent any kind of possible attacks. Under this scenario, a smart card combined with storage and computation abilities [3] is thus developed for its convenience and portability. It usually stores the user's ID together with his password and may allow user's password to be changed freely. Recently, several researches in this area have been proposed [1][3][4][6][7][8][11]. They all can allow a legal user to login to a remote server for accessing the server's facilities. In 1999, Yang and Shieh [1] proposed both of a timestamp-based and a nonce-based password authentication schemes with smart cards. They claimed that their scheme not only needn't to hold a verified table of passwords but also allow the users to select or change passwords freely. However in

2002, Chan and Cheng [2] found that their schemes were vulnerable to both of the given-ciphertext and forgery attacks. But in 2003, Sun and Yeh [4] indicated that Chan and Cheng's attack was unreasonable since the client's ID forged did not exist in the ID table, meanwhile they also showed that Yang and Shieh's schemes were subject to the forgery attack. Moreover, also in the same year Chen and Zhong[5] pointed out that the fundamental computation assumption in the Yang and Shieh's schemes were incorrect. After that, Jian and Pan [10] made a further analysis on Yang and Shieh's protocols in 2004 and deduce that their protocols are not secure. To overcome these problems, in 2005, Yang and Wang [9] proposed an improvement on Yang and Shieh's schemes attempting to resist the existing attacks. However, in this paper, we will demonstrate that both of Yang and Wang's improvements still suffer from the forgery attack. In other words, the design of the remote user authentication using smart card is still an open problem.

The structure of this paper is organized as follows. In Section 2, we will review Yang and Wang's password authentication schemes [9] improved from Yang and Shiehs'. In Section 3, we will describe our attacks on both of Yang and Wang's schemes. Finally, a conclusion is given in Section 4.

2. Review of Yang and Wang's password authentication schemes

In this section, we will introduce both of Yang and Wang's timestamp-based and nonce-based password authentication schemes [9]. In their schemes, there exists a key information center (KIC) whose responsibilities are to generate key information, issue smart cards to new users, and change passwords for the users if needed. And each scheme can be divided into three phases, registration phase, login phase and authentication phase. We will describe both of them as follows.

2.1. Timestamp-based password authentication scheme

2.1.1 Registration phase

After a new user U_n gives his identifier ID_n and password PW_n to the KIC through a secret channel, KIC executes the following steps.

Step1: Selects two large primes, p and q, computes $m = p * q$, where $"*"$ denotes the multiplication operation and then selects a public key e and finds its corresponding secret key d satifying $e * d \equiv 1 mod\, \phi(m)$.

Step2: Finds an integer g which is a primitive root in both GF(p) and GF(q).

Step3: Produces a smart card's identifier CID_n for user U_n, computes two parameters, $S_n = ID_n^{CIDn \cdot d}$ mod m and $h_n = g^{PWn \cdot d}$ mod m, then issues the smart card, which includes (m, e, g, ID_n, CID_n, S_n, h_n) , to the user.

2.1.2 Login phase

When U_n wants to login to the remote server, he inserts his smart card into the input device and keys in his ID_n and PW_n. The smart card then executes the following steps:

Step1 : Produces a random number R_n and computes two parameters, $X_n = g^{PWn \cdot Rn}$ mod m and $Y_n = S_n \cdot h_n^{Rn \cdot T}$ mod m , where T is the current time of the input device.

Step2 : Sends the login message M which consists of (ID_n, CID_n ,X_n ,Y_n , m, e, g ,T) to the remote server.

2.1.3 Authentication phase

After receiving the login message M from U_n, the remote server records the current time T' and executes the following steps:

.

Step1 : Checks to see whether ID_n and CID_n are right. If they are wrong, the login request will be rejected.

Step2 : Checks to see whether (T' – T) is within a specified time interval △T. If it is, the request is legal; otherwise, the login request will be rejected.

Step3 : Checks to see whether the equation $Y_n^e \equiv ID_n^{CID_n} \cdot X_n^T \ mod\ m$ holds. If it holds, the remote server accepts the login request.

2.2. Nonce-based password authentication scheme

2.2.1 Registration phase

After user U_n gives his identifier ID_n and password PW_n to the KIC through a secret channel, the KIC executes the following steps:

Step1: Produces two large primes, p and q, computes $m = p * q$, where "$*$" denotes the multiplication operation and then selects a public key e and finds its corresponding secret key d satisfying $e * d \equiv 1 mod\ \phi(m)$.

Step2: Finds an integer g which is a primitive root in both GF(p) and GF(q).

Step3: Produces a smart card's identifier CID_n for U_n, computes two parameters, $S_n = ID_n^{CIDn \cdot d}$ mod m and $h_n = g^{PWn \cdot d}$ mod m, then issues the smart card, which includes (m, e, g, ID_n, CID_n, S_n, h_n) , to the user.

2.2.2 Login phase

When user U_n wants to login to the remote server, he inserts his smart card into the input device and keys in his ID_n and PW_n. Then the smart card and the remote server together execute the following steps.

Step1: The smart card delivers the login message M_1 which consists of ID_n and CID_n to the remote server.

Step2: After receiving the login messageM_1, the remote server checks to see whether ID_n and CID_n are right. If they are right, the remote server selects a random number R_S , computes a nonce $N = h (R_S)$ and then delivers it to the smart card, where h(•) denotes a one-way hash function.

Step3: The smart card produces a random number R_n and computes two parameters, $X_n = g^{PWn \cdot Rn} \bmod m$ and $Y_n = S_n \bullet h_n^{Rn \cdot N} \bmod m$. Then the smart card delivers the message M_2 that consists of (X_n , Y_n , m, e, g) to the remote sever .

2.2.3 Authentication phase

After receiving message M_2, the remote sever computes to see whether the equation $Y_n^e \equiv ID_n^{CID_n} \cdot X_n^N \ \boldsymbol{mod}\ m$ holds. If it so, the remote server accepts the login request; otherwise, it rejects.

3. Our attacks

In this section, we will demonstrate that both of Yang and Wang's password authentication schemes suffer from the forgery attack. Since we can obtain some of the user's information from the login message and forge the required information to satisfy the verifying process in the authentication phase. We show both of our attacks as follows.

3.1 Attack on the timestamp-based password authentication scheme

By monitoring on the communication line, an attacker U_a can launch an attack by performing the following steps.

Step1: U_a intercepts the legal user's login message M=(ID_n, CID_n ,X_n ,Y_n , m, e, g ,T).

Step2: Since the verifying equation $Y_n^e \equiv ID_n^{CID_n} \cdot X_n^T \ \boldsymbol{mod}\ m$ in the authentication phase can be transformed into $Y_n^e \cdot \left(X_n^T\right)^{-1} \equiv ID_n^{CID_n} \ \boldsymbol{mod}\ m$, U_a can know the fixed value $ID_n^{CID_n}$ of user U$_n$, where the inverse of X_n^T, $(X_n^T)^{-1}$, can be calculated using the extended Euclid algorithm if it is relatively prime to m. Here on, we use the denominator of an element b to represent its multiplicative inverse, b^{-1}, modulus m.

Step3: Then U$_a$ can base on message M got from step1 to substitute the values of X$_n$, Y$_n$ and T by the forged values X_n', Y_n' and T' respectively, which can be computed as follows:

$$
\begin{aligned}
ID_n^{CID_n} &= \frac{(Y_n)^e}{(X_n)^T} \boldsymbol{mod}\ m \\
&= \frac{(K^T Y_n)^e}{(K^e X_n)^T} \boldsymbol{mod}\ m \\
&= \frac{(K^T Y_n)^e \cdot (K^{eT} X_n^T)^e}{(K^e X_n)^T \cdot (K^e X_n)^{eT}} \boldsymbol{mod}\ m \\
&= \frac{(K^T Y_n \cdot K^{eT} X_n^T)^e}{(K^e X_n)^{T+eT}} \boldsymbol{mod}\ m \\
&= \frac{(K^{T(1+e)} X_n^T Y_n)^e}{(K^e X_n)^{T+eT}} \boldsymbol{mod}\ m \\
&= \frac{(Y_n')^e}{(X_n')^{T'}} \boldsymbol{mod}\ m
\end{aligned}
$$

That is, U$_a$ can first choose any random K such that $X_n' = K^e X_n$ has an inverse modulus m, and then let $Y_n' = K^{T(1+e)} X_n^T Y_n$ and $T' = T + eT$ to satisfy the verifying equation. After that, U$_a$ can deliver the forged login message (ID$_n$, CID$_n$, X_n', Y_n', m, e, g, T') to the remote server. Since the equation $(Y_n')^e \equiv ID_n^{CID_n} \cdot (X_n')^{T'}$ $\boldsymbol{mod}\ m$ holds as well in the authentication phase, the attacker U$_a$ can thus impersonate the legal user U$_n$ and subsequently cheat the remote sever successfully. Therefore, we have a successful attack in this timestamp-based password authentication scheme.

3.2 Attack on the nonce-based password authentication scheme

In this attack, U_a can eavesdrop on the communication line to intercept the messages transformed between the user and the remote server for an enough period of time. Suppose that there are several login users recorded in the hacker's (U_a) database and each occurs several times during this period. More precisely, the hacker's database now contains the items for each login user (U_n) in the form [(ID_n, CID_n), N_{nj}, (X_{nj} ,Y_{nj} , m, e, g)], where the subindex nj denotes U_n's jth login, (ID_n, CID_n) is the message M_1 sent by the smart card to the server, N_{nj} is the server's responding random number, (X_{nj} ,Y_{nj} , m, e, g) is the message M_2 sent by the smart card to the server. After constructing this hacker database, U_a can then launch an attack by first finding an user U_i who has the most logged items in the database and then perform the following steps:

Step1: U_a sends U_i's ID_i and CID_i to the remote server. Assume that the remote server responds with a random number N' back, then U_a might be able to find one of all U_i's recorded items in which N_{ij} is smaller than N' and satisfies both $X_{nj}^{N_{nj}}$ modulus m has an inverse and $N' - N_{ij} = \Delta N = B \cdot e \cdot N_{ij}$, where $B \in Z_m$ and smaller than ΔN. If U_a can't find an user with such a N_{ij}, he would find the second, the third, etc, according to the user's occurrence frequency in the database until he can find such an user. In fact, U_a can decide whether $X_{nj}^{N_{nj}}$ modulus m has an inverse in his off-time precomputation stage (Here, we assume the found user is $U_{n.}$)

Step2: U_a then extracts the found user U_n's selected item, (ID_n, CID_n, N_{nj}, X_{nj} ,Y_{nj} , m, e, g), in his hacker's database. For abbreviation, we denote U_n's N_{nj}, X_{nj},Y_{nj} as N, X_n, Y_n respectively in the following. Since the equation $Y_n^e \equiv ID_n^{CID_n} \cdot X_n^N \ \boldsymbol{mod}\ m$ in the authentication phase can be transformed into $\frac{Y_n^e}{X_n^N} \equiv ID_n^{CID_n} \ \boldsymbol{mod}\ m$. So U_a can know the fixed value of the $ID_n^{CID_n}$ in this congruence according to this selected item.

Step3:. U_a substitutes the values of X_n, Y_n, N by the forged values X_n' , Y_n', and the server's responding value N' respectively, which can be computed as follows:

$$
\begin{aligned}
ID_n^{CID_n} &= \frac{Y_n^e}{X_n^N} \boldsymbol{mod}\ m \\
&= \frac{\left(K^N Y_n\right)^e}{\left(K^e X_n\right)^N} \boldsymbol{mod}\ m \\
&= \frac{\left(K^N Y_n\right)^e \cdot \left(K^e X_n\right)^{BeN}}{\left(K^e X_n\right)^N \cdot \left(K^e X_n\right)^{BeN}} \boldsymbol{mod}\ m \\
&= \frac{\left(K^N Y_n\right)^e \cdot \left[\left(K^e X_n\right)^{BN}\right]^e}{\left(K^e X_n\right)^N \cdot \left(K^e X_n\right)^{BeN}} \boldsymbol{mod}\ m \\
&= \frac{\left[K^N Y_n \cdot \left(K^e X_n\right)^{BN}\right]^e}{\left(K^e X_n\right)^{(1+Be)N}} \boldsymbol{mod}\ m \\
&= \frac{\left(Y_n'\right)^e}{\left(X_n'\right)^{N'}} \boldsymbol{mod}\ m
\end{aligned}
$$

That is, U_a can randomly choose any $K \in Z_m$ such that $X_n' = K^e X_n$ has an inverse modulus m and then let $Y_n' = K^N Y_n \cdot \left(K^e X_n\right)^{BN}$ and $N' = (1 + Be)N$ to satisfy the verifying equation. After that, U_a can deliver this forged login message (X_n' , Y_n' , m, e, g) to the remote server. Since the equation $\left(Y_n'\right)^e \equiv ID_n^{CID_n} \cdot \left(X_n'\right)^{N'} \boldsymbol{mod}\ m$ holds in the authentication phase as well, the attacker U_a can thus impersonate the legal user U_n and cheat the remote sever successfully. Hence, we also have a successful attack in the nonce-based password authentication scheme.

4. Conclusion

In this paper, we have pointed out the weaknesses existed in both of Yang and Wang's password authentication schemes. The weaknesses are that an attacker can masquerade as a legal user and cheat the remote server successfully. So, Yang and Wang's password authentication schemes are not secure enough on the execution of their protocol.

Reference

[1] W. H. Yang and S. P. Shieh, “Password authentication schemes with smart cards, ” Computers & Security, 18(8) (1999)727-733.

[2] C. K. Chan and L. M. Cheng, “Cryptanalysis of a timestamp based password authentication scheme, ” Computers &Security, 21(1) (2002)74-76.

[3] C. C. Lee and M.S. Hwang, W.P. Yang, “A flexible remote user authentication scheme using smart cards, ” ACM Operating Systems Review 36 (3) (2002)46—52.

[4] H. M. Sun and H.T. Yeh, “Further cryptanalysis of a password authentication scheme with smart cards, ” IEICE Transactions and Communications E86-B(4) (2003) 1412－1415.

[5] K. F. Chen and S. Zhong, “Attacks on the Yang-Shieh authentication, ”Computers & Security, 22(8) (2003) 725－727.

[6] J. J. Shen and C. W. Lin, “Security enhancement for the timestamp based password authentication scheme using smart cards, ”Computers& Security, 22(7)(2003) 591－595.

[7] S. T. Wu and B.C. Chieu, “A user friendly remote authentication scheme with smart cards, ” Computers & Security,22(6)(2003), 547－550.

[8] W. S. Juang, “Efficient password authenticated key agreement using smart card, ”Computers & Security (2004), 167－173.

[9] C. C. Yang and R. C. Wang, “An improvement of the Yang-Shieh password authentication schemes, ” Elsevier Inc, (2004)1391－1396.

[10] R. Jiang and Li. Pan, “Further analysis of password authentication schemes -based on authentication tests, ” Computers & Security (2004) 469－477.

[11] W. J. Tsaur and C.C. Wu, “A smart card-based remote scheme for password authentication in multi-server Internet services, ” Computer Standards & Interfaces (2004) 39–51.