A Secure YS-Like User Authentication Scheme

Tzung-Her CHEN
Department of Computer Science and Information Engineering
National Chiayi University
300 University Road, Chia-Yi City, Taiwan 600, R.O.C.
e-mail: thchen@mail.ncyu.edu.tw

Gwoboa HORNG, Ke-Chiang WU
Institute of Computer Science, National Chung-Hsing University
250 Kuo-Kuang Road, Taichung 402, Taiwan, R.O.C.

Received: August 2005

Abstract. Recently, there are several articles proposed based on Yang and Shieh's password authentication schemes (YS for short) with the following features: (1) A user can choose password freely. (2) The server does not need to maintain a password table. (3) There is no need to involve a trusted third party. Although there were several variants of the YS-like schemes claimed to address the forgery attacks, this paper analyzes their security and shows that they still suffer from forgery attacks. Furthermore, a new scheme based on the concept of message authentication is proposed to foil the forgery attack.

Key words: remote user authentication, forgery attack, password, smart card, message authentication, mutual authentication.

1. Introduction

In distributed networks, a user can login to a remote server to access the resource. Due to security considerations, the remote server must verify the validity of remote users and reject the login requests from illegal ones. Therefore, authentication mechanisms are necessary. A remote password authentication scheme is such a mechanism used to authenticate remote users through an open channel.

In traditional password authentication systems, every user has an identity (ID for short) and a corresponding password (PW for short). There will be a password table stored in the server which includes al the legal users' ID and their corresponding PW. To login to the system, a user inputs his ID and PW. The system will check the validity of the pair of ID and PW. The traditional password scheme works. However, it is hazardous when the password table leaks out.

Yang and Shieh (1999) proposed two password authentication schemes using smart cards. One is timestamp-based and the other is nonce-based. In these schemes, users can choose and change their own password freely, the remote server does not need a directory of passwords or a verification table to authenticate users, and the authentication can be handled without the help of a third party. The proposed timestamp-based scheme withstands the replay attack by using timestamp. Whereas a nonce-based scheme is a better choice to withstand the potential replay attack when the clocks do not synchronize well. They claimed that their security is based on the difficulty of factoring and the discrete logarithm problems.

Chan and Cheng (2001) pointed out that the YS scheme is vulnerable to forgery attacks. They explained that an attacker can succeed in forging a login request from the intercepted previous login request to pass the authentication of the remote server. Fan *et al.* (2002) also proposed another forgery attack against the YS scheme and presented an improved scheme to foil this attack by limiting ID to a strict format. But soon, Chen and Zhong (2003) proposed an attack on the Fan's scheme. They claimed that Fan's scheme is still insecure against forgery attacks even if they restricted the ID format. In 2003, Sun and Yeh (2003) pointed out that Chan and Cheng's forgery attack on the YS scheme does not work. They showed that ID is meaningful but the forged ID is not, and the remote server can recognize whether the ID is valid or not. Furthermore, they proposed an effective forgery attack on the YS scheme.

In 2003, Shen, Lin, and Hwang (SLH for short) (Shen *et al.*, 2003) proposed a modified YS scheme to foil forgery attacks and further proposed a mutual authentication to prevent the forged server attack. In (Kim *et al.*, 2003), Kim proposed another scheme (KIM for short) using user's fingerprints. Kim's scheme is very similar to the SLH scheme. In 2005, Yang, Wang, and Chang also proposed a modified YS scheme (YWC for short) (Yang *et al.*, 2005) to withstand forgery attacks. They claimed that Sun and Yeh's forgery attack using the extension of Euclid's algorithm on their scheme does not work.

In this paper, we firstly show that the forgery attacks are possible in the SLH, KIM and YWC schemes. Furthermore, we not only propose a new enhanced version of the YS-like schemes to withstand the forgery attack but also highlight a feature, mutual authentication, found in many authentication protocols but never addressed in the YS-like schemes. The simple concept of message authentication is introduced to the YS-like schemes to foil forgery attacks. The main goal of message authentication is to enable secure communication in a hostile environment. Usually, two parties communicating across an insecure channel need a method to detect any attempt to modify the transmitted message sent by one party to the other or forge its origin. For example, HMAC is a simple and efficient tool for message authentication (Bellare *et al.*, 1996).

The rest of this paper is organized as follows. A brief review of the SLH scheme and its security analysis is given in Section 2. Section 3 describes YWC scheme and its security analysis. In Section 4, an improvement YS-like scheme is proposed. Security analysis of the new scheme and conclusions are given in Section 5 and 6, respectively.

2. Review and Security Analysis of the SLH Scheme

2.1. *Brief Review*

This section briefly reviews the SLH scheme. It consists of three phases: registration, login, and authentication. A key information center (KIC) is responsible to generate key information, issue smart cards, and authenticate the validity of users.

Registration Phase

A new user U_i freely chooses his/her identity ID_i and password PW_i. Then he sends ID_i and PW_i to KIC for registration via a secure channel. Subsequently, KIC should do the following:

1. Select two prime numbers p and q such that $n = p \cdot q$.
2. Choose a number e as his public key, where e is relatively prime to $(p-1)(q-1)$ and compute the corresponding d such that $ed = 1 \bmod (p-1)(q-1)$, where d is KIC's private key.
3. Choose a generator g, which is a primitive element both over $GF(p)$ and $GF(q)$.
4. Compute $S_i = ID_i^d \bmod n$ and $h_i = g^{PW_i \cdot d} \bmod n$ as U_i's secret information.
5. Generate the identity of a smart card $CID_i = f(ID_i \oplus d)$, where the notation $\oplus$ denotes an exclusive-OR operation and $f(\cdot)$ denotes one-way function.
6. Store $n, e, g, ID_i, CID_i, S_i$, and h_i into the smart card and issue it to the user U_i.

Login Phase

U_i attaches his smart card into the card reader when he wants to login to the remote server. After U_i keys in a pair of ID_i and PW_i, the smart card should do the following:

1. Generate a random number r_i, and compute
   $X_i = g^{r_i \cdot PW_i} \bmod n$ and
   $Y_i = S_i \cdot h_i^{r_i \cdot f(CID_i, T_1)} \bmod n$,
   where T_1 is the current time used as the timestamp on the input device.
2. Send the login message $\{ID_i, CID_i, X_i, Y_i, n, e, g, T_1\}$ to the remote server.

Authentication Phase

After receiving the login message, the remote server authenticates U_i. It should do the following:

1. Verify ID_i and CID_i by computing $CID_i' = f(ID_i \oplus d)$ and checking if CID_i' is equal to the received CID_i. If it holds, the remote server goes on to step 2; otherwise, he rejects the login request.
2. Check the validation of T_1. If $T - T_1 \geqslant \Delta T$ holds, the remote server rejects the login request, where T is the current time on the remote server and ΔT denotes the expected valid time interval for transmission delay.

3. Check if $y_i^e = ID_i \cdot X_i^{f(CID_i,T_1)} \bmod n$.
   If it is, the remote server accepts the login request; otherwise, it rejects the login request.
4. Compute R for mutual authentication, where $R = (f(CID_i,T_2))^d \bmod n$ and T_2 is the current time on the remote server. Subsequently, the remote server sends R and T_2 to the user U_i.

Upon receiving R and T_2, U_i should do the following:

1. Check whether $(T_3 - T_2) \geqslant \Delta T$, where T_3 is current time on the smart card. If it holds, U_i stops the communication; otherwise, the communication goes on.
2. Compute $R' = R^e \bmod n$.
   If $R' = f(CID_i,T_2)$ holds, the server is authenticated by U_i; otherwise, U_i stops the communication.

2.2. *Security Analysis*

The SLH scheme is shown to suffer from a forgery attack that an attacker can modify X_i and Y_i to pass authentication. More precisely, an attacker can find a value $a = f(CID_i,T_1)$ which is relatively prime to e. Using the extension of Euclid's algorithm, the attacker can compute two integers u and v such that $eu - av = 1$. Subsequently, he computes $\bar{Y}_i = ID_i^u \bmod n$ and $\bar{X}_i = ID_i^v \bmod n$ to satisfy

$$\begin{aligned}\bar{Y}_i^e \bmod n &= ID_i^{eu} \bmod n\\ &= ID_i^{1+av} \bmod n\\ &= ID_i \cdot ID_i^{f(CID_i,T_1)\cdot v} \bmod n\\ &= ID_i \cdot \bar{X}_i^{f(CID_i,T_1)} \bmod n\end{aligned}$$

It means that any attacker can generate a pair of $\{\bar{X}_i, \bar{Y}_i\}$ to illegally pass authentication. The reason that forgery attacks succeed is the lack of the integrity of the login parameters $\bar{X}_i$ and $\bar{Y}_i$.

Since the KIM scheme is very similar to the SLH scheme, the security analysis is omitted here.

3. Review and Security Analysis of the YWC Scheme

3.1. *Brief Review*

Yang, Wang, and Chang presented modified versions of the YS timestamp-based and nonce-based password authentication schemes. Both of the schemes are briefly described.

A.YWC Timestamp-Based Password Authentication Scheme

Registration Phase

Both the new user U_i and KIC perform similar operations as the SLH scheme except $S_i = ID_i^{CID_i \cdot d} \bmod n$ and $h_i = g^{PW_i \cdot d} \bmod n$.

Login Phase

The operations performed are the same as those of the SLH scheme except $X_i = g^{r_i \cdot PW_i} \bmod n$ and $Y_i = S_i \cdot h_i^{r_i \cdot T} \bmod n$, where r_i is a random number.

Authentication phase:

The remote server checks if Y_i^e is equal to $ID_i^{CID_i} \cdot X_i^T$. If it holds, the remote server accepts the login request; otherwise, it rejects the login request.

B.YWC Nonce-Based Password Authentication Scheme

Registration Phase

This phase is the same as the registration phase in the YWC timestamp-based password authentication, so we omitted it here.

Login Phase

U_i keys in ID_i and PW_i, and the login phase goes as follows.

1. The smart card sends $\{ID_i, CID_i\}$ to the remote server.
2. Upon receiving $\{ID_i, CID_i\}$, the remote server checks the validity of ID_i and CID_i. If ID_i and CID_i are valid, the remote server generates $N = f(r_j)$ and sends it back to the user, where r_j is a random number; otherwise, the remote server rejects the login request.
3. After receiving N, the smart card computes
   $X_i = g^{r_i \cdot PW_i} \bmod n$ and
   $Y_i = S_i \cdot h_i^{r_i \cdot N} \bmod n$.
4. Finally, the smart card sends $\{X_i, Y_i, n, e, g\}$ to the remote server.

Authentication Phase

Upon receiving $\{X_i, Y_i, n, e, g\}$, the remote server checks to see if Y_i^e is equal to $ID_i^{CID_i} \cdot X_i^N$. If it is, the remote server accepts the login request; otherwise, it rejects the login request.

3.2. *Security Analysis*

We show that both of two password authentication schemes proposed by Yang *et al.* suffer from forgery attacks. An attacker is able to forge a pair of $\{\bar{X}_i, \bar{Y}_i\}$ to pass the authentication scheme from intercepting the login message request.

In timestamp-based password authentication scheme, an attacker can choose a value a relatively prime to e, where a is equal to the login time. Using the extension of Euclid's algorithm, the attacker can compute two numbers u and v such that $eu - av = 1$. Let $u' = u \cdot CID_i$ and $v' = v \cdot CID_i$. Then $eu' - av' = CID_i$. Subsequently, the attacker computes $\bar{Y}_i = ID_i^{u'} \bmod n$ and $\bar{X}_i = ID_i^{v'} \bmod n$. Since

$$\begin{aligned}\bar{Y}_i^e \bmod n &= ID_i^{eu'} \bmod n\\ &= ID_i^{CID_i + av'} \bmod n\\ &= ID_i^{CID_i} \cdot ID_i^{av'} \bmod n\\ &= ID_i^{CID_i} \cdot \bar{X}_i^T \bmod n\end{aligned}$$

$\{\bar{X}_i, \bar{Y}_i, n, e, g\}$ can pass the authentication scheme. Based on the same reason, let a be N in the nonce-based password authentication. The pair of forged $\{\bar{X}_i, \bar{Y}_i\}$ still satisfies

$$\begin{aligned}\bar{Y}_i^e \bmod n &= ID_i^{eu'}\\ &= ID_i^{CID_i + av'}\\ &= ID_i^{CID_i} \cdot ID_i^{av'}\\ &= ID_i^{CID_i} \cdot \bar{X}_i^N \bmod n.\end{aligned}$$

Hence, both of the authentication schemes are insecure.

4. The Proposed Scheme

In our proposed scheme, we adopt the concept of message authentication by involving two one-time verifiers to ensure the integrity of X_i and Y_i. Differing from the previous YS-like schemes, the user appends to the login message two verifiers, authentication codes, computed as a one-way hash function of X_i/Y_i and the shared secret nonce. At reception, the server re-computes the verifiers using the shared nonce and accepts the login message as valid only if this value matches the verifier attached to the received login message. The details are as follows.

In the registration phase, KIC stores $f(d, ID_i)$ as secret information into the smart card. The remaining operations are the same as those of the SLH scheme and are omitted here.

In the login phase, U_i keys in a pair of ID_i and PW_i, and the smart card should do the following:

1. Generate a random number r_i and compute
   $X_i = g^{r_i \cdot PW_i} \bmod n$ and
   $Y_i = S_i \cdot h_i^{r_i \cdot f(CID_i, T_1)} \bmod n$.
2. Generate a random number s, a one-time nonce, and compute the two verifiers V_X and V_Y, where $V_X = f(X_i, s)$ and $V_Y = f(Y_i, s)$.
3. Compute $C = s \oplus f(d, ID_i)$.
4. Send the login message $\{ID_i, CID_i, X_i, Y_i, V_X, V_Y, n, e, g, T_1, C\}$ to the remote server.

In the authentication phase, after receiving the login message, the remote server should do the following:

1. Verify ID_i and CID_i by computing $CID_i' = f(ID_i \oplus d)$, and check if CID_i' is equal to the received CID_i.
2. Check the validity of T_1.
3. Compute $f(d, ID_i)$ to retrieve the shared secret s from C by XORing $f(d, ID_i)$ and C, and check if the received V_X is equal to $f(X_i, s)$ and the received V_Y is equal to $f(Y_i, s)$. If those hold, the remote server recognizes the integrity of X_i and Y_i; otherwise, the remote server rejects the login request.
4. Check if Y_i^e is equal to $ID_i \cdot X_i^{f(CID_i, T_1)}$. If they are equal, the remote server accepts the login request; otherwise, he rejects it.
5. Compute R for mutual authentication, where $R = f(s, T_2)$ and T_2 is the current time on the remote server. Subsequently, the remote server sends R and T_2 to the user U_i.

Upon receiving R and T_2, U_i should do the following:

1. Check the validation of T_2.
2. Check if $f(s, T_2)$ is equal to R.

If they are equal then the server is authenticated by U_i; otherwise, U_i stops the communication.

5. Security Analysis and Discussions

In this section, the security of the proposed scheme is examined. An attacker may launch the forgery attack to pass authentication and gain access to the server. For examples, an attacker can forge a login message; intercept the login message to guess the password or replay the message; or impersonate a server to cheat the users. Of course, he may try to intrude into the server to steal some sensitive information or just modify it. However, this attack is impossible because no verification table is stored in the server side. The following possible attacks are further discussed.

Forgery Attack

In the proposed scheme, two verifiers (authentication codes) $V_X = f(X_i, s)$ and $V_Y = f(Y_i, s)$, involving a one-time nonce s, are introduced to assure the integrity of

X_i and Y_i, respectively. An attacker can find a pair of $\{\bar{X}_i, \bar{Y}_i\}$ to satisfy the verification equation $\bar{Y}_i^e = ID_i \cdot \bar{X}_i^{f(CID_i,T_1)}$. However the pair of $\{\bar{X}_i, \bar{Y}_i\}$ must further satisfy $V_X = f(\bar{X}_i, s)$ and $V_Y = f(\bar{Y}_i, s)$. It means that an attacker has to know the value of s. But in the login message, s is protected by $f(d, ID_i)$. It is hard to retrieve s from $s \oplus f(d, ID_i)$ without knowing the remote server's private key d. That is, an attacker has no efficient way to find a pair of $\{\bar{X}_i, \bar{Y}_i\}$ to satisfy the verification equation without losing the integrity of the login message.

Password Guessing Attack

Assume that an attacker intercepts $X_i = g^{r_i \cdot PW_i} \bmod n$ from the login request over a public network. When he guesses a password, he still cannot verify it since he has no idea about r_i.

Replay Attack

An attacker may replay the login request to the remote server by intercepting the user's previous login request. The remote server will reject the login request because $(T - T_1)$ will expire the expected valid time interval ΔT. Hence, an attacker cannot login to the remote server by replaying the previous login message.

Server Impersonation Attack

To cheat a legal user, an attacker may impersonate the remote server by generating a forged $\{R, T_2\}$. After the user receives the message, he will check if the received R is equal to $f(s, T_2)$. However, the attacker is not able to know the secret information s. Hence, the attacker cannot forge a valid $\{R, T_2\}$.

Furthermore, mutual authentication is firstly highlighted by (Shen et al., 2003) in the YS-like series. In the proposed scheme, the scheme replaces $R = (f(CID_i, T_2))^d$ in (Shen *et al.*, 2003) with $R = f(s, T_2)$, in which only a one-way hash function is used to lower the computation load rather than the exponential operations.

On the other hand, the two verifiers $V_X = f(X_i, s)$ and $V_Y = f(Y_i, s)$ are introduced to assure the integrity of X_i and Y_i. Fortunately, only one-way hash functions are involved to achieve the goal of integrity. The computation load of one-way hash functions is much lighter than that of exponential operations.

Hence, without adding extra computational cost, the proposed scheme not only fixes the security flaws but also provides mutual authentication.

6. Conclusions

In this paper, the authors not only point out that the latest versions of the YS-like schemes still suffer from the forgery attack, but also propose a new one based on the concept of message authentication to foil the forgery attacks. Other than fixing security weaknesses, the proposed scheme has the following advantages: (1) no password table needs to be stored in the remote server; (2) users can freely choose their identity and password; and (3) mutual authentication is provided between the user and the remote server.

References

Bellare, M., R. Canetti and H. Krawczyk (1996). Keying hash functions for message authentication. In N. Koblitz (Ed.), *Proceedings of Advances in Cryptology – Crypto 96*, *Lecture Notes in Computer Science*, **1109**, Springer-Verlag.

Chan, C.K., and L.M. Cheng (2001). Cryptanalysis of timestamp-based password authentication scheme. *Computers & Security*, **21**(1), 74–76.

Chen, K.F., and S. Zhong (2003). Attacks on the (enhanced) Yang–Shieh authentication. *Computer & Security*, **22**(8), 725–727.

Fan, L., J.H. Li and H.W. Zhu (2002). An enhancement of timestamp-based password authentication scheme. *Computers & Security*, **21**(7), 665–667.

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

Shen, J.J., C.W. Lin and M.S. Hwang (2003). Security enhancement for the timestamp-based password authentication scheme using smart cards. *Computers & Security*, **22**(7), 591–595.

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

Yang, C.C., R.C. Wang and T.Y. Chang (2005). An improvement of the Yang–Shieh password authentication schemes. *Applied Mathematics and Computation*, **162**(3), 1391–1396.

Yang, W.H., and S.P. Shieh (1999). Password authentication schemes with smart cards. *Computers & Security*, **18**(8), 727–733.

T.-H. Chen was born in Tainan, Taiwan, Republic of China, in 1967. He received the BS degree in Department of Information & Computer Education from National Taiwan Normal University in 1991 and the MS degree in Department of Information Engineering from Feng Chia University in 2001. In 2005, he received his PhD degree in Department of Computer Science from National Chung Hsing University. He has been with Department of Computer Science and Information Engineering at National Chiayi University as an assistant professor since August 2005. His research interests include information security, information hiding, multimedia security, digital rights management, security for wireless & mobile networks.

G. Horng received the BS degree in electrical engineering from National Taiwan University in 1981 and the MS and PhD degrees from University of Southern California in 1987 and 1992 respectively, all in computer science. Since 1992, he has been on the Faculty of the Institute of Computer Science at National Chung-Hsing University, Taichung, Taiwan, R.O.C. His current research interests include artificial intelligence, cryptography and information security.

K.-C. Wu received the MS degree in Institute of Computer Science from National Chung-Hsing University in 2005. his research interests include cryptography and infromation security.

Saugi vartotojų autentikavimo schema, panaši į YS

Tzung-Her CHEN, Gwoboa HORNG, Ke-Chiang WU

Pastaruoju metu keli paskelbti straipsniai yra pagrįsti Yang ir Shieh (YS) slaptažodžio autentikavimo schemomis su tokiomis savybėmis: (1) vartotojas gali laisvai pasirinkti slaptažodį; (2) serveris neturi palaikyti slaptažodžių lentelės; (3) nėra reikalo įtraukti patikimą trečiąją šalį. Nors buvo keli į YS panašių schemų variantai, teigiantys valdantys klastojimo atakas, šis straipnis analizuoja jų saugumą ir parodo, kad jie vis dar palaužiami klastojimo atakų. Be to, nauja pranešimo autentikavimu pagrįsta schema yra pasiūlyta klastojimo atakų trukdymui.