Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER Applied Mathematics and Computation 162 (2005) 1391–1396
APPLIED MATHEMATICS AND COMPUTATION
www.elsevier.com/locate/amc

An improvement of the Yang-Shieh password authentication schemes

Chou-Chen Yang [a,*], Ren-Chiun Wang [b], Ting-Yi Chang [c]

[a] *Department of Computer Science and Information and Communication Engineering, Chaoyang University of Technology 168 Gifeng E. Road, Wufeng, Taichung County, 413, Taiwan, ROC*

[b] *Department of Information Management, Chaoyang University of Technology, 168 Gifeng E. Road, Wufeng, Taichung County, 413, Taiwan, ROC*

[c] *Department of Computer and Information Science, National Chiao Tung University, 1001 Ta Hsueh Road, Hsinchu, 413, Taiwan, ROC*

Abstract

Recently, Yang and Shieh proposed two password authentication schemes by employing smart cards. One is a timestamp-based password authentication scheme and the other is a nonce-based password authentication scheme. In 2002, Chan and Cheng pointed out that Yang and Shieh's timestamp-based password authentication scheme was vulnerable to the forgery attack. However, in 2003, Sun and Yeh pointed out that Chan and Cheng's attack was unreasonable. At the same time, Sun and Yeh pointed out that Yang and Shieh's password authentication schemes were still vulnerable to the forgery attack. In this paper, we shall improve Yang and Shieh's schemes to resist Sun and Yeh's attack.

Keywords: Authentication; Forgery attack; Password; Smart card

1. Introduction

In a client/server system, when the client wants to log in to a remote server, the remote server requires a password to authenticate the identity of the client.

* Corresponding author.
E-mail address: ccyang@cyut.edu.tw (C.-C. Yang).

0096-3003/$ - see front matter
doi:10.1016/j.amc.2004.03.017

Therefore, it is important to protect the password in the authentication schemes. There are three ways an attacker can get a user's password and impersonate the user to log in to the server [5]: (1) the attacker invades the system; (2) the attacker eavesdrops on communication messages; and (3) the legal user accidentally reveals his password. In case 3, it is very hard to prevent a user from accidentally revealing his password.

The advantages of smart cards are storage and computation abilities. These advantages are always employed by some scholars [2,4,6,7,9,10], but their schemes have to maintain a verified table of passwords and do not allow passwords to be changed freely. In 1999, Yang and Shieh [11] proposed two password authentication schemes that do not need to maintain a verified table of passwords and that allow users to choose and change their passwords whenever they want. In 2002, Chan and Cheng [1] pointed out that Yang and Shieh's timestamp-based password authentication scheme was vulnerable to the forgery attack.

However, in 2003, Sun and Yeh [8] pointed out that Chan and Cheng's attack was unreasonable because Chan and Cheng forged a client's identity, and the identity did not exist in the ID table. Thus, the attacker could not be verified from the ID table. At the same time, Sun and Yeh pointed out that Yang and Shieh's two password authentication schemes were vulnerable to the forgery attack. Their main idea was first to intercept a legal client's identity and the smart card's identifier. Then they use the idea of extending Euclid's algorithm [3] to find parameters which can satisfy the verification of the formula and the remote server cannot find the attacker is an invalid user. In this paper, we shall improve Yang and Shieh's schemes to resist Sun and Yeh's attack.

The structure of our paper is organized as follows. In Section 2, we shall present our idea. In Section 3, we shall analyze the security of our scheme. Finally, in Section 4, we shall conclude this paper.

2. Improvement on Yang and Shieh's schemes

In this section, we shall improve Yang and Shieh's timestamp-based and nonce-based password authentication schemes. We follow their registration, login and authentication procedures and introduce as follows.

2.1. Timestamp-based password authentication scheme

In this scheme, there is a key information center (KIC). The duties of the KIC are to generate key information, issue smart cards to new users, and change passwords for the registered users.

2.1.1. Registration phase

A new user U_i sends his identifier ID_i and a chosen password pw_i to the KIC via a secure channel. Then, the KIC performs the following steps.

Step 1: Generate two large prime numbers p and q and compute $n = p * q$.
Step 2: Choose a public key e and find a corresponding secret key d that satisfies $e \cdot d \equiv 1 \bmod (p-1)(q-1)$.
Step 3: Find an integer g that is a primitive element in both $\mathrm{GF}(p)$ and $\mathrm{GF}(q)$, where g is a public information. Note that $\mathrm{GF}(p)$ and $\mathrm{GF}(q)$ mean p and q are finite fields.
Step 4: Generate a smart card's identifier CID_i for the user and compute $S_i = \mathrm{ID}_i^{\mathrm{CID}_i \cdot d} \bmod n$.
Step 5: Compute $h_i = g^{\mathrm{pw}_i \cdot d} \bmod n$.
Step 6: Send the smart card, which includes $(n, e, g, \mathrm{ID}_i, \mathrm{CID}_i, S_i, h_i)$, to the user.

2.1.2. Login phase

When the user wants to log in to the remote server, the user first inserts his smart card into the input device and keys in his ID_i and pw_i. Then the smart card performs the following steps.

Step 1: Generate a random number r_i.
Step 2: Compute $X_i = g^{\mathrm{pw}_i \cdot r_i} \bmod n$ and $Y_i = S_i \cdot h_i^{r_i \cdot T} \bmod n$, where T is the current time.
Step 3: Send the login message M to the remote server, where $M = (\mathrm{ID}_i, \mathrm{CID}_i, X_i, Y_i, n, e, g, T)$.

2.1.3. Authentication phase

After receiving the login request message M, the remote server records the current time T' and performs the following steps:

Step 1: Check whether the ID_i and the CID_i are correct or not. If they are not correct, the login request is rejected.
Step 2: Check whether $(T' - T)$ is within the valid time interval ΔT. If it is not true, the login request is rejected.
Step 3: Check whether the following equation holds: $Y_i^e \equiv \mathrm{ID}_i^{\mathrm{CID}_i} \cdot X_i^T \bmod n$. If it is true, the remote server accepts the login request.

2.2. Nonce-based password authentication scheme

2.2.1. Registration phase

This phase is same as the registration phase in the timestamp-based password authentication scheme.

2.2.2. Login phase

When the user wants to log in to the remote server, the user first inserts his smart card into the input device and keys in his ID_i and pw_i. Then the smart card performs the following steps.

Step 1: The smart card sends a request login message M_1 to the remote server, where $M_1 = (ID_i, CID_i)$.
Step 2: After receiving M_1, the remote server checks whether the ID_i and the CID_i are correct or not. If they are correct, the remote server computes a nonce $N = f(r_j)$ and sends it back. Note that r_j is a random number and $f(\cdot)$ is a one-way hash function.
Step 3: After the nonce N is received, the smart card generates a random number r_i and computes X_i and Y_i, where $X_i = g^{pw_i \cdot r_i} \bmod n$ and $Y_i = S_i \cdot h_i^{r_i \cdot N} \bmod n$.
Step 4: Finally, the smart card sends the message M_2 to the remote server, where $M_2 = (X_i, Y_i, n, e, g)$.

2.2.3. Authentication phase

After receiving M_2, the remote server computes whether the following equation holds: $Y_i^e \equiv ID_i^{CID_i} \cdot X_i^N \bmod n$. If it holds, the remote server accepts the login request message; otherwise, the login request is rejected.

3. Security analysis

We analyze some attacks in our improvement.

3.1. Forgery attack

In the timestamp-based password authentication scheme, an attacker can get the ID_i and the CID_i by intercepting the communication messages. e is the KIC's public key and it is a prime number. We can find a and e are relatively prime, where a equals current time T. By employing an extension of Euclid's algorithm, the attacker can find two random numbers u and v to satisfy $e \cdot u - a \cdot v = 1$ and to compute $Y_i = ID_i^u \bmod n$ and $X_i = ID_i^v \bmod n$. Then we can find $Y_i^e \equiv ID_i^{u \cdot e} \equiv ID_i^{1+a \cdot v} \equiv ID_i \cdot X_i^T \bmod n$. Obviously, it is different to our formula: $Y_i^e \equiv ID_i^{CID_i} \cdot X_i^T \bmod n$. Therefore, Sun and Yeh's attack cannot work in our method. For the same reason, Sun and Yeh's forgery attack also cannot work in the nonce-based password authentication scheme.

3.2. Password-guessing attack

In the timestamp-based and the nonce-based password authentication schemes, the attacker has two ways to guess the password pw_i. One way is to

get $h_i = g^{\mathrm{pw}_i \cdot d} \bmod n$ from the smart card; the other way is to get $X_i = g^{\mathrm{pw}_i \cdot r_i} \bmod n$. We can find the attacker cannot guess the password without d and r_i. Therefore, our scheme can resist a password-guessing attack.

3.3. Smart card loss

When a legal user loses his smart card and it is found by an attacker, the attacker can guess the password of the legal user. We find that the attacker cannot succeed, the reason is given in the password-guessing attack section. In the timestamp-based password authentication scheme, even if the attacker uses a smart card to log in to the remote server, the attacker cannot succeed. The attacker inserts the smart card and keys a guessed password into the input device. Then the smart card computes $X_i = g^{\mathrm{pw}_{\mathrm{attacker}} \cdot r_i} \bmod n$ and $Y_i = S_i \cdot h_i^{r_i \cdot T} \bmod n$. Obviously, the attacker cannot pass the verification of the equation: $Y_i^e \equiv \mathrm{ID}_i^{\mathrm{CID}_i} \cdot X_i^T \bmod n$ because $Y_i^e \equiv \mathrm{ID}_i^{\mathrm{CID}_i} \cdot g^{\mathrm{pw}_i \cdot r \cdot T} \bmod n$ and $\mathrm{ID}_i^{\mathrm{CID}_i} \cdot X_i^T = \mathrm{ID}_i^{\mathrm{CID}_i} \cdot g^{\mathrm{pw}_{\mathrm{attacker}} \cdot r_i \cdot T} \bmod n$. For the same reason, the attacker cannot use the same way to log in to the remote server in the nonce-based password authentication scheme.

3.4. Replay attack

In the timestamp-based password authentication scheme, if an attacker tries to replay the verified message $M = (\mathrm{ID}_i, \mathrm{CID}_i, X_i, Y_i, n, e, g, T)$ to the remote server, the remote server would reject it because the attacker cannot pass the verification $(T' - T) \leqslant \Delta T$ in the Step 2 of the authentication phase. In the nonce-based password authentication scheme, if an attacker replays the verified message $(M_1 = \mathrm{ID}_i, \mathrm{CID}_i)$ to the remote server in the Step 1 of the login phase, the remote server sends a new nonce N_{new} back. Then the attacker replays another verified message $M_2 = (X_i, Y_i, n, e, g)$ to the remote server in the Step 4 of the login phase. Obviously, he cannot pass the verification of the formula: $Y_i^e \equiv \mathrm{ID}_i^{\mathrm{CID}_i} \cdot X_i^{N_{\mathrm{new}}} \bmod n$ in the authentication phase because the remote server records the new nonce N_{new} without N.

4. Conclusions

In this paper, we improve Yang and Shieh's two password authentication schemes. After our improvement, the password authentication schemes can resist attacks previously.

Acknowledgements

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract No.: NSC91-2622-E-324-cc3.

References

[1] C.K. Chan, L.M. Cheng, Cryptanalysis of a timestamp-based password authentication scheme, Computers and Security 21 (1) (2002) 74–76.
[2] C.K. Chan, L.M. Cheng, Cryptanalysis of a remote user authentication scheme using smart cards, IEEE Transaction on Consumer Electronics 46 (4) (2000) 992–993.
[3] I.N. Herstein, Topics in Algebra, Xerox Corporation, 1975.
[4] M.S. Hwang, L.H. Li, A new remote user authentication scheme using smart cards, IEEE Transaction on Consumer Electronics 46 (1) (2000) 28–30.
[5] L. Lamport, Password authentication with insecure communication, Communications of the ACM 24 (November) (1981) 770–772.
[6] C.C. Lee, M.S. Hwang, W.P. Yang, A flexible remote user authentication scheme using smart cards, ACM Operating Systems Review 36 (3) (2002) 46–52.
[7] H.M. Sun, An efficient remote user authentication scheme using smart cards, IEEE Transaction on Consumer Electronics 46 (4) (2000) 958–961.
[8] H.M. Sun, H.T. Yeh, Further cryptanalysis of a password authentication scheme with smart cards, IEICE Transactions and Communications E86-B (4) (2003) 1412–1415.
[9] T. Wu, Secure remote password protocol, in: Internet Society Symposium on Network and Distributed System Security Symposium, 1998.
[10] T.C. Wu, Remote login authentication scheme based on a geometric approach, Computer Communications 18 (12) (1995) 959–963.
[11] W.H. Yang, S.P. Shieh, Password authentication schemes with smart cards, Computers and Security 18 (8) (1999) 727–733.