Cryptanalysis of Two Improved Password Authentication Schemes Using Smart Cards

Ren-Chiun Wang[1] and Chou-Chen Yang[2]
(Corresponding author: Ren-Chiun Wang)

Department of Information Management, Chaoyang University of Technology[1]
1F, No.9, Alley 10, Lane 278, Cingshuei Rd., Tucheng City, Taipei County 236, Taiwan R.O.C.
(Email: chiunchiunwang@yahoo.com.tw)
Department of Management Information Systems, National Chung Hsing University[2]
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C. (Email: cc_yang@nchu.edu.tw)

(Received Oct. 14, 2005; revised and accepted Nov. 23, 2005)

Abstract

Recently, Yang et al. improved Yang and Shieh's two password authentication schemes to withstand Sun and Yeh's forgery attacks. However, Kim et al. pointed out that Yang et al.'s improvements still cannot withstand forgery attacks. At the same time, Kim et al. proposed improved methods. In this paper, we shall show that Kim et al.'s improvements also cannot resist the forgery attacks.

Keywords: Authentication, forgery attack, password, smart card

1 Introduction

In a client/server system, a password authentication scheme with smart card is widely used to identify the valid of a remote user [2, 5, 6].

For enhancing the security and efficiency, Yang and Shieh [10] proposed a timestamp-based and a nonce-based password authentication schemes. Their schemes do not need to maintain a verified table of passwords and allow users to choose and to 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 [7] explained 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 of the remote server. 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 some parameters to satisfy the verification of the formula and the remote server cannot find the attacker is an invalid user.

Later, Yang et al. [8] proposed improved methods to withstand Sun and Yeh forgery attack [7]. However, Kim et al. [4] showed that Yang et al.'s schemes are still vulnerable to the forgery attacks [7, 9] and proposed their improvements. In this paper, authors shall show that Kim et al.'s improvement cannot withstand the forger attack.

In Section 2, we shall review Kim et al.'s improvements. In Section 3, we shall show that Kim et al.'s improvements are insecure. In Section 4, we shall make a conclusion for this paper.

2 Review of Kim et al.'s Improved Authentication Schemes

In this section, we shall briefly review Kim et al.'s password authentication schemes. One is timestamp-based authentication scheme; the other is nonce-based. In these schemes, there is a key information center (KIC) that is used to issue smart cards for new users and to change passwords for the registered users.

2.1 Timestamp-based Password Authentication Scheme

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 $n = p \times q$.

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 $GF(p)$ and $GF(q)$, where g is a public information.

Step 4: Generate a smart card's identifier CID_i for the user and compute $S_i = ID_i^{CID_i \cdot d} \bmod n$.

Step 5: Compute $h_i = g^{pw_i \cdot d} \bmod n$.

Step 6: Send the smart card, which includes $(n, e, g, ID_i$, CID_i, S_i, $h_i)$, to the user.

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 $X_i = g^{pw_i \cdot r_i \cdot e} \bmod n$ and $Y_i = S_i^T \cdot h_i^{r_i} \bmod n$, where T is the current time.

Step 3: Send the login message M to the remote server, where $M = (ID_i, CID_i, X_i, Y_i, n, e, g, T)$.

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 $\triangle T$. If it is not true, the login request is rejected.

Step 3: Check whether the following equation holds: $Y_i^e \equiv X_i^d \cdot ID_i^{CID_i \cdot T} \bmod n$. If it is true, the remote server accepts the login request.

2.2 Nonce-based Password Authentication Scheme

Registration phase:

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

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 an one-way hash function.

Step 3: After the nonce N is received, the smart card generates a random number r_i and to compute X_i and Y_i, where $X_i = g^{pw_i \cdot r_i \cdot e} \bmod n$ and $Y_i = S_i^N \cdot h_i^{r_i} \bmod n$.

Step 4: Finally, the smart card sends the message M_2 to the remote server, where $M_2 = (X_i, Y_i, n, e, g)$.

Authentication phase:

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

3 Security Analysis of Kim et al.'s Password Authentication Schemes

In this section, we shall show that an impostor can easily impersonate a valid user to log in to the remote system as follows.

Attack Scenario 1 – An Eve Can Impersonate a Valid Client to Log in to the Remote System in the Timestamp-based Password Authentication Scheme:

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. The attacker can find a random number a and that is relatively prime with e. 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 $Y_i = ID_i^{CID_i \cdot u \cdot T'} \bmod n$ and $X_i = ID_i^{CID_I \cdot T' \cdot a \cdot v \cdot e} \bmod n$, where T' is the attacker's login time. Then we can find $Y_i^e \equiv ID_i^{CID_i \cdot u \cdot T' \cdot e} \bmod n$ and $X_i^d \cdot ID_i^{CID_i \cdot T'} \equiv ID_i^{CID_i \cdot T' \cdot a \cdot v} \cdot ID_i^{CID_i \cdot T'} \equiv ID_i^{CID_i \cdot T' \cdot (1+a \cdot v)} \equiv ID_i^{CID_i \cdot T' \cdot u \cdot e} \bmod n$. Obviously, the attacker can pass the verifying of the remote server and impersonate a valid user to log in to the remote system successfully.

Attack Scenario 2 – An Eve Can Impersonate A Valid Client to Log in to the Remote System in the Nonce-based Password Authentication Scheme:

Using the same way, in the nonce-based password authentication scheme, an attacker can get a new nonce N_{new} by sending M_1 to the server and compute $Y_i = ID_i^{CID_i \cdot u \cdot N_{new}} \bmod n$ and $X_i = ID_i^{CID_i \cdot N_{new} \cdot a \cdot v \cdot e} \bmod n$. Finally, we can find $Y_i^e \equiv ID_i^{CID_i \cdot u \cdot N_{new} \cdot e} \bmod n$ and $X_i^d \cdot ID_i^{CID_i \cdot N_{new}} \equiv ID_i^{CID_i \cdot N_{new} \cdot a \cdot v} \cdot ID_i^{CID_i \cdot N_{new}} \cdot \equiv ID_i^{CID_i \cdot N_{new} \cdot (1+a \cdot v)} \equiv ID_i^{CID_i \cdot N_{new} \cdot u \cdot e} \bmod n$. Similarly, our forgery attack can work in the nonce-based password authentication scheme.

4 Conclusion

In this paper, we show that Kim et al.'s improved authentication schemes are insecure. That is any impostor can easily impersonate valid users to access the resources of the remote system.

References

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

[2] 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.

[3] I. N. Herstein, *Topics in Algebra*, Xerox Corporation, 1975.

[4] K. W. Kim, J. C. Jeon, and K. Y. Yoo, "An improvement on Yang et al.'s password authentication schemes," *Applied Mathematics and Computation*, vol. 170, pp. 207-215, 2005.

[5] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, pp. 770-772, Nov. 1981.

[6] J. J. Shen, C. W. Lin, and M. S. Hwang, "Security enhancement for the timestamp-based password authentication scheme using smart cards," *Computers & Security*, vol. 22, no. 7, pp. 591-595, 2003.

[7] H. M. Sun and H. T. Yeh, "Further cryptanalysis of a password authentication scheme with smart cards," *IEICE Transactions on Communication*, vol. E86-B, no. 4, pp. 1412-1415, 2003.

[8] C. C. Yang, R. C. Wang, and T. Y. Chang, "An improvement of the Yang-Shieh password authentication schemes," *Applied Mathematics and Computation*, vol. 162, pp. 1391-1396, 2005.

[9] C. C. Yang, H. W. Yang, and R. C. Wang, "Cryptanalysis of security enhancement for the timestamp-based password authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 578-579, May 2004.

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

Ren-Chiun Wang received the B.S. and M. S. in Information Management from Ming Chuan University and Chaoyang University of Technology. His current research interests include cryptography, information security, and mobile communications.

Chou-Chen Yang received his B.S. in Industrial Education from the National Kaohsiung Normal University, in 1980, and his M.S. in Electronic Technology from the Pittsburg State University, in 1986, and his Ph.D. in Computer Science from the University of North Texas, in 1994. From1994 to 2004, Dr. Yang was an associate professor in the Department of Computer Science and Information Engineering, Chaoyang University of Technology. Currently, he is a professor in the Department of Management Information Systems, National Chung Hshing University. His research interests include network security, mobile computing, and distributed system.