스마트 카드에서 향상된 비밀번호 인증 암호해독기법

알-사킵 칸 파탄 O, 홍충선

경희대학교 컴퓨터공학과

spathan@networking.khu.ac.kr, cshong@khu.ac.kr

Cryptanalysis of Improved Password Authentication Scheme with Smart Cards

Al-Sakib Khan Pathan O and Choong Seon Hong

Department of Computer Engineering, Kyung Hee University

ABSTRACT

The intent of this paper is to present the flaws and weaknesses of Kim et al.'s timestamp-based password authentication scheme using smart cards. We prove that, in spite of the improvement of Yang-Wang-Chang's scheme, Kim et al.'s solution is still vulnerable to a type of forgery attack. We also note down how the flaw could be overcome to ensure better level of security in remote client-server communication procedure.

1. INTRODUCTION

Timestamp based password authentication schemes are used for verification of identities and passwords of the remote users in e-transaction related technologies. As we generally consider the presence of insecure channels during the remote communication procedures, it is necessary to protect user's password and other critical values passed through the channels so that proper level of security could be ensured for such types of communications.

In 2005, Kim et al. [1] proposed an improved scheme based on Yang-Wang-Chang's [2] timestamp-based password authentication scheme. In an attempt to remove the flaws of [2], they proposed a timestamp-based password authentication scheme using smart cards by modifying some steps presented in [2]. So far, Kim et al.'s scheme has been regarded as flawless and has not been challenged. However, after a detailed analysis of their scheme, we have devised a tricky forgery attack that can break the security of the scheme. In this paper, we present the weakness of Kim et al.'s scheme and suggest the amendments to make it more secure to lower the probability of forgery attacks during remote communications in such settings.

* "This research was supported by the MKE under the ITRC support program supervised by the IITA"(IITA-2008-(C1090-0801-0016))

1.1 Main Contributions of Our Work

1. Review of Kim et al.'s proposed timestamp-based password authentication scheme.
2. Comments on Kim et al.'s scheme and showing the flaws in their scheme.
3. Suggesting possible solution to overcome the vulnerability.

1.2 Organization of this Paper

The organization of this paper is as follows: following the Section 1, Section 2 presents the timestamp-based password authentication scheme proposed by Kim et al., Section 3 analyzes [1], shows the vulnerability which could break its security, and suggests the necessary modification to overcome the flaw, and finally, Section 4 contains the concluding remarks.

2. REVIEW OF KIM ET AL.'S IMPROVED TIMESTAMP-BASED SCHEME

In this section we review Kim et al.'s scheme.

2.1 Basic Terms and Preliminaries

U_i – The ith user seeking for authentication

KIC – The Key Information Center located or associated with the remote server, which is responsible for issuing smart cards to the users and serving their requests for password changing or registration

ID_i – The identity of the user U_i

PW_i – The password chosen by U_i

CID_i – The identity of the smart card associated with U_i

2.2 Working Principle of Kim et al.'s scheme

This scheme has mainly three phases; registration, login, and verification phase. Here, we mention the steps of all the phases in detail.

Registration Phase. This phase is the initialization phase of the entire procedure and occurs over a secure channel. 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. Generates two large prime numbers p and q and computes $n = p \bullet q$.

Step 2. Chooses a prime number e and an integer d which satisfy, $e \bullet d \equiv 1 \bmod (p-1)(q-1)$, where, e is the public key of the KIC that should be published and d is the secret key that is kept undisclosed.

Step 3. Finds an integer g which is a primitive element in both GF(p) and GF(q), where g is the public information of the KIC.

Step 4. Generates a smart card's identity CID_i for the user and computes U_i's secret information S_i as $S_i = ID_i^{CID_i \bullet d} \bmod n$.

Step 5. Computes $h_i = g^{PW_i \bullet d} \bmod n$.

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

Login Phase. When U_i needs to login to the system, the smart card should be attached to the login device, and ID_i and PW_i need to be keyed in. After that, the smart card performs the following operations:

Step 1. Generates a random number r_i.

Step 2. Computes X_i and Y_i :

$$X_i = g^{PW_i \bullet r_i \bullet e} \bmod n \quad \text{and} \quad Y_i = h_i^{r_i} \bullet S_i^T \bmod n$$

Here, T is the current timestamp.

Step 3. Sends the login request message, $M = \{ID_i, CID_i, X_i, Y_i, n, e, g, T\}$ to the remote server.

Verification Phase. After the server has received the message M, it carries out the following steps:

Step 1. Checks the validity of ID_i and CID_i. If the format of any of these is incorrect, the server rejects the request.

Step 2. Checks whether the condition $(T' - T) \le \Delta T$ holds or not, where T' is the timestamp of receiving the login request message and ΔT is the legitimate time interval allowed for the transmission delay. If it is negative, the server rejects the request.

Step 3. Checks the equation, $Y_i^e = X_i^d \bullet ID_i^{CID_i \bullet T} \bmod n$. If it holds, then the remote server accepts the login request and gives access to the U_i. Otherwise, it rejects the login request.

3. CRYPTANALYSIS OF KIM ET AL.'s SCHEME

Kim et al. modified some of the calculation and checking steps keeping the basic working method same as the previous scheme. In their scheme, they kept the *registration phase* exactly similar as in Yang-Wang-Chang's [2] scheme. In the *login phase*, X_i and Y_i were calculated differently as, $X_i = g^{PW_i \bullet r_i \bullet e} \bmod n$ and $Y_i = h_i^{r_i} \bullet S_i^T \bmod n$ where, T was the current timestamp. In the *verification phase*, for the final checking step, the equation was changed to, $Y_i^e = X_i^d \bullet ID_i^{CID_i \bullet T} \bmod n$.

In their security analysis, the authors claimed full security of their proposed scheme against forgery attacks, password guessing attack, and replay attack. For proving that their scheme was resistant to any kind of forgery attack, they showed the invulnerability against two well-known forgery attacks, Sun-Yeh's [3] forgery attack and yang et al.'s [4] forgery attack. They also mentioned one of the major strengths of their scheme was that, it could be really difficult to generate a pair (X_i, Y_i) which could satisfy the equation $Y_i^e = X_i^d \bullet ID_i^{CID_i \bullet T} \bmod n$. Introducing the use of secret value d in the equation, made it resistant against the

known types of attacks.
So far, Kim et al.'s scheme has not been challenged and has been thought to be fully secure. After analyzing their scheme thoroughly, we have found that it could also be broken with a tricky forgery attack. Here we present our novel way of breaking Kim et al.'s proposed scheme.

3.1 Our Novel Forgery Attack

An attacker can impersonate a legitimate user U_i, with identity ID_i, by using the following procedure:

Step 1. It Intercepts the login request message $M = \{ID_i, CID_i, X_i, Y_i, n, e, g, T\}$.

Step 2. Computes, $ID_f = ID_i^{-1} \bmod n$

Step 3. The attacker submits identity ID_f and a random value as his password to the KIC to obtain a valid smart card with information $\{n, e, g, ID_f, CID_f, S_k, h_k\}$.

Step 4. Since, in the registration phase, $S_i = ID_i^{CID_f \cdot d} \bmod n$ and here, $S_k = ID_f^{CID_f \cdot d} \bmod n = ID_i^{-CID_f \cdot d} \bmod n$, the attacker can compute S_i as, $S_i = S_k^{-1} \bmod n$

Step 5. Then, the attacker chooses a random integer y.

Step 6. Sets, $X_f = 1$ and $Y_f = S_i^{T_f} \bmod n$, where T_f is the timestamp for the login request from the attacker and sends the forged login message, $M_f = \{ID_i, CID_i, X_f, Y_f, n, e, g, T_f\}$. The request is validated as the login request from the user U_i because,

$$
\begin{aligned}
Y_f^{\,e} &= (S_i^{T_f})^e \bmod n \\
&= S_k^{-T_f \cdot e} \bmod n \\
&= ID_i^{CID_f \cdot d \cdot e \cdot T_f} \bmod n \\
&= ID_i^{CID_f \cdot T_f} \bmod n
\end{aligned}
$$

and,

$$
\begin{aligned}
X_i^{\,d} \cdot ID_i^{CID_f \cdot T_f} \bmod n &= (1) \cdot ID_i^{CID_f \cdot T_f} \bmod n \\
&= ID_i^{CID_f \cdot T_f} \bmod n
\end{aligned}
$$

3.2 Fixing Up the Vulnerability

This vulnerability could be circumvented by imposing an extra step in the verification phase to check the values of the parameters passed via the login request message. That is, in the step 1 of authentication phase, the sent value of X_i is to be checked and if it equals to 1 in any login request message, the message should be rejected without further processing. This simple amendment could in fact reduce the probability of forgery attacks as the scheme is already proven to be resistant to other known forgery attacks.

After the modification

The User sends the login request message $M = \{ID_i, CID_i, X_i, Y_i, n, e, g, T\}$ to the server in the login phase.

Verification Phase. Server receives the message M and carries out the following steps:

Step 1. Checks the validity of ID_i and CID_i. If the format of any of these is incorrect, the server rejects the request. Checks whether $X_i = 1$ or not. If so, rejects the request. Otherwise, proceeds through the rest of the steps.

Step 2. Checks whether the condition $(T' - T) \le \Delta T$ holds or not, where T' is the timestamp of receiving the login request message and ΔT is the legitimate time interval allowed for the transmission delay. If it is negative, the server rejects the request.

Step 3. Checks the equation, $Y_i^e = X_i^{\,d} \cdot ID_i^{\,CID_i \cdot T} \bmod n$. If it holds, then the remote server accepts the login request and gives access to the U_i. Otherwise, it rejects the login request.

4. CONCLUSIONS

In this paper, we have shown that, Kim et al.'s scheme is still vulnerable and fails to achieve the level of security required for remote password authentication procedure. We also have suggested the solution to fix up the flaw of their scheme, which could effectively make the scheme more robust so that no known attack could be used to break the security for the remote communication procedure.

References

1. Kim, K.-W., Jeon, J.-C., and Yoo, K.-Y.: An improvement on Yang et al.'s password authentication schemes. Applied Mathematics and Computation, 170 (2005) 207-215.
2. Yang, C. C., Wang, R.-C., and Chang, T.-Y.: An improvement of the Yang-Shieh password authentication schemes. Applied Mathematics and Computation 162 (2005) 1391-1396.
3. Sun, H.-M. and Yeh, H.-T.: Further Cryptanalysis of a Password Authentication Scheme with Smart Cards. IEICE Transactions on Communications, Vol. E86-B, No. 4 (2003) 1212-1215.
4. Yang, C.-C., Yang, H.-W., and Wang, R. C.: Cryptanalysis of Security Enhancement for the Timestamp-Based Password Authentication Scheme using Smart Cards. IEEE Transactions on Consumer Electronics, Vol. 50, No. 2 (2004) 578-579.