New Cryptanalysis of an ID-based Password Authentication Scheme using Smart Cards and Fingerprints

MING-JHENG LI
Department of Computer Science and Information Engineering, National Chi Nan University, Nantou, Taiwan, R.O.C.
s3321908@ncnu.edu.tw

JUSTIE SU-TZU JUAN*
Department of Computer Science and Information Engineering, National Chi Nan University, Nantou, Taiwan, R.O.C.
jsjuan@ncnu.edu.tw

*Correspondence author

Abstract:
In 2002, Lee, Ryu and Yoo proposed a fingerprint-based remote user authentication scheme using a smart card. Their scheme would strengthen system security by verifying the smart card owner’s fingerprint. In 2003, Kim, Lee and Yoo proposed two ID-based password authentication schemes without passwords or verification tables, with smart card and fingerprints. The proposed nonce-based and timestamp-based schemes can withstand message replay attacks. In addition, the schemes can withstand impersonation attack. In this paper, we will first review Kim et al.’s ID-based password authentication schemes. Next, we will show that Kim et al.’s scheme still has the disadvantage of being vulnerable to impersonation attack.

Keywords: ID-based scheme; Fingerprint; Password authentication; Smart cards; Impersonation attack.

1. Introduction

Recently, remote user authentication has become an important technique in modern computer network systems, in which, it is used to validate the legitimacy of a remote login user. In a client/server system, when the client wants to login to a remote server, the remote server requires a password to authenticate the identity of the client. So far, multi-user authentication schemes for password or multimedia data have been proposed. In traditional password authentication scheme, a number of remote users/servers have to be able to access/authenticate the server/users with his/her identity and password. In 1981, Lamport [10] first proposed a remote password-based authentication scheme that could authenticate remote users over an insecure channel. In Lamport’s scheme, a remote host system was able to authenticate the remote login users based on identity and password. The password-based authentication schemes with smart card are an important part of security for accessing remote servers. A lot of password authentication schemes using smart cards have been proposed [1, 2, 3, 5, 6, 7, 9, 10, 11, 13, 15, 16, 17, 21]. However, their scheme requires a password table to authenticating the legitimacy of the user. In 1984, Shamir [15] first proposed ID-based cryptosystems. In Shamir’s scheme, the public key directory table is not needed, and the assistance of a trusted third party is not required. In 1990, Hwang, Chen and Laih [5] proposed a non-interaction password authentication scheme without a password table based on Shamir’s ID-based cryptosystem. The advantages of smart cards are their storage and computation abilities. These advantages are always advocated by some scholars [1, 6, 9, 16, 18, 19]. So far, there are many user authentication schemes using smart card that have been proposed, such as [1, 2, 4, 6, 13, 17, 21].

In recently times, bio-information has been playing an important role in modern user authentication schemes, such as fingerprint, iris, voice, face etc. A lot of user authentication schemes using bio-information have been proposed [12, 13, 20, 22]. In 2002, Lee, Ryu and Yoo [11] first proposed a fingerprint-based remote user authentication scheme using a smart card. The authentication scheme, which does not require a passwords table to authenticate its users, is proposed. By removing the password table and introducing smart card and fingerprint verification, it is hoped the scheme can be more secure and reliable. In addition, the scheme is supposed to withstand message replaying and impersonation attacks. In their scheme, they store two secure keys and some public elements in the smart card, but their scheme is still not safe against impersonation attack [8].
Thus, the scheme is unworkable [3]. In 2003, Kim, Lee and Yoo [7] proposed two ID-based password authentication scheme using smart cards and fingerprints based on [11]. Their scheme can withstand message replays attacks through being nonce-based and timestamp-based. Furthermore, Kim et al. mentioned that their scheme can withstand impersonation attack without password table. Unfortunately, Scott [14] pointed out that Kim et al.’s scheme was still insecure. In this paper, we also show why the scheme can not withstand impersonation attack.

In this paper, we shall show that Kim et al.’s scheme [7] is insecure in this scheme. In Section 2, we will first review Kim et al.’s scheme. In Section 3, we will present a cryptanalysis of Kim et al.’s authentication scheme by showing that their scheme is still vulnerable to impersonation attack. Finally, we will draw some conclusions.

2. Review of Kim, Lee and Yoo’s scheme

In this section, we briefly describe Kim, Lee and Yoo’s ID-based password authentication scheme using a smart cards and fingerprints.

2.1. Notations

The following notations are used throughout this paper.

$S$, $U_i$: a system center and user $i$.
$ID_i$: public user identity of a user $U_i$ (or client).
$PW_i$: secret and possibly weak password of a user $U_i$.
$SK$: the system’s secure key.
$PK$: the system’s public key, $PK = g^{SK} \mod n$.
$n$: a large prime number.
$g$: a generator with order $n − 1$ in $\mathbb{Z}_n^*$. 
$f$: a one-way function.
$f(x, y)$: a one-way hash function of input two parameters $x$ and $y$.
$T$: the timestamp.
$CID_i$: the smart card identity of the user $U_i$.

2.2. Kim, Lee and Yoo’s authentication scheme

In this section, we briefly describe Kim et al.’s ID-based password authentication scheme using a smart card and fingerprints [7]. The proposed nonce-based and timestamp-based schemes can withstand message replay attacks. The two schemes consist of three phases: (i) the registration phase, (ii) the login phase, and (iii) the verification phase. In the registration phase, the system issues a smart card to legitimate users who request registration. In the login phase, the user inserts his/her smart card into the card reader. Then user then keys in his/her identity and password, and imprints his/her fingerprints on the fingerprint input device. In the verification phase, the remote sever can verify the login to see whether it should be accepted or not. For withstand message replays attacks, Kim et al. proposed two schemes. One scheme is timestamp-based, and the second uses a nonce for the same purpose. Because Kim et al.’s two schemes not all suffers from the impersonation attack. So, we describe our impersonation attack on the timestamp-based authentication scheme, although it also applies to the timestamp version. The Timestamp-based authentication scheme consists of three phases, registration, login, and verification. We review these three phases in the following:

(i) Registration phase

In this phase, a new user $U_i$ submits his/her identity $ID_i$ and password $PW_i$ to the system for registration. The registration performs the following steps.

1. The user $U_i$ first chooses his/her identity $ID_i$ and password $PW_i$, and sends them to a system center $S$ in a secure channel.
2. Next, the system generates the smart card identity $CID_i$ of $U_i$, and computes
\[ S_i = ID_i^SK \mod n \]  
\[ h_i = g^{r_iSK} \mod n \]  
\[ = PK^{r_i} \mod n . \] (2)

3. Finally, system stores \( n, g, f, ID_i, CID_i, S_i \) and \( h_i \) to the smart card and issues to \( U_i \), where \( f \) is a one-way function. Then, the system registers \( U_i \) to the smart card of \( U_i \).

(ii) Login phase

When \( U_i \) wants to login to the system at time \( T_1 \), he/she inserts his/her smart card into the card reader to login. Key in his/her \( ID_i \) and \( PW_i \), then imprints \( U_i \)'s fingerprints on the fingerprint input device. If the fingerprint authentication is successful, the smart card performs the following steps.

1. Generate a random number \( r \) using the co-ordinate of minutia of input fingerprint. Whenever a fingerprint is input, a different map of minutia is made. Therefore, the input map could be used as a one-time random number.
2. After that, the smart card computes:

\[ X_i = g^{r_iPW} \mod n \] (3)

\[ Y_i = S_i \cdot h_i^{f(CID_i,X_i)} \mod n \] (4)

3. Finally, the smart card sends \( M = \{ID_i, CID_i, X_i, Y_i, T_1\} \) to the remote server.

(iii) Verification phase

When the remote system receives the login request \( M = \{ID_i, CID_i, X_i, Y_i, T_1\} \) at time \( T_2 \), where \( T_2 \) is the current timestamp of the system. The remote system then performs the following steps to authenticate the valid remote login user.

1. The system checks the \( ID_i \) and \( CID_i \), respectively. If it holds, the system accepts the login request. Otherwise, the login request is rejected.
2. Check the validity of the timestamp \( T_1 \). If \( (T_2 - T_1) > \Delta T \), where \( \Delta T \) denotes the expected valid time interval for transmission delay, then the system rejects the login request.
3. Check whether the following equation holds:

\[ Y_i^{SK} \cdot X_i^{f(CID_i,X_i)} \mod n \] (5)

If it holds, the system accepts the login request. Otherwise, the login request is rejected.
4. Finally, \( U_i \) inputs his/her \( PW_i \) into the smart card then computes:

\[ h_i' = PK^{PW_i} \mod n \] (6)

and checks:

\[ h_i = h_i' \mod n \] (7)

If it holds, the system accepts the login request. Otherwise, the login request is rejected.

3. Cryptanalysis of the Kim, Lee and Yoo’s scheme

In this section, we shall present an impersonation attack on Kim et al.’s scheme off-line. Off-line means that the user can successfully login without inserting his/her smart card into the card reader. The impersonation attack means that several users to try to forge another valid \( ID \) and \( PW \) without actually having the other user’s \( ID \) and

ISSN: 0975-5462 6842
PW. Suppose an adversary $U_a$ wants to impersonate another valid user on off-line without knowing the PW of the valid user. Next, we describe the cryptanalysis as follows.

1. First, $U_a$ obtains the $ID_i$ of $U_i$ by eavesdropping on the login request message $M$.
2. Then, $U_a$ picks a random integer $k$, and computes $U_a$’s identity.
   \[ ID_a = ID_i^k \mod n. \]
3. After that, $U_a$ registers the $ID_a$ to the remote system ($PW_s$ without concern). Therefore, $U_a$ can receive $S_i = (ID_i^k)^m \mod n$ from the remote system in the registration phase. By equation (1), $U_a$ can easily compute:
   \[ S_i = (S_i^k)^{1/k} \mod n. \]
4. Thus, $U_a$ has known the $S_i$ of $U_i$. Then $U_a$ computes:
   \[ X'_i = ID_i \mod n, \]
   \[ Y'_i = S_i \cdot S_i^{(CID_s \cdot U)} \mod n. \]

Then, the adversary $U_a$ sends the forged login request $M' = \{ID_a, CID_a, X'_i, Y'_i, T_1\}$ to the remote server, where $U_a$ can successfully pass the verification equation as follows:

\[
(Y'_i)^{1/k} = (S_i \cdot S_i^{(CID_s \cdot U)})^{1/k} \\
= (ID_i^k \cdot ID_i^{X'_i \cdot CID_s \cdot U})^{1/k} \\
= ID_i \cdot ID_i^{X'_i \cdot CID_s \cdot U} (\mod n). 
\]

As a result, $U_a$ can pass his/her one smart card fingerprint verification and easily impersonate many valid users without the $ID$ and $PW$ of many valid users. Because our impersonation attack is off-line, $U_a$ can therefore successfully pass the verification equation without going through the four verification phases. In addition, the system does not store any interrelationship between the user’s identity $ID$ and the smart card number $CID$ in Kim et al.’s authentication scheme. Therefore, $U_a$ can pass the verification phase and only requires the $UID_a$ to be put into the forged login request $M' = \{ID_a, CID_a, X'_i, Y'_i, T_1\}$. However, $U_a$ can pass the verification phase even though the system stores any interrelationship between user’s identity $ID$ and smart card number $CID$. We can obtain the $CID$, from $M = \{ID_a, CID_a, X_i, Y_i, T_1\}$, and put the $CID_a$ into the forged login request $M'' = \{ID_a, CID_a, X'_i, Y'_i, T_1\}$, then $U_a$ can still pass the verification phase.

4. Conclusion

In 2003, Kim et al. proposed a two ID-based password authentication scheme using a smart card and fingerprints. They declared their scheme can withstand replay and impersonation attacks without the need for a password table. In this paper, we presented a cryptanalysis of Kim et al.’s authentication scheme by showing that their scheme is insecure. It is still vulnerable to impersonation attack. However, bio-information is really playing an important role in modern user authentication schemes. In the future, we will try to improve Kim et al.’s authentication scheme and propose an enhanced scheme which improves on Kim et al.’s authentication scheme.

Acknowledgment

This research was supported in part by the National Science Council of the Republic of China under grant NSC-99-2628-E-260-011-.
References