A flexible biometrics remote user authentication scheme

Chu-Hsing Lin*, Yi-Yi Lai

Department of Computer Science and Information Engineering, Box 809, Tunghai University, 181 Section 3, Taichung-kang Road, 407, Taichung, Taiwan

Received 2 December 2003; received in revised form 6 March 2004; accepted 10 March 2004
Available online 2 April 2004

Abstract

Recently, Lee, Ryu and Yoo proposed a fingerprint-based remote user authentication scheme by using smart cards and biometrics. Their scheme is based on two tiers of ElGamal’s private key cryptosystem and fingerprint verification. The scheme is novel by introducing biometrics verification technology into authentication scheme using smart cards. In this paper, we point out that their scheme is vulnerable to masquerade attack. We propose a new scheme to enhance their security. Furthermore, by using our scheme, users can conveniently choose and change their passwords. Our scheme is suitable for applications with high security requirement.

Keywords: Fingerprint verification; Biometrics; User authentication; Smart cards; Masquerade attack; Minutiae extraction; Minutiae matching

1. Introduction

In a traditional password authentication scheme, a system server has to be able to authenticate a remote logon based on identity and password. In 1981, Lamp- ort [1] proposed a remote password authentication scheme that could authenticate remote users over an insecure channel. In 1990, Hwang et al. [2] proposed a noninteractive password authentication without password tables based on Shamir’s ID-based signature. In 2000, Hwang and Li [3] proposed a new remote user authentication scheme using smart cards based on ElGamal’s [4] cryptosystem. Hwang and Li’s scheme only has to maintain a secret key without storing a password table in the system, but this scheme could not withstand masquerade attack. In 2000, Chan and Cheng [5] pointed out a cryptanalysis of Hwang and Li’s scheme. In Electronics Letters, Lee et al. [6] proposed a biometrics remote user authentication scheme using smart cards. The Lee–Ryu–Yoo scheme was also based on the ElGamal’s public key cryptosystem with two secret keys. In addition, the Lee–Ryu–Yoo scheme strengthened the system security by verifying the smart card owner’s fingerprint. Their fingerprint verification method is based on minutiae extraction and matching [7,8]. However, we will address that their scheme cannot withstand masquerade attack by using two secret keys and fingerprint verification. Moreover, one common problem of the above-mentioned schemes is that the users are not allowed to choose and change their own passwords flexibly.

In this article, we point out that the Lee–Ryu–Yoo scheme has weakness in security. We propose
an improved scheme to enhance the security, which allows the users to choose and change their password conveniently. Based on ElGamal’s cryptosystem and the fingerprint verification, our scheme needs only to maintain one secret key, without verification tables such as password and identity tables. The scheme we proposed can withstand the masquerade attack even if the intruder wangles a legal user’s smart card and password. For the reason, our scheme is suitable for applications with high security requirement.

The remainder of this paper is organized as follows. In Section 2, we will review the Lee–Ryu–Yoo scheme. In Section 3, we propose a cryptanalysis of the Lee–Ryu–Yoo scheme. In Section 4, we present our scheme and give the security analysis. In Section 5, we have a conclusion.

2. The Lee–Ryu–Yoo scheme

In this section, we briefly review the Lee–Ryu–Yoo scheme. The security of Lee–Ryu–Yoo scheme is based on the ElGamal’s public key cryptosystem with two secret keys. Moreover, the scheme stores public elements on a smart card and each user accesses his/her smart card by identifying his/her own fingerprint. The fingerprint verification method is based on minutiae extraction and matching. A different map of minutiae will be made when the input device takes a smart card owner’s fingerprint. Then the scheme can generate a one-time random number for the ElGamal’s public key cryptosystem by using the map of minutiae.

There are three phases in the Lee–Ryu–Yoo scheme including a registration phase, a login phase and an authentication phase. Before accessing a remote system, a new user has to personally imprint his/her fingerprint on the input device and offer his/her identity to the system in the registration center. We review these three phases in the following:

2.1. Registration phase

Let $P$ be a large prime number and $f(\cdot)$ a one-way function. $U_i$ denotes a legal user. ID$_i$ and PW$_i$ denote $U_i$’s identity and password, respectively. Assume that a new user $U_i$ offers his/her ID$_i$ to the system for registration. The system computes $U_i$’s password PW$_i$ as follows:

$$\begin{align*}
\text{ID}_i &= (\text{ID}_i)^{\text{SK1}} \mod p \\
\text{PW}_i &= (\text{ID}_i)^{\text{SK2}} \mod p
\end{align*}$$

(1)

where SK1 and SK2 are two secret keys maintained by the system. The registration center stores the public parameters $(f, P)$ on $U_i$’s smart card and delivers PW$_i$ to the user $U_i$ through a secure channel. The smart card contains public element $(f, P)$ and user’s fingerprint data. $U_i$ has his/her own smart card that can authenticate his ownership by matching the fingerprint from the extracted minutiae.

2.2. Login phase

In this phase, the login user $U_i$ first inserts his/her smart card to the card reader and inputs $U_i$’s identity ID$_i$ and password PW$_i$, then $U_i$ imprints his/her fingerprint on the input device. If $U_i$ passes the fingerprint verification [9], the smart card performs the following operations:

1. Generate a random number $r$ using the minutiae extracted from the imprint fingerprint.
2. Compute $C_1 = (\text{ID}_i)^r \mod P$.
3. Compute $t = f(T \oplus \text{PW}_i) \mod (P-1)$, where $T$ is the current timestamp of the input device and $\oplus$ denotes an exclusive or.
4. Compute $M = (\text{ID}_i)^t \mod P$.
5. Compute $C_2 = M(\text{PW}_i)^r \mod P$.
6. Send the message $C = (\text{ID}_i, C_1, C_2, T)$ to the remote system.

2.3. Authentication phase

After transmission delay, the system receives the message $C$ at $T'$, where $T'$ is the receiving timestamp of the system. The system then performs the following operations:

1. The system checks the validity of ID$_i$. If the format of ID$_i$ is incorrect, then the system rejects the login request.
2. If $(T' - T) \geq \Delta T$, where $\Delta T$ denotes the expected valid time interval for transmission delay, the system rejects the login request.
3. If \( C_2(C_1^{SK2})^{-1} \mod P = (ID_i^{SK1})^{(T\oplus PW)} \), the system accepts the login request. Otherwise, the system rejects the login request.

3. Cryptanalysis of the Lee–Ryu–Yoo scheme

In this section, we shall present a masquerade attack on the Lee–Ryu–Yoo scheme. A legitimate user who registers a legal pair of identity and password can pass the fingerprint verification of his/her own smart card and easily masquerade another valid pair of identity and password without knowing the two secret keys of the remote system. We describe the cryptanalysis as follows.

For a legal user \( U_i \), the remote system issues him/her a password and a smart card if the registration is successful. Note that for a legal user \( U_i \), the pair of \((ID_i, PW_i)\) satisfies the following equations:

\[
\begin{align*}
ID_i &= (ID_i)^{SK1} \mod p \\
PW_i &= (ID_i)^{SK2} \mod p = (ID_i)^{SK1\cdot SK2} \mod p
\end{align*}
\]

(2)

Now, assume that \( U_i \) wants to masquerade another pair of valid \((ID_d, PW_d)\) of a legal user \( U_d \). We show that \( U_i \) can compute \( PW_d = (ID_d)^{SK1\cdot SK2} \mod P \) without knowing the two secret keys \( SK1 \) and \( SK2 \). \( U_i \) first computes \( ID_d = ID_i^q \mod P \), where \( q \) is a random number with \( 1 < q < P \). As \( U_i \) does not know the two secret keys \( SK1 \) and \( SK2 \) of the remote system, \( U_i \) cannot derive \( PW_d \) directly from \( ID_d \). However, \( U_i \) can compute the correct \( PW_d \) corresponding to \( ID_d \) as follows:

\[
PW_d = (ID_d)^{SK1\cdot SK2} \mod P
\]

\[
= (ID_i^q \mod P)^{SK1\cdot SK2} \mod P
\]

\[
= (ID_i)^{SK1\cdot SK2} \mod P
\]

\[
= (ID_i)^{SK1\cdot SK2} \mod P^q \mod P
\]

\[
= (PW_i)^q \mod P.
\]

Thus, \( U_i \) can pass his/her own smart card fingerprint verification and easily masquerade many valid pairs of \((ID_d, PW_d)\) that satisfy the authentication phase of \( PW_d = (ID_d)^{SK1\cdot SK2} \mod P \) in the remote system.

4. The enhanced scheme and security analysis

In this section, we propose an improved flexible scheme to enhance the security of the Lee–Ryu–Yoo scheme. Moreover, our scheme allows the users to choose and change their password conveniently.

4.1. Our enhanced scheme

The security of our enhanced scheme is based on the ElGamal’s cryptosystem, fingerprint verification and smart cards. Now, we describe the three phases separately in our scheme as follows:

4.1.1. Registration phase

In this phase, we assume that the format of the user’s identity ID consists of some meaningful information such as names, phone numbers and birthdays etc. A new user \( U_i \) may choose his/her identity ID, and password PW. He/she must personally imprint his/her fingerprint on the input device and offer his/her ID and PW in the registration center.

The system of the registration center performs the following operations:

1. Compute \( PW_i = h(PW_i \oplus S_i) \mod P \), where \( h(\cdot) \) denotes a one-way hash function and \( S_i \) denotes \( U_i \)’s minutiae template and \( \oplus \) denotes an exclusive or.

2. Compute \( Y_i = (ID_i^{SK1} \mod P) \oplus PW_i \), where \( P \) is a large prime number and \( X_i \) denotes the secret key kept securely in the system.

Then, the registration center issues user \( U_i \) a smart card, with \( h, P, Y_i, S_i \) and \( ID_i \) stored on the card.

4.1.2. Login phase

Whenever a user \( U_i \) wants to login, \( U_i \) has to insert his/her own smart card into the card reader and imprint the fingerprint. Then he/she needs only to type in password PW. If \( U_i \) passes the fingerprint
verification, $U_i$’s smart card will perform the following operation:

1. Generate a random number $r$ using the minutiae extracted from the imprint fingerprint. Note that by using the characteristic of fingerprint verification, each time we can generate a different random number.
2. Compute $PW_i^r = h(PW_i \oplus S_i) \mod P$, where $S_i$ is $U_i$’s fingerprint minutiae template stored on smart card.
3. Compute $Y_i' = Y_i \oplus PW_i^r$.
4. Compute $C_1 = (ID_i)^{Y_i'} \mod P$.
5. Compute $M = h(Y_i' \oplus T) \mod P$, where $T$ is the current timestamp of the login device.
6. Compute $C_2 = (Y_i')^M \mod P$.
7. Send a message $C = (ID_i, C_1, C_2, T)$ to the remote system.

**4.1.3. Authentication phase**

After transmission delay, the system receives the message $C$ at $T'$, where $T'$ is the receiving timestamp of the system. The system then performs the following operations:

1. The system checks whether the format of $ID_i$ is correct or not. If the format is incorrect, the system rejects the login request.
2. If $(T' - T) \geq \Delta T$, where $\Delta T$ denotes the expected valid time interval for transmission delay, the system rejects the login request.
3. Verifying whether $C_2 \cdot (C_1^{X_S})^{X_i^{-1}} \mod P = h((ID_i)^{X_S} \mod P) \oplus T) \mod P$, if being successful, the system accepts the login request. Otherwise, the system rejects the login request.

**4.2. Change password**

Whenever a user $U_i$ decides to change the old password $PW_i$ to a new password $PW_i^*$, he/she has to imprint his/her fingerprint, then the smart card compares it with the minutiae template stored on the card. After $U_i$ passes fingerprint verification, he/she inputs the old password $PW_i$ and the new password $PW_i^*$. The client device performs the following operations:

1. Compute $PW_i^{*r} = h(PW_i^* \oplus S_i) \mod P$, where $S_i$ is $U_i$’s minutiae template stored on the smart card.
2. Compute $Y_i^* = Y_i^* \oplus PW_i^{*r} = ID_i^{X_S} \mod P$.
3. Compute new $Y_i^* = Y_i^* \oplus h(PW_i^* \oplus S)$
4. Replace the old $Y_i$ with the new $Y_i^*$ on the smart card.

**4.3. The security analysis of our scheme**

We show that how our scheme withstands the attacks as follows:

1. Because our scheme is based on ElGamal’s cryptosystem and fingerprint verification, from Step 2 in the registration phase, the complexity of computing $X_r$ from $Y_i$ is a discrete logarithm problem. It’s also difficult for the intruder to obtain simultaneously the $U_i$’s password $PW_i$ and fingerprint minutiae $S_i$ to compute $Y_i^*$.
2. An intruder may try to derive a random number $r$ directly from the Step 4 in the login phase. The complexity of computing the random number $r$ from $C_1$ is also a discrete logarithm problem. Note that the random number is generated by using the coordinate of imprint fingerprint minutiae. This method can generate a one-time random number because the picture of matched minutiae is always different [6].
3. Replay attack can be prevented by checking time stamp at Step 2 in the authentication phase. An intruder may try to modify $T$ to achieve the replay attack. It does not work unless he/she also modifies $C_2$ to a correct value. But it’s difficult to modify $C_2$ correctly without knowing $Y_i^*$ and the random number $r$.
4. In case the intruder can wangle the legal user’s smart card and password, he/she still cannot pass the fingerprint verification in login phase. On comparing intruder’s fingerprint minutiae with the minutiae template stored on the smart card, the illegal access will be rejected.

**5. Conclusion**

In this paper, we present a cryptanalysis of the Lee–Ryu–Yoo scheme by showing that their scheme is vulnerable to masquerade attack. Moreover, our scheme allows users to choose and change their passwords conveniently. Based on the fingerprint verification, our scheme needs only to maintain one secret key,
without verification tables such as password tables and identity tables. The scheme we proposed can withstand the masquerade attack and is suitable for applications with high security requirement.

Acknowledgements

This research was partially supported by the National Science Council, Taiwan, under grant NSC92-2213-E-029-017.

References


Chu-Hsing Lin received his BS degree in applied mathematics from National Tsing Hua University in 1980, his MS degree, also in applied mathematics, from National Chung Hsing University in 1987, and his PhD degree in computer sciences from National Tsing Hua University in 1991. From 1983 to 1985, he worked for the Information Department of the Land Bank of Taiwan, joining the team for developing the software system. Now, Dr. Lin is a professor of the Department of Computer Science and Information Engineering, Tunghai University. From 1995 to 1999, he has been the Director of Computer Center at the university. From 2001 till now, he has been one of the Board Directors of the Chinese Cryptology and Information Security Association (CCISA). He was the winner of the 1991 Acer Long-Term Award for Ph.D. Dissertation. His current research interests include information security, cryptology, data engineering, and electronic commerce.

Yi-Yi Lai received the BS degree in Information Engineering and Computer Science from Fengchia University, Taichung City, Taiwan in 1995. He is currently pursuing his master degree in Computer Science and Information Engineering at Tunghai University. His research interests include fingerprint verification system and password authentication scheme.