Robust ECC-based three factor user authentication preserving biometric privacy

Tien-Ho Chen¹, Hsiu-Lien Yeh², Kuwei-Jung Hu³, Wei-Kuan Shih⁴

¹,³,⁴ Department of Computer Science, National Tsing Hua University, Taiwan
² Institute of Information System and Applications, National Tsing Hua University, Taiwan
d918325@oz.nthu.edu.tw, s9865805@m98.nthu.edu.tw, s9962629@m99.nthu.edu.tw, wshih@cs.nthu.edu.tw

Abstract— Recently, to achieve privacy protection using biometrics, Fan-Lin proposed a three-factor authentication scheme based on password, smart card and biometrics. However, we have found that Fan-Lin’s proposed scheme has flaws in the design of biometrics privacy, fails to maintain a verification table, making it vulnerable to stolen-verifier attack and modification attack, and is vulnerable to insider attacks. Thus, we propose an ECC-based authentication scheme that is improved with regard to security requirements. Our proposed scheme overcomes the flaws of Fan-Lin’s scheme and is secured from attacks. Furthermore, we present a security analysis of our scheme to show that ours is suitable for the biometric systems.

Keywords— Security; ECC; Biometrics; Authentication

I. INTRODUCTION

With the current advance of network services, proper user identification for remote user authentication over insecure communication channels is increasingly essential. Contrary to traditional password-based remote user authentication, biometrics-based authentication has greater security and is more reliable for remote user authentication [1]. In addition, three-factor authentication schemes have been proposed in many publications [2-6]. Biometrics-based authentication systems are increasingly common for remote user identity authentication schemes. Due to its physiological or behavioral characteristics, remote authentication schemes can provide enhanced security using such techniques as fingerprint verification, iris analysis, facial analysis, and keystroke analysis [1,7].

Recently, Lee et al. [2] proposed a remote user authentication scheme based on smart card and fingerprint without a verification table to maintain records. In [3], we found that Lee et al.’s scheme is vulnerable to the masquerade attacks and replay attacks, and [4,5] showed that Lin-Lai’s scheme is vulnerable to the server spoofing attack and does not provide proper mutual authentication. However, Li et al. [6] point out that Li and Hwang’s scheme [5] fails to provide proper mutual authentication and is vulnerable to man-in-the-middle attacks. Unfortunately, the Li et al.’s scheme fails to securely update the new password and is also insecure.

The above mentioned schemes consider privacy protection using biometrics on the user’s side without considering biometric characteristics on the server’s side. For privacy protection using biometrics, the biometric data and settings have to be considered. Some methods, such as those based on error-correcting codes and fuzzy encryption, use biometric data to key encrypt a secret and then match the biometric template after extracting the secret. In Fan and Lin’s scheme [7], user data is only stored on the user’s side while still permitting the server to perform the authentication. Despite the benefits of Fan and Lin’s scheme, it is still subject to privacy and security threats. It is obvious that Fan-Lin et al.’s schemes need to maintain a verification table in order to provide protection from inside attacks. In this paper, our authentication scheme employs a different approach. We improve the Fan et al.’s scheme and enhance the security and privacy protection. This leads to a robust three-factor remote authentication protocol based on the Elliptic Curves Cryptosystem (ECC).

The remainder of this paper is organized as follows. In section 2, we analyze the Fan and Lin’s scheme. In section 3, we propose a robust three factor biometric-based authentication scheme with ECC. Then, in section 4, we provide the security analysis and comparisons. Finally, we present some concluding remarks in section 5.

II. CRYPTANALYSIS OF FAN-LIN’S SCHEME

In this section, we have analyzed the security flaws of Fan et al.’s scheme. First, we summarize the notations used throughout this paper as follows.

- \( U_i \): The ith user
- \( \text{ID}_i \): The identity of the user \( U_i \)
- \( \text{PW}_i \): The password of \( U_i \)
- \( h(\cdot) \): A public one-way hash function
- \( \| \) : String concatenation operation
- \( E(\cdot) \): A symmetric encryption function
- \( k \) : A symmetric encryption function
- \( \oplus \) : The function of XOR operation with secret key \( k \)
- \( S_i \) : The Iris template of the user \( U_i \)
- \( E_{S_i}(\cdot) \) : Encryption function with biometric template \( S_i \)
- \( r \) : A random string
- \( A \) : An extracting algorithm
- \( \oplus \) : A string XOR operation
- \( \rightarrow \) : A common channel
- \( \Rightarrow \) : A secure channel

A. Assumption 1

If the adversary successfully manages the server under owning the right of authentication, the adversary can request to login procedure and pass the authentication. Furthermore, the \( y_i = E_{S_i}(\text{ID}_i \| h(\text{PW}_i) \| S_i) \) will be easily retrieved by the adversary due to the identity stored in a verification table. However, a verification table suffers easily from an adversary’s attacks, and further is unable to resist the stolen-verifier attack and modification attack.
B. Assumption 2

Assume that an adversary uses the SID to impersonate SID and replays messages to the remote server to encrypt CI with a random string v. Then, the remote server sends the messages to the user. Until the user’s smart card accepts the pretended SID. Thus, a user will encrypt the function with adversary’s random string v and sends the encryption messages to an adversary. The remote server can be accepted by an adversary’s login request because he/she owns the password and biometrics.

C. Assumption 3

Registration phase, a user Ui has an identity IDi to register the license for remote server. Additionally, the Fan-Lin’s scheme must store IDi to a verification table inside remote server. And then the remote server can perform to check whether the IDi is legimitacy during the authentication phase. When Ui want to register to more than one server with the same identity IDi and authentication key h(PW), any server can impersonate the eligible user and access other servers to obtain a login request. Obviously, the insider attack is possible in the assumption.

III. THE PROPOSED SCHEME

We propose a robust three-factor authentication scheme with Elliptic Curves Cryptosystem (ECC) for the network communication. A three-factor authentication scheme involves a client, a server, and consists of four phrases: initiation phase, registration phase, login phase and authentication phase.

A. Initiation Phase

In the system initiation phase, the server sets up the following system parameters for session key generation:

1) The user and server choose an elliptic curve order n over \( E_p(a, b) \) generated by P, where n is a large prime number for the security considerations.
2) The server computes the corresponding public key \( Q_s = q_s \times P \).
3) The server employs the MD5 one-way hash function \( h(\cdot) \).
4) The smart card is prestored with the secret parameters \( \{W, h(\cdot), P, Q_s\} \) in user and server side respectively, and the encryption function \( \delta(S) \) is prestored in users’ smart card.

B. Registration Phase

The Ui wants to register to the remote server and setup the secret codes into the smart card for the Ui.

1) Step 1: \( U_i \rightarrow \text{server} : \{ID_i, h(PW_i \oplus r), \delta(S_i)\} \)

The \( U_i \) enters his/her username IDi and password PW_i for computing \( h(PW_i \oplus r) \). Here, \( U_i \) scans the biometric characteristic as a template \( S_i \) and chooses a random string \( r \) to encrypt as \( \delta(S_i) = r \oplus S_i \) using an encryption key \( S_i \).

C. Login Phase

After receiving the login request from the user, the server computes the following formulas for the authentication procedure. Recall that \( Q_s \) is the server’s public key in the system initiation phase. \( Q_s = q_s \times Q_s, M_s = N_s \times Q_s \times Q_s, \) where \( N_s \) is chosen by Siemens which is provided by \( U_i \). Then, \( U_i \) sends the message \( m_1 = \{Q_s, Q_s, M_s\} \) to the server.

2) Step 2: \( U_i \rightarrow \text{server} : m_2 = \{Q_s, M_s, Q_s, Q_s\} \)

The user \( U_i \) randomly chooses a private key \( q_s = r_s^* \) and computes \( Q_s = q_s \times P \). The server computes the following formulas for the authentication procedure. Recall that \( Q_s \) is the server’s public key in the system initiation phase. \( Q_s = q_s \times Q_s, M_s = N_s \times Q_s \times Q_s, \) where \( N_s \) is chosen by Siemens which is provided by the server. Then, the server sends the message \( m_3 = \{Q_s, M_s, Q_s\} \) to the server.

3) Step 3: \( U_i \rightarrow \text{server} : m_4 = \{L = N_s \times Q_s \times Q_s\} \)

After receiving the message \( m_4 \), the server computes \( Q_s = q_s \times P \) and \( T_s = N_s \times Q_s + Q_s \times Q_s \) and \( M_s = N_s \times Q_s + Q_s + Q_s \) where the \( N_s \) is chosen by SID which is provided by the server. Then, the server sends the message \( m_5 = \{T_s, M_s, Q_s\} \) to the server.

4) Step 4: \( U_i \rightarrow \text{server} : m_5 = \{L = N_s \times Q_s + Q_s\} \)

After receiving the message \( m_5 \), the server computes \( N_s \times Q_s \times Q_s \) and checks whether \( N_s \times Q_s \times Q_s = T_s - Q_s \times Q_s \) is correct. If it holds true, the \( m_5 \) message surely comes from the server, otherwise, the verification is failure. \( U_i \) computes \( N_s = M_s -
$Q_5 = Q_1 - N_s^*$ and $L = N_s^* + Q_6 + Q_3$, and then sends the $m_3$ message \{L = N_s + Q_4 + Q_1\} to the server.
5) Step5: Server checks $N_s$.

The remote server compares $N_s$ with computed $N_s^{**} = L - Q_5 - Q_3$, and these two are the same. If it holds true, the server accepts the $U_i$'s login request. Otherwise, the server rejects the login request.

IV. SECURITY ANALYSIS AND COMPARISONS

A. Security Against the Diverse Attacks
1) Proper mutual authentication: Our authentication scheme is based on ECC and provides the proper mutual authentication between the user and the server. In login phase, the user’s password can be verified by the server computing $W = h(\langle P \oplus h(PW'_i \oplus r) \rangle)$. During authentication phase, the user $U_i$ sends the $m_1$ message to the remote server. The server first validates whether the $N_s^* = N_s$ is equal, then sends the $m_2$ message \{T_s, M_s, Q_s\} to user $U_i$. Then the user $U_i$ checks the condition whether $N_s^{**} = N_w$. Finally, the server validates whether $N_s^{**}$ is equal to $N_k$.
2) Resist insider attacks: If an adversary masquerades the eligible user to login the system. Note that in our registered phase, a user $U_i$ has the different authentication key for each system or server with the same password $PW_i$. The user $U_i$ computes the authentication key $h(PW'_i \oplus r)$ and access the remote server, where $PW_i$ is chosen by the user $U_i$. Therefore, our scheme can resist insider attacks.
3) Not need of a verification table: Our scheme is based ECC mechanism, and the remote server has no need to store the password or a verification table insider computer. That is, the remote server only maintains the secret parameters. Thus, the proposed scheme can resist the stolen-verifier attack and modification attack.
4) Allow user securely to change or update password: The $U_i$ can compute the new value $h(PW'_i \oplus r)$ and sent the message \{ID_s, h(PW'_i \oplus r), \delta(S)_i\} to the remote server. After receiving the demand for password change, the remote server computes the new value to update $W' = h(\langle P \oplus h(PW'_i \oplus r) \rangle)$ into the smart card.

B. Comparisons

Recall that the scheme of Fan-Li [7] and other [4-6, 8], we compare our scheme with other referenced schemes in security properties and computation cost. Table 1 summarizes the comparisons among our scheme and other referenced schemes. Obviously, our scheme can overcome the security flaws of Fan-Li and other schemes. In terms of the requirements for a remote user authentication scheme, our proposed scheme solves all listed table problems and achieves.

V. CONCLUSIONS

Obviously, biometric-based authentication can assure more reliable authentication than traditional password-based authentication. Additionally, recent concerns in biometric-based authentication focus on the issues of security and privacy protection. In this paper, we propose a robust three-factor remote user authentication scheme based on the ECC. In our assumption analysis, Fan-Lin’s scheme fails to resist insider attacks, stolen-verifier attacks and modification attacks, and has security pitfalls due to storage of a verification table inside the server. In addition, we also found the other referenced schemes to be unsafe. Our proposed scheme can overcome security pitfalls and strengthen the security and privacy protection. Our scheme is practical and suitable for biometrics-based remote authentication.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Proper mutual authentication</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Resist insider attack</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Resist stolen-verifier attack and modification attack</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Without a verification table</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Securely change/update password</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

REFERENCES