Robust ECC-based three factor user authentication preserving biometric privacy

Tien-Ho Chen[1],Hsiu-Lien Yeh[2], Kuei-Jung Hu[3], Wei-Kuan Shih[4]
[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, some 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 *i*th user
- ID_i: The identity of the user U_i
- PW_i: The password of U_i
- h(·): A public one-way hash function
- ||: String concatenation operation
- E(·): A symmetric encryption function
- δ_k : The function of XOR operation with secret key *k*
- S_i: The iris template of the user U_i
- $\mathcal{E}_{Si}(\cdot)$: 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 $y_i = E_x(ID_i || h(PW_i) || SS_i)$ 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 C_1^* 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 U_i has an identity ID_i to register the license for remote server. Additionally, the Fan-Lin's scheme must store ID_i to a verification table insider remote server. And then the remote server can perform to check whether the ID_i is legitimacy during the authentication phase. When U_i want to register to more than one server with the same identity ID_i and authentication key $h(PW_i)$, 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 eligible server randomly selects $q_s \in Z^*_p$ as its own private key, and then computes the point multiplication as user's authentication key. That is, the server computes the corresponding public key $Qs = q_s \times P$.

3) The server employs the MD5 one-way hash function $h(.)$.

4) The smart card is prestored with the secret parameters $\{W, h(.), P, Qs\}$ in user and server side respectively, and the encryption function $\mathcal{E}Si(r)$ is prestored in users' smart card.

B. Registration Phase

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

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

The U_i enters his/her username ID_i 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 $\delta_r(S_i) = r \oplus S_i$ using an encryption key S_i. That is, the user submits his/her ID_i, $h(PW_i \oplus r)$, and $\delta_r(S_i)$ to remote server if the user wants to convert into a new eligible user.

2) Step 2: Server $\Rightarrow U_i$'s smart card: $\{W, h(.), P, Q_s\}$.

After receiving the message from U_i, the server computes $Q_S = q_s \times P$ and $W = h(P \oplus h(PW_i \oplus r))$. Finally, the server stores the secret parameters $\{W, h(.), P, Q_s\}$ to a smart card and issues the smart card to the user over a secure channel.

3) Step 3: The U_i checks the W in the smart card.

U_i 's smart checks whether $W = h(P \oplus h(PW_i \oplus r))$ is correct. If the condition is truth, a user will accept the smart card via a secure channel. Otherwise, the smart card does not come from the server and rejects the smart card.

4) Step4: The sketch $\mathcal{E}_{Si}(r)$ is stored in the smart card using his/her biometric template S_i is an encryption key.

C. Login Phase

1) Step 1: U_i submits a PW_i^* and his/her own biometrics, S_i^*, and the random string $r_i = A(\mathcal{E}_{Si}(r))$ is decrypted by the sketch $\mathcal{E}_{Si}(r)$ function which using S_i^* to retrieve. Then, the smart card will compute the value $SS_i^* = \delta_r(S_i^*) = r_i \oplus S_i^*$.

2) Step 2: The server validates W. The server computes W and validates whether $W = h(P \oplus h(PW_i^* \oplus r_i))$ is correct. If it holds true, the system accepts the login and proceeds the authentication phase. Otherwise, server rejects the login request and authentication is terminated.

D. Authentication Phase

After receiving the login request from the user, the detail descriptions of the authentication phase are described in the following operations.

1) Step 1: $U_i \rightarrow$ Server : $m_1 = \{Q_1, Q_u, M_u\}$.

The U_i randomly chooses a private key $q_u = r_i^*$ and computes $Q_u = q_u \times P$, where Q_u is U_i's public key (Here, let the random string r_i convert to $r_i^* \in Z_p^*$, $r_i^* < n$). And then U_i computes the following formulas for the authentication procedure. Recall that Q_S is the server's public key in the system initiation phase. $Q_1 = q_u \times Q_S$, $M_u = N_u + Q_u + Q_1$, where N_u is chosen by SS_i^* which is provided by U_i. Then, U_i sends the $m_1 = \{Q_1, Q_u, M_u\}$ to the server.

2) Step 2: Server verify whether the m_1 message come from U_i. After receiving the m_1 message, the server computes $Q_S = q_S \times P$ and $Q_1 = q_S \times Q_u$ and then checks whether the $N_u^* = M_u - Q_u - Q_1 = N_u$ is correct. If it holds true, the m_1 message definitely comes from the U_i, otherwise, the verification is failure.

3) Step 3: Server $\rightarrow U_i$: $m_2 = \{T_S, M_S, Q_S^*\}$

The server computes $Q_S^* = q_S^* \times P$ and $T_S = N_u^* + Q_S + Q_1$ and $M_S = N_S + Q_S + Q_1 + N_u^*$ where the N_S is chosen by SID which is provided by the server. Then, the server sends the m_2 message $\{T_S, M_S, Q_S^*\}$ to U_i.

4) Step 4: $U_i \rightarrow$ Server :m_3 $\{L = N_S + Q_u + Q_1\}$

After receiving the m_2 message, U_i computes N_u^{**} and checks whether $N_u^{**} = T_S - Q_S^* - Q_1 = N_u$ is correct. If it holds true, the m_2 message surely comes from the server, otherwise, the verification is failure. U_i computes $N_S^* = M_S -$

$Q_S - Q_1 - N_u^*$ and $L = N_S^* + Q_u + Q_1$, and then sends the m_3 message $\{L = N_S + Q_u + Q_1\}$ to the server.

5) Step5: Server checks N_S.

The remote server compares N_S with computed $N_S^{**} = L - Q_u - Q_1$ 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 $W = h(P \oplus h(PW_i^* \oplus r_i))$. During authentication phase, the user U_i sends the m_1 message to the remote server. The server first validates whether the $N_u^* = N_u$ 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 $N_u^{**} = N_u$. Finally, the server validates whether N_S^{**} is equal to N_S.

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 $\{ID_i, h(PW_i^* \oplus r), \delta_r(S_i)\}$ to the remote server. After receiving the demand for password change, the remote server computes the new value to update $W^* = h(P \oplus h(PW_i^* \oplus r))$ 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 I 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 I. COMPARISON AMONG THE REFERENCED SCHEMES.

Item	*Our scheme*	*Lin-Lai scheme[3]*	*Li-Hwang's scheme[5]*	*Fan-Li scheme[9]*
Proper mutual authentication	Yes	No	No	Yes
Resist insider attack	Yes	Yes	Yes	No
Resist stolen-verifier attack and modification attack	Yes	No	Yes	No
Without a verification table	Yes	Yes	Yes	No
Securely change /update password	Yes	Yes	Yes	Yes

REFERENCES

[1] V. J. Matyas, Z. Riha, "Toward reliable user authentication through biometrics", IEEE Security & Privacy Magazine, vol. 1, 2003, pp. 45-49.

[2] J. K. Lee, S.R. Ryu, K.Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards", Electronics Letters, vol. 38, 2002, pp. 554-555.

[3] C.H. Lin, Y.Y. Lai, "A flexible biometrics remote user authentication scheme", Computer Standards & Interfaces, vol. 27, 2004, pp. 19-23.

[4] M.K. Khan, J.S. Zhang, "Improving the security of a flexible biometrics remote user authentication scheme", Computer Standards & Interfaces, vol. 29, 2007, pp.82-85.

[5] C.T. Li, M.S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards", Journal Network and Computer Applications, vol. 33, 2010, pp. 1-5.

[6] X. Li, J.W. Niu, J. Ma, W.D. Wang, C.L. Liu, "Cryptanalysis and improvement of a biometric-based remote authentication scheme using smart cards", Journal of Network and Computer Applications, vol. 34, 2011, pp. 73-79.

[7] C.I. Fan, Y.H. Lin, "Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics", IEEE Transactions on Information Forensics and Security, vol. 4, 2009, pp. 933-945.

[8] H.L. Yeh, T.H., Chen, P.C. Liu, T.H. Kim, H.W. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography", Sensors, vol. 11, 2011, pp. 4767-4779.