A Novel Biometric-Based Remote User Authentication Scheme Using Quadratic Residues

Zi-Yao Cheng, Yun Liu, Chin-Chen Chang, and Chen-Xu Liu

Abstract—In recent years, so many researchers have focused on the field of remote user authentication schemes. Until now, engineers have figured out a new security mechanism which is based on biometric technology, it can serves for the security of user authentication using a smart card. In this paper, we propose a novel biometric-based remote user authentication scheme which is based on the quadratic residues and biometric verification to achieve efficient and security requirements. Especially, we provide our security analysis to show that our proposed scheme is secure, practical, and trustworthy remote authentication, which will be implemented on different real network environments.

Index Terms—Biometrics, authentication, security, quadratic residues.

I. INTRODUCTION

In 1981, Lamport [1] first proposed a remote authentication scheme which provides authentication procedures between the remote user and server over an insecure channel. However, Lamport’s scheme needs to store password table, the password table makes Lamport’s scheme vulnerable to a stolen-verifier attack. In 1998, Jan and Chen [2] proposed a password based authentication scheme without password table stored in the system. Later, in 2000, Hwang and Li [3] proposed a novel remote user authentication scheme using smart card based ElGamal’s [4] public key cryptosystem. By using smart cards, there are several advantages and properties due to its temper-resistance merit, i.e., such a smart card based scheme helps a legal user with his unique identity or password to login to the remote server by using the smart card, since illegal users cannot get legal one’s information via even insecure channel; the remote server in smart card based system does not have to keep a password table in its database. Thus, the well-known stolen verifier attack can be resisted.

As far as we concerned, there are two categories of the traditional remote user authentication scheme [5-9], including the password based scheme and the cryptographic keys based scheme [11]. However, simple password based scheme is vulnerable to the password dictionary attack, and cryptographic keys based scheme must provide specific memorize to store the corresponding keys so that it is too expensive to maintain the keys in the system. Moreover, the two categories cannot provide non-repudiation since both passwords and cryptographic keys are easily forgotten, lost and no way to identify who the actual user is. Currently, the new technology of biometrics is becoming a popular method for engineers to design a more secure cryptosystem.

In terms of physiological and behavioral human characteristics, biometrics is used as a form of identity access management and access control, and it services to identify individuals in groups that are under surveillance. With the development of computer technology, people’s biometrics information, such as fingerprints, faces, irises, hand geometry, and palmprints can be used to convince their identities. We present three main advantages of biometric technology as follows:

1) The personal biometric information is hard to copy and share.
2) The personal biometric information cannot be forgotten or easily guessed.
3) The personal biometric information is impossible to forge or distribute.

Furthermore, our purpose of system design is to make scheme can be applied for deferent network environments such as wireless system, Wi-Fi, WiMAX, Mobile networks, and vehicle system. Wi-Fi is an advanced technology that allows devices to exchange data wirelessly over a computer network, including high-speed Internet connections. Wi-Fi Alliance defines Wi-Fi as any wireless local area network (WLAN) products that are based on the IEEE 802.11 standards. WiMAX is another brand used to upon wireless MANs and is based on IEEE 802.16d/802.16e.

The remainder of this paper is organized as follows. Section 2 shows the proposed scheme step by step. In Section 3, we provide the relevant security analysis to prove that our scheme is actually secure for applications. At last, we conclude this paper in Section 4.

II. PROPOSED SCHEME

In this section, we introduce detailed steps of the proposed scheme. The proposed scheme consists of three phases: registration phase, login phase, authentication phase. All the related notions are demonstrated in the beginning of this section, and we present the flowchart of the proposed scheme in Fig. 1.
A. Notations
- $n$: the product of two large prime, $p$ and $q$
- $U$: the user
- $R$: the trusted registration center
- $S$: the server
- $ID$: the identity of user
- $B$: the biometric information of user
- $h()$: the one-way hash function
- $x$: the secret information of the server $S$
- $r$: the random number selected by the registration center $R$
- $t$: the random number selected by the user $U$
- $s$: the random number selected by the server $S$
- $\oplus$: the bitwise exclusive-or operation
- $\|$: the concatenation operation

B. The proposed Scheme

1) Registration phase
In this phase, the user $U$ initially registers with the trusted registration center. The following steps are executed:

R1: In the beginning, the user $U$ sends his or her identity $ID$ and the related biometrics $B$ to the registration center $R$ over a secure channel.

R2: After receiving the message $\{ID,B\}$, the registration center $R$ computes $f = B \oplus r$, and $A = x \oplus f \oplus ID$, where $r$ is a random number unique to $R$. And then, $R$ stores the data $\{f,A,ID,r,h()\}$ into a smart card and issues it to $U$.

2) Login phase
This phase is invoked whenever the user $U$ asks the services from the server $S$.

L1: The user $U$ inserts his or her smart card into the card reader, and inputs his or her identity $ID$ and the personal biometrics $B$.

L2: The smart card checks $f \oplus r = B$ to verify the user $U$’s biometrics on the specific device. If it holds, $U$ passes the biometrics verification; otherwise, the scheme is aborted.

L3: Next, the user $U$ randomly selects a number $t$ to compute $D = h(A \oplus f \oplus ID \oplus t)$, $T = t^2 \mod n$, and $M = h(t)$.

L4: And then, the user $U$ forwards the message $\{D,T,M\}$ to the server $S$.

3) Authentication phase
After receiving the login message from the user $U$, both the server $S$ and the user $U$ perform the following steps to achieve mutual authentication.

A1: The server $S$ utilizes the Chinese Remainder Theorem to solve $T = t^2 \mod n$, since $S$ can derive four roots $(t_1,t_2,t_3,t_4)$ with two large primes $p$ and $q$.

A2: Next, the server $S$ compares $h(t_i)$ with the received $M$, for $i = 1$ to $4$, so that it can obtain the correct value of $t$.

A3: Then, the server $S$ checks $h(x \oplus t) = D$. If it holds, $S$ believes the validity of $U$; otherwise, $S$ rejects the user’s login request.

A4: After that, the server $S$ computes $E = h(x \oplus t) \oplus s$, and $N = h(h(x \oplus t) \| s)$, where $s$ is a random number selected by the server $S$, and $S$ forwards the message $\{E,N\}$ to $U$.

A5: After receiving the message, the user $U$ computes $s' = D \oplus E$.

A6: $U$ checks $N = h(D \| s') = h(h(x \oplus t) \| s')$ by using the derived $s'$. If it holds, the user believes the trustworthiness of $S$.

\[U \quad \text{[Registration]} \quad \{ID,B\} \rightarrow \quad R \quad \text{[Login and Authentication]} \quad \{D,T,M\} \rightarrow \quad S \quad \{E,N\} \rightarrow \quad \text{Checks} \quad N = h(D \| s') = h(h(x \oplus t) \| s') \quad \text{by using the derived} \quad s' \quad \text{If it holds, the user believes the trustworthiness of} \quad S.\]

Fig. 1. Proposed scheme

Therefore, the proposed scheme can provide the successful mutual authentication between the user and the server. By the way, both the user and the server computer the session key $sk = h(D \| s' \| r) = h(h(x \oplus t) \| s \| r)$.

In addition, we can achieve parameter update every session in the registration phase, and we provide the detailed procedures as follows:

The smart card first randomly select a new number $r_1$, and then it computes $f_{new} = f \oplus r_1$, and $A_{new} = A \oplus f \oplus f_{new}$, where the above updated parameters are changed on the user’s smart card.

III. SECURITY ANALYSIS

In this section, we present how secure of the proposed scheme with our professional security analysis. As aforementioned in Section 2, the proposed scheme is
A. Replay Attack

Claims: An attacker, named Eve, intercepts the communication messages from the legal user, and attempts to cheat the server by sending the intercepted messages.

Proof: In the proposed scheme, we use the nonce-based mechanism and hash value comparisons of $M$ and $N$ to protect against the reply attacks. More specifically, the random numbers $t$ and $s$ are independently selected, and each of them is different in every session. Therefore, Eve cannot pass the authentication procedures, even if he intercepts the communication messages. It is clear that the proposed scheme can resist the reply attack.

B. Known-Key Attack

Claims: An attacker Eve compromises a past session key, and then he attempts to compromise other session keys.

Proof: In the proposed scheme, the session key $sk = h(D \parallel s \parallel r) = h(h(x \oplus t) \parallel s \parallel r)$ which is protected by the one way hash function, and is relevant to the random numbers $r$, $s$, and $t$. Even if Eve can compromise one session key, he cannot get the correct random numbers $r$, $s$, and $t$, thus he cannot compromise the other versions. Therefore, our scheme can withstand the known-key attack.

C. Impersonation Attack

Claim: An attacker Eve computes the forgery message to fool the user or the server into believing his validity.

Proof:

1) Impersonation of legal user:

Assume Eve computes a forgery message $\{D’,T’,M’\}$, where $T’ = (t’)^2 \mod n$, $M’ = h(t’)$, and $t’$ is randomly selected by Eve, and forwards it to the server. Then, the server can determine the value of $t’$ by executing the Step 1 and Step 2 in authentication phase. However, Eve cannot pass the authentication from the server, since he cannot compute the correct $D$ without knowing the specific number $t$.

2) Impersonation of trusted server:

Similarly, assume Eve calculates a forgery message $\{E’,N’\}$ with randomly selected number $s’$. However, Eve will fail. That is because the attacker cannot calculate the correct $N$ to pass Step 6 in authentication phase without knowing the specific number $s$.

According to the above analysis, we prove that the proposed scheme can resist the impersonation attack on user or server side.

D. Stolen Smart Card Attack

Claims: An attacker Eve obtains a legal user’s smart card and tries to use it to login the server.

Proof: Assume a legal user $U$, who actually loses his or her smart card. Meanwhile, an attacker Eve who gets the smart card tries to pass the login phase in the proposed scheme. First, Eve inserts the smart card and provides his biometric information $B_{Eve}$. Unfortunately, it is obvious that Eve cannot pass the verification $f \oplus r = B_{Eve}$, so that the proposed scheme can withstand such a stolen smart attack.

E. Forward Secrecy

Claims: An attacker Eve gets the master key of the mechanism for some reasons, he attempts to compromise the previous session keys.

Proof: We assume that Eve gets the master key $x$ in our scheme, and he wants to compromise the previously generated session keys. However, he will fail. The reason is Eve cannot compute any past versions of session keys without knowing the randomly changed numbers $r$, $s$, and $t$. Therefore, the proposed scheme can protect the forward secrecy.

IV. PERFORMANCE ANALYSIS

In this section, we provide the performance analysis to show how efficiency of our proposed scheme. More specifically, we compare our security mechanism with the previous published schemes [10-12] based on the computational cost associated with one-way hash function (hash) and modular squaring (squ). From the view of efficiency aspect [13], [14], an example of the cheap modular squaring $f(x) = x^2 \mod n$ where $a$ is a coefficient [13] can replace the original equation $f(x) = x^4 \mod n$. Therefore, the modular squaring is cheaper than the hash function such as MD5 (16 K gates) and SHA-1 (20 K gates), since it costs only a few hundred gates [15].

<table>
<thead>
<tr>
<th>TABLE I: THE PERFORMANCE COMPARISON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Items</td>
</tr>
<tr>
<td>Registration phase</td>
</tr>
<tr>
<td>Assistant channel</td>
</tr>
<tr>
<td>Authentication phase</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

The detailed comparison is shown in Table 1. It is obvious that Khan et al.’s scheme [10] utilizes nine one-way hash functions is cheaper than Li and Hwang’s scheme [11] and Li et al.’s scheme [12], cost ten one-way hash functions and fifteen one-way hash functions, respectively. In our system, we just need six one-way hash functions and two modular squaring. Hence, our proposed scheme is more practical with the biometric technologies, and our design is proved to be more efficient than others.

V. CONCLUSIONS

In this paper, we propose a novel biometric-based user authentication scheme, which does not need the traditional password anymore, it helps the user can prove his or her identity with the relevant biometrics. And, we design the proposed scheme by using the strategy of quadratic residues.
This advantage is that the performance of our system is much cheaper than the hash based system since the implementation of such a modular squaring can be reduced to a few hundred gate-equivalents [14]. In addition, we present that our scheme can withstand to some possible attacks in Section 3. Therefore, the proposed scheme is actually secure, efficient and practical for real network applications such as wireless environment, Wi-Fi, WiMAX, mobile system, and vehicle network. In the future, we will design and adapt our scheme to implement on more network environments.

ACKNOWLEDGMENT

This work is partially supported by National High Technology and Development Program (863 Program) of China under Grant No. 2011AA010104-2, National Natural Science Foundation of China under Grant 61071076, the Academic Discipline and Postgraduate Education Project of Beijing Municipal Commission of Education, the Fundamental Research Funds for the Central Universities under Grant 2012YJS023. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES