A NOVEL ONE-TIME PASSWORD MUTUAL AUTHENTICATION SCHEME USING BIOMETRICS-BASED KEY AND VISUAL SECRET SHARING

1WEI-BIN LEE, 2YU-TING LIN, 3MIN-HSUAN TSAI, 4HSING-BAI CHEN

1,2,3Department of Information Engineering and Computer Science, Feng Chia University, Taiwan, R.O.C.
4Hospital and Social Welfare Organizations Administration Commission, MOHW, Taiwan, R.O.C.
E-mail: wblee@fcu.edu.tw, yoyo21220@gmail.com.tw, rjamwxede@hotmail.com

Abstract- Most websites will ask for user identification and verify the password for authentication. When a user is away from home or office and needs to use a public computer, a static password is dangerous to use because it may be cracked, guessed, or stolen. It implies that a dynamic password instead of static one should be employed in a public computer. A sensitive key token used to generate the dynamic password attracts attackers’ attention and increases the cost of maintaining the token. In addition, it will be not secure that the sensitive token is used in an untrusted computer to generate a dynamic password. In this paper, a novel one-time password mutual authentication scheme is proposed to remedy these problems.

Keywords- Authentication, One-Time Password, Visual Secret Sharing, Biometric

I. INTRODUCTION

Public computers in libraries, hotels, Internet cafes, and airports are vulnerable to the possibility of having been installed with malware that records every keystroke and then sends this information back to the thief. One golden rule is never to type a credit card number while using any public computer. However, rules can’t always be followed. Sometimes people simply have to use a public computer for some reason. A lot of tips can help users improve their security when using a public computer, and protecting their passwords is the most critical. A dynamic password is better than static one because it is automatically revoked after it is compromised by being cracked, guessed, or stolen.

A one-time password (OTP) can be generated using numerous techniques. Some researches use software such as instant messaging (IM) [10] or e-mail [15]. However, the computer itself may be cracked, attacked.

Other researchers use a device to generate an OTP such as smart-card-based [11] or proprietary-token-based OTP schemes, e.g., RSA SecurID [2], Authenex A-Key Token [16], and SafeNet etoken pass [17]. Carrying tokens such as RSA token or smart card will make the user burden.

Most studies have opted to use a smartphone for minimizing the equipment needed and because a large customer-base already owns a smartphone. According to a report by venture capital firm KPCB, 45% of smartphone users access the internet service [3], and the internet-use growth rate is rising every year. To generate an OTP, the smartphone uses either a short
A Novel One-Time Password Mutual Authentication Scheme Using Biometrics-Based Key and Visual Secret Sharing

message service (SMS) [4][9][11] or a software tool [7][12][13]. The SMS sends a message for a high price. Using a software tool can reduce the cost; however, this technique requires the storage and protection of a token, which is less secure than having nothing to store. In 2011, Lee et al. proposed the OTP authentication scheme [8] that employs biometrics-based key to maintain no sensitive token; however, no consideration was given to the fact that the computer may be easily compromised.

Don’t insert the token or key the password into an untrusted computer are the better way, but the OTP is generated by combining something. In this paper, we introduce an OTP authentication scheme that uses biometrics key to generate a secret sharing image (SSI) for using a public computer.

II. BACKGROUND

In this section, the related techniques are reviewed respectively as following:

A. Visual Secret Sharing

In 1995, Naor et al. proposed the visual secret sharing scheme [5], in which an image is separated into two shared images. The first shared image may be selected randomly, and according to the original image and the first shared image, each pixel in the second image is selected from the original and the first shared image. If a pixel from the original image is white, the second shared image would have the same pixel as the first one. If the pixel of original image is black, the second shared image would choose a pixel that is complementary to the first shared image. The content in the original image can be identified if the two shared images are then overlapped. Table 1 shows a synopsis of visual secret sharing, and Figure 1 shows the visual secret sharing model.

B. Fuzzy Extractor

In 2008, Dodis et al. proposed the fuzzy extractor to generate a biometric cryptographic key. With the fuzzy extractor, the biometric Bi is the input of the generation function Gen(.), and the outputs are the secret string Ri and the helper string Pi, written as Gen(Bi)→(Ri, Pi). To obtain the secret string Ri, Pi, and Bi must be generated via the reproduction function Rep(.) if and only if Bi’ is close enough to Bi, written as Gen(Bi)→(Ri, Pi). For more detailed information on the fuzzy extractor, please refer to [5].

III. THE PROPOSED SCHEME

The proposed scheme is composed of two phases: registration and login. The notations used throughout this paper are listed as follows:

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDu</td>
<td>User’s personal identification</td>
</tr>
<tr>
<td>IDs</td>
<td>Service provider’s URL</td>
</tr>
<tr>
<td>MK</td>
<td>Server’s master key (to be kept secret)</td>
</tr>
<tr>
<td>□</td>
<td>XOR</td>
</tr>
<tr>
<td>OTP</td>
<td>One-time password</td>
</tr>
<tr>
<td>TS</td>
<td>Time stamp</td>
</tr>
</tbody>
</table>

Table 1. Visual secret sharing synopsis

<table>
<thead>
<tr>
<th>Original image</th>
<th>Shared image 1</th>
<th>Shared image 2</th>
<th>Overlapping image</th>
</tr>
</thead>
</table>

Figure 1. Visual secret sharing model
A Novel One-Time Password Mutual Authentication Scheme Using Biometrics-Based Key and Visual Secret Sharing

Bu : User’s biometric.
H(.): Hash function.
Gen(.): Fuzzy extractor generation function whose input is a user’s biometric Bu and outputs are a helper string Pu and a secret string Ru.
Rep(.): Fuzzy Extractor reproduction function whose output is a secret string Ru and inputs are a user’s biometric Bu and a helper string Pu.
F1(.): A shadow image generation function whose output is ImgOPS1 and inputs are TS and H(IDu, MK).
F2(.): A shadow image generation function whose output is ImgOPS2 and inputs are ImgOPS1 and ImgOP.
FR(.): A superimposing two-shadow function.
Txt2Img(.): Transform text to image.
Dig2Bar(.): Transform digital to barcode.

A. Registration Phase
The first time a user visits the service page, he/she must register the server. Assuming that the connection between the user and the server in the registration is in a secure channel, the registration steps are as follows (see Figure 2):

Step 1. User inputs registration information.
Step 1-1. Input IDu and IDs on a smartphone.
Step 1-2. Capture biometric (Bu) using a smartphone.
Step 2. The smartphone generates SKu and sends it to the server.
Step 2-1. Generate Ru and Pu using Gen(Bu)→(Ru, Pu).
Step 2-2. Generate SKu = H(IDu, Ru).
Step 2-3. Send registration request, IDu, and SKu to the server.

Step 3. The server generates AK.
Step 3-1. Generate UK = H(IDu, MK) and AK = UK ⊕ SKu after receiving the request.
Step 3-2. Send AK to the user’s smartphone.

Step 4. The smartphone stores AK and Pu and finishes the registration phase.

B. Login Phase
When the user wants to access the service from the registered server, the following login steps are performed (see Figure 3):

Step 1. The user inputs IDs and IDu on the browser.
Step 2. The browser sends IDu and login request to the server.
Step 3. The server generates a barcode and a shared image.
Step 3-1. Generate UK = H(IDu, MK) after receiving the request.
Step 3-2. Generate OTP and transform it to image ImgOP = Txt2Img(OTP).
Step 3-3. Generate a shared image ImgOPS1 = F1(UK, TS).
Step 3-4. Generate ImgOPS2 = F2(ImgOPS1, ImgOP).
Step 3-5. Transform TS to barcode ImgBar = Dig2Bar(TS).
Step 3-6. Send shared image ImgOPS2 and barcode ImgBar to the browser (see figure 4).

**Figure 4. Barcode ImgBar and shared image ImgOPS2.**

**Step 4.** The user captures these images from the browser using the camera of smartphone (see Figure 5).

**Figure 5. CaptureImgOPS2 and ImgBar using the camera of smartphone.**

**Step 5.** The smartphone checks whether TS, scanned from ImgBar, exceeds the expiration time or not. If it holds, the following steps will be performed.

**Step 6.** The user captures biometric Bu’ by using the smartphone.

**Step 7.** The smartphone overlaps shared images.
Step 7-1. GenerateRu’ usingRep(Bu’, Pu)→(Ru’).
Step 7-2. Generate SKu’= H(IDu, Ru’)and UK’= AK=SKu’.
Step 7-3. Generate shared image ImgOPS1’= F1(UK’, TS).
Step 7-4. Overlap the two shared images ImgOPS1’ and ImgOPS2 to be captured by the user.

**Step 8.** The user receives anOTP from the overlapped image.

**Step 8-1.** Get OTP from viewing the overlapped image.
**Step 8-2.** Input OTP on the browser.

**Step 9.** The browser sendsOTP to the server.

**Step 10.** The server checks whether |TS’-TS|<ΔT, where TS’ is current system time of the server, is satisfied and verifies whether the received OTPs correct or not. If they do not hold, return message “Login Failed” and stop the connection with the user. Otherwise, return message “Login Success” to the user.

**IV. SECURITY ANALYSIS**

Hackers can threaten a user’s computer environment using a variety of methods, including a man-in-the-middle attack, a reply attack, phishing, malware injection, and a stolen-verifier attack. In this section, these attacks will be analyzed.

A. Man-in-the-middle attack
By controlling the transmission channel between the server and browser, an attacker may obtain the ImgOPS2 and OTP. However, the server checks whether |TS’-TS|<ΔT when authenticating. Therefore, the server can detect a man-in-the-middle attack.

B. Reply attack
By eavesdropping on the transmission channel between the server and browser, an attacker may obtain the OTP. However, the OTP is changed every login session and then is revoked after authentication. Therefore, an attacker cannot access the server using the same OTP.

C. Phishing attack
Attackers can also attempt to acquire sensitive information by masquerading as the server. However, if the attacker does not have the MK, he cannot generate the corresponding ImgOPS2. Therefore, the phishing server can be detected by the user.
D. Malware injection attack

By injecting malware into the browser, an attacker may steal the OTP and the ImgOPS2. However, the OTP will be changed at the next login. Therefore, this stolen information cannot be used for the next authentication.

E. Stolen-verifier attack

By stealing the verification table from the server, an attacker may acquire some sensitive information. However, in our scheme, the server does not store users’ sensitive information. Therefore, no sensitive information can be stolen from the server.

V. EXPERIMENT

In our experiment, we use the computer to simulate the smartphone. First, when the user wants to login to the server, the server will use the MK, OTP, and TS to generate the first SSI (see Figure 6). Then, the biometrics key is obtained by capturing the face from the smartphone camera (see Figure 7).

The biometrics key and TS will generate the second SSI (see Figure 8). Finally, the mobile image is superimposed on the server image, and the user can view the OTP (see Figure 9).

In Figure 9, we can clearly see the text, which proves that the captured shared image can be overlapped to obtain an OTP.

CONCLUSIONS

In this paper, we have proposed a new one-time password mutual authentication scheme that does not require the use of a network or high-priced SMS to generate an OTP. Nor must the user remember anything during this process. The scheme can directly link to the true user and minimize any equipment burden using a user’s smartphone. In addition, this scheme protects users who must use a public computer.
ACKNOWLEDGMENT
The authors would like to thank the National Science Council of the Republic of China, Taiwan, for its financial support of this research under Contract No. MOST 102－2918－I－035－007－

REFERENCES