Research and Design of Security Scheme on Application Layer of a Web of Things

Yanyan Han, Na Li*, Jing Zhang and Wencai He
Telecommunications Engineering, Xidian University, 710071 Xi’nan, China

ABSTRACT

OIDC protocol is one of the latest applications in the WoT application layer of a single sign-on protocol. In order to solve WoT application layer authentication and authorization issues, this paper presents a multi-secret visual cryptography scheme, combined with OIDC protocol, to achieve WoT application layer authentication and authorization functions. Multi-secret visual cryptography technology can hide a lot of secret information in a small amount of memory, while it can make up for OIDC defects. This solution can improve the security of WoT application layer under the premise of reducing the security.

INTRODUCTION

In recent years, the Internet of things, as the third wave of the information age, has been rapid development. WoT[1], Web of Things, its technology, as a cross platform sharing infrastructure for resources and services, has become the technology choice for ubiquitous computing and heterogeneous resource sharing of the Internet of things [2]. In the current, WoT environment is facing a variety of threats, such as the loss of identity information, disclosure of personal information and abuse of resources, etc. Identity authentication and authorization is an important means to resist these threats[3]. Hasan R [4] and others proposed an authentication and authorization scheme that combines an OAuth protocol with a delegate license, but the scheme has defects such as unable to control token rights and so on. Google has proposed an extension of OpenID and OAuth protocol [5], but the agreement can not meet the relying party (Relay Part, RP) and OAuth users do not have the same certification needs. The OpenID Connect protocol is an important single sign-on authentication protocol standard released in 2014 and it has been widely used in the WoT industry. However, the agreement has incomplete certification and user password security strength is not strong enough [6].

In this paper, we propose a multi-secret visual cipher scheme, which can recover two different secret cryptographic schemes by two superimposing methods. The OpenID Connect protocol can effectively solve the problem that the authentication is incomplete and the password security is not strong enough so that you can also achieve control authority. Visual cryptography can hide multiple secret information in a small amount of memory[7], with the advantages of simple technology implementation and low computational complexity.
BASICS
Multi-Secret Visual Cryptography

The conventional visual cipher scheme generates a shared image that is class noise in order to ensure that the secret information is unreadable. Since it is not possible to determine which shared images are corresponding to the secret images to be restored, the problem becomes complicated once the number of shared images held by the user becomes large. The visual cipher technology with tag information hides the label image in each share, visualizes it by folding each individual shared image, and then through this meaningful label image to identify a specific secret image of the shared pair, so as to facilitate the user to distinguish different managing multiple class noise sharing images. By setting the label image to a unique symbol associated to establish a verification mechanism for an unauthorized or fraudulent participant, a shared image of an unauthorized or fraudulent act will not be properly restored.

Image Camouflage

When the noise image is transmitted, it is not desirable for the attacker to acquire the size of the actual image. Therefore, it is necessary to disguise the size of the transmitted image without changing the original information of the image. The program used in this approach is to expand the original image, from the original image size $H \times W$ to $(H+a) \times (W+b)$ to the size shown in Figure 1. The enlarged $H \times W$ part of the image coincides with the original image and the extra edge part randomly allocates the binary pixel 0 or 1, so that the enlarged image is still the noise figure. Even if the attacker obtains the image, they can not easily determine the original size, increasing the difficulty of breaking the original map of violence. The server and the user in the image transmission processing will be agreed in advance with the size of the image. After receiving the image sent by the user, the server extracts the original image without any error. This method is effective for the camouflage transmission of the noise image, and the meaningful image transmission requires visual image information for specific camouflage.

![Figure 1. Image after camouflage.](image-url)

DESIGN AND IMPLEMENTATION OF THE PROGRAM

This paper first proposes a new TVC (Tagged Visual Cryptography) scheme, which not only has the original performance of the TVC scheme that make the information of the label image hidden in the shared image, but also makes the number of secrets restored
increase so that more information is added for the visual cipher scheme. When the two shared images are superimposed, the first secret image will appear. When a shared image is flipped up and down and superimposed on each other, the second secret image will appear. The secret image and the label image recovered in the scheme have good visual recognition degree.

First list the roles that the program needs, is the EU (End User), RP (Relying Party, OAuth2 trusted client) and OP (OpenID Provider, used to provide RP for the RP Identity authentication information). Among them, OP contains TE (Token Endpoint), authorization server (OAuth2 server) and UserInfo EndPoint and TE is mainly used for token generation and sending. The main flow chart of the program is shown in Figure 2 and the main steps are as follows:

1. The RP sends a request to the OP for authentication;
2. The OP is authenticated and authorized by using the multi-secret visual cipher technology;
3. OP returns ID Token and Access Token to RP;
4. The RP uses the Access Token to send a token request;
5. Token response.

Multi-secret Visual Password Scheme Construction

It is assumed that there are two secret images S1 and S2 of size $H \times W$, and two tagged images T1 and T2 that are to be encrypted to the size of $H/2 \times W$ which means the size of the label image is the same as the size of the secret image. After the program's encryption process, two shared images will be generated. When two shared images are superimposed directly, the secret image S1 will be displayed, making one of the shared images upside down and superimpose on each other, and the secret image S2 will be restored. In addition, each shared image is folded up and down along the horizontal symmetry axis of the image, and a hidden label image is displayed respectively.

The encryption process is divided into the following stages: The first step uses the (2,2) random raster technique [2] to encrypt the given two secret images S1 and S2 into a set of transition images G1, G21 and G22. In the second step, the tag image is encrypted into two transition images L1 and L2. Finally, the five transition images G1, G21, G22 and L1, L2 are combined to form the final shared images F1 and F2.
Step 1: According to the secret images, S1 and S2 use the (2,2) random grid technique [8] to generate the transition image G1, g2. A certain pixel G1 (i, j) in the shared image G1 is randomly subjected to 0 (white) or 1 (black) operation with the same probability until all the pixels G1 (i, j) are processed. S1 and S2 and G1 are respectively generated in accordance with (2,2) random grid technology transition G21 and G22, and then G22 up and down to G22'. A number k is randomly generated and $0 \leq k \leq 1$. If $k \leq \frac{1}{2}$, the pixel G21 (i, j) is assigned to G2 (i, j), otherwise G22 ' (i, j) is assigned to G2 (i, j) until all pixels are processed.

Step 2: Transition images L1 and L2 are generated according to the flag images T1 and T2. The two transition images Cx1 and Cx2 are generated by Tx (x = 1, 2) according to (2, 2) random raster technology, and then Cx2 is inverted up and down and then concatenated with Cx1 to form Lx, x = 1, 2.

Step 3: The transition shared images Gx (x = 1, 2) and Lx (x = 1, 2) are combining into the final shared image Fx (x = 1, 2). A probability value p is given, then randomly generate a number q is generate and $0 \leq q \leq 1$. If $q \leq p$, the pixel Gx (i, j) is assigned to Fx (i, j), otherwise Lx (i, j) is assigned to Fx (i, j).

The decryption process of the scheme only needs to be simply superimposed and flipped. When the shared images F1 and F2 are superimposed, the secret image S1 can be restored, and F1 is superimposed on F2 with F2 up and down, and the secret image S2 can be restored. And the label image hidden in the shared image can be seen by folding the shared image at its lateral axis of symmetry.

The simulation of the above process is as follows:

(a) Secret image S1  (b) Secret image S2

TAG1 TAG2

(c) Tag image T1  (d) Tag image T2

Figure 3.1. Secret images S1, S2 and tag images T1, T2.

(e) Share Figure F1  (f) Share Figure F2

Figure 3.2. Shared images F1, F2.

(g) F1 directly superimposes F2  (h) F1 overlaps up and down with F2

Figure 3.3. Recovery of the secret image. $q = 0.5$
**Overall Program Design**

**CERTIFICATION REQUEST**

Figure 4 is the certification process of the program. RP to obtain the EU in the OP on the private data, first to the OP to send identity authentication request information including five important parameters client_id, response_type, scope, redirect_uri and state. Client_id refers to the client’s id; response_type refers to the type of response to the authorization method; scope refers to the access threshold; redirect_uri refers to the redirect address; state refers to state value between the request and feedback.

**TWO-WAY CERTIFICATION AND AUTHORIZATION**

The Authorization Server first determines the validity of the client_id from the request information sent by the RP, and stops the authentication if it is invalid[9]. If so, the Authorization Server generates a request message for the authentication EU. EU stores a random raster image g and a logout authentication code, and automatically generates a temporary random number N and then generates the corresponding mark image TUSER according to the own ID and the corresponding random number image SN according to the random number N. The image SN and the TUSER are used as two secret images, and the image g, as one of the share of the image, uses the previous multi-secret visual cryptography algorithm to encrypted to generate another share of the image F1. The size of the F1 is disguised and sent to the Authorization Server.

Authorization Server first determine the validity of the ID. If it is invalid, the server will stop the certification. If it is valid, the Authorization Server finds the corresponding image g based on the ID, extracts the real F1 image from the camouflaged F1 image, superimpose g and F1, reads the EU flag information ID from the restored first secret image and verify that the ID sent by Authorization Server is consistent. And then F1 goes up and down and then superpose with g, from the recovery of the second secret image to read the random number sent by the user N. The above process completes the Authorization Server's authentication to the EU.

Then, the Authorization Server generates the corresponding shared image F2 by using the image SN and its own logo image TSERVER as two shared images to be hidden, and share the EU shared image g as one of the shared images. And then the image F2 size is disguised and sent to the EU for verification.

When the EU receives the camouflage image F2, it extracts the true F2, superimposes it with g, reads the flag information from the restored first secret image, and verifies that the server if it is consistent with this time’s communication server. And then it turns the F2 and then overlays with g, from the recovery of the second secret image to read the random number sent by the user N, and verifies whether the session is consistent with the random number that Authority Server sent. If all are consistent, this process completes the EU Authorization Server authentication.
After the two-way authentication, it will send the authorization verification code. The EU generates the image SN + 1 with the random number N + 1, uses the image (2) as a shared image, and generates another shared image F3, uses the (2,2) random raster visual cipher algorithm and sends the F3 size masquerade to Authorization Server. Authorization Server receives the camouflage size image F3, extracts the real F3 from it, overlaps the shared image g directly and verifies the received image information. If it is N + 1, it can be confirmed as the EU of the session just now and begin distributing authorization authentication codes. Authorization Server randomly generate the session key m, and then generate the corresponding verification code image Sm, and then the image SN + 1 and image Sm as two hidden images, the EU shared image g as one of the shared image. The constructed multi-secret visual cipher algorithm encrypts the corresponding shared image F4. The image F4 is subjected to size disguise processing and returned to the EU.

![Figure 4. Certification process.](image)

When the EU receives the disguised F4, extracts the true F4 from it, overlays it with g, reads the random number from the restored first secret image, and verifies that it is N + 1 to ensure that the key sending to the Authorization Server is a session server, which means it has not been spoofed by a third party. If not, it will reject the session. If it is, then F4 will be rotated and then overlaid with g, from the recovery of the second secret image to read the authorization verification code information m, then the user needs to manually enter the verification code m, and the client will generate the corresponding image. The text at this time is no longer distorted so that the Authorization Server can automatically recognize it. EU will verify the code and random number N + 2 as two secret and share the image g with the same algorithm to generate another shared image F5 to the Authorization Server. Finally, the Authorization Server verifies whether that the received random number is equal to N + 2, and whether the verification code is equal to m. And if it is equal, the EU generates an authorization message End_user grant to the Authorization Server. The authentication and authorization process is shown in Figure 3.
CERTIFICATION RESPONSE

After the Authorization Server receives the EU authorization message, the authentication response message containing the authorization code and the identity token id_token respectively generates two images S1 and S2 that contain the authorization code and the token id_token and through the mentioned multi secret visual cryptography scheme, encryption send to RP.

TOKEN REQUEST

RP receives a secret image, firstly decryption processing to access to the authorization code. And then it checks whether the authorization code is qualified. Once the validation is successful, a token request is generated. The request message contains four main parameters, including code, client_id, redirect_uri, RP and OP common random raster image g. among them. RP needs to use the authorization code in exchange for access token Access Token. Finally, the RP sends a token request (Token Request) to the OP.

TOKEN RESPONSE

When the OP receives the token request message, it first verifies the authorization code and the timestamp. After the authentication is successful, the token response message Token Response is generated. Among them, the token response message includes four main parameters, including: Access Token, token_type, id_token and express_in (Access Token life cycle).

PERFORMANCE ANALYSIS

Feasibility Analysis

In this protocol, the (2,2) double secret visual cipher algorithm is used to transmit the secret information[10]. The EU and the Authorization Server have a shared image. According to the secret image and the shared image g, they use this multi-secret visual cipher algorithm to encrypt and generate another shared image. By transmitting the shared image, each flag image information is transmitted secretly. Random number information and verification code information are judged and authenticated, and any information of the original secret image is not obtained from each shared image. When the two shared images are superimposed, the original logo image, the random number image and the verification code image can be displayed, and both sides authenticate each other by transmitting the respective logo images. In each interactive communication process, an important security measure is the transmission of random number information. The protocol takes the random number as the main line, and ensures that the authentication process must be the legitimate user and the legitimate server in the session. At the end of the protocol interaction authentication, the server sends a verification code that only the human visual system can recognize, ensuring human participation, and avoiding the use of computer agent technology to automatically log in instead of taking action.
Security Analysis

Posing as an attack

Assuming that the attacker has guessed a legitimate user ID and forged a random number N, trying to generate a shared image sent to the server, but the user can generate a legitimate share of the image on the premise that the user and the server share the shared image g. Attackers know the probability of success by about \((1/2)^{\frac{h+w}{1}}\) when they know the true size of the image to be shared. If the attacker intercepts the shared image F1 sent by the user to the server, attempts to simulate the legitimate server, the attacker needs to generate the shared image F2, and F2 is determined by the server's logo image and the random number N and the shared legal image g. Since the attacker has only F1, there is no way to launch random number information, and there is no share of the image g information, even if the forgery of the server's logo image can not be verified by the user. Therefore, posing attacks can not be achieved.

Replay attack

For each new login request, this protocol generates a different random number N. If an attacker gets the F1 that was used in the previous authentication and forwards it to the server, the attacker can not decrypt the session in the session, even if the attacker receives the F2 returned by the server. Without the shared image g of the user and the server, the attacker could not decrypt the random number N in the session, and could not construct the F3 to continue requesting the authentication code image from the server, so it can effectively resist the replay attack.

Password guessing attack

The security of the authentication protocol in this scheme is largely determined by the shared image g before the user and the server. Once the image g has been successfully guessed, the attacker will complete the control of the entire authentication process. But guessing the correct shared image g has two major problems. First, because the size of the image transmitted in the channel is forged, and each size is different, so the attacker can not determine the size of the shared image g. Second, even if the attacker determines the size of the shared image, assuming a total size is \(128 \times 128\), the probability of success can be broken is \((1/2)^{128}\). Consolidated these two factors, trying to guess the sharing g is basically impossible to succeed.

Efficiency Analysis

The encryption method adopted in this paper is based on the multi-secret visual cipher algorithm of random raster. The encryption method adopted in the conventional authentication protocol mainly includes symmetric encryption algorithms such as AES and asymmetric encryption algorithms such as RSA[11]. In this paper, the visual cipher algorithm based on random grid is based on the logical operation of image pixel. The AES algorithm is based on the arrangement and replacement of data. The RSA algorithm is based on the large number of decomposition, and the computational complexity of the three algorithms is increased. In order to quantitatively analyze these three algorithms, we test their encryption and decryption speed, that is, the same time to encrypt the same length of the plaintext and compare the three algorithms to complete the encryption and decryption of the total time consumed as shown in TABLE I.
In addition to the use of visual cipher program [12], the use of symmetric encryption algorithm and MAC message verification code, in contrast, the authentication efficiency is relatively high. Literature [13] uses the public key to update the image key in the scheme, and this scheme only re-generates the random grid to achieve the key update, and the program in the calculation of cost also decreased. Compared with the literature [14], the two schemes use the random number generator, but the literature [14] uses the message verification code to verify the message, and this program uses the random number N to achieve the verification function to ensure that the message has not been tampered with, which is more efficient.

<table>
<thead>
<tr>
<th>Encryption algorithm</th>
<th>(2,2) Multi-secret visual cipher algorithm</th>
<th>AES</th>
<th>RSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation hours</td>
<td>0.11s</td>
<td>1.06s</td>
<td>858s</td>
</tr>
</tbody>
</table>

In conclusion, the OIDC protocol proposed in this paper can effectively accomplish the two-way authentication between the EU and the server, and can resist the common attack, and has good security performance. In addition, compared with the conventional modern cryptographic algorithm, it is more simple, easy to implement, and encryption and decryption faster, which means this program can save more overhead under WoT and improve computing performance.

CONCLUDING REMARKS

The OIDC protocol uses a secure transport layer protocol to ensure its security, but the deployment of secure transport layer protocols requires a large and very complex overhead, greatly reducing the efficiency of communication. At the same time, the agreement in the EU and the authorization server on the two-way authentication, assuming that the attacker obtains the relevant parameters to attack, will make the two sides lose mutual authentication. And, the attacker can intercept the user password, which makes the user password to lose the secret. This scheme adopts the multi-secret visual cipher technology, which guarantees the safe and effective completion of the two-way authentication of the EU and the Authorization Server. In this process, it does not involve the user's password, so as to ensure the user's password Confidentiality. The program can pass two secret messages in the process of interaction, and the random number information is used to ensure the consistency of the session and enhance the security performance of the scheme. In addition, the program's login verification code can prevent the machine from cracking. Feasibility, security and efficiency analysis show that this protocol can provide effective and secure authentication and authorization functions. This scheme has advantages not only in operational efficiency, but also in security.

REFERENCES