Research on Identity Authentication Scheme in WiFi Environment

Yun-Feng Lian
Mechanism Technology Institute,
Shijiazhuang, Hebei,
Post-Doctoral Research Center,
66393 Force, Baoding, Hebei,
E-mail: lianyf100@163.com

Zeng-Guang Wang, Jie Yan
Six Department,
Mechanical Engineering College,
Shijiazhuang, Hebei
lianyf100@163.com

Abstract—A secure two-way identity authentication scheme of WiFi environment is raised from the perspective of security and the load capacity mobile terminal according the increasing serious of wireless network security. The scheme is based on one-time password authentication technology and the digital signature is realized by using the elliptic curve cryptosystem. It is known that the scheme can resist the common network attacks by analyzing the security of this scheme, which is suitable for the application to the WiFi environment with high security requirements.

Keywords—wireless network; authentication; one-time password; elliptic curve cryptosystem

I. INTRODUCTION

With the rapid development of information technology, internet technology and mobile terminal, the network has brought great convenience for the people’s life and work. In this case, WiFi has been generally used by public places and companies because of its convenience and speed. It is one of the wide range of applications of wireless network access. But, it is a big risk for WiFi because of its openness. Authentication technology is the most basic security services. The essence of authentication is that the information of the user is verified by the verifier to prevent illegal personnel illegal operation to obtain improper benefits[1]. If the authentication system is damaged, the security will suffer tremendous damage. At present, the authentication of WiFi mainly adopts the weak authentication mode such as the static password[2]. Authentication is mainly realized by each wireless access point. In this authentication model, the coverage of the wireless network is small and it is difficult for the administrator to manage the network. Because of that, it is important for the popularity of wireless networks to build a secure authentication model.

At present, there are some research results of the identity authentication scheme in the wireless network environment. An authentication scheme of mobile intelligence terminal based on S/Key was proposed. It is to achieve certification through the relevant password sequence[3]. However, the number of iterations is limited, the client needs to reinitialize the password because of S/Key authentication process using Hash chain encryption. Longyang Gong uses pseudo random function to generate mutual independent OTP to achieve two-way authentication[4]. The scheme can resist the fake attack and replay attack, because there is no use of Hash chain to encrypt the information. But in the certification process, the security risks are existing because of data identification directly on the network transmitted in plaintext. Tuseler Torben proposed the identity authentication scheme based on the geographical location of the mobile terminal as the authentication factor[5]. But the client location is collecting through the GPS positioning, WiFi positioning and cellular network positioning. It will have a better effect only in a specific location which results the key space limited.

A secure two-way authentication scheme is designed through analyzing identity authentication scheme in wireless environment, combining with the characteristics of the security requirements of the higher according to some occasions. The features of mobile terminal computing and the limitation of storage capacity is considered. It is no doubt that the scheme is suitable for higher security requirements under wireless environment.

II. STRUCTURE OF IDENTITY AUTHENTICATION SYSTEM

The structure of identity authentication system based on WiFi environment is shown in Figure 1. It is consist of users, mobile terminal, wireless access, access switch, the switch core, authentication server, firewall and internet. The wireless access point has the function of data forwarding and not the authentication function through upgrading the wireless access appoint. The request of the user authentication is redirected to the authentication server by the wireless access point and unified authenticated by the authentication server. It is convenient for management and enhanced safety certification. What’s more, it expands the coverage of the WiFi signals.
The client is connected to the network through the wireless access point. The same area within the scope of the wireless access point is connected to the switch through the cable. The authentication server, firewall and switches in different areas are interconnected by the core switch. Specific certification process is as follows: firstly, user should input the correct user name and password which proves its legal status to the mobile terminal. Then the request of the users is redirected to the authentication server by the wireless access point through HTTP. The bidirectional identity authentication is completed by the authentication server. The visit to the resources and operation is allowed only after successful authentication.

III. DESIGN OF IDENTITY AUTHENTICATION SCHEME

A. Military Ideas of Identity Authentication Scheme

The scheme is applied to the high security requirements of WiFi environment. The following principles need to be followed. (1) The bidirectional identity authentication between user and authentication server is carried out in order to improve the security of identity authentication. (2) The amount of calculation for the client is minimized considering that the effect of the mobile terminal operation ability is limited. (3) A lot of work should be done to simplify the certification process in order to reduce the amount of communication in the network[6].

Specific design and implementation are as follows:

- The implementation of two-way identity authentication is based on the challenge/response authentication scheme. The two-way identity authentication is achieved through the difficulty of solving the elliptic curve discrete logarithm combined with authentication technology.
- The selection of Hash function: Hash function commonly used with MD5 and SHA-1. The security of SHA-1 is higher than MD5 and the energy consumption is only slightly higher than that of MD5 in the energy consumption test of mobile terminal to perform Hash function. So SHA-1 is selected as the hash function[7].
- The construction of one time password: the International Mobile Equipment Identity is used as the generation factor of one-time password. At the same time, the hash function is used to construct a one-time password by join the random number in order to prevent from the root of the decimal attack.
- The choice of encryption algorithm: ECC has the advantage of small amount of calculation, fast processing speed, small storage space and high strength of the key unit in the security compared with the widely application of RSA and DES system under the same security intensity. So ECC is selected as the encryption algorithm.

B. The Description of Identity Authentication

The identity authentication scheme is divided into two parts: the registration phase and the authentication phase. The registration stage mainly completes the selection of the user’s password and the exchange of the public key between the client and the authentication server. The authentication phase mainly completes the two-way authentication between the user and the authentication server. The symbols and descriptions involved in this scheme are shown in table 1.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>user</td>
</tr>
<tr>
<td>AP</td>
<td>Wireless access point</td>
</tr>
<tr>
<td>AS</td>
<td>Authentication server</td>
</tr>
<tr>
<td>LS</td>
<td>Log server</td>
</tr>
<tr>
<td>DS</td>
<td>Database server</td>
</tr>
<tr>
<td>Internet</td>
<td>Internet resource</td>
</tr>
<tr>
<td>ID_x</td>
<td>Identity of X</td>
</tr>
<tr>
<td>P_u</td>
<td>Password of user</td>
</tr>
<tr>
<td>k_u</td>
<td>Public key of user</td>
</tr>
<tr>
<td>k_s</td>
<td>Private of user</td>
</tr>
<tr>
<td>k_s</td>
<td>Public key of server</td>
</tr>
<tr>
<td>k_s</td>
<td>Private key of server</td>
</tr>
<tr>
<td>PECC</td>
<td>Parameters of elliptic curve cryptosystem</td>
</tr>
</tbody>
</table>
1) The registration phase: In the registration stage, the client can use the ECC parameter set to generate public key and private key of the authentication server and the client. Then the identity and public key are exchanged between the client and the authentication server. The registration process is as shown in figure 2.

After receiving the message, the authentication server uses its private key to decrypt the message to get \( ID_U, P_W, K_{UR} \) and IMEI. The registration is successful if the \( ID_U \) is not consistent with the \( ID_U \) in the database after decryption.

If the registration is successful, the \( ID_U \) will be stored in the database server binding with \( IMEI, K_{UR} \) and \( P_W \). The successful registration information is sent to the client, so is the identity of authentication server encrypted by the \( K_{UR} \).

The client decrypts the message to get \( ID_{AS} \) after receiving the message. The registration phase has been completed.

2) The authentication phase: In the authentication scheme, the authentication request will be redirected to the authentication server after the request is made. The client has an access to the Internet in the case that the authentication is completed by the authentication server. The identity authentication phase process is shown in Figure 3.

- The authentication selects the suitable elliptic curves for initialization and then chooses \( K_{SR} \) and \( K_{SS} \) as the key pair. In order to accelerate the speed of encryption and decryption, it chooses the smaller tarsus factor under the premise of ensuring safety.
- The user initiates a registration request to the authentication server through secure channels.
- The PECC will be sent to the user together with \( K_{SR} \) after the authentication server receiving the registration request.
- The user stores \( K_{SR} \) and selects \( K_{UR} \) and \( K_{US} \) as its own key pair.
- The user input \( ID_U \) and \( P_W \), and then encrypts \( ID_U, P_W, K_{UR} \) and IMEI by \( K_{SR} \) to get \( E(K_{SR}, ID_U || K_{UR} || IMEI || P_W) \). The result will be sent to the authentication server.

U → AP: \( ID_U || ID_{Internet} \) The clients search for the corresponding wireless access points and request access to resources through the browser.
Advances in Computer Science Research, (ACSR), volume 52

The user’s request is redirected to the authentication server for authentication after the access point receiving the user’s http request. The authentication server verifies whether the user is legitimate based on the data of the inventory server. If the information of the user cannot be find in the inventory, it does not have access to resources.

- AP → AS: \( ID_U \) The public key of the client will be inquired according to \( ID_U \) after the relevant client is found in the database storage server. The authentication server generates a random number \( R \). Then the identity of authentication server and the random number \( R \) are encrypted by \( K_{UR} \) to get \( E(K_{UR}, ID_{AS} \| R) \). The result is sent to the client and a copy of \( R \) is retained at the same time.

- AP → U: \( E(K_{UR}, ID_{AS} \| R) \) The client decrypts the message got from the wireless access point to get \( ID_{AS} \) and \( R \). If the comparison of \( ID_{AS} \) and \( ID_{AS'} \) is different, the client refuses to step down the authentication.

- \( U → AP: E(K_{SR}, ID_U \| H(IMEI \| R \| P_w) \| R_U) \)\n  \[ \text{Sign}_{K_{AS}}(E(K_{SR}, ID_U \| H(IMEI \| R \| P_w) \| R_U)) \]

- The client hashes the random \( R \), \( P_w \) and \( IMEI \) to get \( H(IMEI \| R \| P_w) \) and then generates a random number \( R_U \). It encrypts \( R_U, H(IMEI \| R \| P_w) \) and \( ID_U \) by the public key of authentication server and then uses the private key of the client to sign the result. The final result will be sent to the wireless access point and the copy of \( R_U \) will be retained.

- \( AP → AS: E(K_{SR}, ID_U \| H(IMEI \| R \| P_w) \| R_U) \)\n  \[ \text{Sign}_{K_{AS}}(E(K_{SR}, ID_U \| H(IMEI \| R \| P_w) \| R_U)) \]

- The wireless access point sends the message got from the client to the authentication server. The authentication server knows the \( R_U, H(IMEI \| R \| P_w) \) and \( ID_U \) by decrypting the message. The authentication server searches \( IMEI \) and \( P_w \) in the database by \( ID_U \). Then it hashes \( IMEI, P_w \) and \( R_U \) to get \( H(IMEI \| R \| P_w) \). The authentication result can be known through the comparison of \( H(IMEI \| R \| P_w) \) and \( H(IMEI \| R \| P_w') \). If the result is different, the client is considered to be a risk.

- AS → AP: \( E(K_{UR}, ID_{AS} \| H(IMEI \| R_U)) \)\n  \[ \text{Sign}_{K_{AS}}(E(K_{UR}, ID_{AS} \| H(IMEI \| R_U))) \]

- If the client’s identity is verified, the authentication hashes \( R_U \) and \( IMEI \) to get \( H(IMEI \| R_U) \). And then it encrypts \( H(IMEI \| R_u) \) and \( ID_{AS} \) by the public key of the client and then uses the private key of the authentication server to sign the result. The final result will be sent to the wireless access point.

- \( AP → U: E(K_{UR}, ID_{AS} \| H(IMEI \| R_U)) \)\n  \[ \text{Sign}_{K_{AS}}(E(K_{UR}, ID_{AS} \| H(IMEI \| R_U))) \]

- The wireless access point sends the message got from the authentication server to the client. The client knows the \( H(IMEI \| R_u) \) and \( ID_{AS} \) by decrypting the message. The comparison of \( ID_{AS} \) and \( ID_{AS'} \) is done firstly. If the comparison of \( ID_{AS} \) and \( ID_{AS'} \) is different, the client refuses to step down the authentication. If same, the client hashes \( R_u \) and \( IMEI \) to get \( H(IMEI \| R_u) \). The authentication result can be known through the comparison of \( H(IMEI \| R_u) \) and \( H(IMEI \| R_u') \). If the result is different, the authentication server is considered to be a risk. The administrator will take measures to deal with abnormal situation.

- AS → LS: \( LOGS \) Whether the authentication result is success or failure, the authentication will request to generate a log by the log server.

- AP → Internet: \( ID_{Internet} \) The client has an access to the Internet resources through the wireless access point.

### IV. SAFETY ANALYSIS OF IDENTITY AUTHENTICATION SCHEME

The safety of the identity authentication protocol is analyzed from the perspective of the attacker.

- A replay attack. In this authentication scheme, it is assumed that the attacker cannot carry out replay attack on the authentication server’s reply message or the client’s request message, because the message contains random number. Even message retransmission, the client and authentication server will verify the efficiency of the random number after receiving the retransmission message. Apparently retransmission message could not be validated, in other word, it cannot complete the certification process.

- Fake server attack. This scheme uses two-way authentication different from the traditional one-way WiFi authentication scheme. It is assumed that the attacker impersonating authentication server by “fishing” prompt user authentication. The attacker intercepts the user’s authentication request and then forges it. The client decrypts the message forged by the attacker to get \( ID_{Adv} \). The comparison of \( ID_{Adv} \) and \( ID_{AS} \) is different, so the forgery of authentication is failure.
The small number attack. It is assumed that the attackers intercepted a certain number of certified seeds and iterative values and then carry out a small number of attacks. The authentication scheme does not save the authentication information of last successful login password, so it can prevent the small number attack fundamentally.

The network eavesdropping attack. This scheme ensures the security of the transmission information by encryption and hash technology. It is assumed that the attackers intercept authentication packet between the client and the authentication server. However, in the process of certification, all messages are passed through the encryption processing. Only the client and the authentication server have the corresponding private key which can be used to decrypt the encrypted message. Therefore, the attacker cannot get the corresponding content because of no the private key after the message eavesdropping.

The message tampering attack. It is assumed that the attackers intercept authentication packet between the client and the authentication server. However, in the process of certification, all messages are passed through the encryption processing. The attacker could not get the content of the text, so the authentication message could not be tempered with.

The man-in-the-middle attack. The scheme uses a two-way authentication. Generally speaking, middle attack can break any agreement which does not involve some kind of secret. The man in the middle without a corresponding private key still cannot get the correct password even if he intercepts the message between the user and the server[8].

V. CONCLUSIONS
This paper analyzes the security threats of identity authentication in the wireless environment based on the current status of the identity authentication scheme. A bidirectional identity authentication scheme is proposed, in the view of the characteristics of identity authentication in WiFi environment combined with the characteristics of high security requirements in some occasions. It is easily to know that this scheme can effectively prevent replay attack, fake server attack, small number attack, network eavesdropping attack, message tampering attack and man-in-the-middle attack. It is suitable for application to the security requirements of the higher WiFi wireless authentication environment. The next step will be to carry out the simulation of the authentication scheme and formal analysis of the scheme to prove the practicability and rationality of the authentication scheme.

REFERENCES