The Design and Implementation of the Wireless Network Identity Authentication System based on the Hybrid Encryption Algorithm

Yongbing Xu[a], Junyi Wang[b]

The computer college of Inner Mongolia University,Hohhot China 010021

[a] fengjiexyb@163.com, [b] Corresponding author wjyi@imu.edu.cn

Keywords: Wi-Fi; Identity Authentication; SM2;SM4

Abstract. Wi-Fi is a combination of the computer network and wireless communication technology. It uses wireless channel to access networks. With its characteristics of high speed,flexible,easy to manage and extension,etc,it has quickly become one of the most effective way of broadband access. But it was also because of it is widely used, gives some people with bad intent an opportunity.In this text, based on SM2 and SM4 algorithm which is recommended by the state password administration, a hybrid encryption algorithm has been designed and a Wi-Fi identity authentication system has been implemented, to increase security on the basis of ensure the Wi-Fi use convenience.

Introduction

Everybody is familiar with wireless hotspots. It is very common at the airport,restaurants, hotels and other places. Even in daily life,family,work place,it is also common occurance. Wi-Fi[1] hotspots is working in the end of the "mobile scenario" access the wireless Internet.Just as 3G / 4G mobile phone networks, there is a great demand for free Wi-Fi, faster Internet connection can have more application scenario.

The security of Wi-Fi is generally guaranteed by two parts[2], the access control and encryption. Access control is to ensure that only authorized users can access to confidential data. Encryption is to ensure only legitimate users can decrypt confidential data. In order to solve the Wi-Fi network security problem, The Wi-Fi alliance launched a Wi-Fi Protected Access (WPA) mechanism[3]-[4] in 2003.

For certification, the WPA forces users to provide relevant data to prove their legitimacy of access to some of the network resources. Certification of WPA is divided into two kinds[5]. One is 802.1 x + EAP[6], each user has a different password, verify legitimacy when user login the system. The other one is pre Shared key, set the password of the Wi-Fi hotspots, users who can connect the Wi-Fi hotspots need to know the password, but this way will have the following questions:

1) Need oral request password to access to free Wi-Fi in public, this will make the password leaked more likely.

2) In private, Wi-Fi password won't leak in oral way, but with the popularity of Wi-Fi password cracking software, simple Wi-Fi password is hard to resist brute force and dictionary attacks.

This article mainly aims at the shortcomings of the second authentication,has designed and implemented a Wi-Fi identity authentication system. The server software is installed on the computer which is connected to a wireless router.The client software is installed on the equipment which is prepared to link the Wi-Fi hotspots. The server software that allows the computer has capacity to manage all the equipment linked to the Wi-Fi hotspots,prevent unauthorized users "net" and safeguard the franchisor and the host user’s efficiency and security of Internet use. At the same time, to device users who have installed the client software, can have a good management to their used Wi-Fi hotspots, and avoid users connect to the forged hotspots which is provided by people with ulterior motives who fake own Wi-Fi hotspots into some well known in order to steal users' personal information.

The state password administration issued announcement no.23 on March 21, 2012. Some of the latest standard in password field published. In this paper, a hybrid encryption schem has been designed,implemented and applied which is based on the SM2[7] and SM4[8] algorithm reported by the announcement. Here is a simple introduction of the two algorithm.

Introduction of the encryption algorithm

SM2 algorithm. With the development of ciphergraph and computing technology, at present ,the commonly used 1024-bit RSA algorithm faces serious security threats. After research, the national cipher management department decided to adopt SM2 elliptic curve algorithm to replace the RSA algorithm, And asked the existing electronic authentication system based on RSA algorithm ,the key management system, and the application system to upgrade. SM2 algorithm belongs to the asymmetric keys algorithm, using the public key encryption and the private key decryption, and has shown that use the public key calculate the private key is not feasible. The sender encrypt the message with the recipient's public key, the receiver decrypt the ciphertext received with its own private key back into the original message.

SM4 algorithm. SM4 is a grouping symmetric key algorithm. The length of the plaintext is 16 bytes,so do the length of the key and ciphertext. The encryption and decryption key are the same. The encryption algorithm and key expansion algorithm adopts 32 rounds of nonlinear iterative structure. Decryption process is similar to the structure of the encryption process, just round keys using the reverse order.

The design and implementation of hybrid encryption algorithm

Modern cryptography plays a vital role in information security. SM4 algorithm computing speed is fast, but there is a disadvantage of complex key management and low security. SM2 algorithm with high security and simple key management, but it is slow and low efficiency when encryption and decryption the large chunks data. So almost no user will fully use public key cryptography,but it has played a big role in the traditional password distribution instead. Now design a hybrid encryption algorithm as follows:

Suppose A and B will communicate, then

① A generate a key pair (pk, uk)of SM2 algorithm, then send the public key uk to B.

② B generate a key sk of SM4 algorithm, and encrypt plaintext with the sk, then send it to A.

③ B encrypt sk with the public key uk from A,then send to A.

④ A decrypt the ciphertext from step ③ with pk ,then sk is available .

⑤ A decrypt the ciphertext from step ② with sk to get the original plaintext.

The implementation of SM2 - SM4 hybrid encryption algorithm

Because the SM2 algorithm need to generate a integer of dozens of bits, a free large numbers operation library named LibTomMath project is used in the program design, Mainly the mp_int data type and related operations of it.

First of all, communication sponsors generate the public and private keys of SM2 algorithm, which is the step ① in the process of the above algorithm, as shown in figure 1.

```
Step 01:On the client ,the public key and the private key of SM2 algorithm are g
enerated
parameters of SM2 algorithm are as follows:
the finite field p:122231814963284453970427532529463937309705477380721777840290 9

the parameter A of curve:553278779
the parameter B of curve :570938691199
the X coordinate of G point of curve:967600499
the Y coordinate of G point of curve:30098449625819
the private key dB:17478496821957212648417360423828565850 7
the X coordinate of public key:32915636719150588616983072339881433477796522867 06
08541119213
the Y coordinate of public key:11891553037991935995859827949428757566298127758 47
147010024664
```

Figure 1 the step ① of hybrid encryption algorithm

Then the communication receiver step into ②③ of the hybrid encryption algorithms, the random

number which used to encrypt plaintext generated by the program automatically, as shown in figure 2.

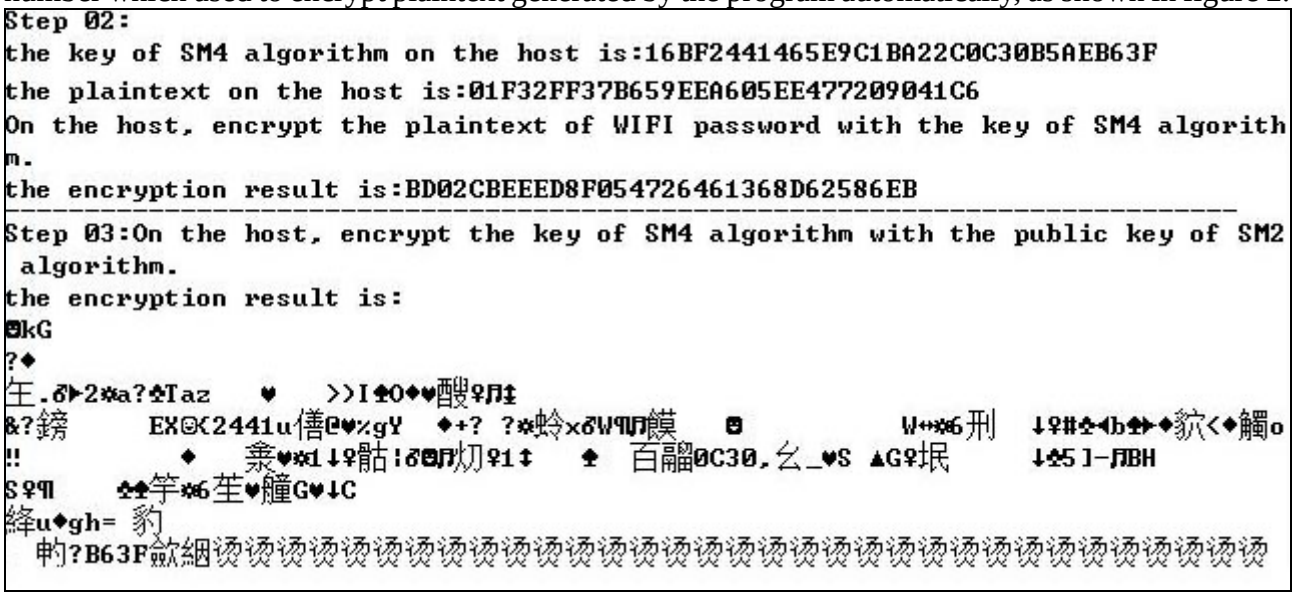

Figure 2 the step ② and ③ of hybrid encryption algorithm

At last,the communications sponsors step into ④⑤ of the hybrid encryption algorithms, and get the plaintext sent by the receiver, as shown in figure 3.

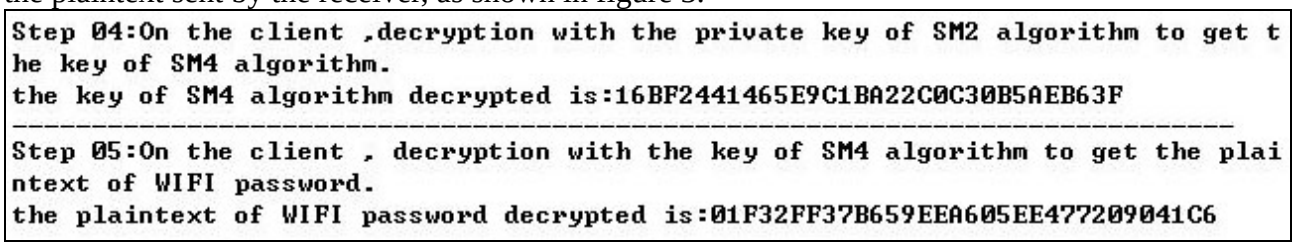

Figure 3 the step ④ and ⑤ of hybrid encryption algorithm

Run the program 10 times, and record the run time with functions in the time.h library every time. The test results are shown in table 1,and the average time is 1049.2 ms, which is in an acceptable range.

Table 1 algorithm running performance tests

times	1	2	3	4	5
run time（ms）	945	1010	1036	1124	1041
times	6	7	8	9	10
run time（ms）	1220	1010	1041	1016	1049

The design of Wi-Fi identity authentication system

The administrator add trusted users to the system database

The system administrator can add the trusted user’s information to the server database. When the users request for Wi-Fi hotspots connection, the system will send connection license information directly to the client, and allow them to use. The system administrator can avoid redundant work to confirm a large number of trusted user connection request .

Untrusted users request for connection to the system administrator

When users prepare to request for a Wi-Fi hotspots connection, the client first exchange the key with the hybrid encryption scheme, then collect user’s information to send to the server . The service remind the owner of Wi-Fi hotspots whether to allow the user to connect. If do not allow the user to connect, the owner can refuse or add the user to the blacklist.

If allowed to connect, then the owner of Wi-Fi hotspots adds the user into the whitelist,and sends the Wi-Fi password back to the client through the serve with the hybrid encryption algorithm. Then the user can access to the Internet through the Wi-Fi hotspots.

Trust the user to login

When connecting a used hot spots ,the user sends a registered users connection message to Wi-Fi hotspots owner. The owner may terminate or acquiesce its login. But registered users need to register again to ensure safety when Wi-Fi hotspots changed.

References

[1] Crow B P, Widjaja I, Kim L, et al: IEEE Communications Magazine, 1997, 35(9): 116-126.

[2] William Stallings: Cryptography and network security: principles and practices (Pearson Education,India 2006).

[3] Bulk F: Network Computing-Niles, 2006, 17(2): 65-70.

[4] Merino A S, Matsunaga Y, Shah M, et al.: Mobile Networks and Applications, 2005, 10(3): 355-370.

[5] Limin Zhu:The Research and Improvement of Wireless LAN Encryption Algorithm. Suzhou University, 2009.

[6] IEEE 802.1 Working Group: IEEE Draft P802. 1X/D11, 2001.

[7] GM/T0003-2012,SM2 elliptic curve public key cryptographic algorithms. In Chinese Information on http://www.oscca.gov.cn/News/201204/News_1229.htm

[8] GM/T0002-2012,SM4 the block cipher algorithm. In Chinese Information on http://www.oscca.gov.cn/News/201204/News_1229.htm

