The Research on NSC Key Service Mechanism in Mobile Network

Chenhe Zhu[1], Zhiyi Fang[2], Ying Wang[3], Qian Xu[4], Borui Jin[5]
Compute Science and Technology. Jilin University
Changchun, China
e-mail:yingw0517@hotmail.com

***Abstract*—Mobile Network Security Center (NSC) and its key service mechanism is an important part of the mobile network security management. In this paper, based on the analysis of the security requirements of the mobile network, put forward a key service mechanism for mobile networks (NSC), including the management structure, the hybrid encryption methods as well as key distribution mode. Through comparative analysis proved the effectiveness and practicality of the hybrid encryption method D_R.**

Keywords-NSC; key distribution; encryption methods;DES; RSA

I . INTRODUCTION

Different from the traditional network, the characteristics of the mobile network node distribution dense, limited bandwidth, limited storage space and computing power, open to the environment, vulnerable to a variety of attacks and some other features, this makes it more difficult to obtain a higher level of security in a wireless network, transmission security issues is one of the particularly important issues. Key encryption transmission was the way to solve this problem.

In the key generation algorithm, symmetric key encryption technology in the DES encryption algorithm and asymmetric key cryptography RSA algorithm is the focus of this discussion. Key exchange symmetric encryption technology for secure communications in a safe manner, and the complexity of its size; Asymmetric cryptography encryption and decryption is slow; the size of the key is large; cannot apply to large amounts of data encryption and decryption.

Based on the above issues, This paper is to study the choice of key generation algorithm in the Linux-based Network Security Center (NSC) in the key distribution process, put forward a based on mixed confidential mechanism security service architecture, has significantly improved response speed and security.

II . RELATED WORK

The characteristic of mobile networks' open determines it's more vulnerable to the threat of attack than traditional computer networks form hacking, interception, modification, forgery and replay. At the same time, both in terms of mobile network system or from the network equipment and terminals, mobile network is faced with the complex and diverse security threats. These security threats can be divided into according to the network equipment security threats, in view of the wireless link security threats and security threat for mobile devices. Specifically, in view of the network equipment security threats, including: denial of service attack, unauthorized access, etc. In view of the wireless link security threats, including: malicious bandwidth, malicious listening (such as hijack, modify, and forged); Security for mobile terminal equipment, including: privacy, mobile software copyright protection, to prevent malicious software, and other issues.

A. Security services architecture

Mobile security key distribution mainly has two ways: the receiver gets keys from NSC and receiver gets the key from the originators, as shown in the Figure 1 below:

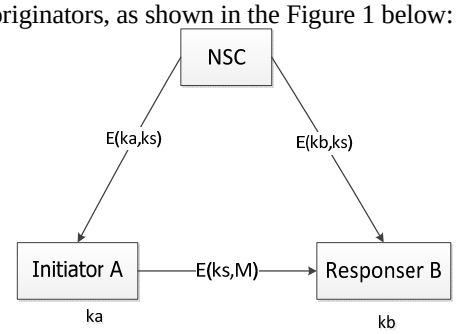

Figure 1.(a)Receiver gets the key from the NSC

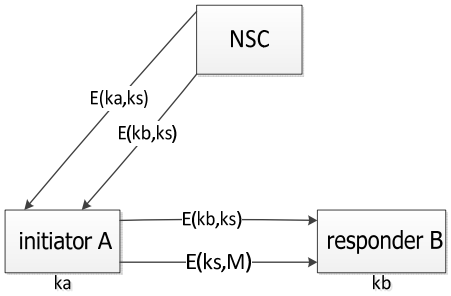

Figure 1.(b) Receiver gets the key from the initiator

Method of figure (a) there is a problem: if A is the initiate of the dialogue, sending message M to B, then the receiver B should get the key E (kb, ks) from NSC , and then get a message E (ks, M) from A , so that B can decrypt the received M. But B is likely to receive an encrypted message first, then gets the keys, and so cannot be to decrypt the message. Figure (b)'s method is more convenient: NSC transmits E (ka, kb) and E (kb, ks) to A, again by A transfers E (kb, ks) to B, A and B get key of ks, then A sends

message to B. In this article security service center uses the second security services architecture , that avoids the responder side B's packet which arrives ahead of the key, which is treated as rubbish disposal in figure (a), to save the link bandwidth, shorter the time of packet distribution, but also improves the efficiency of communication.

B. DES encryption algorithm

The earliest, the most famous secret key and symmetric key encryption algorithm DES (Data Encryption Standard) is developed by IBM in the 70s. DES is selected by American government in government's encryption standard, and then accepted by the National Bureau of Standards and the American National Standards Institute. The diagram below shows the schematic diagram of DES[1].

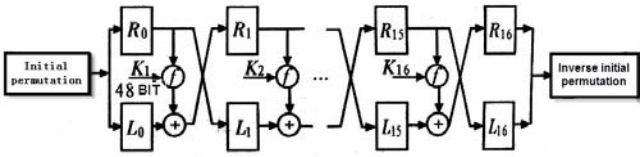

Figure 2. The principle of DES encryption algorithm

DES use 56-bit key to encrypt 64-bit data block. There are 16 identical stages of encryption processing, termed rounds. The keys used for each rounds are generated by the original 56-bit key.

C. RSA encryption algorithm

RSA encryption technology is a public key encryption; its name comes from the first three inventors Rivest, Shamir and Adleman. Here is a brief introduction to how to use this method.

First of all calculate some parameters [1]:

a) Choose two prime numbers p and q;

*b) n = p * q and z = (p-1) * (q - 1);*

c) Choose a number d which is z's co-prime;

*d) Identify e, making e*d = 1 mod z.*

Determine the public key and secret key: the public key consists of (e, n), secret key consists of (d, n).

When encryption, consider plaintext as bit string, and divided the bit string into blocks of k-bit, each can be seen as a positive integer m, which m < = n, so the size of the block k should be: 2k < n.

Encryption process is very simple: set X is plaintext information to encrypt, computing $Y = X^e \pmod n$, Y is the encrypted cryptograph.

Decryption process is very simple: set Y is plaintext information to encrypt, computing $X = Y^d \pmod n$, then X is decrypted by the ciphertext.

The security of RSA algorithm is based on the difficulty of large number's decomposition .People can find p and q by the factorization of public n, and then get z. If get z and e, it's easy to calculate d by Euclid's algorithm. But, for a very large number n, it is extremely difficult to do factorization problem, so it is difficult to get p and q from n. Compared with the traditional DES algorithm, the security of the RSA algorithm is higher, but the speed compared to other symmetric algorithm and DES is much slower.

III . SECURITY CENTER BASED ON A HYBRID ENCRYPTION METHOD

A . *Overview of security service center*

If user A and user B want to communicate with each other, first of all, they must obtain safety communication channel, the respective communication key ka and kb which only security service center known, with security service center; Second, communication sponsor A take an agreement with security service center by the key ka obtained from security service center to set up a Shared key ks which used between user A and user B when they communicate. After generating Shared communication key ks, security service center sent E(ka, ks) encrypted by the key ka and E (kb, ks) encrypted by the key kb to the user A. Then user A sent E (kb, ks) to the user B, waiting for confirmation of receipt of user B. Now the process of establishing secure communication channel between user A and user B is completed; finally, user A sent E (ks, M) to the user B to complete the interaction with user B. The specific process is shown in figure 3.1.

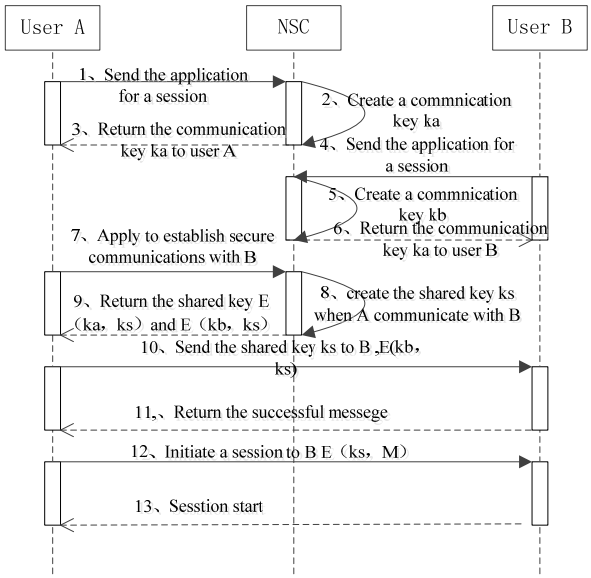

Figure 3. Security Service Center interaction diagram

In Figure 3, the sequence of the applications of user A and user B for the key is not fixed. And it's easy to find that the main work of security service center is to generate and distribute keys. Therefore, the focus of this research is the step2, step5 and 8 in the above, and the main consideration is how to choose the key generation algorithm in order to improve the efficiency of security service center.

B . *Mechanism of hybrid encryption algorithm*

Traditional security service center consists of a fixed encryption algorithm to complete all of the encryption work, such as DES encryption algorithm, RSA encryption algorithm and so on. For the safety performance of DES encryption algorithm is not high, and the realization of RSA encryption algorithm is slower which dues to the low efficiency problem, we introduce the D_R mixed encryption algorithm.

The mechanism of hybrid encryption algorithm D_R is the mixed use of DES encryption algorithm and RSA encryption algorithm, which combines the advantages of DES and RSA, and cleverly made up the problem of two kinds of encryption algorithm. Main idea: Based on the fast speed characteristics of DES encryption algorithm, adopts the DES algorithm to encrypt communication both sides specific communication content (including pictures, music, video, etc.)Between the user A and user B; Based on the high safety characteristics of RSA, in the network communication, RSA algorithm was used to encrypt the transmission key. The process is mainly used for key distribution to both sides of communication in the security service center. The specific application is shown in Figure 4 and Figure 5.

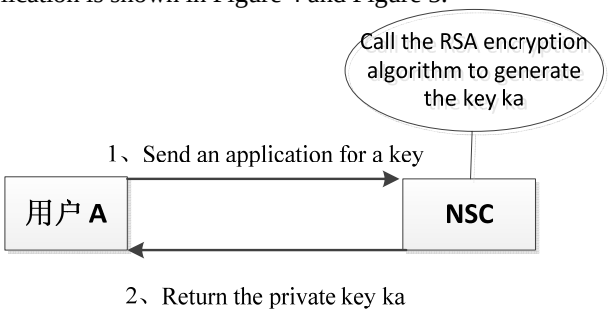

Figure 4. User application the key for the session

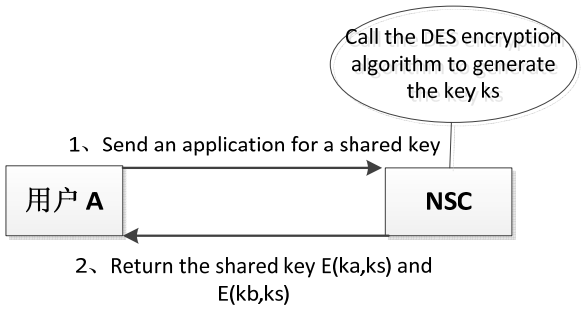

Figure 5. User session share the key

Figure4 and Figure5 is the specific application process of the hybrid encryption algorithm in the security service center .The security service center based on hybrid encryption algorithm, generally, is where using the DES encryption algorithm to generate a shared key used to realize secure communication between the two client and adopting symmetric encryption algorithm RSA to generate the key which is used to realize secure communication between the single client and the server. On one hand, it's a full use of the fast and highly efficiency characteristic of the DES, on the other hand, it takes the high safety characteristics of RSA into account. At the same time it makes up for the shortcomings of the low safety performance and the slow realizing speed in the encryption algorithm.

C . *Algorithm application processes*

The work process of the security service center based on hybrid encryption algorithm is similar to that of a traditional security service center. There's certain change only on the choice of encryption algorithm. The specific flow chart is shown in Figure 6.

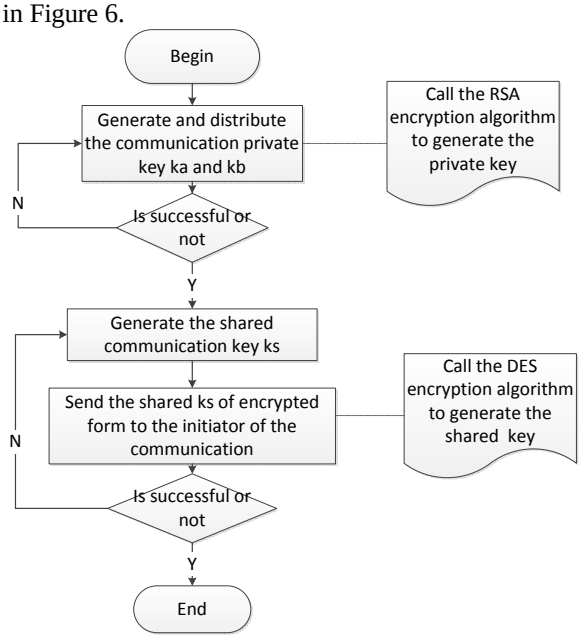

Figure 6. Security service center key distribution diagram

Figure 3.3 shows the workflow of the security service center based on hybrid encryption algorithm. When two web clients communicate, security service center work steps are as follows:

a) Respectively, assign individual session key ka and kb for the user A and user B . Here, in view of the limited data quantity of the communication content, we use the RSA encryption algorithm to generate personal session key;

b) Receive the application for a session which needed a shared key;

c) Generate a shared key ks used when the two clients communicate. Because both sides of the communication involves the transmission of large data files, we use the DES encryption algorithm to generate the shared key;

d) Security service center send two the shared key ks in the form of the ciphertext severally encrypted by the key ka and kb to the session initiator;

e) After confirming the receipt of the shared key by both sides, the security service center completed a communication key distribution.

IV . THE TESTING AND EVALUATION IN PROPERTY

Based on the traditional Security Service Center, Security Service Center which is based on mixed encryption algorithm changes something in the choice of algorithm next is the main reflection of result after changing:

a) Security: Security Service Center which is based on Mixed encryption algorithm has a high security which is inherited from RSA, and it provides a communication channel with a high security for both sides of communication.

b) The speed of response: Security Service Center which is based on Mixed encryption algorithm, does not have the disadvantage that it encrypts many data with a low speed by RSA, however, it is by DES. It improves the response speed of Network Service Center by improving the encryption speed.

c) The novelty: Security Service Center which is based on Mixed encryption algorithm, employs the secret apparatus of Mixed encryption algorithm. In the subsequent study, we can accomplish the encryption of Security Service Center with one or more better algorithm.

d) The practicability: Security Service Center which is based on Mixed encryption algorithm, uses two traditional encryption algorithms, and it can be accomplished simply and used easily.

Security Service Center which is based on mixed encryption algorithm improves the response speed and maintains the security in the communication process compared with the traditional Security Service Center. So it improves the whole efficiency. The next is the table which compares the access control based on role and attribute with the one based on implicit role and attribute.

TABLE I. COMPARISON OF APPLICATION EFFECT

Advantage and disadvantage / Security service architecture	**Advantage**	**Disadvantage**
（DES）	Fast response, simple implementation	Weak security
（RSA）	Simple implementation，high security	Response slowly , not suitable for large data encryption
（DES&RSA）	Fast response speed, high security, easy realization	Control of complex processes

From the table we can conclude that Security Service Center which is based on mixed encryption algorithm has a distinct improvement compared with the traditional Security Service Center, such as high security, high response speed and high practicability.

V . CONCLUSION

With the development of information technology, people have more and more strict requirement for the security of Network communication. Therefore, it is very important to improve the security of Network Security Service Center. This page shows a study in the architecture of traditional Network Security Service Center, and some changes in the application of encryption algorithm, and the improvement in the whole property of Security Service Center. However, actually, there is an extensive improvement place in the model, Such as the improvement of security service architecture and the choice of encryption algorithm. Therefore, we must do more study just for better security service architecture.

REFERENCES

[1] M. Xu. Gaochao. Distributed Computing Systems, Beijing:High Education Press., pp. 124–141, January 2004.

[2] Y.Jun Fan., Research on Authenticated Key Exchange Protocals Applications in Wireless Mobile Network, Beijing: Beijing University of Posts and Telecommunications,March 2012.

[3] P. He, Q. Xu, R. Liu, “An improved tripartite authenticated key agreement protocol from pairings,” IEEE Transl. Hubei, China, vol. 2, pp. 110–113, January 2010.

[4] K. Elissa, “A novel key management scheme using biometrics,” unpublished.

[5] Y.Zhou,Y.Fang, A scalable key agreement scheme for large scale networks,J. Name Stand,CA: Networking, Sensing and Control,2006.

[6] S.Yan, Y. Kai,D.Yingzi,O. Scott, Z.Xukai, A novel key management scheme using biometrics, CA: Mobile Multimedia/Image Processing, Security, and Applications 2010, 2010.

[7] Diffie W, Hellman M. New Direction in Cryptography. IEEE Transaction on Information Theory, (22)6,1976,pp. 644-654.

[8] S. Blake-Wilson, D. Johnson, and A. Menezes. Key agreement protocols and their security analysis. In Proceedings of the 6th IMA Int.l Conf on Cryptography and Coding, LNCS 1355:30-45, 1997.

[9] T.H. Chen, W.B. Lee, Anew method for using hash functions to solve remote user authentication, Computers and Electrical Engineering 34 (2008) 53-62.