Solution to Secure Instant Messaging Based On Hardware Encryption

Hong-Bao Qin, Xin Xu

Hangzhou Dianzi University, Hangzhou310018, China
silencewonder@163.com, xuxin@runcore.com

Abstract: For a verity of security issues such as privacy breaches in Instant Messaging（IM）, this paper proposes a security solution based on hardware encryption. The solution applies symmetric encryption to ensure data security, asymmetric encryption to ensure the safety of the session key transmission, and the security of both kinds of key is ensured by hardware encryption, which enables secure key management. The performance analysis showed that the solution proposed in this paper was more efficient and security.

Keywords: Hardware encryption; Key management; Asymmetric encryption; Symmetric encryption; Instant Messaging

1 Introduction

Instant messaging (IM) is a real-time Internet communication [1]. By IM, users on the network can transfer text, voice, video and other information in real time, and exchange data in the way of peer to peer [2]. With the development of mobile Internet technology, instant messaging has been increasingly applied to work communication and government office, in the process of communication transmission, chat content and sensitive data can be easily intercepted [3]and that would reveal important information of users. Security issues have been taken more seriously [4].

The current studies of instant messaging more focus on the realization of the communication function, the security mostly is based on the protocol of the communications protocols. In the security scheme of instant communication system, it is mostly assumed that the servers are totally credible [5], however they are actually not. Plug-in units or software encryption are applied for existing instant messaging systems in other studies[6].In the existing encryption methods for instant messaging, keys are often visible to servers. As a result, user personal information would be exposed when a server provider was not dependable [7] or servers were attacked[8]. On the other hand, it is easier to be cracked when software encryption is used. In order to solve the security problem in communication among IM users, the agreement of Instant Messaging Key Exchange (IMKE) [9] was designed by Mannan and Van Oorschot at 2006, which was easy to integrate into existing IM systems. However, a temporary pair of public key and private key pair is used in the agreement. The security of the agreement is based on credible servers, so that non-repudiation of messages cannot be ensured.

In modern cryptography technology, cryptography and cryptographic algorithm are published, while the key is the real secret in cryptographic system. The security of data is entirely dependent on the security of key management [10]. Therefore, key management becomes the most critical and difficult part of cryptography.

A secure instant messaging solution based on hardware encryption [11] is proposed in this paper. In the solution, the symmetric encryption method is introduced for communication data security, the asymmetric encryption method is introduced for the session key transmission security, and the hardware encryption method is proposed to solve the problem of key management. The solution presented in this paper shows high execution and effectiveness, to ensure the safe and reliable IM.

2 Relatedtechnologies

Cryptography is the core of information security technology [12]. The modern cryptography system is divided into two types: symmetric cryptosystem and public key cryptosystems. In the symmetric cryptosystem, the encryption and decryption use the same key or can derive each other, there is simple calculation of the relationship between the encryption and decryption key. Symmetric encryption algorithm is based on the popular DES, AES algorithm. Asymmetric cryptography is also called public key cryptosystem. It refers to the encryption and decryption keys are not the same, or that cannot be deduced from one another. The most widely used asymmetric algorithm is RSA algorithm. In the Symmetric encryption algorithm encryption and decryption use the same key, resulting in the need to transfer key in the encryption and decryption process. Once key intercepted, data will be deciphered. Although there is a key management problem in symmetric encryption algorithm, but its encryption speed, suitable for large amount of data encryption, has been widely applied to data encryption. Unlike symmetric encryption algorithms, asymmetric encryption algorithm requires two keys: public key and private key. Public key and private key are a pair, if the public key used to encrypt the data, only using the

978-1-4673-7005-9 /15/$31.00 ©2015 IEEE

corresponding private key can decrypt; if the private key used to encrypt the data, then only the corresponding public key can be used decryption. Because encryption and decryption using two different keys, so this algorithm is called asymmetric encryption algorithm. The public key can be made public, while private key is saved personally. Non-symmetric encryption algorithm is the basic process of exchange of confidential information is that:

1. Party A will generate a pair of keys which a public key to the other side as the public;
2. Get the public key of B using the key pair to encrypt sensitive information sent to the owner;
3. Party then the other to save their own private key pair to decrypt the encrypted information.

Party only with their private key decrypts the encrypted public key by any of the information. Even if the public key is intercepted, the corresponding private key cannot be derived to decrypt. Non-symmetric encryption algorithm is good at confidentiality, it eliminates the need for end-users share a secret, but the encryption and decryption takes a long time, slowly, it is not suitable for file encryption and is only applicable to encrypt data on a small amount.

In fact, the safety and reliability of the information encryption system relies on the key and the key is the key information of encryption and decryption algorithm, so the key management is very important. Key is a life-cycle, which includes the effective time of the key and certificate, and the withdrawal of key and certificate maintenance time. Since the secret key requirements, which relate to key management issues, poor management, the key may be unintentionally leaked the same, not have the key to peace of mind, any password is only relative, is a prescription. Key management mainly refers to the key of the security management, including key generation, key backup, key recovery and key updates... Key management not only affects the security of system, and relates to the reliability, effectiveness and efficiency of the system.

In the hardware encryption system， encryption technology is solidified in the hardware control chip. Encryption is accomplished independently by hardware without outside interference. The message is transmitted in the form of cipher text and is not visible to the server. The message cannot be cracked even if the cipher text is intercepted because the key is stored in the hardware throughout and cannot be extracted. With respect to software encryption, hardware encryption is faster and more secure.

3 Design of schemes

The security solution based on hardware encryption proposed by this paper is implemented thought end to end encryption. The sender sends message in the form of encrypt text and the receiver decrypts the cipher text. The information of the message remains cipher text in the entire procedure and cannot be cracked, that makes the security of chat content and sensitive data. Even if the node is destroyed, the personal information is not exposed.

The structure of hardware encryption module is shown in Figure 1. It is responsible for key generation and key preservation. And it receives the data sent by communication terminal, encrypts data and sends them by communication terminal. Hardware generates keys including public/private key pairs and symmetric session key, and then submits his own public key to the server. The private key is used for signature, while public and private keys are used for symmetric session key exchanging management. The key which has proof of identity is stored in hardware and server beforehand and is used for verifying the legitimacy of the hardware. To ensure safety, the hardware cannot be disassembled and automatically will be destroyed when under attack[13], which making encryption circuit cannot be copied and cracked[14]. At the same time the hardware would send a notification to the server to replace and update the key. This makes the security of key management .All the keys includes asymmetric keys and symmetric keys are persisted in hardware.

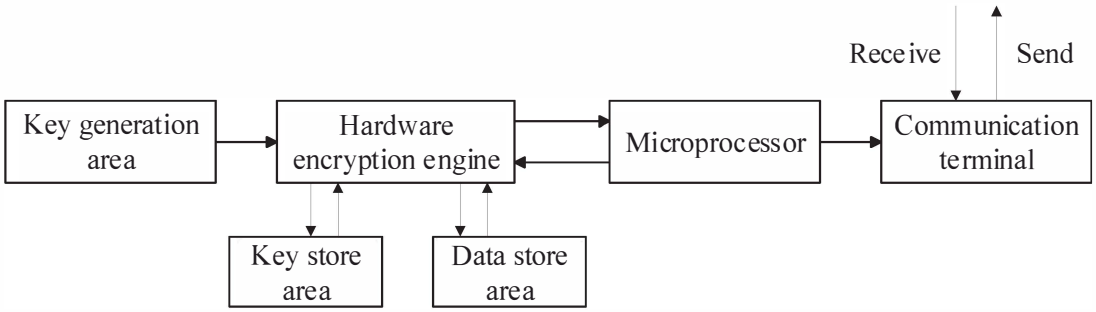

Figure1 Handware Encryption Module Structure

The server is involved in the exchange of public key, while there is mutual verification between the sever and communication parties A and B. Server issues digital certificates, receives and maintains the user's public key, cooperates with the user's public key exchange, cancels or abandoned user and his public keys and certificates. Figure 2 shows the process of the public key exchange in asymmetric encryption.

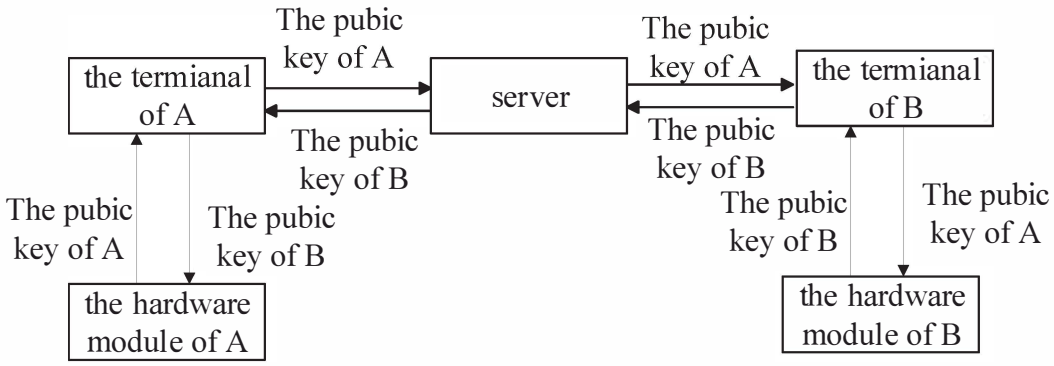

Figure 2 Key Exchange in Asymmetric Encryption

After the transmission of the session key as shown in the Figure 3, we can communication absolutely securely.

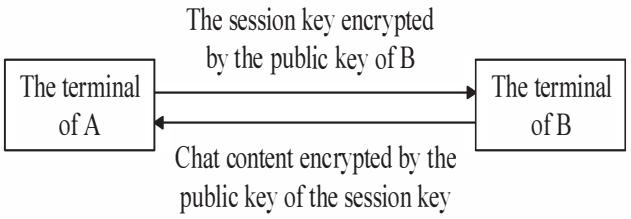

Figure 3 Transmission of the Session Key and the Cipher

Encryption and decryption process: data encryption used symmetric algorithm, which is implemented by hardware. After the process startup, the system automatically sends the hardware instructions to encrypt data, and the hardware receives this instruction. Firstly the hardware receives plaintext data from the host, data encryption, and then calculates the encrypted hash value, and sign with his own private key. In the decryption time, the system send decryption instruction to the hardware, the hardware received this instruction. Firstly the hardware receives cipher text from the host, decrypts the information of the other party with his public key and gets the hash value; and then calculates the hash based on the cipher text data, and compares with the received hash value. If the two values are equal, then use the appropriate corresponding key to decrypt the data to get the plaintext.

4 Analysis of security and performance

We have symmetric encryption for chat content and asymmetric encryption for the transmission of session key. The hardware module is responsible for encryption and decryption process as well as key generation and key preservation.

4.1 Analysis of security

If the current communications between the two sides, there is an attacker to obtain the communication content, there are two main ways: one is based on the intercepted cipher text information and the communication characteristics of symmetric encryption algorithm, analyze out plaintext;The two is to intercept the session key,decrypt thought the intercepted cipher text;The three is to obtainthe private key which is used for transferring the session keys.

For the first method, its difficulty depends on the strength of the symmetrical encryption algorithm in the scheme adopts, using one-time encryption strategy, it is difficult to achieve the known cipher text attack; For the second method, the difficulty is the equivalent of cracking the solution of non symmetric cryptography. Because of the essence of asymmetric cryptography, it is difficult or not the impractical in the calculation; For the third method, interception is not possible because the private key cannot be derived from the hardware. For the hardware attack, that depends on the encryption hardware itself. Using the strategyproposed inthis scheme, the security of the key can be ensured.

4.2 Analysis of performance

When users communicate, the speed mainly lies in the key generation and the encryption of the symmetric encryption algorithm. The symmetric encryption algorithm is well known for its encryption speed and has been widely applied to data encryption.Compared to software encryption, hardware encryption speed has obvious advantages.

From the result of analysis: this scheme not only has high safety, and high efficiency.

5 Conclusions

Although the instant messaging is more and more important, the existing communication system cannot meet the needs of the user security and privacy. We have present a new instant messaging scheme based on hardware encryption. The scheme makes full use of the well effect and speed of hardware encryption and decryption as well as the security and reliability of key generation and key preservation. We can achieve the security of key management and keep its usability,ensure the privacy and securitywhile not affecting the efficiency. The message in the transmission process remains in the form of cipher text and there is no risk of cracking. The result of analysis shows that the scheme we propose can further increase the reliability and security of

communication.

References

[1] Si-li Chen. The characteristics and developing trend of IM instant communication technology. Wireless Internet Technology, 2014, (12).

[2] Schoen I, Boberski M. Secure PKI proxy and method for instant messaging clients: U.S. Patent Application 10/133,202[P]. 2002-4-26.

[3] Jiang-Min Chen. Research and implementation of the protocol analysis technology for instant communication. University of Electronic Science and Technology of China, 2014.

[4] William S, Stallings W. Cryptography and Network Security, 4/E [M]. Pearson Education India, 2006.

[5] Hai Yang,Wen-tao,et al.Design and implementationof independent controllableinstant messagecommunication system based on Android. Electronic Design Engineering, 2015, (6).

[6] Shao-Lei Wang. The design and implementation of the Android client for“Mixun”- a secure communication software. Beijing Jiaotong University, 2014.

[7] Tong Yi, Xue-Bao Li, Hong-Chao Chen.A novel key exchange protocol for frequent communication. Computer Engineering &Science, 2014, 36(7).

[8] Zhi-QuanLv, Cheng Hong, Min Zhang, et al. Privacy-preserving scheme for social networks. Journal on Communications, 2014, 35(8):23-32.

[9] Mannan M, Van Oorschot P C. A protocol for secure public instant messaging [M]//Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2006: 20-35.

[10] Barker E, Barker W, Burr W, et al. Recommendation for key management-part 1: General (revised[C]//NIST special publication. 2006.

[11] Harper S, Athanas P. A security policy based upon hardware encryption[C]//System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on. IEEE, 2004: 8 pp.

[12] Venter H S, Eloff J H P. A taxonomy for information security technologies [J]. Computers & Security, 2003, 22(4): 299-307.

[13] Hong Shen, Shu Chen, Bi-Hai Tan. Key Protection Technology of Wireless POS Machinewith Self-destruction Function. Communication & Audio and Video, 2014, (2).

[14] Yu-Hao Zhang, Zhi-PengXu, Xin-RuiXu, et al. Design of Copy Prevention Circuit and SystemBased on AES Encryption Circuit. Chinese Journal of Electron Devices, 2015, (1).