2012 IACSIT Hong Kong Conferences
IPCSIT vol. 29 (2012) © (2012) IACSIT Press, Singapore

A Fair and Secure Key Escrow Scheme under Diverse Transmission Circumstances with Lawful Investigation

Bing-Chang Chen[+]

Department of Information Communication, Southern Taiwan University, Taiwan

Abstract. For achieving the purposes of protecting privacy of messages and enforcing law investigation simultaneously, the key escrow system was proposed. By the key escrow system, the messages can be sent confidentially between users. If necessary, an investigator can play the role of judge to wiretap the suspicious communication. In this paper, we introduce the original key escrow system proposed by US government and show some weaknesses which make them unfair. In order to make a key escrow scheme fairer, we propose a new key escrow scheme in which only the investigator who has the law authentication can recover the messages.

Keywords: Cryptography, Data Security, Privacy, Key Escrow System

1. Introduction

It is important to protect a communication message using a cryptosystem no matter what the cryptosystem is, a symmetric encryption like DES [11] or an asymmetric encryption such as RSA [8]. Especially, a most confidential and sensitive document is going to be transmitted to the opposite person. Usually, a confidential document is encrypted by a session key or the receiver's public key, and hence a ciphertext is generated, then the ciphertext is decrypted by the same session key or the receiver's secret key. In the symmetric encryption mode, two parties had to generate a session key cooperatively before.

The purpose of key escrow scheme[1,4,5,6,7,10] is for the privacy of messages and also preventing the criminal behavior. The messages can be transmitted confidentially between users and monitored by the investigator for the law enforcement authentication.

In order to prevent the criminal activities between the two communicating persons, it needs an agent or government to play the role of eavesdropping the suspicious messages. In April 1993, the US government announced a new proposal called key escrow system [2] which presented for the sake of providing the communicated information secretly and preserving the ability of law enforcement agents to wiretap the dubious documents.

In 1994, US government announced the Escrowed Encryption Standard (EES) which composes of a symmetric encryption algorithm SKIPJACK and a key escrow algorithm embedded in a tamper-free chip [3, 12]. The security of EES depends on the physical protection of the tamper-free chip.

In this paper, we review the US key escrow system and describe the defects of this scheme in Section 2. In Section 3, we propose a new key escrow scheme which prevents the investigator to monitor the messages without law authentication.

2. The US Key Escrow System

For the law enforcement, the key escrow system was proposed by the US government to monitor the communication contents. The scheme is implemented by the SKIPJACK algorithm in a tamper-resistant

[+] Corresponding author. Tel.: +886-6-2533131; fax: +886-6-3010020.
E-mail address: bcchen@mail.stut.edu.tw.

hardware device. This device is a chip which consists of unique identifier, device unique key, and common family key of the group. In this section, we introduce the system as follows.

Before user A transmitted an encrypted message to user B, A had to negotiate a session key KS with B. The session key KS is used to encrypt and decrypt the message. Then A input the message M and KS to $Chip_{\mathrm{A}}$. After that, $Chip_{\mathrm{A}}$ generated an initial vector(IV) and a law enforcement access field($LEAF$), where

$$LEAF = ((KS)_{\mathrm{KU_A}},UID_{\mathrm{A}},EA)_{\mathrm{KF}}$$

$$EA = h(UID_{\mathrm{A}},KS, IV\,)$$

$LEAF$ is the message encrypted by the common family key of the group KF. In $LEAF$, $(KS)_{\mathrm{KU_A}}$ represents the session key KS encrypted by A's device key KU_{A} which was escrowed by two key escrow agents, UID_{A} is A's identifier, and EA is the one-way hash function including UID_{A}, KS, IV.

User A generated and transmitted the ciphertext $(M)_{\mathrm{KS}}$ which was encrypted by SKIPJACK with the session key KS to B . Also, IV and $LEAF$ were delivered to B. After receiving the ciphertext, B could decrypt the message by the session key KS. For the assurance, $Chip_{\mathrm{B}}$ decrypted $LEAF$ by KF and got EA. The accuracy of communication can be checked by verifying EA. If it is true, B can obtain the plaintext M by decrypting the ciphertext using KS.

On the other hand, the investigator has the right to monitor the doubtful message for law enforcement. Once the investigator wants to request this obligation, he has to apply for the two partial key components which are safeguarded by two key escrow agents. By these two partial key components, he can acquire A's device unique key KU_{A}. Therefore, the investigator uses KF to decrypt $LEAF$ and then gets KS by KU_{A}. Eventually, the investigator can wiretap the communicated message between A and B by using the session key KS. The security of this system is based on the tamper-free hardware device.

Although the system solve the probable criminal problem, it seems unfair to the users who transmit the normal information. This scheme is aimed at the suspicious person not the doubtful message. The investigator can get the user's device unique key when he asks for the two key escrow agents. The investigator can keep this key after finishing the inspection. Hence he needs no help of the two agents and uses the preservative device unique key to obtain the subsequent session key between two users. Without law authentication, the investigator can easily listen to the secret communication messages.

Due to this disadvantage, we propose a new key escrow scheme which eavesdrops in accordance with the message only. The investigator can merely check one alleged message at one law authentication.

3. The Proposed Key Escrow Scheme

In this section, a new key escrow scheme is presented. Similarly, user A and user B have $Chip_{\mathrm{A}}$ and $Chip_{\mathrm{B}}$ to help them accomplishing the communication. These chips have their own device unique keys. These device unique keys have to be escrowed by two or more key escrow agents. In the US key escrow system, one investigator may obtain the device unique key from the cooperation of key escrow agents who still have no idea what the key is. As mentioned above, the investigator can store the device unique key and then get the later session key encrypted by the device unique key to wiretap the future communicated messages without applying for the law authentication. In our proposed scheme, the investigator has to request and recover the session key from the key escrow agents on each investigation. The investigator only knows the encrypted key of the investigated message. The device unique key is still secret.

Before A sends an encrypted message to B, they have to reach an agreement and generate a session key KS on each transmission. On user A's side, the session key KS is encrypted by KU_{A}, i.e. $(KS)_{KU_{\mathrm{A}}}$. Let e=KU_{A} be the encrypted key and $d=(KU_A)^{-1}\bmod\phi(n)$ be the decrypted key using RSA cryptosystem, where n = $p \cdot q$, p, q are large prime numbers, and $e\cdot d=1\bmod\phi(n)$.

User A selects two subkeys KU_{A1} and KU_{A2} and transmits to two key escrow agents securely. These two subkeys will be escrowed by the two agents individually. Even if the cooperation of the agents, the device unique key KU_A or the session key KS will not be leaked. Let

$d = KU_{\mathrm{A1}} \cdot a + KU_{\mathrm{A2}} \cdot b$

Find out a and b of the above equation, and then input them and the session key KS to the device. The device will generate the following messages.

$LEAF = ((KS)^{\mathrm{KU_A}}, a, b, UID_{\mathrm{A}}, EA)_{\mathrm{KF}}$

$EA = h(UID_{\mathrm{A}}, KS, IV)$

Afterward user A sends the ciphertext $C = (M)_{KS}$ along with $LEAF$ and EA to user B. User B can decrypt $LEAF$ and verify EA to assure the authenticity of session key. If it is true, user B can decrypt the ciphertext and recover the message.

On the investigation stage, the investigator first decrypts $LEAF$ and gets a, b, and $(KS)^{KU_A}$. Then the investigator forwards $(KS)^{KU_A}$ to the two agents. The agent $A1$ computes $K_1 = ((KS)^{KU_A})^{KU_{A1}}$ $(mod\ n)$ and returns K_1 to the investigator. Also, the agent $A2$ computes $K_2 = ((KS)^{KU_A})^{KU_{A2}}$ $(mod\ n)$ and returns K_2 to the investigator. On receiving K_1 and K_2, the investigator computes

$$K_1^a \cdot K_2^b (\mathrm{mod} n) = ((KS)^{KU_A})^{a \cdot KU_{A1} + b \cdot KU_{A2}} (\mathrm{mod} n) = (KS)^{KU_A \cdot KU_A^{-1}} (\mathrm{mod} n) = KS$$

Therefore, the investigator can use the session key KS to wiretap the suspicious message. During the investigation, the investigator only knows the session key, the device unique key is still secret. If the investigator keeps the session key, he cannot eavesdrop the future communicated messages without law authentication unless the users use the same session key.

In this scheme, we acquire the following advantages. (1)The receiver can conform the session key and retrieve the origin message; (2)The key escrow agents help the investigator obtain the session key and they have no idea what the session key or device unique key are even if the conspiracy. Without these keys, they cannot wiretap the messages illegally; (3)The investigator can only get the session key to monitor the doubtful message at each investigation. He is unable to obtain user's device unique key and messages can not be retrieved without legal authenticated investigation.

4. Security Analysis

The key escrow system has at least two basic properties. One is the user can securely transmit a message to one person. The other property is that it helps the investigator to wiretap the messages while the suspicious affairs were found. That is if there was no dubious found, no one can decrypt the ciphertext except the real receiver. In our proposed scheme, it has to satisfy these characteristics. In this section, we discuss the security analysis of proposed key escrow system. We classify the possible attacks into three types.

(1) The adversary is an outsider

When an outsider is going to wiretap the communication messages, the trivial method is to get the ciphertext and try to decrypt it. The first thing he has to do is to find the decryption key (session key). If he doesn't try to find this decryption key, he can only use brute-force attack to decrypt the ciphertext. But the brute-force attack is useless while the security parameter is large enough. The adversary can use two ways to try to attack. Because the session was escrowed by the agents, it was embedded in $LEAF$ and EA, where $LEAF = ((KS)^{KU_A}, a, b, UID_A, EA)_{KF}$, $EA = h(UID_A, KS, IV)$. From $LEAF$, if the attacker had the family key of the group, he can decrypt $LEAF$ and then obtain the inside messages. Unfortunately, KF was only known by the group members. Even if he can decrypt LEAF, he can't get the session key KS by $(KS)^{KU_A}$ without KU_A either. Unless he can solve the factoring problems of RSA and get d, where $d = (KU_A)^{-1}$. The attacker can use another way to find the session key by using the equation $d = KU_{A1} \cdot a + KU_{A2} \cdot b$. If $LEAF$ was broken, he could get a and b. In addition to these two numbers a and b, it still needs two secret keys, KU_{A1} and KU_{A2}, to compose of d. These two secret keys are kept by two key agent $A1$ and $A2$ respectively. Unless the attacker can conspire with these two agents and also decrypt $LEAF$ to get a and b, he couldn't get the session key KS. In another way, an attacker can get the message EA to try to attack. But EA was computed by one-way hash function, it cannot be converted, the only way to find the session key KS is to guess and try. It is also useless because it is an brute-force attack. From above, if the adversary is an outsider, he can't get any useful message to find the session key. Therefore, the illegal wiretap is impossible.

(2) The adversary is one of the key escrow agents

The missions of key escrow agents are to help the investigator to get the session key. But the key escrow agents have no idea what the session key is even they collude. If one or both of the key escrow agents are attackers, no one can get the session key using their secret key and the message the investigator transmitted. When the investigator wishes to solve the session key, he has to decrypt *LEAF* first, and then transmit $(KS)^{KU_A}$ to the key escrow agents. If one of the key escrow agents stores the message, he will get the session key when he can find the decryption key *d*. But *d* is composed of four elements including the secret keys of key agents,KU_{A1} and KU_{A2}, and two secret parameters, *a* and *b*, which are embedded in *LEAF*. None of the key escrow agents can get decryption key *d* without *a* and *b* even these two agents are colluded. Because these two secret keys *a* and *b* are embedded in *LEAF* which is encrypted by the family key *KF*, the key escrow agents can get *a* and *b* if they have the family key. But the family key only shares by the same group which doesn't include the key escrow agents. Therefore, the key escrow agents can't get the session key either.

(3) The adversary is the investigator

The investigator has the right to obtain the session key to wiretap the suspicious messages when he got the authority. On the contrary, the investigator should not ask the key escrow agents for the assistance of getting session key to eavesdrop the communication messages if there was no authority issued. Although the investigator may have the family key and then decrypt *LEAF*. If there is no assistance of key escrow agents, the investigator cannot get the session key by the decrypted messages, KS^{KU_A}, *a*, and *b* unless he can solve the RSA factoring problems and obtain $(KU_A)^{-1}$.

Finally, we conclude the above three situations, the proposed scheme is secure in any circumstances.

5. Conclusions

In this paper, we described the US key escrow system and pointed out some weaknesses in this scheme. It is unfair to the users who escrowed their keys. Although the investigator has the inspection authority, he cannot keep the key and retrieve the encrypted messages without law authentication. Especially, the sender can cheat the investigator to prevent the monitor in the later scheme. In order to resolve the weakness and make a key escrow scheme fair, a new key escrow scheme is proposed. In the proposed key escrow system, the investigator can eavesdrop the suspicious messages only when he got the authority.

6. Acknowledgements

This work was supported in part by the National Science Council of the Republic of China under the Grant NSC 100-2221-E-218 -037

7. References

[1] M. Bellare, and S. Goldwasser, "Verifiable partial key escrow," *The Fourth Annual Conference on Computer and Communications Security*, ACM, pp. 78-91, 1997.

[2] D. Denning, "The US key escrow encryption technology," *Computer Communications*, 17(7), pp.453-457, 1994.

[3] D. Denning, and M. Smid, "Key escrowing today," *IEEE Communications Magazine*, pp. 58-68, 1994.

[4] Y. Desmedt, "Securing traceability of ciphertexts: towards a secure software key escrow system," *Eurocrypt*'95, Springer-Verlag, pp. 147-157, 1995.

[5] J. He, and E. Dawson, "A new key escrow cryptosystem," *Cryptography: policy and algorithms conference*, Australia, pp. 105-114, 1995.

[6] L. Knudsen, and T. Pedersen, "On the difficulty of software key escrow," *Eurocrypt*'96, Springer-Verlag, pp. 237-244, 1996.

[7] Y.C. Lee, and C.S. Laih, "On the key escrow system without key exchange," *Computers and Electrical Engineering*, 25, pp. 279-290, 1999.

[8] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Commun. ACM*, 21(2), pp. 120-126, Feb. 1978.

[9] A. Shamir, "How to share a secret," *Communications of the ACM*, 22(11), pp. 612-613, 1979.

[10] K. Viswanathan, C. Boyd, and E. Dawson, "Hybrid key escrow: a new paradigm," *Computers & Security*, Vol. 21, NO. 1, pp. 77-92, 2002.

[11] FIPS 46-2, "Data Encryption Standard," National Bureau of Standards, U.S Department of Commerce, Jan, 1988.

[12] National Institute of Standards and Technology, "Escrowed Encryption Standard," Federal Information Processing Standards Publication, 1994.