http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (16): 3825-3830, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.3825.3830
© 2013 Asian Network for Scientific Information

A Key Escrow Scheme of the Escrow Agent with the Denial Right

[1]Qiang Fan, [1]Xu-chong Liu, [2]Hai-yun Liu and [3]Tianming Zhang
[1]Department of Computer Science, Hunan Police Academy, Changsha, China
[2]School of Computation Management, Hunan University of Commerce, Changsha, China
[3]Hunan Changgao High Voltage Switchgear Group Co., Ltd, Changsha, China

Abstract: The large-scale application of network heavily relies on the information security and the cryptography is the core of information security. The key escrow is one of the hot topics of encryption technology in recent years. As for the general key escrow scheme, the private key is divided into n parts and the private key can be reconstructed if k (k = n) escrow agents hand over their hosting parts. At the same time, one or several escrow parties can be also given several (fewer than k) key parts so as to have greater weight. But this is only the simplest weight consideration. The flexible set of the escrow parties (escrow agent) hasn't been considered in these schemes. In this paper, an important problem that is widely overlooked has been addressed, namely an escrow party is the most trusted or the most important who has the denial right. And the joint stratagem of all other agents is not workable over monitoring users without its participation. In this paper, the design of the key escrow scheme in which an escrow agent must participate has been described. The most important escrow party can be the notary public, the reliable department designated by the government or the authorities recognized by the government and the civil society. It should be cooperated with other escrow parties and the number of co-escrow parties should reach to the threshold value. Then the private key can be recovered.

Key words: Key escrow, escrow agent, denial right, advanced threshold scheme

DESCRIPTION OF SYSTEM

Assuming that there is a Key Management Center (KMC) in the cryptosystem that is responsible for issuing the public key certificate of the communication users. The escrow user (trustee) is represented by A, P^* is the most reliable escrow agent and Q is the set of other escrow agents $Q = \{Q_i|Q_1, Q_2,..., Q_{n-1}\}$. E refers to the monitoring of law enforcement agencies for the communications of users. a is the private key hosted by the user A. Ks is the session key which is used to encrypt the communication information among users. At the same time, the private key a can be divided into n parts which are respectively entrusted to P* and $Q_1, Q_2,..., Q_{n-1}$.

The monitoring of escrow user can be implemented by the cooperation of P* and k-1 ($k \leq n-1$) Q_i (the one-off online monitoring within the validity period or the perpetual off-line monitoring). However, the monitoring can't be implemented by the cooperation of P* and k-2 Q_i. Meanwhile, the cooperation of more than k Q_i (or even the all Q_i) can't achieve the monitoring and the information of a can't be obtained.

As for the public key cryptosystem, it is not required to change the keys before the communications. The safety is good and the speed of implementation is slow. Therefore, the actual security system always employs the public key cryptosystem to exchange the session keys and adopts the symmetric encryption system (such as the Triple-DES, IDEA) to encrypt the messages (Shamir, 1995; Fan and Xie, 2005; Nechvatal, 1996). The session key can be changed according to each connection or each message. However, the public key as well as the private key of public key cryptosystem is relatively fixed (Xie and Zhang, 2001; Fan *et al*., 2012a; Micali, 1993). Assuming that the users have adopted the traditional cryptosystem (such as DES and IDEA, etc.) to encrypt the message M. And the employed session key is Ks. The ELGamal public–key cryptosystem used by Ks has been cryptographically transmitted among users.

GENERATION AND THE ESCROW OF KEY

Generation of key: The Key Management Center (KMC) should select a large prime P and a primitive element g of GF (P). The private key of users can be generated through the following methods.

The user A should randomly select $a' \in Z_p$, calculate $Y' = g^{a'} \bmod p$ and send Y' to KMC.

Then KMC will randomly choose k, $a'' \in Z_p$ so as to make $Y = g^{a''} Y' \neq 1 \bmod p$.

$Y_1 = g^k \bmod p$, $Y_2 = a \approx Y^{rk} \bmod p$ should be calculated and (p, g, Y) should be public. Then (Y_1, Y_2) should be sent to user A.

Corresponding Author: Qiang Fan, Department of Computer Science, Hunan Police Academy, Changsha, China

The user A will calculate:

$$a'' = Y_2 (Y_1^{a'})^{-1} \bmod p,\ a \equiv a' \oplus a'' \bmod (p-1)$$

If a = 0, A will reapply the public key certificate. Otherwise, a will be considered as the private key of user A.

Partition of key:

- The user A is required to select k-2 random number c_j ($0<c_j<p$), j = 1, 2,..., k-2 to construct the polynomial:

$$f(x) = c_{k-2}x^{k-2}+c_{k-3}x^{k-3}+...+c_1x+a' \in Z_p[x],$$

in which f (0) = 1'

- The user A should randomly select t. t is a primitive element in GF (P). Meanwhile, it is required to calculate n-1 key pieces:

$$a_i = f(t^i) \bmod p,\ i = 1, 2,..., n-1.$$

- The user A should calculate

$$Y_i = g^{a_i} \bmod p$$

and Y_i, t should be public.

Recovery of private key: Firstly, it is required to construct the polynomial f (x) so as to get a':

$$f(x) = \sum_{i=1}^{t} d_i \prod_{\substack{j=1 \\ j\neq i}}^{t} \frac{x - c^i}{c^j - c^i} \bmod p$$

then:

$$a_i' = f(0) = \sum_{i=1}^{t} d_i \prod_{\substack{j=1 \\ j\neq i}}^{t} \frac{-c^i}{c^j - c^i} \bmod p$$

Afterwards, a'' will be obtained and we can calculate $a = a' \oplus a''$.

Key escrow:

- The user A should apply to KMC for escrow business and obtain ID_A
- The user A will encrypt (a_i, ID_A) by the public key of escrow parties and then send it to the escrow agent Q_i (i = 1, 2,..., n-1)
- The escrow agent Q_i uses its own private key for decryption so as to obtain a_i. At the same time, it is also necessary to verify whethter $a_i \in Z_p$ and $Y_i = g^{a_i} \bmod p$ are tenable

If they are tenable, it will be required to calculate the signature:

$$s_i = Sig_i (h (ID_A, Y_i, Y)),$$

in which h (.) is the secure one-way hash function. What's more, it is also necessary to send (ID_A, Y_i, Y, s_i) to KMC. Otherwise, the signature will be refused.

- KMC will secretly send a? to the important escrow party P*. When P* receives it, it is required to calculate $Y_{P'} = g^{aP} \bmod p$ and $s_{P'} = Sig_i (h (ID_A, Y_{P'}, Y))$

At the same time, it is also necessary to send (ID_A, $Y_{P'}$, Y, s_P) to KMC.

- When KMC receives (ID_A, Y_i, Y, s) of each escrow agent P* and Q_i (i = 1, 2,..., n-1), it will judge whether:

$$\equiv \prod_{i=1}^{n-1,P^*} Y_i \bmod p$$

is tenable through verifying the signature

If it is tenable, KMC will calculate the signature $s = Sig_{KMC} (h (ID_A, p, g, Y))$ and issue the public key certificate $C (A) = (ID_A, p, g, Y, s)$ of user A. Otherwise, the registration of user A will be refused.

SENDING AND THE RECEIVING OF KEY ESCROW

The core problem of key escrow is: How to effectively prevent the fraud behaviors of users and make the users not escape the track of custodian. In order to prevent the users from escaping the escrow, the implementation of key escrow technology requires the mandatory measures of government. The users must entrust the key escrow agents with the key escrow. After obtaining the escrow certificate, they can apply for the certificate authorized authentication center to encrypt the certificate (Duan, 2008; Fan *et al*., 2012b). The certificate authorized authentication center should issue the corresponding public key certificate after receiving the private key escrow certificate corresponding to the encrypted public key.

In order to prevent the key escrow agent from abusing the power and avoid the escrow key to be compromised, the private key of users should be broken down into several parts which are respectively preserved by different key escrow agents. The effectiveness of the private key of users can be restored through putting the private key components together.

- The users will select a number of key escrow agents and divide several private keys and public keys to each agent. According to the obtained private key component, the escrow agent will produce the corresponding escrow certificate. The certificate includes the Unique Identify (UID) of users, the entrusted public keys and private keys and the number of escrow certificate. The key escrow agent should encrypt the escrow certificate by using their own signature private keys so as to generate the digital signature. Then the signature will be attached to the escrow certificate
- When the user receives the all escrow certificates, the certificates and the complete public keys will be submitted to the certificate authorized authentication center in order to apply for the encryption

The communication initiator A generates K_S and the transmitted data has adopted K_S as the private key. It is required to employ the symmetric encryption algorithm for encryption which can be represented as $(M)K_S$. Meanwhile, K_S also regards K_{AB} as the private key and employs the symmetric encryption algorithm so as to form $(K_S)K_{AB}$. DRF includes the timestamp T, $(K_S)K_{AB}$ and the encrypted certificate of A. The messages that A sends to B can be shown in the following figure. The digital signature of A is generated by the encryption of message M and timestamp T (MT) conducted by the signature private key of A which can be shown as follows:

$(M)K_S$	Digital signature of A	Escrow certificate of A	T	$(K_S)K_{AB}$	Encrypted certificate of A

When the user B receives the messages, the signature certificate and the encrypted certificate of A will be firstly verified so as to confirm the true identity of A. Afterwards, the messages will be decrypted.

- The generation of K_{BA}. $K_{BA} = K_{AB}$
- The recovery of K_S. K_{BA} has been regarded as the key and it is required to decrypt $(K_S)K_{AB}$ in order to obtain K_S
- The obtainment of plaintext. It is necessary to use K_S to decrypt $(M)K_S$ and recover the plaintext M.
- The verification of digital signature. B has adopted the signature public key provided by the signature certificate of A and combined with T and M to verify the digital signature of A. If the verification is correct, it is indicated that B has received the true and correct information

As K_S is encrypted by K_{AB} and K_{AB} is the secret shared key between A and B which is not known to the third parties, so the confidentiality of information can be protected. The verification of digital signature has ensured the authenticity of information.

COMMUNICATIONS BETWEEN USERS

Assuming that A prefers to communicate with B. Firstly, A will check the public key certificate C (B) of user B from the public key manual. A will randomly select K_s and $t \in Z_p$. K_s is the session key of encrypted message M and t is the timestamp. Calculating:

$$Y_1 = g^t \bmod p,\ Y_2 = K_s Y^t \bmod p,$$
$$s = Sig_A (h (Y_1, Y_2, t, ID_A, ID_B)$$

According to the law enforcement field LEAF = (Y_1, Y_2, t, ID_A, ID_B, s), the message M should be encrypted into the cipher text $c = E_{ks} (M)$ and (LEAF, c) should be sent to B. When the user B receives (LEAF, c), it is required to calculate $K_s = Y_2 (Y_1^a)^{-1}$ and use K_s to decrypt the cipher text c so as to obtain the plaintext M = D (c, k).

ELECTRONIC MONITORING

It is required to employ the once monitoring method within the validity period and the perpetual off-line monitoring method to monitor the users.

One-off online monitoring within the validity period:

- Firstly, the government monitoring agency should apply for the monitoring certificate from the court. The monitoring time is provided in the certificate
- The government will monitor and intercept the cipher text c and LEAF. And the monitoring certificate will be also presented to each escrow agent P* and Q_i (i = 1, 2,..., n-1)
- When the escrow agent verifies that the validity of certificate is the same as t, it is required to calculate $Z_i = (Y_1)^{ai} \bmod p$ and send Z_i to the government monitoring agencies

- When the government monitoring agency receives Z_{P^*} and k-1 (k = n-1) Z_i, it is required to calculate:

$$Z \equiv \prod_{i=1}^{n-1,P^*} Z_i \equiv \prod_{i=1}^{n-1,P^*} Y_i^{ai} \equiv \prod_{i=1}^{n-1,P^*} g^{bi} \equiv g^t \sum_{i=1}^{n-1,p} a_i \equiv Y^t \bmod p,\ ks \equiv Y_2 z^{-1} \bmod p$$

- The government monitoring agency can adopt ks to decrypt c so as to get the plaintext M. Then the monitoring can be achieved.

Perpetual off-line monitoring:

- Firstly, the government monitoring agency should apply for the monitoring certificate from the court. The monitoring time is provided in the certificate
- The government will monitor and intercept the cipher text c and LEAF
- The monitoring certificate will be also presented to each escrow agent P* and Q_i (i = 1, 2,..., n-1)
- When the escrow agent verifies that the validity of certificate is the same as t, it is required to secretly send a" and a_i (i = 1, 2,..., n-1) to the government monitoring agencies
- When the government monitoring agency receives a" and k-1 ($k \le n-1$) a_i, it is required to calculate

$$a' = \sum_{i=1}^{t} d_i \prod_{\substack{j=1 \\ j \neq i}}^{t} \frac{-c^i}{c^j - c^i} \bmod p$$

- The government monitoring agency can use a to get the session key ks. And ks is also employed to decrypt c so as to get the plaintext M. Then the monitoring can be achieved.

PERFORMANCE ANALYSIS

Safety performance analysis:

- The safety of the scheme (the generation, the partition, the escrow, the communication and the monitoring of key in scheme) is based on the following two points which have the unconditional security

The difficulty of solving the discrete logarithm in ElGamal cryptosystem is equivalent to the solution of discrete logarithm which belongs to the NP problem.

Any k-1 or less than k-1 sub-keys in Shamir (k, n) threshold scheme can't reconstruct the security of the threshold theory of system key.

- The key sharing scheme of escrow agents can be flexibly established due to the employment of the advanced threshold scheme idea. The system will have greater flexibility and adaptability but the security will not be reduced. According to the specific circumstances of escrow agents, the design can be appropriately made

A kth equation has been constructed in this scheme which is the product (XOR value) between a kth equation (namely, the threshold sharing equation of key a') and a zeroth equation (the random constant, namely, the key a"). The random constant is mastered by the most important escrow agent and other escrow agents can be given a key fragment. This key fragment is the solution value of kth equation (namely, the threshold sharing equation of key a'). The general escrow agent can reconstruct the kth equation (namely, the threshold sharing equation of key a'). However, no matter how many key pieces it has, it can't get any information of the secret (namely, the key a). At the same time, the important escrow agent can't get more information needed to reconstruct the private key. When the important escrow agent is cooperate with other escrow agents, the two equations can be multiplied so as to reconstruct the private key a.

- The ElGamal private key a of the users in this scheme is generated by the cooperation between the random number a' selected by users and the random number a" selected by KMC. The random number a" is managed by the important escrow agents and the random number a' is hosted by other escrow agents after partition

The shortcomings which include the subliminal attack and the shadow public key attack caused by the independent selection of a can be effectively prevented. At the same time, the phenomenon that the security of the private key is lower as the KMC or the user doesn't have a good random number generator can be also avoided.

- This scheme can effectively prevent the conspiracy of some escrow agents or the illegal recovery of private key a due to the leakage of the keys of some escrow agents

This scheme can well restrict some escrow agents. The monitoring for user A can be implemented when the required conditions are met (the important escrow agents should be involved and the number of escrow agents should reach to the threshold requirements).

- When the sender sends S (H (M, d)) to the receiver, a timestamp is also attached. The sender should also sign this timestamp. When the monitoring is implemented, the monitoring agencies should present the licenser of court to the clients. At the same time, they should also explain the monitoring time to the clients

On the one hand, it can prevent the authorities from forging the user's signature after getting the private keys of users. On the other hand, the users don't have to re-generate their own private keys when the monitoring permitted by law is finished.

- The escrow can be effectively confirmed. On the one hand, as the key escrow scheme has the signature of trustees, it can prevent the posing for escrow agents. On the other hand, the trustee has connected the escrow requests with the private key pieces. They can be encrypted by the public key of escrow agents and then sent to the escrow agents. Only the escrow agents can recover them. Afterwards, the escrow agents will confirm that they have got the private key pieces which has ensured the interests of escrow agents
- According to the one-off online monitoring within the validity period and the perpetual off-line monitoring, the monitoring rights of the monitoring agencies have been effectively limited

When the monitoring agencies get the certificate of the one-off online monitoring within the validity period, they can only send the LEAF monitored in the validity period to the escrow agents. At the same time, they can also find Y' used in this communication from the information provided by escrow agents. Afterwards, the session key Ks can be also found so that the monitoring can be implemented. However, the ElGamal private key a of users can't be got. According to the characteristics of ElGamal public key cryptosystem, we can find that the Ks of other communications can't be obtained. Therefore, this monitoring has to be implemented so as to prevent the monitoring agencies from abusing the rights. When the monitoring agencies get the perpetual off-line monitoring, they will get the private key a of users from the information provided by the escrow agents. Then they can permanently monitor the users and the effectiveness of monitoring can be also ensured.

- The scheme can ensure the authenticity of the private key pieces hosted by each escrow agent so that the lawful monitoring can be effectively implemented

In this scheme, the public key certificate of users can be issued when the KMC verifies the effectiveness of all (ID_A, Y_i, Y, s) which ensures that there is:

$$a \equiv \prod_{i=1}^{n} Y_i \bmod p$$

for each i. At the same time, all i, Y_i should be verified by T_i, namely $Y_i = g^{ai} \bmod p$. And:

$$a \equiv \sum_{i=1}^{n} a_i \bmod p - 1$$

can be got from:

$$Y \equiv \prod_{i=1}^{n} Y_i \equiv g^{\sum_{i=1}^{n} a_i} \equiv g^{a} \bmod p$$

that is the private key a of users has been effectively hosted by each escrow agent. If the users provide the false Y_i or a_i, then:

$$Y \equiv \prod_{i=1}^{n} Y_i \bmod p \, Y_i \equiv g^{ai} \bmod p$$

which won't be tenable for all i. Therefore, the registration of users will be failed.

According to the several aspects discussed above, it is proved that this scheme is feasible and safe.

Overall performance analysis:

- Each escrow agent can verify the correctness of its hosted sub-keys. During the monitoring period, the monitoring agencies can exactly know which escrow agents have forged or tampered the sub-keys in the threshold key escrow scheme
- This scheme belongs to the threshold key escrow scheme. After the participation of important escrow agents, as for the other escrow agents, if one or several escrow agents are unwilling to cooperate with them or can't cooperate with them (the number of threshold should be reached), some escrow keys in each group will be still reconstructed

The employment of threshold scheme can effectively prevent several escrow agents from plotting together, or being corrupted, or refusing the cooperation (for example, some escrow agent suddenly loses its hosted sub-key or suddenly dies).

- This scheme applies to the one-way communication (such as Email) and the two-way communication (such as the telephone, etc) with any forms

- This scheme can be implemented through the software or the hardware
- This scheme has employed the standard DES, IDEA or 3-DES to encrypt the messages. The used session key has adopted the ElGamal public key cryptosystem for encryption and transmission which ensures the safety of messages
- It has effectively prevented the fraud behavior of users, namely escaping the track of escrow agent which is a verifiable problem. In particular, any third parties are allowed to verify the authenticity of the share which the users send to the escrow agents and the information can't be leaked

When the all verifications are correct, CA will issue the certificates to users. The users can communicate with others only after obtaining the certificates.

CONCLUSION

The general threshold secret sharing system has two unrealistic assumptions: First, the holders of the confidential information (also called the distributors) are always honest; second, n share depositaries (the sharers or the participators) have the equal status and rights as well as the same security and reliability. The two assumptions are often difficult to be met in reality. Therefore, the secret sharing scheme adopted in the safe cryptographic protocols must not rely on the two assumptions (Esnaashari and Meybodi, 2008; Fan *et al*., 2012c).

In this study, a key escrow scheme of escrow agents with the denial rights has been analyzed. This scheme can't rely on the above two assumptions. First, the design of this scheme doesn't rely on the holder of confidential information. The key is co-generated by the holder and KMC. When the keys are distributed, the trustee can verify the authenticity of the hosted key pieces. Second, the trustee has the different status and rights and there are also some important trustees. The key of users will not be recovered without the participation of the most important trustees. However, if the other trustees don't participate, the key of users can be recovered as long as the number of the most important trustees and other trustees reaches to the threshold value.

ACKNOWLEDGMENTS

This study is supported by Projects of Science and Technology of Hunan Province (No. 2013FJ4215), Projects of Science and Technology of Hunan Province (No.2013TZ2020), Projects of Science and Technology of Hunan Province (No.2013FJ4216).

REFERENCES

Duan, S.S., 2008. Certificateless undeniable signature scheme. Inform. Sci. Int. J., 178: 742-755.

Esnaashari, M. and M.R. Meybodi, 2008. A cellular learning automata based clustering algorithm for wireless sensor networks. Sensors Lett., 6: 723-735.

Fan, Q., M. Tan and Y. Zhang, 2012a. Typical applications and progress research of key escrow technology. J. Convergence Inform. Technol., 7: 375-382.

Fan, Q. and D.Q. Xie, 2005. Key escrow scheme for flexible placing of escrow agent. Comput. Eng. Appl., 41: 122-123.

Fan, Q., M.J. Zhang and Y. Zhang, 2012b. Key escrow scheme with the cooperation mechanism of multiple escrow agents. Przeglad Elektrotechniczny, 88: 116-118.

Fan, Q., M.J. Zhang and Y. Zhang, 2012c. Key escrow attack risk and preventive measures. Res. J. Applied Sci. Eng. Technol., 4: 2818-2823.

Micali, S., 1993. Fair cryptosystems and methods for use. Patents US 5315658 A. http://www.google.com/patents/US5315658

Nechvatal, J., 1996. A public-key-based key escrow system. J. Syst. Software, 35: 73-83.

Shamir, A., 1995. Partial key escrow: A new approach to software key escrow. Proceedings of the Key Escrow Conference, September 15, 1995, Washington, DC., USA.

Xie, D.Q. and D.F. Zhang, 2001. A key escrow scheme for escrow agency of arbitrary number. Chinese J. Electron., 29: 172-174.