Research Journal of Applied Sciences, Engineering and Technology 4(16): 2818-2823, 2012
ISSN: 2040-7467

Submitted: March 26, 2012 Accepted: April 23, 2012 Published: August 15, 2012

Key Escrow Attack Risk and Preventive Measures

Qiang Fan, Mingjian Zhang and Yue Zhang
Department of Computer Science and Technology, Hunan Police Academy,
Changsha 410138, China

Abstract: Cryptographic technology is always a highly sensitive dual-use technology. All nations have to face a dilemma in terms of password usage: on the one hand, to fully guarantee the safety and confidentiality of personal communication, as well as personal privacy and communication freedom required by law; on the other hand, to make sure law-enforcing departments and security organs crack down and prevent crime. It might be a great help for crime and terrorist organizations that the wide application of cryptography is made public. Many people believe that plain text communicated through the public network is accessible to an appropriate government agency if law permits. Therefore, it has become a continuous hot issue of cryptographic technology that how to design a cryptographic system through which legal persons are able to protect the safety of their information, yet being monitored by government in the range permitted by law. In this study, an in-depth study is carried out on the controversial key escrow technology, analyzing its composition and algorithm and pointing out possible attacks and preventive measures.

Keywords: Attacks and preventions, key escrow, main algorithm

INTRODUCTION

Because key escrow system has the function of key synthesis when it is permitted by law, government can intercept directly when necessary without paying a huge price on decryption. The idea is widely accepted and adopted. With large-scale applications of cryptographic technology, each and every country has adopted different forms of key escrow policies. That is to say, users deposit their encrypted private key with an appointed key escrow center, so that users themselves or relevant departments of the state can get the key in specified circumstances. Many countries now stipulate that: an encryption system must be equipped with a key recovery mechanism that guarantees law-enforcing departments will be able to acquire plain text conveniently. Otherwise, promotion and application of the encryption system will not be permitted.

In order to guard against cyber-terrorism and collect intelligence of criminals, governments of Western powers have significantly strengthened the protection of computer network security and substantially increased the investment in information security. The American government has laid down new regulations and plans of information security and also has specially established a Department of Homeland Security in order to strengthen law enforcement. The government has further improved the key escrow policy and especially strengthened the work of key escrow. It is hoped that regulation and control of government on password usage can be reinforced in this way. Initially, the American government stipulated that all keys of confidential communications should be managed by special departments of the government. Afterwards, the policy was altered that keys should be managed by impartial agencies designated by the government and be used by law-enforcing departments according to legal procedures. Key management regulations in our country require a mandatory key escrow policy that key management center must be entrusted with encrypted private keys before providing users with generated keys. Nechvatal (1996) have a research of a public-key-based key escrow system. Qiang and Dongqing (2005) study the key escrow scheme for flexible placing of escrow agent. NIST (1994) propose the esrowed encryption standard. Zhongmei *et al*. (2010) study the security mediated certificateless signatures without pairing. Goyal (2007) have a research of reducing trust in the PKG in identity-based Cryptosystems. Lu *et al*. (2009) analyse the threshold certificate-based encryption. Xie and Zhang (2001) propose a key escrow scheme for escrow agency of arbitrary number. Lu and Jiguo (2010) study the forward-secure certificate-based encryption and its generic construction. Lein *et al*. (2009) design the DL-based certificateless digital signatures. Shan-shan (2008) study the certificateless undeniable signature scheme.

Corresponding Author: Qiang Fan, Department of Computer Science and Technology, Hunan Police Academy, Changsha 410138, China

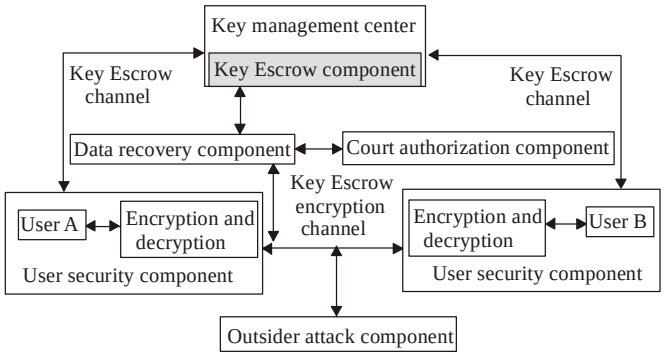

Fig. 1: The logic model of key escrow

In this study, we study an in-depth on the controversial key escrow technology, analyzing its composition and algorithm. Moreover, we point out possible attacks and preventive measures. From our research result, the key escrow is helpful for recovering forgotten or lost keys that belong to others.

AN OVERVIEW OF KEY ESCROW

Functions of of key escrow: In order to promote the smooth implementation of key escrow, many countries provide that, in Public Key Infrastructure (PKI), users have to divide their key into *k* parts and deliver them to *k* reliable trustees before applying to CA for data encryption certificate. Any one of the trustees is unable to recover the complete password with the partial key. The complete password of user can be only recovered when all keys kept by *k* trustees are together.
Important functions of key escrow are as follows:

- **Government monitoring:** Government, legal functional department or legitimate third party needs to acquire the key of two communicating parties so as to track or intercept communications of criminal suspects. Here, legitimate monitors can get user's key for monitoring through collecting key fragments from user's trustees.
- **Key recovery:** Users are able to gather key fragments from their trustees in order to recover the forgotten key.
- **Anti-repudiation:** The *k* trustees can prevent user's repudiation by composing user's key with their own part of key fragment.

Logic parts of key escrow:

- **USC (User Security Component):** It refers to hardware devices or software programs that provide functions like encryption and decryption of data and key escrow, including algorithm of data encryption and decryption, stored identity and key, DRF mechanism, etc.
- **KEC (Key Escrow Component):** It is mainly used for managing storage and release of data recovery key. It could also be a management system of public key certificate or one part of a key management center, including escrow agent, data recovery key, data recovery service, protection of key escrow, etc.
- **DRC (Data Recovery Component, government monitoring):** DRC recovers encrypted data back to plain text with information provided by KEC and information in DRF. It includes recovery of data encryption key and protection of decryption.
- **CAC (Court Authorization Component):** The main duty is to authorize DRC monitoring appropriately after comprehensive consideration according to information intercepted by DRC, relevant legal provisions and practical situations. Authorized content mainly includes monitoring time limits and monitoring target limits.
- **OAC (Outsider Attack Component):** Except the above-mentioned four parts, all members that attack the key escrow encryption system belong to this part, especially attacks on key escrow encrypted channel.

The model of key escrow encryption system is shown in Fig. 1:

Relationships between each part of key escrow:

- **The relationship between USC and KEC:** They mainly use key escrow agreement to get in touch with each other through key escrow channel. On the one hand, users who want to communicate by key escrow encryption system should first entrust their key to key escrow agents so as to obtain qualification and guarantee of confidential communication. On the other hand, key escrow agents have to ensure the validity and authenticity of entrusted keys. This is an interactive activity involving the two parties.
- **The relationship between USC and DRC:** DRC mainly intercepts communication information of users through key escrow encryption channel and prepares for monitoring. This is a unilateral activity

of DRC, which includes its active movements (namely, monitoring institutions replay or modify user's communication information).

- **The relationship between DRC and KEC:** This is an interactive activity that involves the two parties. On the one hand, in order to decrypt the encrypted data, monitoring institutions should deliver monitoring authorization granted by legal authorization institutions and partial intercepted information to key escrow agents. On the other hand, escrow agents should verify the validity and authenticity of authorization before releasing data recovery key.
- **The relationship between DRC and CAC:** This is an interactive activity involving the two parties. On the one hand, monitoring institutions should first state reasons for monitoring and related conditions to legal authorization institutions in order to acquire data recovery key from escrow agents. On the other hand, before authorizing monitoring institutions with appropriate power, legal authorization institutions should considerate comprehensively according to legal provisions and practical situations.
- **Relationships between OAC and each internal constituent part:** OAC is able to conduct active or passive attacks on any internal constituent part, of which the most important one is the attack on key escrow encryption channel.
- **USC has no relation to CAC:** And there is no connection between KEC and CAC.

ALGORITHMS OF MAJOR APPLICATIONS

The threshold idea and advanced threshold scheme: Suppose GF (P) is a finite field, randomly take $c_1, c_2,...,c_{k-1}$ GF(P), a is the key that needs to be entrusted. A polynomial can be constructed as:

$$f(x) = c_{k-1}x^{k-1}+c_{k-2}x^{k-2}+...+c_1x+a$$

Let *c* be the primitive element of GF (P) field, make $d_i = f(c^i) \bmod n$, i = 1, 2, ..., *n*, which is called sub-key and entrust d_i to escrow agent A_i. When the escrow agent provide more than *k* key fragments d_i, reconstruct:

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

Thus, the key *a* is recovered:

$$a = f(0)=\sum_{i=1}^{k} d_i \prod_{\substack{j=1 \\ j\neq i}}^{k} \frac{-c^i}{c^j-c^i} \bmod p$$

Common threshold schemes include:

- **Lagrange interpolation polynomial of shamir:** It uses polynomial equation of finite field to construct threshold scheme.
- **Vector scheme of blakly:** It uses points in space to construct the scheme. Message is defined as a point in *m*-dimensional space. Each shadow is an equation of (m-1)-dimensional hyperplane including the point. Intersections of any *m* hyperplanes determine the point.
- Asmuth and Bloom distribute shadows with properties of prime number and recover key with Chinese remainder theorem.
- The scheme of Karnin-Greene and Hellman of using matrix multiplication.

Weighing method of general threshold scheme: Different numbers of shadows can be distributed according to various privileges of different trustees. For example, trustees with more privileges can be distributed with more shadows, while trustees with less privileges are distributed with less shadows. Different people get different numbers of shadows and two or more people get multiple shadows. No matter how shadows are distributed, any *m* shadows can always recover key. However, even if there are m-1 shadows, no matter owned by one person or several people, the key still can not be recovered.

Advanced threshold scheme refers to combination of multiple linear equations of threshold idea, constructing an equation set corresponding to the specific scheme. For example, the product of an i^{th} power equation and a j^{th} power equation will be an $(i+j)^{th}$ power equation. Thus, a more flexible key sharing scheme can be achieved only by conceiving an equation set corresponding to the specific scheme.

The escrow scheme based on lagrange interpolation threshold scheme: Suppose there are *n* trustees $T_1, T_2, \ldots, T_n$ and any *t* ($t \le n$) of them can recover the key *a*. But it can not be recovered if the number of trustees are less than *t*. In order to realize the scheme, users can choose $(t-1)^{th}$ power polynomial from GF (*p*), satisfying $f(0) = a$. Assign each trustee T_i a value $K_i = f(i)$ as the key fragment. Suppose B = {1, 2, , t}, make a mapping:

$$\prod_B: B \rightarrow \{1, 2, ..., n\}$$

t trustees can be got from this mapping, namely $T_{\prod B(1)}, T_{\prod B(2)}, \ldots, T_{\prod B(t)}$. Key fragments kept by them are respectively $K_{\prod B(1)}, K_{\prod B(2)}, \ldots, K_{\prod B(t)}$. It can be got according to Lagrange interpolation formula that:

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

$X_{\prod B(j)}$(j = 1, ..., t) is open. If $K_{\prod B(i)}$(i = 1, ..., t) are gathered together, f(x) can be determined as well as the key a. If the number of collected $K_{\prod B(i)}$ is less than t, the above-mentioned $(t-1)^{th}$ power polynomial f(x) can not be determined. Consequently, when the number of trustees is less than t, a can not be recovered. So the scheme is secure from the angle of threshold.

ElGamal public key crypto-system: In numerous public key crypto-systems, there are now three types are considered secure and effective, respectively based on integer factorization (e.g., RSA), divergence logarithm (e.g., ElGamal) and elliptic curve divergence logarithm (e.g., ECC).

The security of ElGamal algorithm is the difficulty of divergence logarithm calculation based on finite field. Let p be a large prime number (at least 512 bit). It is usually required that p-1 contains large prime factors, so as to guarantee the difficulty of divergence logarithm calculation based on GF (p). g is a primitive element of the finite field GF (p). A user can choose a random number $c\in(0, p)$ and calculate $Y \equiv g^c \bmod p$. c is the private key of the user and (p, g, Y) is the public key. Any user, who wants to encrypt message M to user A, only needs to randomly select an integral number $t\in(0, p)$, calculate $y_1 = g^t \bmod p$, $y_2 = M * Y^t \bmod p$ and pass (y_1, y_2) to A. After receiving (y_1, y_2), plain text M can be restored from $M \equiv y_2*(y_1^c)^{-1} \bmod p$.

The impartial crypto-system: When Blakley (1979) and Shamir (1979) first introduced the secret sharing scheme, a variety of secret sharing schemes have been introduced continuously. Blakley and Shamir found a difficulty of the secret sharing scheme that sharing can be only restored when everyone reveals their own secret.

The impartial crypto-system can eliminate this shortcoming, which restores their sharing without revealing secrets. If the sharing secret is a private key signature on file, each one of the *n* sharers is able to complete partial signature of the file. After *n* signatures, the file is signed by the shared private key. None of these sharers is able to acquire anything about other sharers. Besides, sharers can verify the correctness of partial sharing.

In the Diffie-Hellman scheme, the process making it impartial is as follows:

- User A chooses n integral numbers $s_1, s_2, \ldots, s_n$, which are smaller than p-1.

  The private key of user A is $s = (s_1+s_2+\ldots+s_n) \bmod (p-1)$.
  The public key is $t = g^s \bmod p$.
  User A calculate $t_i = g^{si} \bmod p$, i = 1, 2, …, n.
  The public shared key of user A is t_i and the private shared key is s_i.
- User A distributes a sections of private key and a corresponding public key to each trustee. s_i and t_i are distributed to trustee No. i. And then t is distributed to KDC.
- Each trustee verifies that: $t_i = g^{si} \bmod p$.

  If it is true, the trustee signs t_i and sends it to KDC. Then the trustee stores s_i in a safe place.
- After receiving all n sections of public keys, KDC verifies that $t = (t_1*t_2*\ldots*t_n) \bmod p$.

If it is true, KDC recognizes this public key.

Now KDC knows that each trustee has a section of effective key. If necessary, they are able to reconstruct the private key together. However, the private key of user A can not be reconstructed neither by KDC nor by n-1 trustees.

The threshold scheme and the impartial crypto-system can be also combined, so that m of the n trustees can restructure the private key.

Various kinds of attacks threatening to key escrow security and preventions: According to relationships between each component of key escrow encryption system, there might be fraud in system. Attacks existing in system can be divided into internal attacks and external attacks. Key escrow encryption system is very complex, so attacks that may occur in system are much more complex than those in encrypted channel.

Internal attacks: Internal attacks refer to those between the four parts, USC, KEC, DRC and CAC. According to relationships between them, possible attacks are:

Attacks between USC and KEC: Both sides are likely to attack in this sense.

On the one hand, users may entrust false keys to entrusted agencies in order to escape escrow (including reset, falsification and other frauds). General methods to prevent such attacks: time stamp and Verifiable Secret Sharing protocol (VSS), etc.

On the other hand, some escrow agencies that do not meet system conditions might also conspire for certain benefits. They strive to recover user's key or decrypt data when system conditions are not met so as to reach their own objectives, bringing attack to user. The general method of preventing such attacks is to adopt an appropriate sharing protocol with high security in accordance with specific conditions, such as multipart and multilevel complete secret sharing protocol, etc.

Attacks between USC and DRC: In this sense, both sides are likely to attack each other.

On the one hand, users may have some fraud in order to make monitoring invalid (namely escaping escrow), so that monitoring institutions are unable to recover intercepted encrypted data. For example, "shadow key", conspiracy of users and other attacking methods. Normally, the way of preventing such attacks is to devise a system with high security, which at least should not provide obvious ways for users to conspire to escape escrow easily. Basically, anti-crosstalk chip (hardware) and methods proposed by Kilian and Leighton (1995) are able to prevent such attacks.

On the other hand, the unreasonable design of key escrow encryption scheme might also provide opportunities of abusing monitoring power for monitoring institutions. For example, monitoring institutions are authorized by legal authorization institutions to monitor user's communication at a certain time. Once a monitoring institution obtains a user's escrow information, it is able to carry out permanent monitoring on this user, resulting in the phenomenon of abusing monitoring power. The way of preventing such attacks is to make system consistent with limits of monitoring time and targets. Proposals put forward by Lenstra *et al*., (1995) can be used for preventing such attacks.

Attacks between DRC and CAC: Attacks of this kind generally occur in monitoring institution unilaterally. In order to acquire authorization with great power, monitoring institutions might apply for some unreasonable authorizations. It mainly relies on strict comprehensive assessment of legal authorization institution to prevent these attacks. In addition, legal authorization institution is a reliable part in system assumption. Otherwise, there is no guarantee for user's security.

Attacks between DRC and KEC: These are also unilateral attacks of monitoring institution. Monitoring institutions might provide key escrow agencies with intercepted information beyond authorization, such as information before authorized date, etc. The way of preventing such attacks should rely on functions provided by system as well as verification capability of key escrow agency.

Attacks between internal users: Internal users attack key escrow encryption channel by making use of mastered system information and their own specific information.

In addition, from system assumption and contrariety of rights and responsibilities between various parts, it can be known that conspiracies between each part are impossible. Hence, there is almost no attack caused by conspiracies between each part. Otherwise the system may break down.

External attacks: External attacks refer to those on the whole key escrow system participated by external members, including independent attacks on system from external members and attacks from conspiracies of external members and certain part of internal members.

Independent attacks on system from external members: External members are able to attack any part of the internal system independently. The uppermost attacks are passive and active attacks on key escrow encryption channel. It requires not only highly secure encryption algorithm and authentication mechanism but also highly secure escrow agreement to prevent such attacks. Thus, attackers will not be able to recover plain text according to DRF and ciphertext, as well as to obtain any relevant information of user's key from escrow agreement.

Attacks from conspiracies of external and internal members: Attacks of this kind mainly include conspiracy of users and external members of escaping escrow, conspiracy of part escrow agents and external members of recovering user's key, etc.

CONCLUSION

Security application system should be equipped with key escrow function. Key escrow is able to enhance the high-tech supporting capability of social management and law-enforcement of government judiciaries, as well as the capability of intelligence departments of fighting in information war, to provide services of information security and confidentiality for army, vital government department, sensitive information, business information and individual privacy, to strongly support counterintelligence, nonproliferation of nuclear weapons and preventions of such transnational activities as terrorism, drug trafficking, organized crime, international smuggling and money laundering, so as to promote the stability of a country and resist foreign aggression.

From the perspective of national interest, key escrow policy has its positive side that it provides law-enforcing departments with legal monitoring on criminals using encrypted public communication (such as terrorist threat, organized crime, drug trafficking, etc.), so as to maintain social stability and security. In addition to monitoring of government agencies, key escrow is helpful for recovering forgotten or lost keys that belong to others.

ACKNOWLEDGMENT

This study is supported by: Projects of Science and Technology of Hunan Province (No. 2011FJ3011),

Application Innovation Project of Ministry of Public Security (No. 2009YYCXHNST002).

REFERENCES

Blakley, G.R., 1979. Safeguarding cryptographic keys. Proc. AFIPS Note. Comput. Conf., New York, 48:313-317.

Goyal, V., 2007. Reducing trust in the PKG in identity-based Cryptosystems. Adv. Cryptol. Crypto. LNCS, 4622: 430-477.

Killian, J. and T. Leighton, 1995. Fair Cryptosystems, revied. In: Copperrmoth, D. (Ed.), Advances in Cryptology-CRYPTO 195, USA, August, pp: 208-221. Springer Verlag (LNCS 963), Berlin.

Lein, H., R. Jian and L. Changlu, 2009. Design of DL-based certificateless digital signatures. J. Syst. Software, 82(5): 789-793.

Lu, Y. and L. Jiguo, 2010. Forward-secure certificate-based encryption and its generic construction. J. Network., 5(5): 527-534.

Lu, Y., L. Jiguo and X. Junmo, 2009. Threshold certificate-based encryption. J. Software, 4(3): 210-217.

Lenstra. A.K., P. Winkler and Y. Yacobi, A key escrow system with warrant bounds, Advances in Cryptolog-CRYPTO'95, USA, August. Springer-Verlang (LNCS, 963), Berlin.

Nechvatal, J., 1996. A public-key-based key escrow system. J. Syst. Software, 35(1): 73-83.

NIST, 1994, Esrowed Encryption Standard. Federal Information Processing Standard Publication, pp: 185.

Qiang, F. and X. Dongqing, 2005. Key escrow scheme for flexible placing of escrow agent. Comput. Eng. Appli., 41(10): 122-123.

Shamir, A., 1979. How to share a secret. Comm. ACM, 22: 612-613.

Shan-shan, D., 2008. Certificateless undeniable signature scheme. Inform. Sci. Int. J., 178(3): 742-755.

Xie, D. and Z. Dafang, 2001. A key escrow sche me for escrow agency of arbitrary number. Chin. J. Electr., 29(2): 172-174.

Zhongmei, W., W. Jian and L. Jiguo, 2010. Security mediated certificateless signatures without pairing. J. Comput., 5(12): 1862-1869.