Security Analysis of Two Inter-Organization Cryptographic Schemes

Fanyu Kong[1,2, a], Jia Yu [3], Dashui Zhou[1,2], Yali Jiang[1,2], Jianwei Shang[1,2]

[1] Institute of Network Security, Shandong University, Jinan, 250100, China

[2] Key Lab of Cryptologic Technology and Information Security, Ministry of Education, Jinan, 250100, China

[3] College of Information Engineering, Qingdao University, Qingdao, 266071, China

[a]email: sdufanyukong@163.com

Keywords: Information Security; Cyberspace Security; Cryptography; Cloud Computing

Abstract. Data sharing among organizations is a practical application problem. In 2015, T. Miyamoto, Y. Murakami and M. Kasahara proposed two inter-organization cryptographic schemes for secure communication among organizations. Firstly, we give a security analysis of their RSA-based inter-organization cryptographic scheme and show that this scheme suffers from the well-known common modulus attack. Secondly, we analyse the ElGamal-based inter-organization cryptosystem and show that it is insecure for multi-receiver setting.

Introduction

Cloud computing and storage infrastructure [1, 2] provides users with powerful and on-demand computing and storage resources. The security and privacy problems have become one of the most critical issues of cloud system. Data sharing among various organizations/users is an important problem in cloud service and other information systems. One simple method for data sharing is that the sender encrypts the files and transmits the cipher-text files to the receiver. The practical difficulty of this method is to establish and maintain a large key management system for all the organizations and users. Furthermore, classical cryptosystems lack flexibility for various complex data sharing setting. Attribute-based encryption schemes [3, 4, 5] maybe be one of the most attractive method for data sharing and access control in cloud environment and other systems.

In [6, 7], T. Miyamoto, Y. Murakami and M. Kasahara designed two inter-organization cryptosystems to achieve secure communication among various organizations (government, company, school, hospital, etc.). The fundamental idea of two schemes is that Alice (sender) transmits the encrypted messages or files to the president Bob of the organization who will forward the message to the expected receiver. One scheme is built based on RSA cryptosystem and the other scheme is founded based on ElGamal cryptosystem. These schemes need much less computational amount than the direct re-encryption method.

In this paper, we propose security analysis of two inter-organization cryptosystems. Firstly, we give a security analysis of their RSA-based inter-organization cryptographic scheme and show that this scheme suffers from the well-known common modulus attack. Thus the RSA-based inter-organization cryptosystem is totally insecure. Secondly, we analyse the ElGamal-based inter-organization cryptosystem and show that it is insecure for multi-receiver setting.

The rest of the paper is organized as follows. Firstly, we review two inter-organization cryptographic schemes, RSA cryptosystem and ElGamal cryptosystem. Secondly, we analyze two inter-organization cryptographic schemes and find their security flaws. Finally, we give the conclusion and future research work.

Review of Two Inter-organization Cryptosystems

In this section, we review two inter-organization cryptographic schemes [6, 7], RSA cryptosystem [8] and ElGamal cryptosystem [9].

RSA cryptosystem [8] is one of the earliest and most important public key cryptosystems. It is

established on the integer factoring hard problem. RSA cryptosystem can be applied to data encryption, digital signature and electronic payment protocol.

RSA cryptosystem consists of three phases: key generation, encryption and decryption. In key generation phase, the system generates two random large primes, namely p and q. The product $N=pq$ is called the modulus. The system chooses a public exponent e and computes the private exponent $d=e^{-1} \pmod{\phi(N)}$.

The plaintext m is encrypted by computing the modular exponentiation as follows.

$$c=m^e \pmod{N} \tag{1}$$

To improve the computational efficiency of encryption, the public exponent e can be chosen as a small integer, for example 65537.

The cipher-text c is decrypted by computing the modular exponentiation

$$m=c^d \pmod{N} \tag{2}$$

The Chinese remainder theorem can be used to speed up the computation of RSA decryption.

ElGamal cryptosystem [9] is another well-known public key cryptosystem besides RSA cryptosystem. It is built based on the intractability of discrete logarithm problem.

Similarly, ElGamal cryptosystem consists of key generation, encryption and decryption phase. In key generation phase, the system chooses a large prime p and the primitive element g of finite field $F(p)$. For a user, the system chooses randomly a secret integer x as his private key and $y=g^x \pmod{p}$ as his public key.

To encrypt a plaintext m, the sender selects randomly an integer k and computes the cipher-text (c_1, c_2) as follows.

$$c_1=g^k \pmod{p} \tag{3}$$

$$c_2=my^k \pmod{p} \tag{4}$$

The cipher-text c is decrypted by computing the following equation.

$$m=c_2(c_1{}^x)^{-1} \pmod{p} \tag{5}$$

T. Miyamoto, Y. Murakami and M. Kasahara [6, 7] proposed two schemes to implement secure communication among organizations. They claimed that in some setting the sender is not allowed to exchange secret information with the specific person in charge in the organization. The sender should transmit the cryptographic information to the president/manager of the organization, who can forward the message to the expected receiver. A simple method is encryption-decryption-encryption protocol which need much computational amount. In T. Miyamoto et al.'s schemes [6, 7], the president can transform the sender's cipher-text into the corresponding cipher-text for the receiver without decrypting and re-encrypting the cipher-text.

In 2015, T. Miyamoto and Y. Murakami [6] proposed a practical RSA-based inter-organization cryptosystem. This scheme consists of four phases, namely key generation, encryption, forwarding and decryption.

In key generation phase, the president Bob of the organization generates his/her own RSA public key (e, N) and private key (d, P, Q), where the modulus $N=PQ$. Furthermore, Bob generates two random large primes P', Q' and computes $N'=P'Q'$ as the RSA key system parameters of all the users in the organization.

Let $L'=lcm(P'-1, Q'-1)$ and lcm denotes the least common multiple of two or more integers. For each user ID_i, Bob generates his/her RSA public key (e_i, N') and private key d_i. Bob sends the private key d_i to the user ID_i via a secure communication channel.

In encryption phase, the sender Alice encrypts the plaintext message M_i and its header M_H respectively as follows.

$$C_H= M_H{}^e \pmod{N} \tag{6}$$

$$C_i= M_i{}^{Ei} \pmod{N'} \tag{7}$$

In forwarding phase, Bob computes the decryption key $D_i=E_i^{-1} \pmod{L'}$ and sends the receiver ID_j's decryption key $r_j=e_j D_i \pmod{L'}$.

In decryption phase, the receiver ID_j decrypts the cipher-text C_i by using the decryption key $r_j=e_j D_i \pmod{L'}$.

$$M_i= (C_i{}^{dj})^{rj} \pmod{N'} \tag{8}$$

The detailed description of RSA-based inter-organization cryptosystem is seen in [6].

In 2015, Y. Murakami and M. Kasahara [7] constructed an inter-organization cryptosystem based on ElGamal cryptosystem. This scheme consists of four phases, namely key generation, encryption, forwarding and decryption.

In key generation phase, Bob chooses randomly a large prime p and the primitive element g of finite field $F(p)$ as public parameters. Bob generates his/her private key x_B and public key $y_B=g^{xB}$ (mod p). For each user ID_i, Bob generates his/her private key s_i and public key $z_i=g^{si}$ (mod p).

In encryption phase, Alice encrypts the plaintext message M_i and its header M_H respectively as follows.

$$C_H= E_{PK}(P_B, M_H) \tag{9}$$

$$(y_i, C_i)=(g^{xi}, M_i y_B{}^{xi})(\text{mod } p) \tag{10}$$

In forwarding phase, Bob recovers x_i and computes the receiver ID_j's decryption key $t_j= x_i x_B s_j^{-1}$ (mod p–1).

In decryption phase, the receiver ID_j decrypts the cipher-text C_i.

$$M_i=C_i(z_j^{tj})^{-1} (\text{mod } p) \tag{11}$$

The detailed description of ElGamal-based inter-organization cryptosystem is seen in [7].

Security Analysis of RSA-based Inter-organization Cryptosystem

In RSA-based inter-organization cryptosystem [6], the manager Bob of the organization receives the encrypted message and forwards it to the corresponding receiver. In the system establishment phase, Bob generates and distributes all the users' public/private key pairs in the organization.

The security flaw is that all the users share a common RSA modulus $N'=P'Q'$, which leads to a total break of the RSA-based inter-organization cryptosystem [6]. G. J. Simmons [10] proved that if two users have the public keys (e_1, N) and (e_2, N), which share the same modulus N, anyone can decrypt the cipher-text by using two cipher-texts encrypted with these public keys. Furthermore, J. M. DeLaurentis [11] gave a complete break of common-modulus RSA cryptosystem. The fundamental result is seen in the following theorem [11, 12].

Theorem 1. [11, 12] Let (e, N) and (d, N) be one user's RSA public/private key pair, and let (e_1, N) be another user's public key such that $e_1 \neq e$. Given e, d, N and e_1, a valid private exponent d_1 for (e_1, N), given by

$$d_1=e_1^{-1} (\text{mod } (ed-1)/\gcd(e_1, ed-1)), \tag{12}$$

can be computed in time polynomial in log(N).

Based on the above Theorem 1, we propose a security analysis and show that RSA-based inter-organization cryptosystem [6] is totally insecure. By using the computational method in Theorem 1, anyone can recover other users' private key in the organization. Thus not only the corresponding receiver ID_j but also any other user can decrypt the cipher-text. Without loss of generality, let ID_1 be the attacker who tries to recover other users' private key and the cipher-text C_i. The attack method is described as follows.

Attack 1. Attack method of RSA-based inter-organization cryptosystem.

Input: The user ID_1's public/private key pair (e_1, N') and (d_1, N'), any other user's public key (e_j, N'), the cipher-text C_i.

Output: Any other user's private key (d_j, N') and the plaintext M_i.

1. Given any other user's public key (e_j, N'), the attacker ID_1 can directly recover his/her private key $d_j=e_j^{-1}$ (mod $(e_1d_1-1)/\gcd(e_j, e_1d_1-1)$). Thus the attacker ID_1 can decrypt any cipher-text encrypted by using the public key (e_j, N').

2. For the cipher-text C_i encrypted by Alice, the attacker ID_1 can eavesdrop the information sent from Bob to the receiver ID_j. Then the attacker ID_1 obtains the cipher-text C_i and the decryption key r_j.

3. With the private key d_j computed in Step 1, the attacker ID_1 can decrypt and recover the plaintext M_i as follows

$$M_i= (C_i{}^{dj})^{rj} (\text{mod } N')$$
$$= C_i{}^{Di} (\text{mod } N') \tag{13}$$

According to the attack method, anyone can recover any other user's private key in the organization. Thus no privacy and security exists among the users in the organization. The improved idea is to generate a different RSA modulus for each user.

Security Analysis of ElGamal-based Inter-organization Cryptosystem

In another inter-organization cryptosystem [7], ElGamal cryptosystem is used to implement secure communication among organizations.

In [7], the encryption parameter x_i is kept secret and relevant with the plaintext M_i. Firstly, we note that x_i must not be revealed to the receiver ID_j. Or not, the receiver ID_j can recover Bob's private key x_B. With the encryption parameter x_i and the decrypt key t_j, the receiver ID_j computes Bob's private key x_B as follows.

$$x_B = x_i^{-1} t_j s_j \pmod{p-1} \tag{14}$$

For practical application, Alice may send the message to more than one receiver. In this setting, Bob should forward the cipher-text and different decryption keys to a few receivers. Now we give a security analysis and show that one receiver can recover another receiver's private key if he/she have another user's decryption key. Without loss of generality, let ID_1 be the attacker who tries to recover another users' private key. The attack method is described as follows.

Attack 2. Attack method of ElGamal-based inter-organization cryptosystem.

Input: The user ID_1's public/private key pair z_1 and s_1, any other user's public key z_j.

Output: Any other user's private key s_j.

1. The attacker ID_1 eavesdrops the information sent from Bob to the receiver ID_j. Then the attacker ID_1 obtains the cipher-text C_i and the decryption key t_j.
2. The attacker ID_1 can recover any other user's private key s_j as follows

$$\begin{aligned} s_j &= ((t_1 s_1)^{-1} t_j)^{-1} \pmod{p-1} \\ &= ((x_i x_B s_1^{-1} s_1)^{-1} x_i x_B s_j^{-1})^{-1} \pmod{p-1} \\ &= ((x_i x_B)^{-1} x_i x_B s_j^{-1})^{-1} \pmod{p-1} \\ &= (s_j^{-1})^{-1} \pmod{p-1} \\ &= s_j \pmod{p-1} \end{aligned} \tag{15}$$

Therefore, ElGamal-based inter-organization [7] must not be applied to multi-receiver setting. Attribute-based encryption schemes [3, 4, 5] are one of the best method for data sharing and access control in multi-receiver setting.

Comments on Two Inter-organization Cryptosystems

In two inter-organization cryptosystems [6, 7], Bob generates a transformed decryption key to the receiver. According to the above attack methods, the decryption key must be secretly sent to the receiver via a secure channel. Or not, the valid user can recover another user's private key once he/she obtains another user's decryption key.

However, if there is a secure channel between Bob and the receiver, Bob can directly send the fixed decryption key to the receiver and it is not required to establish the complex key management system in the organization. That is to say, for reducing the computational amount, they design the inter-organization cryptosystems and have to spend more computational cost to maintain the security.

Conclusion

Generally, two inter-organization cryptosystems [6, 7] are classical cryptographic schemes due to the usage of RSA cryptosystem and ElGamal cryptosystem. Thus they suffer from the well-known common modulus attack and our attacks.

In this paper, we propose security analysis of two inter-organization cryptosystems and show their insecurity. RSA-based inter-organization cryptosystem is totally insecure and must not be used in practice. ElGamal-based inter-organization cryptosystem has a security flaw in multi-receiver setting. Data sharing among organizations or in cloud system is still an interesting problem.

References

[1] I. A. T. Hashem, I. Yaqoob, N. B.Anuar, S. Mokhtar, A. Gani, S. U. Khan. The rise of “big data” on cloud computing: Review and open research issues [J]. Information Systems, 2015, no. 47, 98-115.

[2] S. Chhabra, V. S. Dixit. Cloud Computing: State of the Art and Security Issues [J]. ACM SIGSOFT Software Engineering Notes (SIGSOFT), 2015, 40(2), 1-11.

[3] A. Sahai, B. Waters. Fuzzy identity-based encryption [C]. Advances in Cryptology-EUROCRYPT 2005, Springer Berlin Heidelberg, 2005, 457-473.

[4] V. Goyal, O. Pandey, A. Sahai, et al.. Attribute-based encryption for fine-grained access control of encrypted data [C]. Proceedings of the 13th ACM Conference on Computer and Communications Security, ACM, 2006, 89-98.

[5] J. Bethencourt, A. Sahai, B. Waters. Ciphertext-policy attribute-based encryption [C]. IEEE Symposium on Security and Privacy -SP'07, IEEE, 2007, 321-334.

[6] T. Miyamoto, Y. Murakami. An implementation of inter-organization cryptosystem based on RSA cryptosystem [C]. IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2015, pp. 380-381.

[7] Y. Murakami and M. Kasahara. Hybrid inter-organization cryptosystem using ElGamal cryptosystem [C]. IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2015, pp. 378-379.

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

[9] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms [C]. Workshop on the Theory and Application of Cryptographic Techniques, Springer Berlin, 1984, 10-18.

[10] G. J. Simmons. A “weak” privacy protocol using the RSA crypto algorithm[J]. Cryptologia, 1983, 7(2):180-182.

[11] J. M. DeLaurentis. A further weakness in the common modulus protocol for the RSA crypto algorithm [J]. Cryptologia, 1984, 8(3):253-259.

[12]M. J. Hinek. Cryptanalysis of RSA and its variants, CRC press, 2009.