ISSN 2959-6157

Time-Based Cryptosystem

Rui Gan

Department of Software Engineering, Nanchang University Nanchang, China
E-mail: 8008121184@email.ncu.edu.cn

Abstract:

In this paper we introduce a Time-Based Cryptosystem (TBC) scheme. This scheme requires a Time-Based Key Generation Center (TBKGC) to broadcast a set of public keys based on the Multi-prime RSA (MPRSA) at every new interval. The sender encrypts the plaintext with a specified period of time and the corresponding public key broadcast by the TBKGC. And the receiver acquires the corresponding key from the TBKGC to decrypt the ciphertext. We discuss the difference between TBC and Time-Specific Encryption (TSE). Finally we suggest extension and directions of improvement of TBC.

Keywords: Encryption, Time-Specific Encryption, Cryptosystem, Multi-prime RSA

1. Introduction

There are three existing public key cryptosystems:

Traditional public key system / identity-based public key system / certificateless public key system

Among them, the identity-based public key system and the certificateless public key system both use identity as a factor in key generation. The identity here can be the user ‘s IP address, mailbox, then we can also use time as a factor in its key generation, so that the key is time sensitive. As mentioned above, a new cryptosystem is realized, which we name Time-Based Cryptosystem.

In 1984 Shamir [1] designed a structure for Identity-Based Encryption (IBE). His motivation was to simplify certificate management by the Identity-Based Encryption (IBE) in which the public key can be an arbitrary string. The first widely recognized IBE scheme was published by Dan Boneh and Matt Franklin in 2001[2], in which a preliminary form of TBC was proposed. They proposed a assumption that using the year or date to replace the identity as a parameter in the IBE scheme, so that the key can be time-sensitive. In a IBE scheme there are four algorithms: (1) setup generates global system parameters and a master-key, (2) extract uses the master-key to generate the private key corresponding to an arbitrary public key string ID 2 f0; 1g*, (3) encrypt encrypts messages using the public key ID, and (4) decrypt decrypts messages using the corresponding private key. There are two problems in directly using the year or date to replace the identity as a parameter in the IBE scheme:(1) Using timestamp instead of identity weakens the security of IBE scheme. (2) The decryption scope of public key timestamp is fixed by day or year.

In 2010 Paterson K G and Quaglia E A r introduced and explored a new concept of Time Specific Encryption (TSE) [3]. The TSE scheme can be described in three steps:(1) broadcast a time server broadcast Time Instant Keys (TIK) and corresponding decryption time interval at the beginning of each time unit. (2) encrypt encrypts messages with a specified time interval. (3) decrypt decrypts messages using the corresponding TIK. There is a possible extension of the TSE proposed in [3]: Hiding the decryption time interval of ciphertexts from adversaries, which is called DTIC (Decryption Time Interval Confidentiality). Our research is mainly focused on the improvement of the TSE scheme, from which we finally proposed the Time-Based Cryptosystem (TBC).

2. Implementation

2.1 Constructing the Time Binary Tree

To specify and select any time interval as a unique factor, we import the Time Binary Tree (TBT) which is cited from [3]:

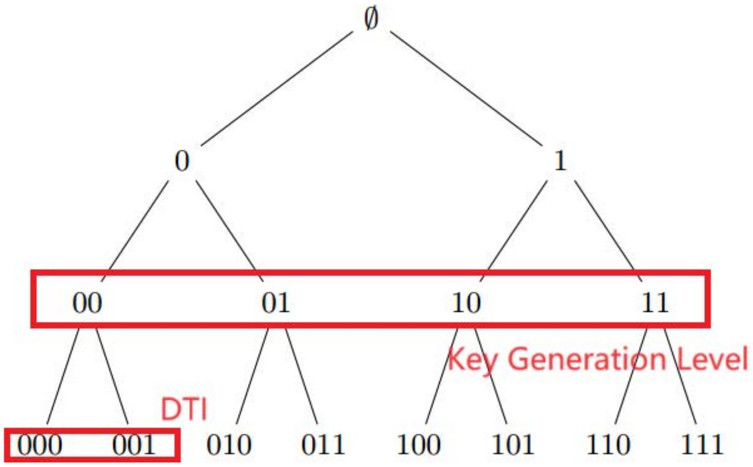

Figure 1 Example of TBT of depth d = 3

In this binary tree, every leaf is viewed as a timestamp. The combination of any two of them is unique, which can reflect from any Decryption Time Interval (DTI) to a unique factor.

2.2 Constructing the Service Group

(1) Defination

l Service Group: A cluster of roles that are parts of the TBC(Time-Based Cryptosystem), including users and the TBKGC.

l Users: Users in the service group send and receive ciphertexts which are encrypted with public keys generated by the TBKGC. Meanwhile, the private keys are received from the TBKGC as well.

l TBKGC: There's only one TBKGC (Time-Based Key Generation Center) in a service group. The TBKGC generate keys and deliver the keys to users via broadcast and confidential channels.

(2) Authorization for each role in the service group

The fundamental of this scheme is to construct a service group composed of a Time-Based Key Generation Center (TBKGC) and users. Each user in the service group is authorized to send ciphertexts to other users in this service group and receive ciphertexts from other users in this service group. Meanwhile, each user in the service group is restricted to send messages to the TBKGC via a confidential channel only. But each user in this service group is not restricted to receive messages from the TBKGC.

(3) Structure

Structure of a service group is shown in the Figure 2 below.

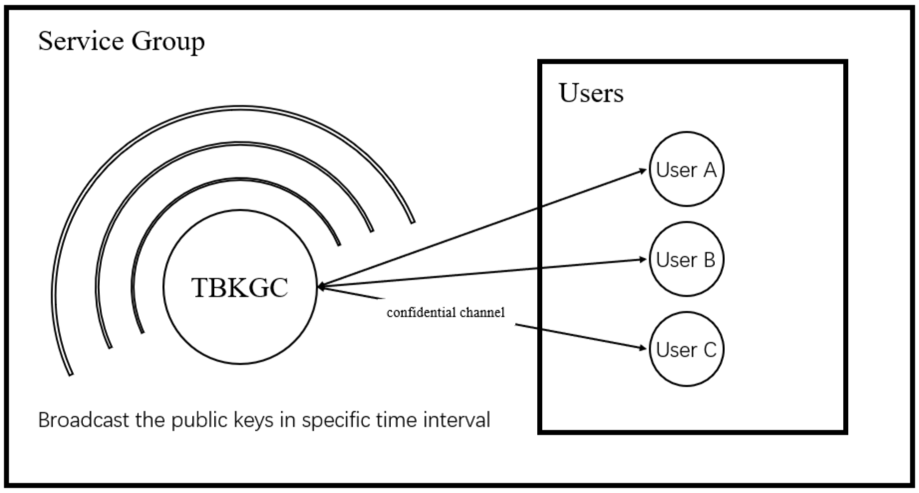

Figure 2 The structure of a service group

2.3 Generating Key Set Group

The key set is generated from the Time-Based Key Generation Center (TBKGC) with Multi-prime RSA(MPRSA) [4]. The TBKGC select a level in the TBT as a Key Generation Level. At the beginning of every node in this level, the TBKGC generates a Key Set Group (KSG) containing every key set corresponding with every DTI included in this unit.

There are 5 steps in the key set generation process:

(1) Transform DTI to a huge prime in generating the multiplication of multiple primes

As mentioned above, the DTI can be reflected into a unique factor by combining any two leaves in the TBT.

Import a random seed algorithm which reflect seeds to primes:

$$p = Random(dti, byte)$$

In this case we accomplish the transform from DTI to a prime of selectable size.

(2) Multi-prime RSA

Since DTI is reflected into a prime(p), the DTI can be functioned as a multiplier in the first step of MPRSA.

Multi-prime RSA algorithm in TBC [5]:

Step 1: Select 3 prime numbers p1, p2 and pt(reflected from DTI) and set N = p1p2pt:

Step 2: Compute Euler's phi function φ(N):

Step 3. Choose the public exponent 1 < e < φ(N) such that gcd(e, φ(N)) = 1

Step 4: Encryption: c = m^e mod N:

Step 5: Compute the decryption exponent d such that ed ≡ 1 mod φ(N): That is for some k, ed = 1 + φ(N):

Step 6: Decryption: compute c^d mod N to obtain the message.

The public key is (e, N) while the private key is (d, N). Sender encrypts the messages with public key (DTI, N), in which the DTI is selected by the sender. Receiver decrypts the messages with private key (d, N), in which the d is transmitted from the TBKGC via a secure channel

2.4 Updating the parameter N

Key Generation Level (KGL) is selected in fig 1. Consider depth = d, the depth of KGL = l,the minimum value of DTI = t, then the length of update cycle(T) is

$$T = (2^{d-l} - 1)t$$

At the beginning of every update cycle, the TBKGC will update the parameter N (obtained from Step 1 of MPRSA) and broadcast it in the user group.

2.5 Encryption

Sender selects a DTI which is effective in current key update cycle. By TBT the DTI can be reflected into a unique parameter e. Since the parameter N is broadcast by TBKGC, then the encryption algorithm is: c = m^e mod N.

It is obvious that the encryption is fully dependent on DTI. With parameter N changes over time, the TBC scheme guarantees the security against future.

2.6 Decryption

Receiver maintains a secure channel with TBKGC. After receiver receives encrypted message from the sender, the receiver will apply for a private key(d) from the TBKGC. Then the decryption algorithm is :m = c^d mod N.

3. Conclusion and Extensions

TBC scheme requires TBKGC to broadcast a public key set group while TSE scheme requires Time Server to broadcast Time Instant Keys (TIK) which are used in decryption. Obviously, broadcasting a public key set group ensures a higher level of security against broadcasting TIK.

Meanwhile, the DTLC (Decryption Time Interval Confidentiality) problem is eased since we only broadcast public key.

In total, the TBC scheme has explored several directions of extensions of TSE and constructs a new cryptosystem.

There are some possible extensions for this TBC scheme. Constructing the cryptosystem and analyzing the security of this scheme can be interesting. Especially the security of MPRSA used in this scheme is worth analyzing.

Acknowledgment

I would like to thank Professor Ping LUO for very precious suggestions and courses.

References

[1] Shamir A. Identity-based cryptosystems and signature schemes[C]//Advances in Cryptology: Proceedings of CRYPTO 84 4. Springer Berlin Heidelberg, 1985: 47-53.

[2] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C]//Annual international cryptology conference. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001: 213-229.

[3] Paterson K G, Quaglia E A. Time-specific encryption[C]// International Conference on Security and Cryptography for Networks. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010: 1-16.

[4] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

[5] Kumar R S, Prakash K, Krishna S R M. An improved cryptanalysis of multi-prime RSA with specific forms of decryption exponent[J]. CRYPTOLOGIA, 2023.