Performance Evaluation of Server-Clinet system with cryptograph

Yuka Yamada s1070222 Supervised by Prof. Hiroshi Toyoizumi

Abstract

When some data are exchanged between the server and the client, it is likely to be wiretapped and altered. To keep secure communication, we often need to cryptology. We found a method to calculate the average waiting time which the case that alredy has a common key, and the case that new client who do not have a common key is included, and we found what kind of time performance deteriorates at.

1 Introduction

In the nineteen-seventies, the exchange of information began to be done by using private lines. But it was large, so it was used only in special government organizations, big enterprises, universities and so on. In the nineteen-nineties, the Internet has become popular with the development of E-mail software and the browser, and networking proceeded so that even small and medium-scale enterprises and an ordinary family might exchange information. Virtual shopping and dealings of bank and stock company which used the Internet began to be done prosperously.

The advantages and convenience of the dealings in the Internet is that they are available from the personal computer in their house and the cellular phone. And, there is an advantage of the cost reduction in the bank and the stock company because they can reduce equipment and personnel expenses. But when the individual information and the number of the credit is transmitted over the Internet, there are some problems to be wiretapped and altered if there is no user authentication. There is a need to emphasize security to protect Internet users from wiretapping and alteration. One of the methods which solves that problem is encripherment. By changing it to a cryptogram that information cannot be understood is connected to prevent wiretapping and renewal, and to protect personal information.

There are two methods in cryptography. : a symmetric key system method, which is the transmit side and the reception side has a common key, and to carry out encryption and decryption to use it: a non-symmetric key system method to carry out encryption and decryption to use a private-key of encryption and a private-key of decryption. As for a symmetric key system method, processing speed is high, but it is often intercepted because a key must be delivered to the receiving person. In addition to managing the key is difficult. As for non-symmetric key system method, it is safe because it doesn't need to send a key, and managing the key is easy. But the processing speed is from 10 to 100 times slower in comparison with processing speed of symmetric key system method [1].

In this paper, the flow of the data which used encripherment from the server to the client is modeled. It is divided into already has a common key and does not have a common key, and we find each methods of the average sojourn time and each limit value. And the probability that a new client comes is changed, and we find limit value at that time.

2 Function of PKI

PKI (Public Key Infrastructure) is an environment for safe communication by using the non-symmetric system and the electronic signature on the Internet. A public-key base must cope with the following problems.

- The preparation of the strong key
- The confirmation of the client for the first time
- The issue, renewal and extinction of the certificate
- The verification of the certificate
- The distribution of the certificate
- The safe storage and restoration of the key
- Establish a relationship of mutual trust

2.1 The necessary elements of the public-key base

On PKI, there are some indispensable elements as the following.

1. Certification Authority(CA)
   CA is the organization which does the establishment of the nature, and makes a digital certificate to relate the nature, public key and secret key pair.

2. Registration Authority(RA)
   RA is the the organization of the registrant's registration and does the initial authentication. The registrant points at the user who takes the issue of the certificate after a demand for registration is agreed officially.

3. Certificate confirmation
   A user must verify a received certificate, and the following confirmation is necessary.

   - The preparation of the signature of the certificate signer
   - Confirmation that a certificate is effective at present
   - The check of the use purpose of the certificate
   - A certificate checks that the effect is not lost by CA

4. Key recovery service
   The pair of the public-key and the secret-key is formed as a physical device such as a smart card, and the key storage place in the application. The offer of the service that case keeps a code-key and which recovers at the time of the loss is necessary.

2.2 Modeling of PKI

Look at Figure1. We show a simple example of PKI (Public Key Infrastructure).

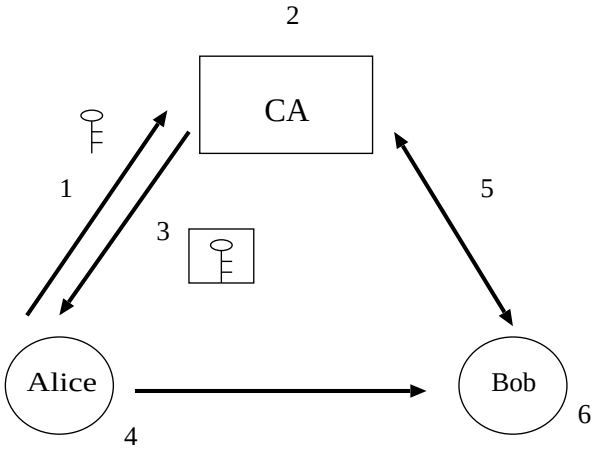

Figure 1: PKI model

Step 1 Alice sends her public-key to CA, and applies for the issue of the electronic certificate.

Step 2 CA confirms whether Alice is herself based on an application.

Step 3 CA sends the certificate of Alice is name that attaches to a public key

Step 4 Alice enciphers an electronic document with her private key, and sends an electronic certificate and an electronic document to Bob.

Step 5 If Bob wishes, he can check whether the electronic certificate is effective in CA.

Step 6 Bob picks out the public key of Alice from an electronic certificate.

2.3 The transmition side

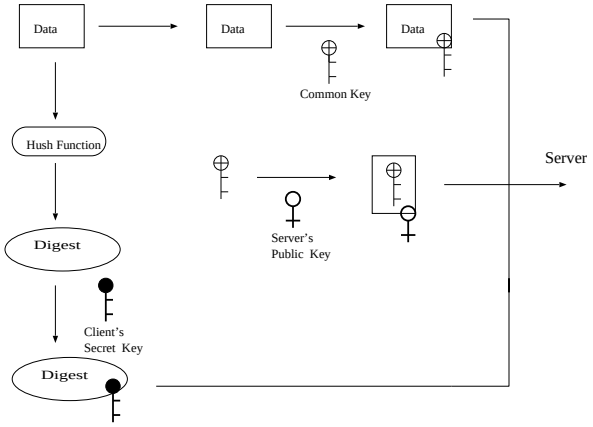

Figure 2: The Transmition side

There are three steps. First, the data is encrypted with a common key because the data is not altered. Second, the common key is encrypted with a public key of the server. Third, it passes through the data in hush function, a digest is made, and the digest is encrypted with private key of the client. An encrypted data, an encrypted common key and an encrypted digest are sent to machine server.

2.4 The reception side

There are three steps. First, the common key being encrypted with a public key of the server is decrypted by using the secret key of the server, and the common key is acquired. Second, a data is decrypted by using the common key, it passes through the data in the hush function used for the encryption, and a digest is made. Third, an encrypted digest is decrypted by using the public key of the client, the digest is acquired. These two digests

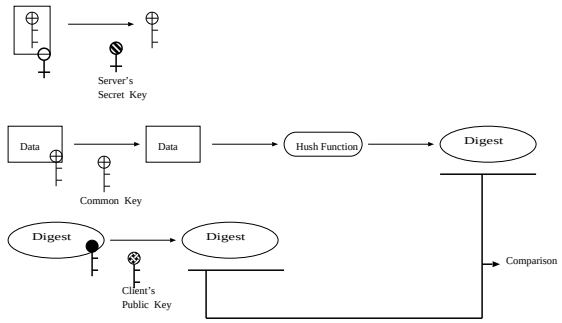

Figure 3: The Reception side

are compared, if they correspond, this data sent by a real client. Moreover, it is understood that it has not been altered halfway through the process.

3 Queueing model of Server-Client PKI

3.1 Queueing model

We show a modeling of the system between the server and the client in which encipherment was used. This method is of a server and a clients prescription.

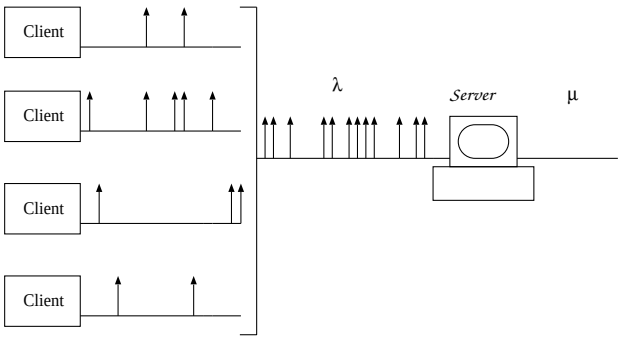

Figure 4: The Basic System

Many data are published from clients, and they are sent to machine server. It is defined that the average of the number of data go into the server machine is Poissom process λ with rate. All the data are encrypted, the server of the reception side taken decrypts them. The service time that machine server can decrypt, and the time that output them are assumed to be constant.

4 Performance evaluation of queueing model

We evaluate queueing model. There are two pattern. One is the case which already has a common key, the other is the case which the new client who does not have a common key is included. We suppose the average of service time S is $\frac{1}{\mu}$, and it is divided into case of two.

4.1 The system with no new client

The user who already has a common key join in the system, it does not need to certify the person. This case, work of the server is divided into three parts.

- Decod enciphered data.
- Make a digest through Hush function.
- Compare it to the original digest.

Let s_c be the time required for above process, so $S = s_c$
Then, the average sojourn time of this system $E[T_{M/D/1}]$,

$$E[T_{M/D/1}] = \left(1 + \frac{1}{2} \cdot \frac{\rho}{1-\rho}\right) \cdot s_c. \quad (1)$$

λ is given to it as follows.

$$\rho = \frac{\lambda}{\mu}. \quad (2)$$

When they are substituted, we found the average sojourn time of the system which already has a common key,

$$E[T_{M/D/1}] = \left(1 + \frac{1}{2} \cdot \frac{\lambda s_c}{1-\lambda s_c}\right) \cdot s_c. \quad (3)$$

We suppose the service time is 1 second, and the average of the number of data going into the server machine is 10.

Figure 5 is an example of waiting time *lambda* = 10 ~ 60 where the arrival rate in the system. The figure shows that the average sojourn time until data go into the server and it is deposited.

λ	E[T M/D/1]
1	0.0168
10	0.0183
20	0.0208
30	0.0250
40	0.0333
50	0.0583
59	0.5083

Table 1: The average sojourn time of system which already has a common key.

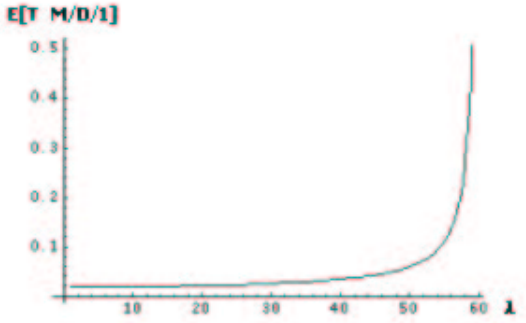

Figure 5: The average sojourn time of system which already has a common key.

5 The system with occasional new clients

Until now, we show the exchange of the server and the client who has already had a common key. Look at Figure 6. Now on, we show the system in which a new client was joined. We assume a new client does not have a common key.
At this point, the probability that a new client is included in the system is supposed $P[new]$.

$$P[new] = \frac{Numbero\,fnewdata}{Numbero\,folddata+Numbero\,fnewdata} = a. \quad (4)$$

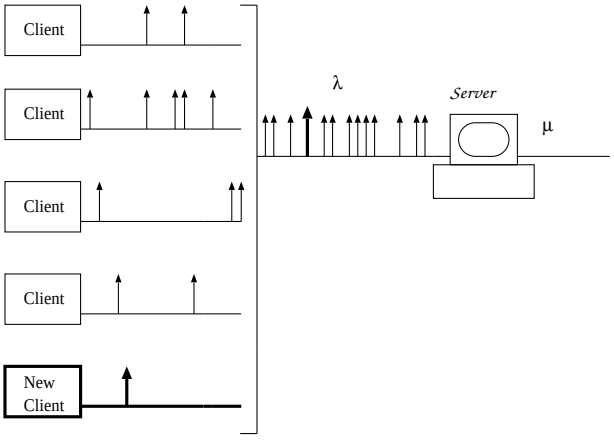

Figure 6: The system with new client.

5.1 The service time

If a new client joins in the system, server needs to do additional works;

- It asks whether a certificate is effective.
- The preparation of the common key.
- A common key is enciphered with a public-key of the new client.
- It is decoded with a secret key of the new client.

Let s_p be the service time for these additional work. Thus,

$$S = \begin{cases} s_c & ,if\ known\ client \\ s_c + s_p & ,if\ new\ client. \end{cases} \quad (5)$$

By Pollaczek-Kninchin formula, the average sojourn time of this system $E[T_{M/G/1}]$ can be given by,

$$E[T_{M/G/1}] = E[S] + \frac{\lambda E[S^2]}{2(1-\rho)}. \quad (6)$$

$E[S]$ and $E[S^2]$ are given as follows,

$$E[S] = s_c + a \cdot s_p. \quad (7)$$
$$E[S^2] = 2as_cs_p + as_p{}^2 + s_c{}^2. \quad (8)$$

When they are substituted, we found the average sojourn time of the system which a new client was included in.

$$E[T_{M/G/1}] = as_p + s_c + \frac{\lambda\left(2as_cs_p + as_p{}^2 + s_c{}^2\right)}{2\left(1-\lambda\left(s_c + as_p\right)\right)}. \quad (9)$$

We suppose the number of the data from the client who already has a common key is harf, and the number of the data from the new client is 1, $a = \frac{1}{2}$, $s_c = 1$ second and $s_p = 0.5$ second.

λ	**The average sojourn time**
1	0.0211
10	0.0237
20	0.0286
30	0.0389
40	0.075
47	0.53

Table 2: The average sojourn time of system which a new client join.

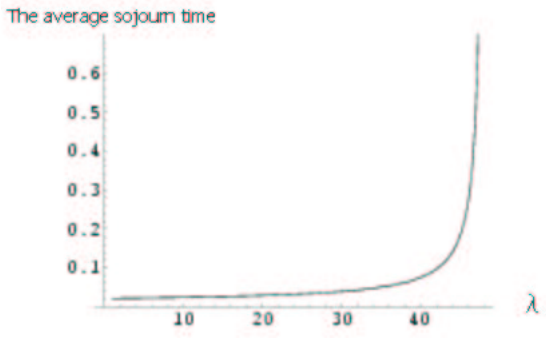

Figure 7: The average sojourn time of system which a new client join.

5.2 Change the parameter

We change the probability which the new client join in the system. Figure 8, it is the graph $a = 0.01$, $a = 0.5$ and $a = 1$.

6 Conclusion and Future Work

When the clients who already has a common key join in the system, the method og the average sojourn time is $E[T_{M/D/1}] = \left(1 + \frac{1}{2} \cdot \frac{\lambda s_c}{1-\lambda s_c}\right) \cdot s_c$, and when the new clients who does not have a common key join in the system, the method of the average sojourn time is $E[T_{M/G/1}] = as_p + s_c + \frac{\lambda\left(2as_cs_p + as_p^2 + s_c^2\right)}{2\left(1-\lambda\left(s_c + as_p\right)\right)}$.

We compare the three graphs of the Figure 8. When all data was sent by the known client, sojourn time does not change to the range that lambda is 50, but performance deteriorates between *lambda* = 50 ∼ 59 rapidly. Moreover, when all data was sent by the new client, sojourn

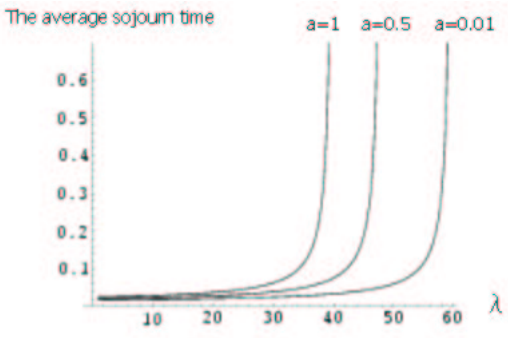

Figure 8: The average sojourn time, a=1, a=0.5 and a=0.01.

time does not change to the range that lambda is 30, but performance deteriorates between *lambda* = 30 ∼ 37 rapidly. We found that the number of processed data changes drastically according to the probability that a new client join in the system, and the performance of the system deteriorated.

In the all case, we have to consider processing time which take by CRL check that is sent from CA, and network delay. 。

7 Acknowledgement

Many people helped me. I would like to thank to Prof.Hiroshi Toyoizumi and Mr.Takaya for their helpful comments in this paper. I would also like to thank to Prof. Martha Cummings for correcting my English.

References

[1] Andrew Nash, William Duane, Celia Joseph, Derek Brink, *PKI Implementing and Managing E-security*, syoueisha, Japan, 2002.

[2] Steve Burnett, Stephen Paine, *RSA Security's Official Guide to CRYPTGRAPHY*, syoueisha, Japan, 2002.

[3] Sheldon M.Ross, *Applied Probability Models With Optimization Applications*, Dover Publications, 1970.

[4] Norihiro Sakamoto, "A development of a User Authentication System Based on Public Key Certificates for Healthcare Information Services in Na-

tional University Hospitals," *The Institute of Electronics, Information and Communication Engineers Trance*, Vol. J84-D-I, No. 6, 2001, pp. 130-139.

[5] Matsuyoshi Takaya, "Performance Evaluation of group security with key management.", graduated thesis 2001, Performance Evaluation Laboratory The University of Aizu.