Joint Conference of 1996 International Computer Symposium
December 19~21, Kaohsiung, Taiwan, R.O.C.

Access control by common key cryptography using KPS

Masaaki Ishikane and Hideki Imai

Institute of Industrial Science
The University of Tokyo
7-22-1 Roppongi, Minato, Tokyo 106, Japan
E-mail: masaaki@imailab.iis.u-tokyo.ac.jp, imai@iis.u-tokyo.ac.jp

Abstract

Today, as network develops, illegal access to personal data or secret data becomes serious problem. To solve this, access control is used. But it relies extensively on the security of the system manager. In order to increase safety, we should decrease the relied part to the manager and encrypt data. In this report, we think about access control by encrypting data. Especially, we think about the system changing by every S and O using KPS.

1 Introduction

Information on the image and the voice data, etc. increases rapidly with the development of the multi media in recent years. And, subjects can access objects freely with the development of the network. Though information has been opened to the public along the flow of informationization, it is important to defend the individual secret data surely at the same time.

To protect the individual data, it is needed to control totally including physically control. Especially the access control under a certain control part or inside computer is used and important assuming that a substantial effect is shown.

The control part is the part like the kernel in certain system and certain group. It is put as a place and a position where the access control is done in.

Because all the access subjects and objects can be recognized, it is enough in a usual access control in the system which does not go out to the network defended by the control part.

However, the data once output to an outside network becomes threats of reading stealthily and the falsifying, etc.

To ensure the access control in the place where danger on such communication roads exists and to improve safety, it is thought that it is a powerful method to attest subjects certainly to decrease the part relies on the control part and to encrypt data.

So in this text, we think about encrypting data in the access control.

First of all, we think about the necessity of encryption in the network of the access control in Chapter 2. And, the encryption is applied and the method with a common key is explained especially in Chapter 3. In addition, the method of using KPS as the key delivery is proposed in Chapter 4. And, we bring it together at the end.

2 Necessity of encrypting in network

In the access control in the network, authentication of access subject, peeping on communication road and safety when the manager is different become problem. And we should consider them.

The following one is enumerated as a strategy of the access control being done now. First of all, it is the way of making the group controlled the right of an individual subject is not specified in detail but collectively in some group, for an increase in the number of access subjects. Moreover, by using the one like Firewall to improve safety from the outside, the method of closing the system has been used and the exchange is limited to the minimum.

In this text, the environment which is connected two or more systems and accessed each other frequently is assumed. And, we think about the method of achieving safer access control in the communication road by using encryption.

3 Application of the encryption to access control

According to encrypting object individually,

1. Significant information is not obtained even if it is peeped on the communication road.

2. The subject without the key can not obtain significant information.

Such advantages can be obtained and the access control is achieved.

There are two kinds of encryption - public key cryptography and common key cryptography. Previously we roughly brought together the difference of the system using each encryption [1].

This time, we reconfirm the system composition, outline of the protocol, profit and fault, when access control is achieved with common key.

In addition, we think about details. Moreover, the method of using KPS as a key delivery method of common key is proposed.

3.1 System using common key cryptography

Here, we consider the system which achieves the access control when the common key encryption is used with the system which uses public key encryption.

System composition

First of all, a basic composition with a common key is to encrypt the object by the common key encryption. The common key is offered only to the subject which the access is permitted. That is, the object side is kept in encrypted state. On the other hand, the bunch of a common key to the object which can be accessed will be kept on the subject side. When this is made figure, it becomes following.

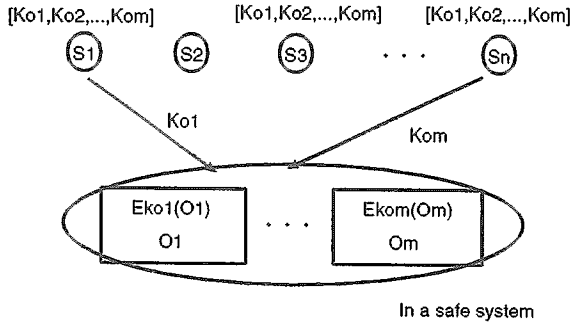


Figure 1: composition of the system using common key

We can say that this system is near Capability List, as installing the list on the subject side. Therefore, to make right known like the network, it is suitable.

Next, we think about the system that the subject's key is one and objects are encrypted with each key by one. In this case, it can be said near ACL because of putting the list on the object side. That is, it can be said in this system that there is an advantage on the owner side. However, because this system should change all keys to the object side when the key to the subject is changed, the processing becomes very much.

In addition, we think about the case where the key to each subject and each object is changed (Figure 3).

With the access right to the same object, the same contents will be obtained by each subject by decrypting it. However, the key is different. The number of keys is increased seemingly uselessly. Difference of keys by each subject means that if one subject gets another subject's key, it can not decrypt the encrypted object sent to the subject.It is an operation necessary to do the access control more strongly. However, it is a condition that the key and the object are separately sent.

It is thought of as making the session key once as once and to encrypt it, as encrypting of e-mail.

However, the system including the check on right can be composed by deciding the relations between the subject and the object (right or wrong of the access) beforehand.

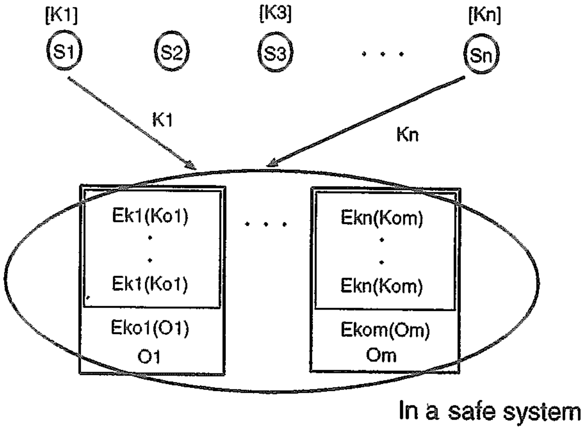


Figure 2: composition of the system changing by every subject

Moreover, the number of keys which the subject side should have does not change. Therefore, the load of the subject side does not increase.

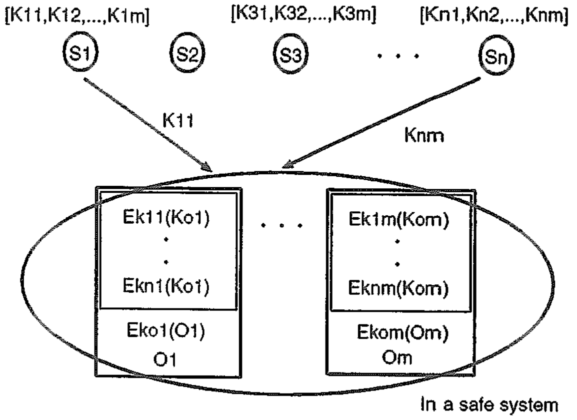
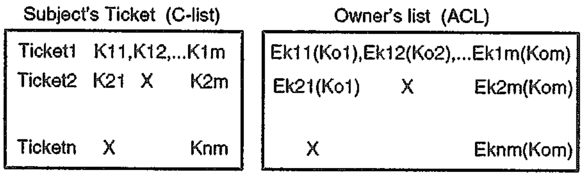


Figure 3: In case of changing by every subject and object

Compared with the public key base system [2], in this composition, lists exist in both subject side and object side. So we can say that it is in the middle of ACL and Capability List (Figure 4). That is, each subject is shape that permission descends by having the ticket and having it checked.

A stronger access control can be achieved by passing the check on double like this. It can be said that leadership is on the owner side of the object because of final access permission in passing the check on ACL though both characteristics exist. It is easy for this to be accepted compared with the system only of the ticket.



Subject's Ticket (C-list)

Ticket1	K11,K12,...K1m		
Ticket2	K21	X	K2m
Ticketn	X		Knm

Owner's list (ACL)

Ek11(Ko1),Ek12(Ko2),...Ek1m(Kom)		
Ek21(Ko1)	X	Ek2m(Kom)
X		Eknm(Kom)

Figure 4: key managing method of encrypted object

To make the access right known, all are described in the list of the object side. And not to make the access right known and to make it known opposite, the list of the object side is limited strictly.

In addition, it is necessary to change the key every fixed period because it differs from encrypting by the communication road and the object is preserved for a long term in the place like the data base.

Protocol

First of all, the control part of the access control exists in a certain system and it assumes to be a safe part which might not be influenced by another there. It can be thought the one like the kernel in the computer. The control part is enabled to recognize all subjects which exist in the system and objects and for right to be checked. The key is assumed to be kept safely. This control part is assumed to be a physically safe place.

It can be thought that the access from a certain subject to the object is done by putting such assumption through the control part of each system. That is, one subject will access other system through the control part of its system and the control part of opponent's system so that a certain subject may access the object of other systems.

As assumption, we think about the case where subject B in another system attempts accessing for object A in a certain system. A usual access control is not enough in this case, because each access control part is different.

The protocol is as follows.

1. B →A: Access demand + signature is sent.

2. A: Check on signature + right (Whether the object is encrypted or not?).

3. A→B: The encrypted object (key) is sent.

The common key between each subject and object is distributed necessary. The key delivery is described in the following chapter.

It is still necessary to think about the concrete method for signature.

Advantage and disadvantage

As the advantage, the speeds are faster than the public key cryptography. When e-mail is encrypted, this is apparent from encrypting the text with a common key and encrypting the common key with the public key. Moreover, in change of the key, we don't have to make the cancellation certificate known.

That is, it becomes possible by changing the key between persons concerned. In addition, when the key is different in each subject, it becomes more easy.

In addition, the achievement methods of the access control can take the shape of a double check which uses both ACL and Capability List and a stronger, more flexible access control is achieved.

Moreover, plural common keys to the file can be handled by using the key delivery system named KPS [3] at this time. That is, the amount of the memory can decrease even if the number of keys increases. And, some system can be constructed. Moreover, the time of the key delivery of a common key decreases. It is convenient to become considerably easy to construct the system. The load of each subject and the (key management) center can be small though it is necessary to install the key delivery center.

The fault is a point that the key which the subject should have increases overwhelmingly.

4 Method of using KPS as key delivery method

Here, the method of using KPS as a common key delivery method when the system is constructed is devised.

If the common key between the subject and the object is distributed once, the access control can be achieved by whether keys are distributed or not(Whether the object is encrypted with the key or not?).

Thus the system based on a common key can be constructed. First of all, we explain the advantage when KPS is used to distribute the key. And we think about the achievement method.

4.1 KPS

First of all, an easy explanation of KPS(Key Predistribution System) is done.

KPS is a method that a group consists of any plural entity in a network (consist of plural entity communicate each other.) share a same key with a center.

1. Generation of center algorithm

2. Key sharing generation and distribution of secret algorithm for each entity

3. Key sharing by group

This time, in s system we think to achieve access control, in many cases, group composition members are object (actually control part) and subject permitted to access.

Because we think the key to each different subject to which the access to the same object is permitted is changed, the necessity for using more than three persons is assumed not to be especially.

Next, the characteristic of KPS is brought together.

In KPS, if process 1 and process 2 end, each entity does not have the necessity of accessing the center and other entities for the key sharing at all.

Needing it to share the key is only an identifier of the entity. That is, the key can be generated independently of opponent's entity and the center as long as opponent's (object) identifier is known. That is, when accessing one time once even if some taking time to construction and restructuring the system, the key can be easily obtained.

Moreover, the method of various key sharing is obtained depending on the method of the composition of the identifier. For instance, character *a* and *b*... If the identifier is hierarchically made from like *a* and *b* and etc. , the access is permitted only to the (plural) entity with the character named *a*. And the access can be permitted only to the (plural) entity with the character named *a* and *b*.

Actually, the composition of the object is most the layered structure and can significantly use this advantage.

4.2 Method of using KPS

The advantage of using KPS as key delivery system is as follows.

1. It is not necessary to search key from key list.
2. In order to access object, it is necessary only to appoint object name.
3. The amount of memory is little.

It is necessary to apply the identification name like the layered structure, as described previously, in KPS-ID. The access control can be efficiently done by doing so and the system which matches to a present computer system can be constructed.

It is not necessary to authenticate subject at each access at the following if it does firmly only once at the distribution of the key. The ticket of the access right was obtained by the key's having been given. However, this system is located in the middle of ACL and Capability List and is checking double. That is, right can not be obtained completely if it is not recorded in ACL (It is not encrypted with the key) even if only the ticket is given.

Both the subject and the object are entered in each entity. In such case that object is a program, it is because this program may access another object. That is, the number of KPS system total entities becomes object + subject of a certain system. Moreover, the object is treated individually in the same system.

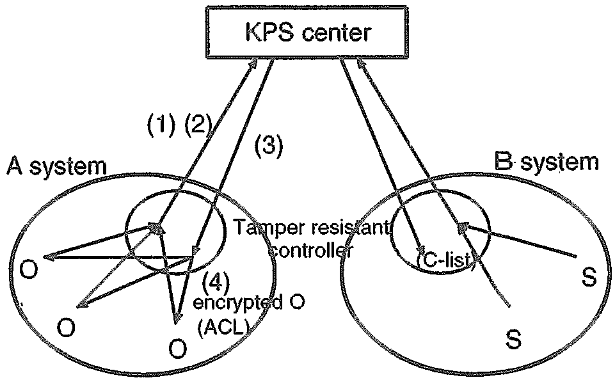
We assume system as follows.

The secret key algorithm is distributed to an individual entity and it is kept in each of tamper resistant module safely in the control part of each system which belongs. This is assumed to be a physically safe part.

In each system, all entities (S and O) are authenticated by the system controller. The controller must confirm the consistency of the relation between S and KPS-ID.

As key distribution center, we establish KPS center.

First, we will show the transaction in constructing system.



(1) (2) authentication
(3) secret key algorithm
(4) encrypt O with selected common key

Figure 5: In constructing system

1. Temporary key is created between each system controller and KPS center after authentication.
2. Through each system's controller, all subject and object are authenticated by KPS center. In object side, at the same time, the controller sends the list of access right (ACL).
3. Following its list (ACL), KPS center create the best secret key algorithm. And to each entity, the center sends the algorithm encrypted with temporary key.
4. In object side, the system controller encrypt O with S's key using secret key algorithm. And controller put encrypted O in each O as ACL.

KPS is used to connect each system like firewall.

Next, we will show the transaction in each access.

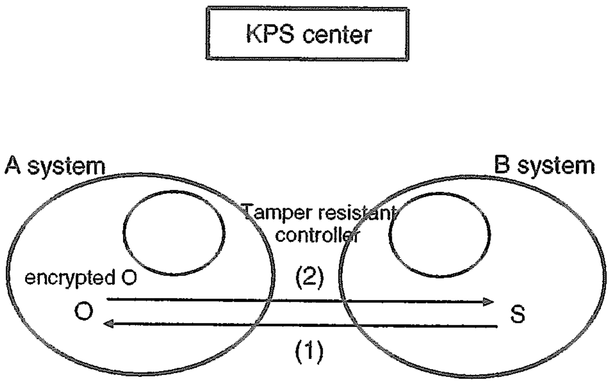
1. Subject S in B system send access demand.
2. If there is encrypted O with S's key, the O's owner send back it to S.

The memory space can be a little though an easy processing to obtain the key is needed. Even if each entity increases, it is not too much a problem. The only problem is how to achieve a tamper resistant module.

In such a case that tamper resistant part is assumed, absolutely safe part is ensured inside each system.

So, it is thought that all objects are inside the part and encrypted in going out.

But the physically safe part becomes very large. It is able to encrypt objects and to put only its key in



(1) access demand
(2) if there is O encrypted with S's key, send encrypted O

Figure 6: In each access

the safe part. However, in this case, as the number of each entity becomes large, the storage part becomes large, too. So, only secret key algorithm of each entity in KPS (linear scheme) is put in each tamper resistant part, space is saved.

And other problem is the change of the number of each entity (subject and object) with creation or deletion of S or O. In order to cope with this, following measure is considered.

For creation of S or O, in constructing system, in advance, we should make the number of total entity very large. When creation is happened, using new KPS-ID, we add it to remaining entity.

For deletion of S or O, at the object side, target encrypted object must be deleted. Because in secret key algorithm, it is difficult to delete keys. (That is, it is unable to delete key of C-list.)

5 Conclusion

It was enough in a usual access control inside a safe system. However, the exchange with the outside of the system has become active with the development of the network. In such situations, we thought about a stronger, more flexible access control by encrypting the object.

And, the case where the access is done especially frequently was assumed and the composition, the protocol, and the advantage, etc. were considered about the system using the common key cryptography.

In addition, we thought about the method of using KPS as a distribution method of a common key.

Though the part relied on a tamper became important in KPS , we set it at this time as the system management part to which each subject belonged.

A stronger access control that lightens the burden imposed on each entity can be achieved by using such system.

The problem in the future is an authentication of each subject when the system is constructed.

References

[1] Ishikane, Imai, "Data encryption in access control, "ISEC(Oct,1996).

[2] Ronald L.Rivest, and Butler Lampson, "SDSI-A Simple Distributed Security Infrastructure," (Apl,1996).

[3] Matsumoto, Imai,"One method of Key Predistribution System,"9th information theory and its application symposium(Oct,1986).

[4] Harrison, M.A., Ruzzo, W.L., and Ullman, J.D., "Protection in Operating Systems," Comm.ACM Vol.19(8) pp.461-471(Aug.1976).

[5] Conway, R.W., Maxwell, W.L., and Morgan, H.L., "On the Implementation of Security Measures in Information Systems," Comm.ACM Vol.15(4) pp.211-220(Apr.1972).

[6] Dennis, J.B., and VanHorn, E.C., "Programming Semantics for Multiprogrammed Computations," Comm.ACM Vol.9(3) pp.143-155(Mar.1966).

[7] David K.Gifford, "Cryptographic Sealing for Information Secrecy and Authentication," Comm.ACM Vol.25(4) pp.274-286(Apr.1982).

[8] Virgil D.Gligor, and Bruce G.Lindsay, "Object Migrationand Authentication," IEEE Transaction on Software Engineering Vol, SE-5, No.6 pp.607-611(Nov.1979).

[9] Ehud Gudes, "The Design of a Cryptography Based Secure File System," IEEE transaction on Software Engineering Vol. SE-6, No.5 pp.411-420(Sep,1980).