通信情報保護學會論文誌
第6卷 第4號, 1996. 12

# Design of Secure Information Center Using a Conventional Cryptography

Jun-Hyuk Choi*, Tae-Gap Kim**, Byung-do Go*, Jae-Cheol Ryou**

## Abstract

World Wide Web is a total solution for multi-media data transmission on Internet. Because of its characteristics like ease of use, support for multi-media data and smart graphic user interface, WWW has extended to cover all kinds of applications. The Secure Information Center(SIC) is a data transmission system using conventional cryptography between client and server on WWW. It's main function is to support the encryption of sending data. For encryption of data IDEA(International Data Encryption Algorithm) is used and for authentication mechanism MD5 hash function is used. Since Secure Information Center is used by many users, conventional cryptosystem is efficient in managing their secure interactions. However, there are some restrictions on sharing of same key and data transmission between client and server, for example the risk of key exposure and the difficulty of key sharing mechanisms. To solve these problems, the Secure Information Center provides encryption mechanisms and key management policies.

## 1. Introduction

Internet is the biggest inter-communication network in the world. It has several millions of hosts because of its useful characteristics for example, openness, extensibility, and commercial use. Hence it has become the focus of attention world. The introduction of GUI(Graphic User Interface) based web browsers such as netscape and mosaic have extended the notion of Internet to World Wide Web(WWW). WWW supports various multi-media data including normal data, voice, sound, image, video data, etc and provides easy access mechanism to its users. Because of such capabilities, WWW is considered as a total solution for almost all types of applications.

As the use of Internet increases, its users demand ever faster response and integrated service. Practically, the transmissions of multi-media data or real time interactions require considerable transmission capacity and the users want to be served by one integrated channel for various services. The development of high speed transmission media

* Electronics and Telecommunications Research Institute

** Chungnam National University

like fiber optic resulted in the introduction of B-ISDN(Broadband Integrated Service Digital Network). Since a B-ISDN provides several Mbps transmission capability, it can cover the transmissions of most kinds of data. This fact coincides with the request for multi-media data and B-ISDN will be widely used in future. In Korea, such a trend exists and the government hastened to construct B-ISDN. It is called HAN-BISDN(Highly Advanced National Broad band Integrated Service Digital Network).

Through the evolution of intercommunication technologies like WWW or B-ISDN, the interactions and information sharing among its users and groups become an important issue. To support interactions and information sharing in specific user groups, it is required to collect and store the information generated in that group and to publish or provide that information only to its authorized members. For this management task, Information Center is needed. But the lack of security in WWW makes it impossible to protect such an information sharing mechanism. It provides a background for the design of a Secure Information Center.

In this paper, we propose a mechanism for information sharing and management such as file transmission from client to server, and vice versa. After analyzing security problems in WWW, we propose a solution for it. It is called Secure Information Center. The Secure Information Center is based on conventional cryptography and key management mechanisms. In section 2, we describe what the Information Center and the general security mechanisms in WWW are. We describe the overall structure of a Secure Information Center including key management mechanisms in section 3. Section 4 describes detail implementation features of the Secure Information Center. Finally we make conclusions in section 5.

## 2. What is a Secure Information Center

The data transmission on WWW represents a typical client and server model. The client requests data and the server responds to that request. Figure 1 describes data transmission on WWW.

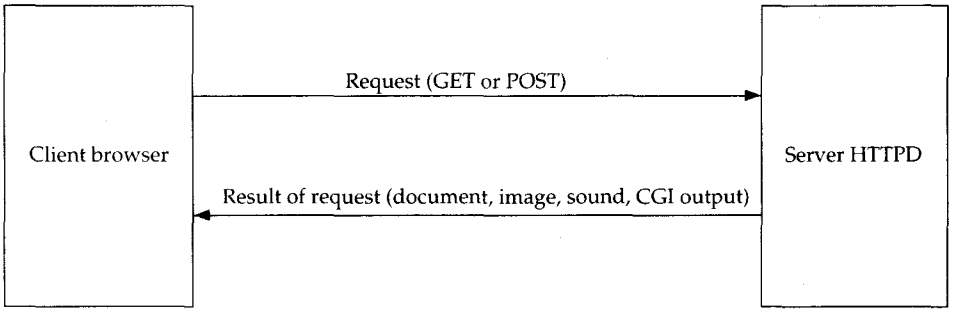



Figure 1. General data transmission mechanism on WWW

As described in Figure 1, a general data transmission mechanism on WWW is very simple. A client browser requests data from the server, normally using GET or POST method, and the server's HTTPD services the client's request. It finds the target document from its data base and sends the result to the client. If the client's request is to execute a program, which is called CGI(Common Gateway Interface), the server executes the target program and returns the program's output. In case of normal WWW data transmission mechanism, the client is only a receiver of data sent from the server. But in the Information Center structure, a client can also send data to the server. It is a main feature of the Information Center. Such a feature can be used in various applications. Figure 2 describes such a use of Information Center.

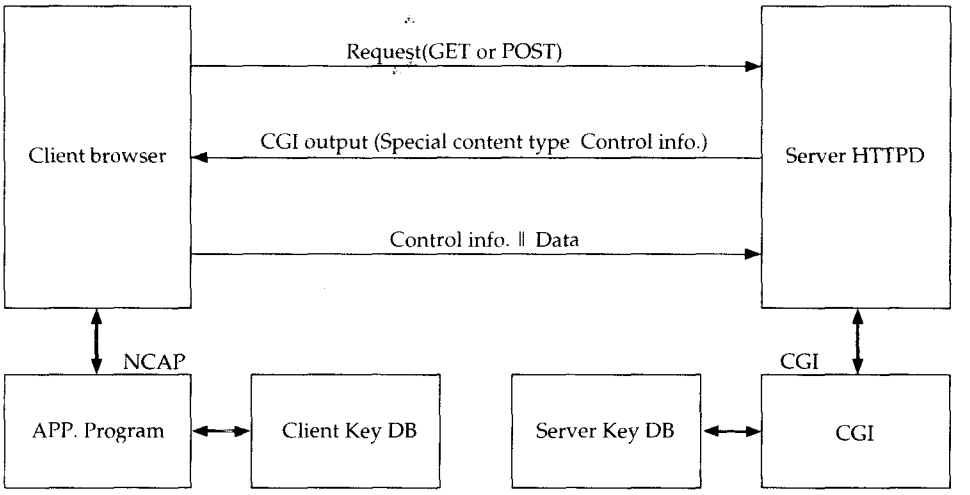



Figure 2. data transmission mechanism in HIC system

To send data, the client uses an application program which is invoked by the CGI's output. When the client browser receives the special content type from the server, it invokes an appropriate client application according to the content type. The client application program reads necessary data from the client's data base and delivers it to the browser again. The control info is used to manage the data transmission. It contains a information about the reading or writing status of each part. The detail description is given in section 3. If the Information Center is used without security features in its applications, it may pose serious security problems. So it is better to consider adding security mechanisms to the Information Center structure. In the rest of this section, we will describe the general problems in WWW and security mechanisms that can be applied to an Information Center structure.

Thanks to its simple structure and being a part of the UNIX kernel, TCP/IP forms the

basis of Internet[1]. Since TCP/IP does not consider security problems, there is no policy to prevent unauthorized access in the network. The HTTP(Hyper Text Transfer Protocol), being a base protocol of WWW, also depends on TCP/IP. As such there is also no security mechanism in the HTTP. This means that it cannot be used if there is a need for security. For this reason, EIT(Enterprise Integration Technologies) proposed a security enhanced version of HTTP(S-HTTP )[2] and Netscape company also proposed a security enhanced protocol, SSL(Secure Socket Layer)[3]. Since S-HTTP is a high level security enhanced mechanism, it can be used easily with other security applications. On the other hand, SSL is a more general and low level security mechanism, defined for the network layer.

Secure Information Center is designed to ensure secure document transmission using WWW protocols like S-HTTP and SSL. Its main mechanism is based on conventional cryptography. We can consider the use of a public key system which is a more general mechanism in a network environment, but because the use of Information Center is restricted to an authorized user group, it can be efficiently managed only using conventional cryptography. Basically, it is desirable to have same key between Information Center server and client and to manage their key sharing procedures. Using Secure Information Center, client can push(get) his document to(from) Information Center server's data base in secure channel.

To support general WWW security issues, Secure Information Center has to satisfy following requirements.

1) Data confidentiality

No one, except client and Information Center server, must be able to read data. Such a feature can be easily implemented using conventional cryptosystem with key sharing mechanisms.

2) User Authentication

Server or client must confirm each other. In other words, server must distinguish between authorized client's request and unauthorized client's request. Similarly, client must confirm if the received acknowledgement is sent from the authorized server.

3) Message Authentication

Client or server must confirm if the received data is not modified by unauthorized user in their transmission time. This requirement can be implemented using the message digest mechanism.

The satisfaction of these requirements must be followed by the system security and access control of data. It is no use preventing unauthorized access in communication network level if the server system is not secure against unauthorized user's access.

## 3. Design of Secure Information Center

Figure 3 describes the overall structure of a Secure Information Center. The client's web browser (specially Netscape) sends a request to Information Center server's HTTPD.

According to the server's acknowledgement, which is the type of specific application, the web browser invokes the client application program and communicates with it. For the interaction between the browser and the application program, NCAPI(Netscape Client Application Programming Interface) is used. To establish a secure communication channel, the client program encrypts all sending data. At the same time a hash value, which is a result of message digest, is generated. When all data to be sent is generated, the application program passes it to the browser using NCAPI and then the browser sends the passed data to the server using HTTP. Both GET and POST methods can be used for this but POST method is preferable because of its security advantages. For encryption of data, IDEA(International Data Encryption Algorithm)[4] module is used. MD5(Message Digest Algorithm)[4] is used to generate the hash value for message digest. The server's HTTPD receives the data sent. According to the client's request, the HTTPD invokes a corresponding CGI(Common Gateway Interface)[5] program which is generally used to serve various client's requests in WWW. The invoked CGI program reads the encrypted data and hash value through standard input channel(in the case of POST) or environment variables(in the case of GET). Since CGI program has IDEA and MD5 module, the encrypted data can be decrypted, and the server can confirm user and message authentication using hash value. The same method can be applied when the server sends data to the client. But this time, the server encrypts the data and the client decrypts it.

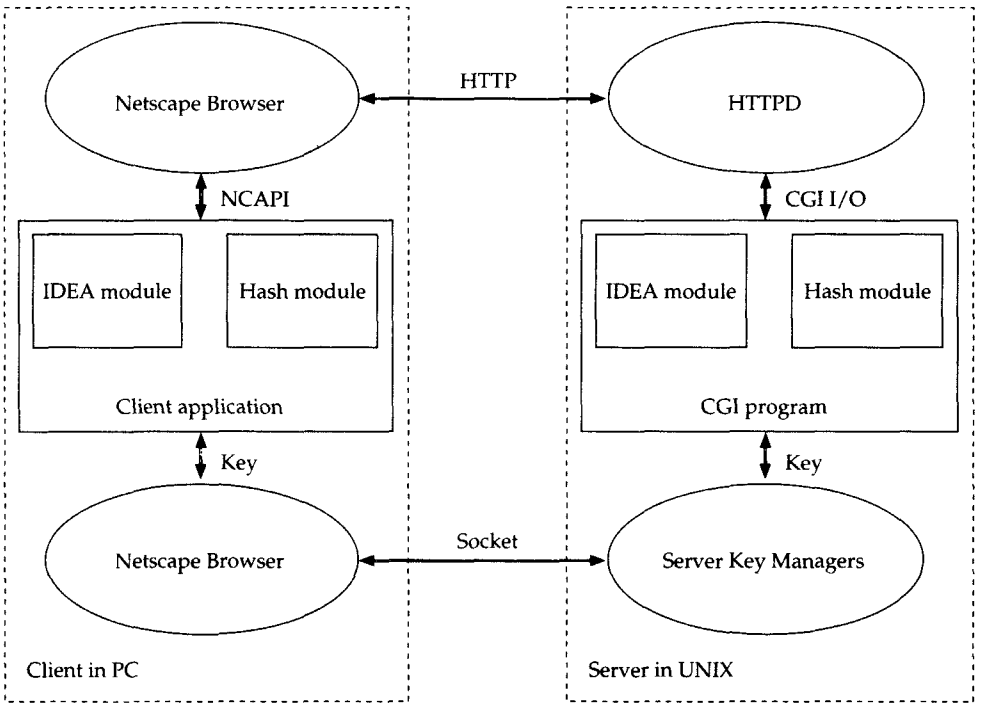



Figure 3. Overview of Secure Information Center

In Figure 3, we can see that the Secure Information Center makes use of original HTTP, not modified, but for security enhancement cryptography method and application program are used. The client application program and CGI program are used to help web browser and HTTPD. The client's key manager is used to manipulate the keys which are used in the Information Center system. At this point we must emphasis one important aspect of the system: key sharing between client and server. It is a premise of conventional cryptography. In the Secure Information Center, the key managers accomplish the sharing procedures. Their main functions are sharing of same key and updating of their key database. It is therefore natural that key management mechanisms be independent of the HTTPD and the browser. So they are implemented using socket interface. The detail description of key managers and key server is explained later in this section.

## 3.1 Key definitions

In Information Center system there are five different keys. Each of them is used for encryption or decryption of data and key. The detail description is as follows:

### 3.1.1. Base Key(Kb)

It is a pair of 128 bit keys for secure communication between client and server. It is consists of two 128 bit keys, Kb1 and Kb2. Kb means Kb1 ⊕ Kb2. The base key must be shared by both client and server. Base key is not used directly for communication due to its secrecy but used for only making and sharing of a temporary session key which is a real key for encrypted communication. The server must have all base keys of its clients in an Information Center key file. The Information Center key file's format is "ID:EncryptedKeyPairs:". The manager of Information Center system must distribute each client's base key using floppy disk to decrease chances of exposure. The procedure for distribution and confirmation of base key is described later in this section. The base key is encrypted with the client key in client key file, but it is encrypted with server key in the Information Center key file. IDEA module is used for their encryption and ID is a format of e-mail addresses.

### 3.1.2. Server Key(Kv)

The server key is a 128 bit key for encryption of client's base keys. It is stored in the Information Center key file in encrypted form using UNIX password mechanism with root ID. The format of server key is "root:EncryptedKey:". The Encrypted Key is of 208 bit length. Since the server key is 128 bit, it is required to apply the password mechanism, which is for 64 bit key, twice. The UNIX password mechanism reads 64 bit input and generates 104 bit encrypted output which consists of 16 bit salt (a kind of key) and 88 bit output[6]. When someone tries to retrieve client base key in Information Center key file, he must know the server key. For example, when the Information Center system manager wants to update the Information

Center key files contents, he must pass the server key checking routine.

As the UNIX password mechanism is based on 1-way hash function, crypt, it can't be decrypted with key(specially the salt). The 128 bit server key size is chosen because of two reasons: one is that compared to 64 bit DES(Data Encryption Standard) key it is more secure and the other reason is convenience of conversion to IDEA key.

#### 3.1.3. Message Key(Km)

The message key is used to generate session key which is real key of secure communication. Message key consists of a 64 bit random number and is combined with base key to make a session key. Since the message key is a temporary key it does not need to be stored.

#### 3.1.4. Session Key(Ks)

The session key is a real key used for encryption of sending data and decryption of receiving data. It must be shared between both client and server. When a client wants to send a file to its server or get a file from the server, a session key is generated. For generation of a session key, a base key and a message key are needed. The procedure of making session key is as follows :

$$Ks = Kb_1 \oplus Kb_2 \oplus Km$$

Kb1 and Kb2 is a base key pair and Km means a message key. As a session key must be shared by both client and server, it must be sent to the server in a secure channel using base key. The encrypted session key can be successfully decrypted, because the server can retrieve all client's base key using its server key. After the client and the server know the session key, the encrypted data transmission is started. The detail description of this is described in section 4.

#### 3.1.5. Client Key(Kc)

It is important to protect the base key from the unauthorized users. For this reasons of security and convenience of delivery, the Information Center manager distributes the client base key using floppy disk. But this is not enough. Usually a client does not keep in mind the needs of security of his own key. So there is another mechanism called client key which is used to encrypt the client's base key. Using the 128 bit client key, the client's base key is encrypted and stored in client key file. So the client must know his client key to retrieve the base key. There is no reason that the client must know the base key. For checking the validity of client key, the base key's hash value is stored with encrypted base key.

### 3.2 Key managers

To manage 5 Information Center keys described in 3.1, various key managers are designed. The key managers provide a convenient and efficient access interface to the Information Center's 5 keys for the client and the Information Center manager. To increase the usability of programs(independent from HTTPD), the socket based design mechanism is considered. The communication

between key managers is accomplished in a secure, encrypted, channel. Figure 4 describes the overall structure of key managers. The only key manager which is related with the base key uses a socket interface to confirm or update the base key between client and server. Other modules update the key file or generate the keys described in section 3.1. The rest of this section describes the key managers which use network facility.

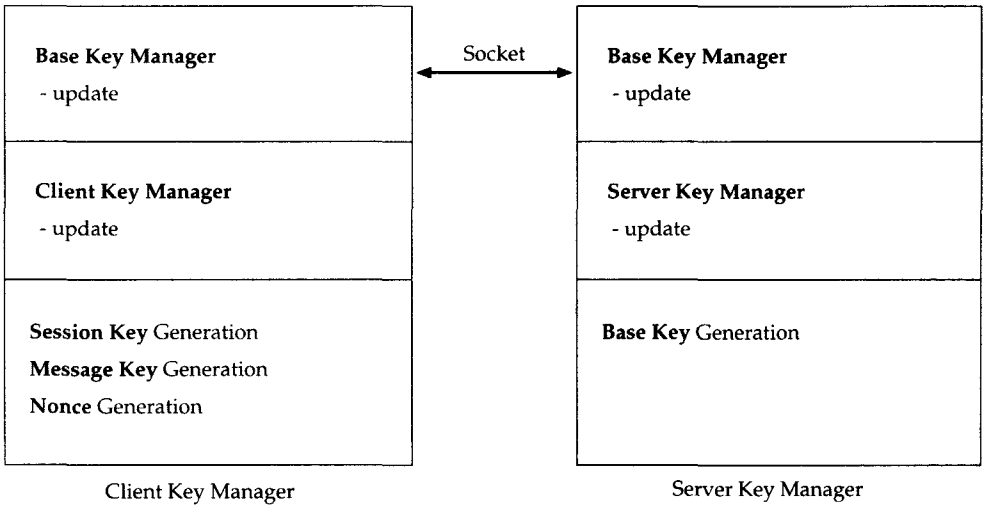



Figure 4. Key managers

### 3.2.1. Base Key Generation

The base key generator is normally used by Information Center manager. It generates a client's base key and stores it in the Information Center key file in encrypted form. Before it generates client's base key, it requests the server key to check the authority of the user. If the authorization check is passed, the user can generate a base key, and it is encrypted with the entered server key. Like a generation of client's base key, the server key can be changed using this module, but another mechanism is applied. IDEA

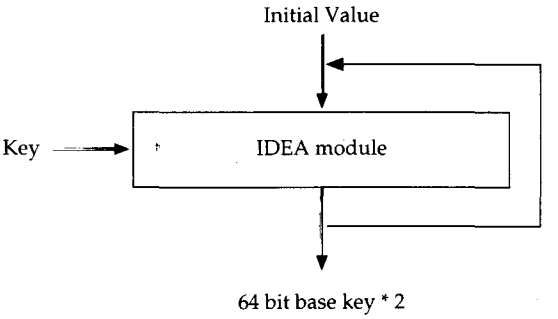



Figure 5. Generation of client's base key

module is used to encrypt the base key. Figure 5 describes the mechanism to generate a base key.

The reason that such complex mechanism is used to generate a client's base key is to increase the difficulty of guess. In Figure 5, the key and initial value is a kind of random number. This mechanism can be applied with other random number generations.

### 3.2.2. Base Key Update

Because the base key is a source of the secure communication between client and server, its secure maintenance is a critical problem. The client must change his base key when he doubts the exposure of his base key. In addition to such a situation, it is desirable to update base key regularly. Figure 6 describes a base key updating procedure.

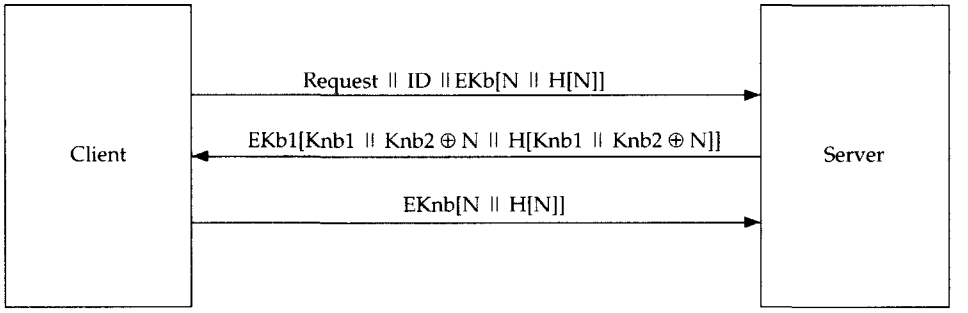



Figure 6. Base Key Update

The client sends a request with ID, encrypted nonce(N) using a part of current base key(Kb1) and the hash value. The compound of Kb1 and nonce gives key server an identification of valid client's request. If the received message can be successfully decrypted, the server makes a new base key(Knb(Knb1, Knb2)) and with received nonce encrypts it again. Although Kb(Kb1 ⊕ Kb2) is exposed, Kb1 is still secure. So the use of Kb1 or Kb2 is secure. Then the client can extract the Knb using Kb1 and nonce. If the procedure ends here, the base key consistency between client and server may be broken when there is an error in transmission media or unauthorized update of messages. To prevent such inconsistency, client sends an acknowledgement which is encrypted using new base key. If the received acknowledgement is correct then the key update is complete, otherwise the key server marks that client's base key is inconsistent. If the client base key is marked with inconsistent, all requests from that client are rejected and the base key must be reassigned to the client by the Information Center manager.

The client key update module updates the client key which is used to encrypt the base key stored in the client key file. The base key is stored in encrypted form with client ID of server's. The server key update module updates the root's server key. Initially, it

makes the encrypted server key using the UNIX password mechanism. Later, it modifies all the list of client's base keys with a newly entered server key. However in this case, all applications related with Information Center key file must be stopped for the consistency of the base keys and the contents of the Information Center key file must be regenerated. This requires serious consideration.

The message key generation and nonce generation modules have similar mechanism to the base key generation which generates a 128 bit random number. Therefore, its detail description is not described here.

### 3.2.4. Implementation

Information Center system is a typical client and server model. The client part is implemented on PC(Personal Computer) and the server part is implemented on a UNIX system. We use C++ language which is a representative general purpose object oriented language. The Information Center server part is based on OSF Motif environment to support the Graphic User Interface(GUI) and gcc compiler is used to make execution files. The server key manager can serve maximum 10 concurrent requests and for general usage, socket interface is supported. In the case of client program, it interacts with PC netscape browser. It is necessary to distinguish normal reply and special reply from the server to invoke the helper applications in netscape, so special content types are used. With this type, client netscape browser invokes the client application programs. For interactions between browser and application program, NCAPI(Netscape Client Application Programming Interface), which is a kind of library, is used. Like a server part, the client application is based on GUI, typically MS windows environment.

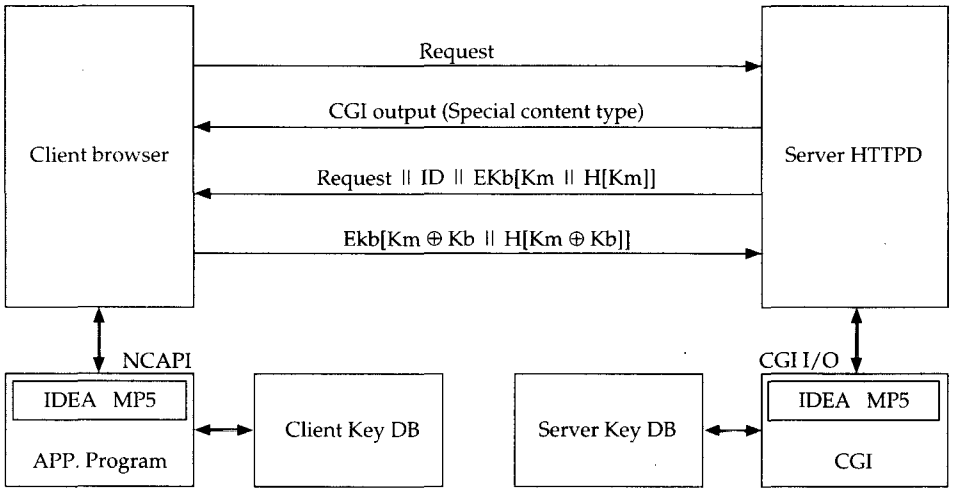



Figure 7. Session key sharing mechanism

Now, we will describe the detailed design specifications of secure Information Center. It is divided into two parts: one is for session key sharing mechanism and the other is for encrypted data transmission. As described in section 3, the base key is not used in encrypted data transmission, instead temporary session key is used. Figure 7 describes session key sharing mechanism.

When a client wants to send or receive the data, he sends a request to the server. Then the server's HTTPD recognizes the request and invokes a appropriate CGI program. The CGI program generates the reply containing a special content type. With this special content type the client browser, typically netscape, can invoke a client application program. This mechanism depends on netscape's helper application facility. After the client application is invoked, the communication between the browser and client application is performed using NCAPI(Netscape Client Application Programming Interface). Initially, the client application program makes a message key using the client key manager and encrypts it and its hash value with base key. After the message key generation is complete the application program sends it to browser using NCAPI. Then the client browser sends the message key to the server. Finally the server receives the encrypted message key and decrypts it. At this point the user and message authentication mechanism is executed. From the Figure 7, we can see that a message key(Km) is generated by the client every time, because the client always requests a data sending or receiving. After the client and server acquires common message key, they generate a session key using the base key(Kb) and message key as described in section 3.

After the session key exchange is finished, the encrypted data transmission is enabled. The basic mechanism is similar to session key exchange. But in the encrypted data transmission, a session key is used to encrypt the data. Figure 8 describes the encrypted data transmission from the client to the server.

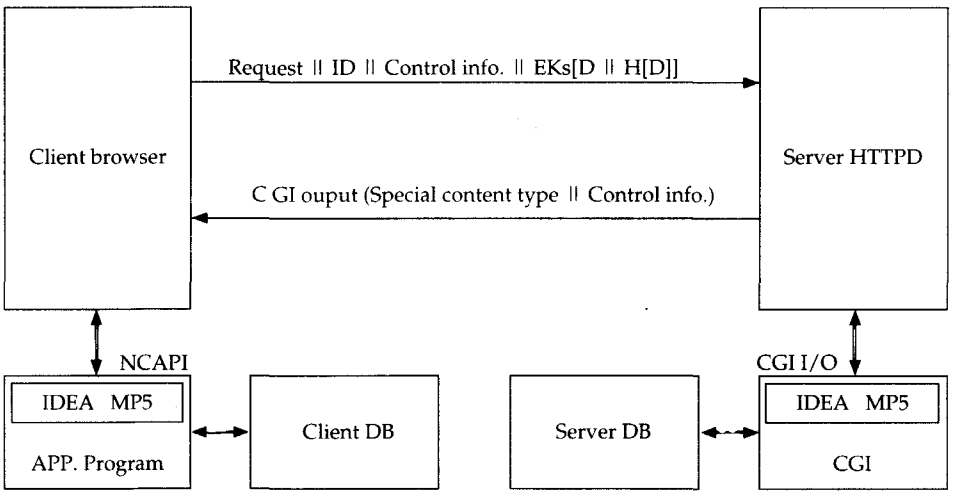



Figure 8. Data sending from client to server

The client requests data sending with his ID, Control info. and encrypted data. Control info is a data structure which contains a file name, file size, transmission ratio, and current status. With this information server makes a client's data file. If no error conditions are detected, the server sends a special content type and control info. and this procedures are repeated utill all the contents of data file are sent.

The mechanism by which the server sends data to the client is also similar to the case of sending data to the server. Therefore, its detail description is omitted. Figure 9 describes this situation.

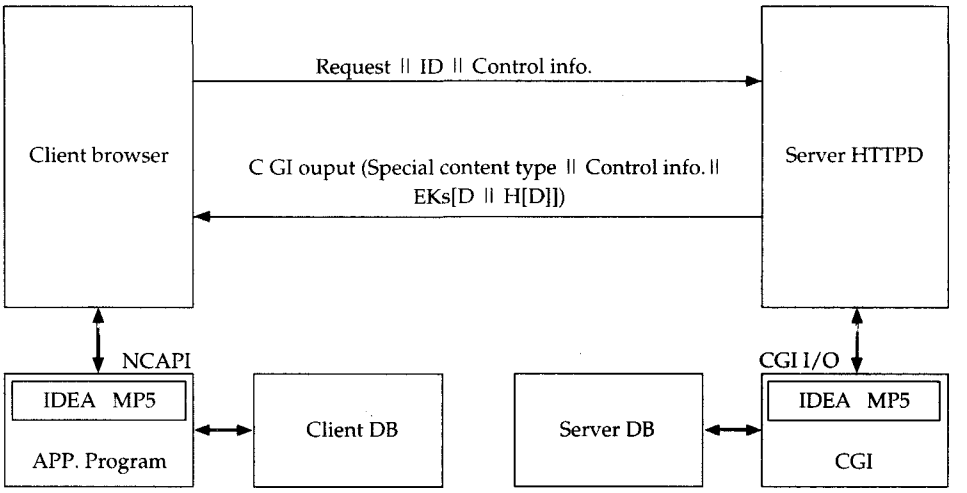



Figure 9. Data sending from server to client

Besides the encrypted data transmission and the key managers, we implemented a user interface program. For example, the GUI program is required to perform the following functionality. The Secure Information Center manager must make a floppy disk that contains the encrypted base key with the client key to assign a base key to client.

### 3.2.5. Conclusion

The Information Center system offers mechanisms using which a client can send his files to the server and also receive files from the server on WWW. The file sending mechanism from the client to the server can not be implemented easily with normal data transmission mechanism in WWW because the browser is normally used to get data from the server. To implement such a facility, it is required to develop application programs for the client part and CGI programs for the server part. But this simple file transmission mechanism has serious problems of lack of security. It is required to add some security mechanisms to such a

transmission system. In this paper we described the methods of secure data transmission using conventional cryptography. In Secure Information Center, we use IDEA algorithm for data encryption and decryption. To support the authentication mechanism, MD5 module is used. The IDEA and MD5 can be used to support general security requirements on WWW, if some other key management mechanisms are added. Because our cryptosystem is designed for authorized user group, requiring access restrictions for others, the conventional cryptography mechanism can support security mechanism using key sharing. The keys which are needed in key sharing are the base key and the session key. The base key is used to generate session key and to share the session key using secure encrypted channel between client and server. The session key is a temporary key which is used in encrypted data transmission. The session key is designed to preserve the base key in a secure state and to decrease the chances of exposure of the base key. We provided various key managers to manage the five keys which are used in Secure Information Center. Through this security mechanism, the WWW's authorized users can transfer their secret documents with confidence. The proposed system can be easily used because it is a application level cryptosystem and no modifications are apllied in protocol layer, like SSL or S-HTTP. But the range of service are restricted to specific service which needs a encryptied channel. To facilitate users, we provides all these programs in a GUI based environment. To provide extensibility, C++ language was used for these programs. The first version of Information Center System is based on conventional cryptography mechanism, but in later versions we will implement more general mechanisms using public key system[4] or PGP(Pretty Good Privacy)[7] mechanism.

## References

[1] Richard Stevens, "TCP/IP Illustrated, Volume 1", pp. 1-19, Addition-Wesley, 1994.

[2] Rescorla, "Secure HTTP", http://www.eit.com/creations/s-http, 1994.

[3] Kipp E.B. Hickman, "The SSL protocol", http://www.netscape.com/newsref/std/SSL.html, 1996.

[4] William Stallings, "Network and Internetwork Security", pp. 282-293, Prentice Hall International Edition, 1995

[5] Web Document, "World Wide Web Journal", pp. 75-87, O'Reilly & Associates, Inc, 1995

[6] Sun OS manual, "crypt : UNIX system call".

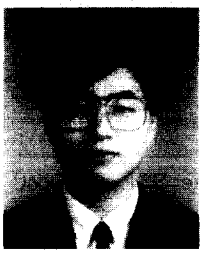
[7] Phillip Zimmerman, "PGP:Pretty Good privacy", O'Reilly & Associates, Inc.

## □ 著者紹介


**고 병 도**

1981년 2월 숭실대학교 전자계산학과 학사
1983년 2월 숭실대학교 전자계산학과 석사
1993년 3월 ~ 현재 충남대학교 전자계산학과 박사과정
1983년 3월 ~ 현재 한국전자통신연구소,광대역서비스연구실장

※ 관심분야 : 데이타베이스, 망관리, 정보통신망구조



**류 재 철**

1985년 2월 한양대학교 산업공학 학사
1988년 5월 Iowa State Univ. 전산학 석사
1990년 12월 Northwestern Univ. 전산학 박사
1991년 2월 - 현재 충남대학교 컴퓨터과학과 조교수

※ 관심분야 : 컴퓨터 및 통신 보안체제, 네트워크 관리, 분산처리 .

**김 태 갑**

1995년 - 충남대학교 전산학과 졸업(학사)
1997년 - 충남대학교 전산학과 졸업(석사)
1997년 - 현재 (주) 건인 부설 연구소 연구원

※ 관심 분야 : 시스템/네트워크 보안, 디지탈 통신

**최 준 혁**

1986년 - 동국대학교 전자계산학과 졸업(학사)
1988년 - 동국대학원 전자계산학과 졸업(석사)
1989년 - 현재 한국전자통신연구원 선임연구원

※ 관심분야 인터넷/인트라넷 응용 시스템, 실시간 멀티미디어 서비스