3 Security

Chapter Objectives

Advances in computer networks are being accompanied with increasing security risks such as the leakage of personal information, hacking of credit information, and computer virus infection. Accordingly, it is becoming increasingly important to take effective security measures.
In this chapter, the reader is expected to acquire knowledge about security and learn the necessity of security measures. The objectives are as follows:

① Learning the basic concepts and importance of information security.
② Understanding the kinds of risks involved in information processing systems and the management of those risks.

3.1 Information Security

3.1.1 What Is Information Security?

Information security means protecting information systems from various threats, including natural disasters, accidents, failures, errors, and crimes. In Japan, the Ministry of Economy, Trade and Industry (former Ministry of International Trade and Industry) has the Standards for Information System Safety Measures. Internationally, the OECD (Organization for Economic Cooperation and Development) has security guidelines.
The OECD guidelines, "Guidelines on the Security of Information Systems," defines "security" as protecting those who are dependent on information systems from hazards that may result from the absence of confidentiality, integrity, or availability.
In this context, the words "confidentiality," "integrity," and "availability" mean the following:

- Confidentiality means the state in which data, information, and the like can be disclosed only when an authorized person has gone through a prescribed procedure as authorized.
- Integrity, also called maintainability, means the state in which data and information have been maintained in an accurate, complete condition.
- Availability means the state in which data, information, and the like can be used at any time through a prescribed procedure.

3.1.2 Physical Security

Physical security means protecting information system facilities from intrusions, floods, lightning strikes, earthquakes, air pollution, explosions, fires, and other threats.

(1) RAS (Reliability, Availability, and Serviceability) Techniques

RAS is an acronym for Reliability, Availability, and Serviceability. These three elements are major yardsticks to measure the performance of information processing systems. RAS techniques are required to increase the time in which information processing systems can operate normally.
Major RAS techniques are described below.

① Redundancy system

A redundancy system means a system configuration in which a stand-by system is provided to prepare against equipment failures. Examples include parallel systems such as a duplex system and a dual system.

② Fail-safe system

"Fail-safe" refers to the idea of securing safety by preventing a failure of one part from affecting other parts. A fail-safe system is based on this idea.

③ Fail-soft system

"Fail-soft" refers to the idea of preventing a failure from halting major important functionalities at the sacrifice of some other functions. A fail-soft system is based on this idea.

(2) Standards for Information System Safety Measures

The Standards for Information System Safety Measures provide guidelines for securing the confidentiality, integrity, and availability of information systems. Last amended in 1995 by the Ministry of Economy, Trade and Industry (the former Ministry of International Trade and Industry), these standards enumerate the measures that must be taken by information system users.
The standards fall into three categories: installation standards (100 items), technological standards (26 items), and operation standards (66 items). By the magnitude of impact on society and industry, the contemplated threats are also divided into groups A, B, and C, and necessary measures are presented against them.
Other standards and guidelines regarding information systems include the following:

- Guidelines on the Security of Information Systems (1982, OECD)
- Standards for Preventing Illegal Access to Computers (1995, Ministry of Economy, Trade and Industry [former Ministry of International Trade and Industry])

3.1.3 Logical Security

Logical security means protecting information assets by encryption, user access control, and other systematic means of protection.

(1) Encryption

Encryption is a means of preventing tapping in communications. Encryption is the process of converting information into a ciphertext by using an encryption key so that it cannot be read by unauthorized people. The process of converting the ciphertext back into the plain text is called "decryption."
Decryption methods fall into two major categories:

- Common key cryptosystem: The same key is used for both encryption and decryption. The sender and the recipient need to have the same key. It is also called private key or symmetric key system.
- Public key cryptosystem: Different keys are used for encryption and decryption. The encryption key is made public, while the decryption key is kept confidential.

It should be noted that encryption is costly and requires management of the keys, which is a difficult task.

(2) Monitoring External Connection Points

It is becoming increasingly important to prevent intrusions from the outside by limiting or monitoring the points of connection with external networks, including the Internet. Routers and firewalls are monitored for this purpose.
A firewall has a filtering function to restrict the passage of data. It controls direct access to the internal network from the outside.

(3) User Authentication

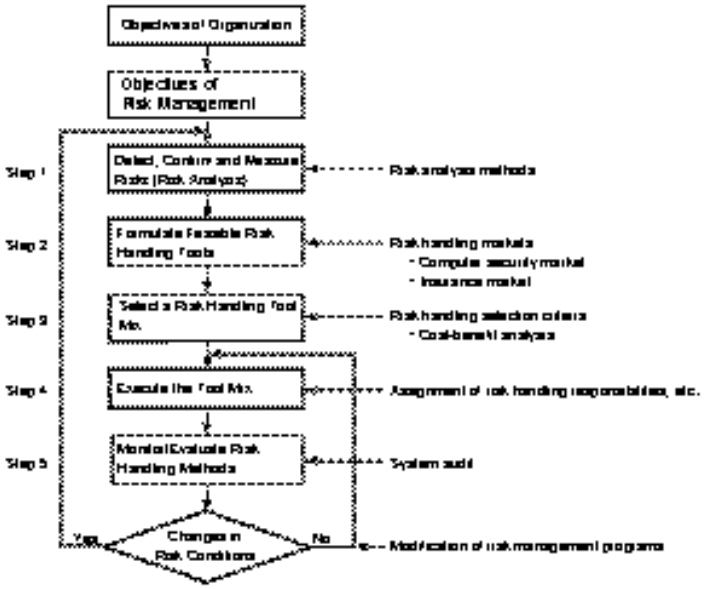
When an internal network accepts access from outside networks, it is necessary to authenticate users. A general method of user authentication requires users to enter their passwords, but this method loses its effectiveness once passwords are leaked. Hence the increasing popularity of the method using one-time passwords, which vary each time of use.

3.2 Risk Analysis

3.2.1 Risk Management

A logical process is required to cope with risks threatening an organization. It is necessary to identify possible accidents and other unfavorable events that could cause damage to an organization and take measures to deal with them in advance. This is called "risk management." It is defined as "planning, organizing, directing, and controlling the various activities of an organization in order to minimize the unfavorable operating and financial effects of contingent losses occurring in the organization."
Risk management is performed through such a procedure as shown in Figure 3-2-1.

Figure 3-2-1
Risk Management Procedure



3.2.2 Types, Evaluation, and Analysis of Risks

(1) Kinds of Risks

Risk analysis is the process of detecting risks present in an information system, determining their frequency and intensity, and analyzing how they will affect the achievement of the organization's targets. The causes of risks are referred to as "perils" or "threats." They include the following:

- Accidents and disasters
- Failures
- Errors
- Computer crimes and computer viruses
- Leaks of confidential or personal information

The factors promoting the occurrence or spread of perils are called "hazards." Examples of hazards are:

- Physical hazards: Losses resulting from physical factors such as the locations or structures of buildings and facilities
- Moral hazards: Losses caused intentionally or out of malice
- Morale hazards: Losses resulting from carelessness

(2) Risk Evaluation and Analysis

Risk analysis is performed by measuring deviations from standard values. The larger the deviations, the larger the risks.
There are two risk analysis methods: quantity method and quality method. Specific risk analysis methods include JRAM (JIPDEC Risk Analysis Method) developed by the Japan Information Processing Development Corporation (JIPDEC).

3.2.3 Risk Processing Methods

There are two risk processing methods:

- Risk control
- Risk finance

Information system security is based on risk control.

(1) Risk Control

Risk control is any of the methods of preventing the occurrence of risks or reducing their impact at their occurrence. Specific risk control methods include the following:

- Risk avoidance
- Loss prevention
- Loss reduction
- Risk separation
- Risk transfer by leasing contracts and the like

(2) Risk Finance

Risk finance refers to a financial means of ensuring a smooth recovery from the occurrence of a risk. Specific risk finance methods include the following:

- Risk holding
- Risk transfer by insurance

3.2.4 Security Measures

Procedures for risk analysis and security measures are described below.
First, risk analysis is carried out to clarify what risks are present and where in the information system. Annual losses are calculated based on the sizes and frequencies of losses. Next, security measures are worked out at a cost less than the amount of the losses.
That is, security measures are meaningless if they cost more than the losses that could result if they were not taken.

3.2.5 Data Protection

The information society is flooded with enormous volumes of data and information. Businesses hold huge volumes of accumulated information and protect them as trade secrets. For the security of information systems, the Ministry of Economy, Trade and Industry formulated and released the System Audit Standards, the Standards for Information System Safety Measures, and the Standards for Preventing Computer Viruses.
Of the risks mentioned above, computer crimes and computer viruses are explained below from the viewpoint of data protection.

(1) Computer Crimes

Crimes in which computers are directly or indirectly involved are called "computer crimes." Data-related crimes such as those mentioned below could be committed:

① Illegal input

Illegal input is the entry of invalid data. It is difficult to prevent illegal input by online terminal operators.

② Destruction

Acts of destruction include data corruption by hackers via terminals as well as physical destruction by blasting.

③ Eavesdropping

Information could be stolen when recorded on paper or in storage media, when being processed by computer, or when being transmitted.

④ Falsification

Falsification means any unauthorized modification or deletion of data or programs.

(2) Computer Viruses

A computer virus is a program that destroys or falsifies the contents of memories and disks. It is often difficult to identify the route and time of virus infection. Some computer viruses remain dormant for some time after infection before becoming active. Typical symptoms of virus infection include the following:

- Program destruction
- Destruction of file data
- Sudden appearance of graphics or characters on the display
- Occurrence of trouble at a specific date or time (such as Friday, the 13th)

It is often too late to take some action after finding a symptom of infection. Therefore, floppy disks brought in from outside should be checked by anti-virus software before they are used. It is safe not to use media whose origins or owners are not known. On this issue, the Ministry of Economy, Trade and Industry formulated and released the Standards for Preventing Computer Viruses.

The type of virus that has been particularly prevalent in recent years is the macro virus. Macro viruses take advantage of the macro functions of applications programs sold on the market. A macro virus infects a data file of an applications program, and when the file is opened by the user, the macro function is executed without the user's knowledge. Macro viruses can spread more widely than the conventional types of viruses dependent on operating systems and hardware. One such example was the powerful "Melissa" virus, which emailed itself to all of a user ’s address book entries.

3.2.6 Protection of Privacy

In their sales activities, businesses obtain personal information from order forms and applications prepared by consumers. The information obtained this way is usually stored in databases for use in subsequent sales activities. These databases hold enormous volumes of information, including address, gender, date of birth, family members earnings, and property held. Public organizations also hold huge volumes of personal information stored in the resident, taxpayer, driving license, social insurance, and other registries.

Personal information should naturally be kept confidential because of its character. Should it be disclosed by mistake or otherwise, privacy is inevitably violated. The protection of privacy is opposite to disclosure. Any organization holding personal information must take every precaution to prevent the leakage of information.

For the protection of personal information, the OECD's privacy guidelines contain eight basic principles. In Japan, the Act for Protection of Computer Processed Personal Data held by Administrative Organs was established in 1988 to properly regulate the use of personal information (such as social insurance, tax payment, driving licenses, and resident registration) held by administrative agencies.

At present, however, Japan has only several guidelines in this field, including the Guidelines for

Individuals' Information Protection established in 1989 by the Ministry of Economy, Trade and Industry and the Guidelines for the Protection of Personnel Information in Computer Processing in the Private Sector established in 1995 by the ministry. No legislation has been established yet to regulate the use of personal information in the private sector.

Exercises

Q1 **Which of the following measures is least effective for warding off, detecting, or eliminating computer viruses?**

A. Do not use software of an unknown origin.
B. When reusing floppy disks, initialize them in advance.
C. Do not share floppy disks with other users.
D. Clear the memory before executing a program.

Q2 **Which is the correct statement about the recent increase in macro viruses?**

A. The execution of an infected application loads the macro virus into the main memory, and in this process, the virus infects program files of other applications.
B. Activating the system from an infected floppy disk loads the macro virus into the main memory, and then the virus infects the boot sectors of other floppy disks.
C. A macro virus infects document files opened or newly created after an infected document file is opened.
D. Since it can be easily determined as to whether a macro function is infected by a virus, infection can be prevented at the time of opening a document file.

Q3 **Which is the appropriate term to describe the information given to users for the purpose of checking the authenticity to use a computer system and grasping the condition of use?**

A. IP address B. Access right C. Password D. User ID

Q4 **Which is the most appropriate practice for user ID management?**

A. All the users involved in the same project should use the same user ID.
B. A user having multiple user IDs should set the same password for all the IDs.
C. When privileges are set for a user ID, they should be minimized.
D. When a user ID is to be deleted, an adequate time interval should be taken after the termination of its use has been notified.

Q5 **Which is the inappropriate statement about the use or management of passwords?**

A. If a password is incorrectly entered a predetermined number of times, the user ID should be made invalid.
B. Passwords should be recorded in a file after being encrypted.
C. Users should try to use those passwords which are easy to remember, but those which are hard to be guessed by other people.
D. Users should be instructed to change their passwords at predetermined intervals.
E. Passwords should be displayed on terminals at the point of entry for the purpose of confirmation.

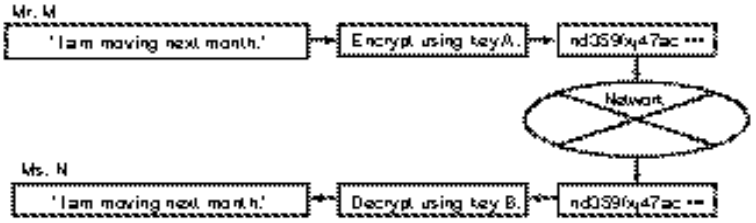
Q6 **Which is in an inappropriate way of handling passwords and a password file in the system management department?**

A. The security managers should regularly check whether or not passwords can be easily guessed, and recommend that problem passwords be changed.
B. The department should recommend that users record their passwords in their notebooks in order to minimize the frequency of inquiring about their passwords.
C. If it is possible to set the term of validity of passwords, the term should be used for checking password validation.
D. Even if a password file records encrypted passwords, the department should make it inaccessible to general users.

Q7 **From the viewpoint of security, which is the <u>inappropriate method of operating</u> a computer system using a public switched telephone network?**

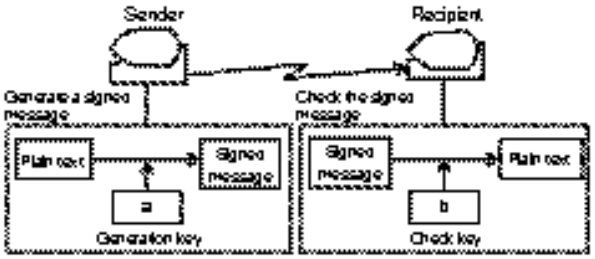
A. Make a password unusable for connection unless it is changed within predetermined intervals.
B. When a connection request is made, establish connection by calling back to a specific telephone number.
C. Display a password on a terminal at the point of entry so that the user will not forget the password.
D. Disconnect the line if a password is wrongly entered a predetermined number of times.

Q8 **When as shown in the figure below, Mr. M sends to Ms. N a message they want to keep confidential, which is the appropriate combination of the keys used for encryption and decryption?**



	Key A	Key B
A	M's private key	M's public key
B	N's public key	N's private key
C	Common public key	N's private key
D	Common private key	Common public key

Q9 **The figure shows the configuration of electronic signature used into the public key cryptosystem. Which is the appropriate combination of the terms to be put into a and b?**



	a	b
A	Recipient's public key	Recipient's private key
B	Sender's public key	Sender's private key
C	Sender's private key	Recipient's public key
D	Sender's private key	Sender's public key

Q10 **There is a transposition cryptosystem in which plain text is divided into four-character blocks and in each block, the first character is replaced by the third, the second by the first, the third by the fourth, and the fourth by the second. In this system, which is the correct cipher text for the plain text "DEERDIDDREAMDEEP"?**

A. DIDDDEEPDEERREAM
B. EDREDDDIARMEEDPE
C. ERDEIDDDEMRAEPDE
D. IDDDEPDEERDEEMRA
E. REEDDDIDMAERPEED