UNIT 7 DATA SECURITY AND MANAGEMENT

Structure

7.1 Introduction

7.2 Objectives

7.3 Security Problem vis-à-vis Internet

7.3.1 Threats to Computing System

7.4 Security Measures to Protect the System

7.5 Security Policy

7.5.1 Purpose of Security Policy

7.5.2 Who should be Involved When Forming Policy?

7.5.3 What Makes a Good Security Policy?

7.6 Identification and Authentication

7.7 Access Control

7.8 Data and Message Confidentiality

7.9 Security Management

7.10 Security Audit

7.11 Summary

7.12 Terminal Questions

7.13 Answers and Hints

7.14 References and Suggested Readings

7.1 INTRODUCTION

During the first few decades of their existence, computer networks were primarily used by defense personnel for security by university researchers for research purposes and by corporate employees for sharing printers and other peripherals. Under these conditions, security of data transmission did not get much attention as there were very few people using the networks. But in the new corporate scenario, millions of ordinary citizens are using networks for online banking, shopping and filling their returns through E-governance etc.and so data security is looming on the horizon as a potentially massive problem.

7.2 OBJECTIVES

After studying this unit, you should be able to:

- describe threats posed to computing systems;
- enlist security measures to protect the system;

- explain the need and aim of security policy;
- enlist who should be involved in forming policy;
- determine what makes a good security policy and security mechanisms that could be implemented to provide identification and authentication services;
- describe how to control access and types of security mechanisms that could be implemented to provide access control service; and
- explain the concept of security management.

7.3 SECURITY PROBLEM VIS-À-VIS INTERNET

With the huge growth in the number of Internet users all over the world, the security of data and its proper management plays a vital role for future prosperity and potentiality. Security is a broad topic and it covers a multitude of issues. In its simplest form, it is concerned with making sure that nosy people cannot read, or still worse, modify messages intended for other recipients. It is concerned with people trying to access remote service is that they are not authorized to use.

Security problems can be generally divided into four areas: secrecy, authentication, non repudiation and integrity control. Secrecy has to do with keeping information from the unauthorized users. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a commercial deal. Non repudiation deals with signatures and being sure that a message you received was really the one sent and not something that a malicious adversary modified in transit or concocted.

Security violations (misuse) of the system can be categorised as being either intentional (malicious) or accidental. It is easier to protect against accidental misuse than to protect against malicious misuse. Among the forms of malicious access are the following:

– Unauthorized reading of data (theft of information)

– Unauthorized modification of data

– Unauthorized destruction of data

Absolute protection of the system from malicious abuse is not possible, but the cost to the perpetrator can be made sufficiently high to deter most, if not all, attempts to access, without proper authority, the information residing in the system.

7.3.1 Threats to Computing System

There are basically two types of threats to a computing system. Both are briefly highlighted below:

Program Threats:

i) Trojan Horse

ii) Trap doors

Trojan Horse: Many systems have mechanisms for allowing programs written by users to be executed by other users. If these programs are executed in a domain that

provides the access rights of the executing user, they may misuse these rights. For example, inside a text-editor program, there may be a code to search the file to be edited for certain key words. If any one found it, the entire file may be copied to special area accessible to the creator of the text editor. A code segment that misuses its environment is called a TROJAN HORSE.

Trap Door: The designer of a program or system might leave a hole in the software that only he or she is capable of using. This type of security breach was shown in the movie "WAR GAMES". For instance, the code might check for a specific user identifier or password, and might circumvent normal security procedures. There have been cases of people being arrested for embezzling from banks by including rounding errors in their code, and having the occasional half-cent credited to their accounts. This account crediting can add up to a large amount of money, considering the number of transactions that a large bank executes.

A clever trap door could be included in a compiler.

System Threats

The two most common methods for achieving misuse in an operation system are worms and viruses.

Worms: A worm is a process that uses the spawn mechanism to clobber system performance. The worm spawns copies of itself, using up system resources and perhaps locking out system use by all other processes. On computer networks, worms are particularly patent, since they may reproduce themselves among systems and thus shut down the entire network.

Viruses: Another form of computer attack is virus. Like worms, viruses are designed to spread into other programs and can wreak havoc in a system including modifying or destroying files and causing system crashes and program malfunctions. A worm is structured as a complete, standalone program while a virus is a fragment of a code embedded in a legitimate program. Viruses are major problems for computer users, especially users of microcomputer systems.

The best protection against it is prevention, or the practice of safe computing. Another safeguard, although it does not prevent infection, does permit early detection.

Worms and viruses are generally considered to pose security, rather than protection, problems.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

Fill in the blanks?

i) Security problems can be divided into four areas:

Secrecy, _____, _____ and _____

ii) Absolute protection of the system from malicious abuse is _____

7.4 SECURITY MEASURES TO PROTECT THE SYSTEM

To protect the system, security measures must be taken at two levels:

Physical: The site or sites containing the computer systems must be physically secured against armed or surreptitious entry by intruders.

Human: Users must be screened carefully so that the chance of authorizing a user who then gives access to an intruder is reduced.

7.5 SECURITY POLICY

The security-related decisions you make or fail to make as administrator largely determines how secure or insecure your network is, how much functionality your Network offers, and how easy your network is to use. However, you cannot make good decisions about security without first determining what your security goals are. Until you determine what your security goals are, you cannot make effective use of any collection of security tools because you simply will not know what to check for and what restrictions to impose. For example, your goals will probably be very different from the goals of a product vendor. Vendors are trying to make configuration and operation of their products as simple as possible, which implies that the default configurations will often be as open (i.e. insecure) as possible. While this does make it easier to install new products, it also leaves access to those systems, and other systems through them, open to any user who wanders by.

Your goals will be largely determined by the following key tradeoffs:

Services offered versus security provided

Each service offered to users carries its own security risks. For some services the risk outweighs the benefit of the service and the administrator may choose to eliminate the service rather than try to secure it.

Ease of use versus security

The easiest system to use would allow access to any user and require no passwords; that is, there would be no security. Requiring passwords makes the system a little less convenient, but more secure. Requiring device-generated one-time passwords makes the system even more difficult to use, but much more secure.

Cost of security versus risk of loss

There are many different costs to security: monetary (i.e. the cost of purchasing security hardware and software like firewalls and one-time password generators), performance (i.e. encryption and decryption take time), and ease of use (as mentioned above). There are also many levels of risk: loss of privacy (i.e. the reading of information by unauthorized individuals), loss of data (i.e. the corruption or erasure of information), and the loss of service (e.g. the filling of data storage space, usage of computational resources, and denial of network access). Each type of cost must be weighed against each type of loss.

Your goals should be communicated to all users, operations staff, and managers through a set of security rules, called a “security policy”. We are using this term,

rather than the narrower "computer security policy" since the scope includes all types of information technology and the information stored and manipulated by the technology.

Finally, a security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide.

7.5.1 Purpose of Security Policy

The main purpose of a security policy is to inform users, staff and managers of their obligatory requirements for protecting technology and information assets. The policy should specify the mechanisms through which these requirements can be met. Another purpose is to provide a baseline from which to acquire, configure and audit computer systems and networks for compliance with the policy. Therefore, an attempt to use a set of security tools in the absence of at least an implied security policy is meaningless.

Another major use of an AUP is to spell out, exactly, the corporate position on privacy issues and intellectual property issues. In some countries, if the company does not explicitly state that e-mail is not secure, it is considered to be so and any breach could cause privacy and confidentiality liabilities. It is very important to spell out what is and is not acceptable in intellectual transfers and storage and what the corporate privacy policies are to prevent litigation about the same.

An Appropriate Use Policy (AUP) may also be part of a security policy. It should spell out what users shall and shall not do on the various components of the system, including the type of traffic allowed on the networks. The AUP should be as explicit as possible to avoid ambiguity or misunderstanding. For example, an AUP might list any prohibited USENET newsgroups. (Note: Appropriate Use Policy is referred to as Acceptable Use Policy by some sites.)

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 3 Min.*

What is a Security Policy?

.....

.....

.....

.....

.....

.....

7.5.2 Who should be Involved When Forming Policy?

In order that a security policy be appropriate and effective, it needs to have the acceptance and support of all levels of employees within the organization. It is especially important that corporate management fully support the security policy process otherwise there is little chance that they will have the intended impact. The following is a list of individuals who should be involved in the creation and review of security policy documents:

⇒ Site security administrator

⇒ Information technology technical staff (e.g. staff from computing center), administrators of large user groups within the organization (e.g., business divisions, computer science department within a university, etc.)

⇒ Security incident response team

⇒ Representatives of the user groups affected by the security policy

⇒ Responsible management

⇒ Legal counsel (if appropriate)

The list above is representative of many organizations, but is not necessarily comprehensive. The idea is to bring in representation from key stakeholders, management who have budget and policy authority, technical staff who know what can and cannot be supported, and legal counsel who know the legal ramifications of various policy choices. In some organizations, it may be appropriate to include EDP audit personnel. Involving this group is important if resulting policy statements are to reach the broadest possible acceptance. It is also relevant to mention that the role of legal counsel will also vary from country to country.

7.5.3 What Makes a Good Security Policy?

The characteristics of a good security policy are:

1) It must be implementable through system administration procedures, publishing of acceptable use guidelines, or other appropriate methods.

2) It must be enforceable with security tools, where appropriate, and with sanctions, where actual prevention is not technically feasible.

3) It must clearly define the areas of responsibility for the users, administrators, and management.

The components of a good security policy include:

1) Computer Technology Purchasing Guidelines, which specify required, or preferred, security features. These should supplement existing purchasing policies and guidelines.

2) A Privacy Policy which defines reasonable expectations of privacy regarding such issues as monitoring of electronic mail, logging of keystrokes, and access to users' files.

3) An Access Policy, which defines access rights and privileges to protect assets from loss or disclosure by specifying acceptable use guidelines for users, operations staff, and management. It should provide guidelines for external connections, data communications, connecting devices to a network, and adding new software to systems. It should also specify any required notification messages (e.g., connect messages should provide warnings about authorized usage and line monitoring, and not simply say "Welcome").

4) An Accountability Policy, which defines the responsibilities of users, operations staff, and management. It should specify an audit capability, and provide incident

handling guidelines (i.e., what to do and who to contact if a possible intrusion is detected).

5) An Authentication Policy which establishes trust through an effective password policy, and by setting guidelines for remote location authentication and the use of authentication devices (e.g., one-time passwords and the devices that generate them).

6) An Availability statement.

Please answer the following Self Assessment Question.

Self Assessment Question 3 *Spend 3 Min.*

What are the main components of good security policy?

.....

.....

.....

.....

.....

.....

7.6 IDENTIFICATION AND AUTHENTICATION

The first step toward securing the resources of a LAN or network is the ability to verify the identities of users [BNOV91]. The process of verifying a user's identity is referred to as authentication. Authentication provides the basis for the effectiveness of other controls used on the LAN. For example, the logging mechanism provides usage information based on the user ID. The access control mechanism permits access to LAN resources based on the user ID. Both these controls are only effective under the assumption that the requestor of a LAN service is the valid user assigned to that specific user ID.

Identification requires the user to be known by the LAN in some manner. This is usually based on an assigned user ID or in some other format like user certificate or user token. However the LAN cannot trust the validity that the user is in fact the person who he/she, claims to be, without being authenticated. The authentication is done by having the user supply something that only the user has, such as a token or credential, something that only the user knows, such as a password, or something that makes the user unique, such as a fingerprint. The more of these that the user has to supply, the less risk there is of someone masquerading as the legitimate user.

A requirement specifying the need for authentication should exist in most LAN policies. The requirement may be directed implicitly in a program level policy stressing the need to effectively control access to information and LAN resources, or may be explicitly stated in a LAN specific policy that states that all users must be uniquely identified and authenticated.

On most LANs, the identification and authentication mechanism is a user ID/ password scheme. [BNOV91] states "password systems can be effective if managed

properly [FIPS112], but seldom are. Authentication which relies solely on passwords has often failed to provide adequate protection for systems for a number of reasons. Users tend to create passwords that are easy to remember and hence easy to guess. On the other hand users that must use passwords generated from random characters, while difficult to guess, are also difficult to be remembered by users. This forces the user to write the password down, most likely in an area easy accessible in the work area". Research works such as [KLEIN] detail the ease with which passwords can be guessed. Proper password selection (striking a balance between being easy-to-remember for the user but difficult-to-guess for everyone else) has always been an issue. Password generators that produce passwords consisting of pronounceable syllables have more potential of being remembered than generators that produce purely random characters. [FIPS180] specifies an algorithm that can be used to produce random pronounceable passwords.

Password checkers are programs also called password policy that enable a user to determine whether a new password is considered easy-to-guess, and thus are unacceptable.

Password-only mechanisms, especially those that transmit the password in the clear (in an unencrypted form) are susceptible to being monitored and captured. This can become a serious problem if the LAN has any uncontrolled connections to outside network.

Networks agencies that are considering connecting their LANs to outside networks, particularly the Internet, should examine [BJUL93] before doing so. If, after considering all authentication options, LAN policy determines that password-only systems are acceptable, the proper management of password creation, storage, and destruction become all the more important. [FIPS 112] provides guidance on password management. [NCSC85] provides additional guidance that may be considered appropriate.

Because of the vulnerabilities that still exist with the use of password-only mechanisms, more robust mechanisms can be used. [BNOV91] discusses advances that have been made in the areas of token-based authentication and the use of biometrics. A smartcard based or token based mechanism requires that a user be in possession of the token and additionally may require the user to know a PIN or password. These devices then perform a challenge/response authentication scheme using real time parameters. Using real time parameters helps prevent an intruder from gaining unauthorized access through a login session playback. These devices may also encrypt the authentication session, preventing the compromise of the authentication information through monitoring and capturing.

Locking mechanisms for LAN devices, workstations, or PCs that require user authentication to unlock can be useful to users who must leave their work areas frequently. These locks allow users to remain logged into the LAN and leave their work areas (for an acceptable short period of time) without exposing an entry point into the LAN.

Modems that provide users with LAN access may require additional protection. An intruder who can access the modem may gain access by successfully guessing a user password. The availability of modem use to legitimate users may also become an issue if an intruder is allowed continual access to the modem. Mechanisms that provide a user with his or her account usage information may alert the user that the

account was used in an abnormal manner (e.g. multiple login failures). These mechanisms include notifications such as date, time, and location of last successful login, and number of previous login failures. The type of security mechanisms that could be implemented to provide the identification and authentication service are listed below.

⇒ password-based mechanism,

⇒ Smartcards/smart tokens based mechanism,

⇒ Biometrics based mechanism,

⇒ Password generator,

⇒ Password locking,

⇒ Keyboard locking,

⇒ PC or workstation locking,

⇒ Termination of connection after multiple failed logins

⇒ User notification of 'last successful login' and 'number of login failures',

⇒ Real-time user verification mechanism,

⇒ Cryptography having unique user keys.

Please answer the following Self Assessment Question.

Self Assessment Question 4 *Spend 3 Min.*

Fill in the blanks:

i) On most LANS, the identification and authentication mechanism is a _____.

ii) Modems that provide user with LAN Access requires additional protection from _____.

iii) _____ and _____ are security mechanisms that could be applied to provide identification and authentication services.

7.7 ACCESS CONTROL

This service protects against the unauthorized use of LAN resources, and can be provided by the use of access control mechanisms and privilege mechanisms. Most file servers and multi-user workstations provide this service to some extent. However, PCs which mount drives from the file servers usually do not. Users must recognise that files used locally from a mounted drive are under the access control of the PC. For this reason it may be important to incorporate access control, confidentiality and integrity services on PCs to whatever extent possible.

According to [NCSC87], access control can be achieved by using discretionary access control or mandatory access control. Discretionary access control is the most common type of access control used by LANs. The basis of this kind of

security is that an individual user, or program operating on the user's behalf is allowed to specify explicitly the types of access other users (or programs executing on their behalf) may have to information under the user's control.

Discretionary security differs from mandatory security in that it implements the access control decisions of the user. Mandatory controls are driven by the results of a comparison between the user's trust level or clearance and the sensitivity designation of the information.

Access control mechanisms exist to support access granularity for acknowledging an owner, a specified group of users, and the world (all other authorized users). This allows the owner of the file (or directory) to have different access rights than all other users, and allows the owner to specify different access rights for a specified group of people, and also for the world. Generally access rights allow read access, write access, and execute access. Some LAN operating systems provide additional access rights that allow updates, append only, etc.

A LAN operating system may implement user profiles, capability lists or access control lists to specify access rights for many individual users and many different groups. Using these mechanisms allows more flexibility in granting different access rights to different users, which may provide more stringent access control for the file (or directory). (These more flexible mechanisms prevent a situation in which a user has to be given more access than necessary, a common problem with the three level approaches.) Access control lists assign the access rights of named users and named groups to a file or directory. Capability lists and user profiles assign the files and directories that can be accessed by a named user.

User access may exist at the directory level, or the file level. Access control at the directory level places the same access rights on all the files in the directory. For example, a user who has read access to the directory can read (and perhaps copy) any file in that directory. Directory access rights may also provide an explicit negative access that prevents the user from any access to the files in the directory. Some LAN implementations control how a file can be accessed. (This is in addition to controlling who can access the file.) Implementations may provide a parameter that allows an owner to mark a file sharable, or locked. Sharable files accept multiple accesses to the file at the same time. A locked file will permit only one user to access it. If a file is a read only file, making it sharable allows many users to read it at the same time.

These access controls can also be used to restrict usage between servers on the LAN. Many LAN operating systems can restrict the type of traffic sent between servers. There may be no restrictions, which imply that all users may be able to access resources on all servers (depending on the user access rights on a particular server). Some restrictions may be in places that allow only certain types of traffic, for example only electronic mail messages, and further restrictions may allow no exchange of traffic from server to server. The LAN policy should determine what types of information need to be exchanged between servers. Information that is not necessary to be shared between servers should then be restricted.

Privilege mechanisms enable authorized users to override the access permissions, or in some manner legally bypass controls to perform a function, access a file, etc. A privilege mechanism should incorporate the concept of least privilege. [ROBA91]

defines least privilege as "a principle where each subject in a system be granted the most restrictive set or privileges needed for the performance of an authorized task".

For example, the principle of least privilege should be implemented to perform the backup function. A user who is authorized to perform the backup function needs to have read access to all files in order to copy them to the backup media. (However the user should not be given read access to all files through the access control mechanism.) The user is granted a 'privilege' to override the read restrictions (enforced by the access control mechanism) on all files in order to perform the backup function. The more granular the privileges that can be granted, the more control there does not have to grant excessive privilege to perform an authorized function. For example, the user who has to perform the backup function does not need to have a write override privilege, but for privilege mechanisms that are less granular, this may occur. The types of security mechanisms that could be implemented to provide the access control service are listed below.

- Access control mechanism using access rights (defining owner, group, world permissions),
- Access control mechanism using access control lists or "ACLs", user profiles, capability lists,
- Access control using mandatory access control mechanisms (labels),
- Granular privilege mechanism,

Please answer the following Self Assessment Question.

Self Assessment Question 5 *Spend 3 Min.*

What is the use of Access Control Service?

.....

.....

.....

.....

.....

7.8 DATA AND MESSAGE CONFIDENTIALITY

The data and message confidentiality service can be used when the secrecy of Information is necessary. As a front line protection, this service may incorporate mechanisms associated with the access control service, but can also rely on encryption to provide further secrecy protection. Encrypting information converts it to an unintelligible form called cipher text, decrypting converts the information back to its original form. Sensitive information can be stored in the encrypted cipher text form. In this way if the access control service is circumvented, the file may be accessed but the information is still protected by being in encrypted form. (The use of encryption may be critical on PCs that do not provide an access control service as a front line protection.)

It is very difficult to control unauthorized access to LAN traffic as it is moved through the LAN. For most LAN users, this is a realised and accepted problem. The use of encryption reduces the risk of someone capturing and reading LAN messages in transit by making the message unreadable to those who may capture it. Only the authorized user who has the correct key can decrypt the message once it is received.

7.9 SECURITY MANAGEMENT

Businesses all over the world are adopting the BS7799 Information security management system to systematically plug loopholes that exist due to the constant and varied means of information exchange that form part of daily routine.

BS7799 is the British standard for Information Security Management. It is the most widely recognised security standard in the world. It has now become an International Standard, ISO 17799. The standard is divided into two parts:

BS7799 Part-1 (ISO-17799: 2000)-Code of Practice for Information Security Management.

BS7799 Part-2, Specifies requirement for establishing, implementing and documenting ISMS.

ISO/IEC 17799:2005 is a standard code of practice and can be regarded as a comprehensive catalogue of good security things to do. Now it may be called ISO/IEC 27001.

It contains 11 basic frameworks and 132 sets of controls. The major components of Information Security Management System (ISMS) are.

A) Plan - It contains Scope, Policy, Risk Assessment (RA), Risk Treatment Plan (RTP), Statement of Applicability (SOA)

B) DO - It contains controls, awareness training, manage resources and prompt dedication and response to incidents.

C) Check- It contains management review, internal ISMS audit.

D) Act- It contains ISMS improvements, prevention action, and concentrative action.

Basic Frameworks are as follows:

1) Security Policy
2) Organizing Security
3) Asset Management
4) Human Resource Security
5) Physical and Environmental Security
6) Communication and Operation Management
7) Access Control
8) Information System Acquisition Development and Maintainance
9) Information Security Incident Management
10) Business Continuity Management
11) Compliance

7.10 SECURITY AUDIT

One of the most important and critical reasons for conducting a security audit is to ensure that the efforts spent on security is coherent with business objectives ultimately yielding cost effective benefits. Although this may seem obvious, it is possible that efforts might go off the requisite target missing out on the key areas where the effort is needed. The objective of Security Audit is to find out the vulnerabilities that an organization is facing with its IT infrastructure.

Physical Security Audit

Physical Security is one of the most neglected areas in Security. Global E-Secure helps companies to plug this area by identifying the threats in terms of location of hosted servers, perimeter and barrier protection followed and physical measures adopted currently to protect sensitive data such as: cages, racks, Personnel controls, Biometrics devices, Alarm Systems and others.

Network Security Audit

Internal employees, customers or partners access the organizational network internally, through a public gateway or through VPNs, Leased Lines, ISDN or even Dial-Up connections. The Network conducts a study of the access policies and procedures for internal LAN access, as well as the connectivity of the organization with its branches and remote locations and highlights the vulnerabilities in the network.

Application Security Audit

This involves a complete detailed analysis of the mission critical applications of the enterprise such as web servers, directory servers, mailing applications and enterprise solutions of the company to which its employees, customers or partners may have access. Since security has to complement business and should be transparent to the user, it is essential for security to integrate seamlessly with the application.

Please answer the following Self Assessment Question.

Self Assessment Question 6 *Spend 3 Min.*

What are the major components of ISMS?

.....

.....

.....

.....

.....

.....

Let us now summarize the points covered in this unit.

7.11 SUMMARY

- Security policy is totally dependent upon requirement and what the type of network.
- Purpose of Security policy is to inform users, staff and managers of their obligatory requirement for protecting technology and information assets.
- Following personnel must be present when forming policy. Site security manager, all IT staff, managers of all divisions, Security Incident Response team and Legal Counsellor.
- A good security policy is one which is implementable, enforceable and defines the areas of responsibilities.
- The process of verifying user's identity is referred to as Authentication.
- Access control can be achieved by using discretionary access control and mandatory access control.
- The data and message confidentiality service can be used when the secrecy of information is necessary.
- BS7799 is the widely used ISO/IEC standard having 11 frameworks and 132 set of controls.
- Security audit is mostly needed in case of vulnerabilities that an organization has to face at physical, network and application level.

7.12 TERMINAL QUESTIONS

1) Why is security policy needed? How will you choose a good security policy?
2) Define access control. Give a practical example of the same.
3) BS7799 is only one choice for security management. Explain it critically

7.13 ANSWERS AND HINTS

Self Assessment Questions

1) (i) Authentication, Non-repudiation and Integrity Control, (ii) Not possible
2) A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide.
3) A good security policy has the following components:

   Computer Technology Purchasing Guidelines, A Privacy Policy, An Access Policy, An Accountability Policy, An Authentication Policy, An Availability statement.

4) (i) User ID/Password, (ii) Intruders, (iii) Password based mechanism and smart card/smart tokens based mechanism.

5) Access control service protects against the unauthorized use of LAN resources. This service can be provided by the use of access control mechanisms and privilege mechanisms.

6) The major components of ISMS are :

A) Plan - It contains Scope, Policy, Risk Assessment (RA), Risk Treatment Plan (RTP), Statement of Applicability (SOA)

B) DO - It contains controls, awareness training, manage resources and prompt dedication and response to incidents.

C) Check- It contains management review, internal ISMS audit.

D) Act- It contains ISMS improvements, prevention action, and concentrative action.

Terminal Questions

1) Refer to section 7.4 and 7.5 of the unit.

2) Refer to section 7.7 of the unit.

3) Refer to section 7.9 of the unit.

Please also go through other reference books for more details.

7.14 REFERENCES AND SUGGESTED READINGS

1. Andrew S. Tanenbaum. Computer Networks. 5th ed. New Delhi: Prentice Hall of India Pvt. Ltd., 2003.

2. Behrouz A Forouzan. Data Communication and Networking. 2nd ed. Tata Mcgraw-Hill Edition, 2003.

3. ICANN - Internet Corporation for Assigned Names and Numbers. 24 Mar. 2006 <http://www.icann.org>.