CHAPTER 4

Prevention and Technical Defenses

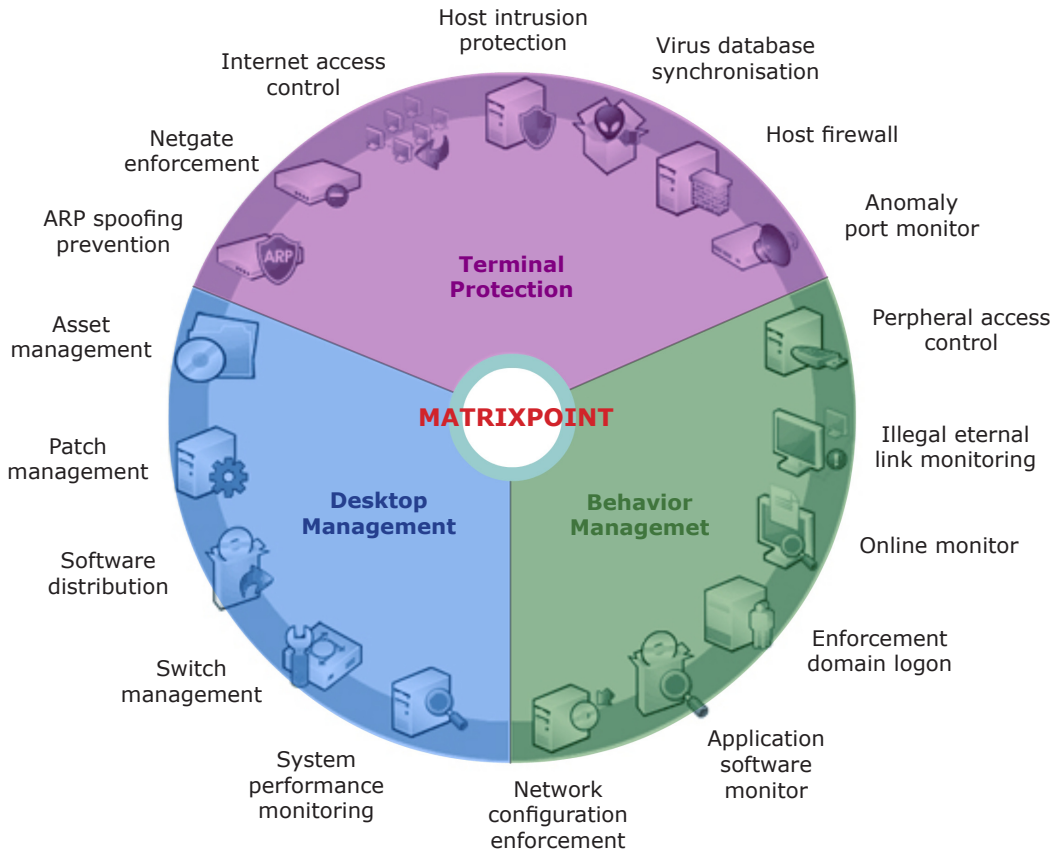
LEARNING OUTCOMES

By the end of this chapter, you should be able to:

1. Define the meaning of information infrastructure;
2. Identify the risk and threats of information infrastructure and steps to overcome the risks;
3. Determine the prevention and technical defence of OS security, LAN, Firewalls and Antivirus Technology;
4. Explain the piracy and anti-piracy techniques; and
5. Identify the anti-piracy techniques.

INTRODUCTION

Observe the diagram below.



The diagram shows how a defence system works in an organisation. Can you identify and elaborate on technical defence system?

To ***"prevent"*** literally means ***"to avoid something from happening"***. Computer disaster prevention is not very commonly sought, but computer disaster recovery is. This is unfortunate because your success in computer disaster recovery is directly related to how well you have prepared for it. Technical defences consist of an enormous range of methods designed to deter, prevent, detect and react to attack and to adapt over time to improve those defences.

Generally, technical defences are mechanism that come into direct contact with the content or the mechanism that store, process, or communicate it. Creating and operating a set of technical defences requires a serious effort over a long time and involves a lot of specialised expertise and resource commensurate with the risk being addressed.

4.1 PROTECTING INFORMATION INFRASTRUCTURE

Protecting infrastructure from disaster has always been important for industry, government and society. Yet with more activities dependent on computer networks - from banking and aviation to emergency services - the reliability and security of information and communication systems against disasters, both natural and man-made, are in doubt. The question of protection is difficult due to the majority of critical information infrastructure is privately-owned, interlinked with other firms, and crosses international borders. Evidence suggests there are currently insufficient incentives for protection to be adequately implemented. Companies internalise the costs and hope for the best. Indeed, without really knowing the risk profile, it is not even clear what constitutes adequate protection in the first place.

Due to society depends largely on information technology; it faces new kinds of unknown threats in the past. The security incidents in the global character of IT networks can cause disruptions or total failure to the information infrastructure. In national level, the incidents are not necessarily originated from our country but it can be from other country. Criminals and terrorists increasingly try to damage complex technical systems with targeted attacks and it cannot be ruled out that vital information infrastructure can become the target of such attacks. Therefore internal security is inseparable from secure information infrastructures and their protection is a key priority for national security policy.

4.1.1 What are the Threats and Risks to Information Infrastructure?

Technical defects, human error or deliberate acts of damage or destruction are a frequent cause of system disruption or breakdowns which in turn may directly affect other sectors because of the network architecture of information infrastructure failure. This can affect the economy and society as a whole.

IT systems are always vulnerable to hacking attacks or threats posed by computer viruses and worms. A growing number of malicious software programmes and targeted attacks can be attributed to organised crime and terrorist groups. Their main objective is to gain profit financially from such attacks or harm the national economy. Primary targets of such attacks are large companies, banks or public institutions. For private household computers, criminals try to penetrate to steal online banking details or spread computer viruses and spam.

The attackers use a whole range of different methods, some example are in the following list as shown in Figure 4.1.

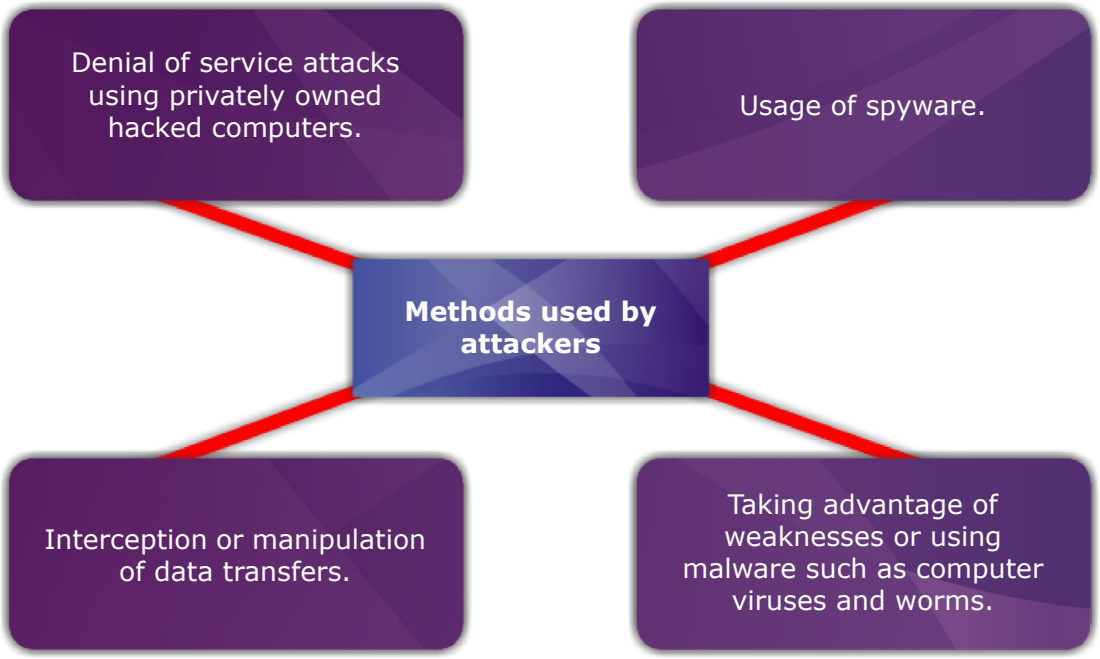


Figure 4.1: Examples of methods used by attackers

Today, organised criminals have shifted their attention away from single computer toward routers, firewalls and other security applications intended to protect the IT systems of business and public administrations. This type of attack affects not only individual computer, but possibly thousands of computers in the attached network. In worse-case scenario, manipulation of central IT systems may cause the entire information infrastructure to collapse, resulting in significant economic damage.

4.1.2 Steps to Protect Information Security

Security risks can be reduced by spreading knowledge about the threats and possibilities for protection, clearly assigning responsibilities for security matters, implementing security measures and using reliable products and processes. There are few steps that should be followed in order to protect the information security (see Figure 4.2).

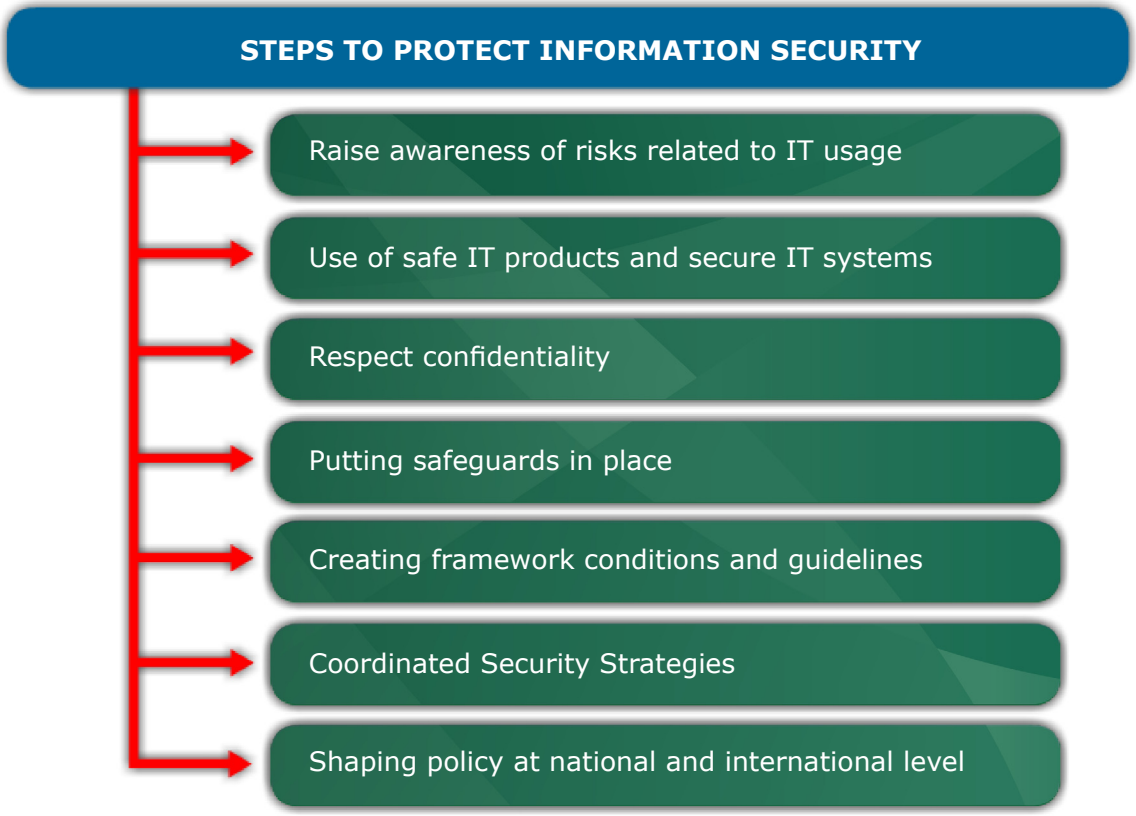


Figure 4.2: Steps to help protect the information security

From Figure 4.2, let us look into details each of the steps given.

1. Raise awareness of risks related to IT usage

Raise the awareness and inform the general public and the business sector about the risks to IT use. Initiatives can be launched directed to people at all levels, from corporate management and high-level public administration to ordinary employees and private individuals as PC users.

2. Use of safe IT products and secure IT systems

Users should support the use of reliable IT products and systems trusted IT security application. Certain IT security group should improve its capacity to examine and evaluate IT products and systems under security aspects and issue relevant certificates.

3. Respect confidentiality

Unprotected digital communications are extremely vulnerable, easy to intercept and manipulate. Therefore, it is advisable to choose product that depend on availability of reliable, innovative and trusted encryption products that guarantee the confidential communication. The business sector should be made particularly aware of the risks

associated with information theft and the possibilities and benefits of preventing such theft by using reliable encryption products.

4. Putting safeguards in place

It is necessary to put coordinated technical, physical, organisational and structural safeguards in place. Responsibilities, duties and roles for all tasks related to IT protection must be clearly defined. Adequate IT security measures are being implemented in all public authorities at federal level. All businesses and organisations are firmly called upon to make adequate arrangements for protecting their IT systems.

5. Creating framework conditions and guidelines

Adequate framework conditions and guidelines should be created, taking account of international norms and standards in order to ensure full protection in all security-relevant areas. Appropriate guidance should be given to those branches of the economy where special requirements apply to IT security. All other areas of society will be provided with recommendations and guidelines on IT security.

6. Coordinated security strategies

It is important to synchronise security-relevant processes and mechanisms. Therefore, it is advisable to advocates defining joint standards and coordinated application concepts, in order to optimise systems with regard to their security, technical, economic and data protection properties.

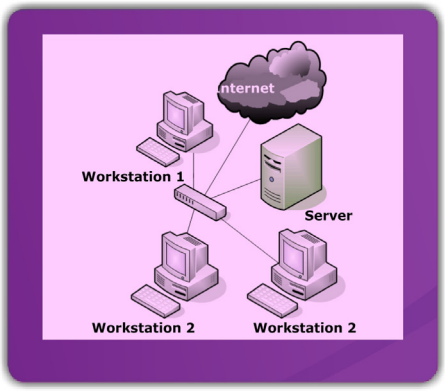
7. Shaping policy at national and international level

The government should intensify its effort to actively shape policy with regard to existing and new forms of cooperation for protecting information infrastructures. In addition,it will strengthen the national and international cooperation when formulating guidelines, directives and other legal instruments.

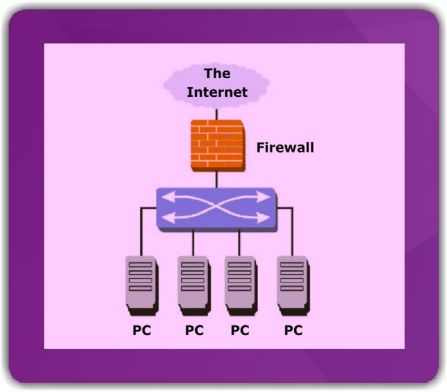
4.2 OS SECURITY, LAN, FIREWALLS AND ANTIVIRUS TECHNOLOGY

Let's observe the photos below.

Operating Systems



Local Area Network



Firewall

Antivirus

Have you come across or noticed these four photos? Define the functions of each of the photos provided. Then, compare your answer with your coursemate.

4.2.1 Operating System Security

What do you know about Operating System?

An operating system (commonly abbreviated to either OS or O/S) is an interface between hardware and user; an OS is responsible for the management and coordination of activities and the sharing of the resources of the computer.

The operating system acts as a host for computing applications that are run on the machine. As a host, one of the purposes of an operating system is to handle the details of the operation of the hardware.

4.2.1.1 Overview of Operating System Security

A clear understanding of core concepts of OS security and how they are used and implemented in operating systems are shown in Table 4.1.

Table 4.1: Core Concepts of OS Security and Descriptions

Core Concepts of OS Security	Descriptions
Protection	The mechanism for coherent access to shared resources (files, directories, memory, processors, devices, etc.) by users and programs.
Authentication	The means of verifying the identity and permissions of a user or program.
Access Control	A method of protection that attaches permissions to the objects to be protected.
Capability	A method of protection that attaches permissions to users or programs.
Principle of Least Privilege	The notion that no user or program should have more permission than is required for the task at hand. Related to the "need to know" principle, by which entities are allowed access to information only according to their present needs.

4.2.1.2 Protection of Operating System

Protection is mediated by permissions that an entity has to access the objects in the system. Table 4.2 below describes the protection of operatin system in a computer.

Table 4.2: Protection of Operating System

Protection System	Description
System Model	• Entities: users and processes. • Objects: - Hardware objects: CPU, memory, printer, disk,terminals. - Software objects: file, program, semaphore.
Protection policies	• Use and sharing of data. • Allocation of resources. - CPU time - Disk quotas - Memory • Access to devices. • Organisation of entities. - Users - Groups
Protection domains - permission contexts for a process	• Protection context of a process. • Static or dynamic, but static systems tend to waste resources. • Variety of organisations. - by user - by process - by procedure (code unit). - by role (e.g. as user, as sysadmin, as operator) etc. • Domain switching. - by request for permission. - by assuming a new role. - by asserting a new identity.
UNIX	• The user is a domain.

	• Switch by asserting a new username (su program). • Switch by implicit change (suid, sgid programs). • Extension by request to daemon process (database).
MULTICS	• Ring structure, inner ring has the most privilege. • Process has an access bracket, and current ring. • Access within the bracket is allowed. • Access outside the bracket traps to the OS. • Calls to outer rings may need to copy their arguments. • Calls to inner rings must occur through a "gate".
Access Matrix Match domains to objects.	• The access matrix is an object, and can be accessed. • The domains are objects, with the permission to "switch". • The access right can be read, write, execute, print, switch.

4.2.1.3 Security Methods of Operating System

The basis of protection is separation which keeping one user's objects separate from other users. The separation can be described in Figure 4.3.

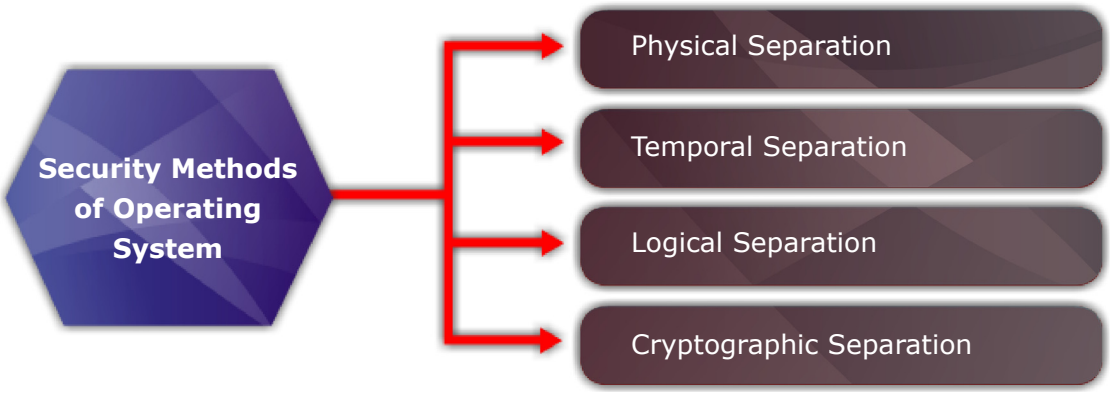


Figure 4.3: Security methods of operating system

- **Physical Separation:** Different processes use different physical objects such as separate printers for output requiring different levels of security.
- **Temporal Separation:** Processes having different security requirements are executed at different times.
- **Logical Separation:** Users operate under the illusion that no other processes exist as when an operating system constrains a program's accesses so that the program cannot access objects outside its permitted domain.
- **Cryptographic Separation:** Processes conceal their data and computations in such a way that they are unintelligible to outside processes.

Although separation is the basis protection, the problem will arise when the operating system provide sharing for some of the objects because separation means that it separate users and their objects.

Because of that, there are several ways an operating system can assist by offering protection at any of several levels which are described in Figure 4.4:

Figure 4.4: Several ways on how an operating system can assist in offering computer protection

- **Do not protect**
  Operating systems with no protection are appropriate when sensitive procedures are being run at separate times.

- **Isolate**
  Different processes running concurrently are unaware of the presence of each other. Each process has its own address space, files and other objects. Other processes are completely concealed.

- **Share all or share nothing**
  The owner of an object declares it to be public or private. Public objects will available to all users whereas private object is available only to its owner.

- **Share via access limitation**
  With protection by access limitation, the operating system checks the allow ability of each user's potential access to an object. Access control is implemented for a specific user and a specific object.

- **Share by capabilities**
  Protection allows dynamic creation of sharing rights for objects. Sharing can depend to the owner or the subject on the context of the computation or on the object itself.

- **Limit use of an object**
  This form of protection limits not just the access to an object to an object but the use made of that object after it has been accessed.

The purpose of a protection system (see Figure 4.5) is to prevent accidental or intentional misuse of a system.

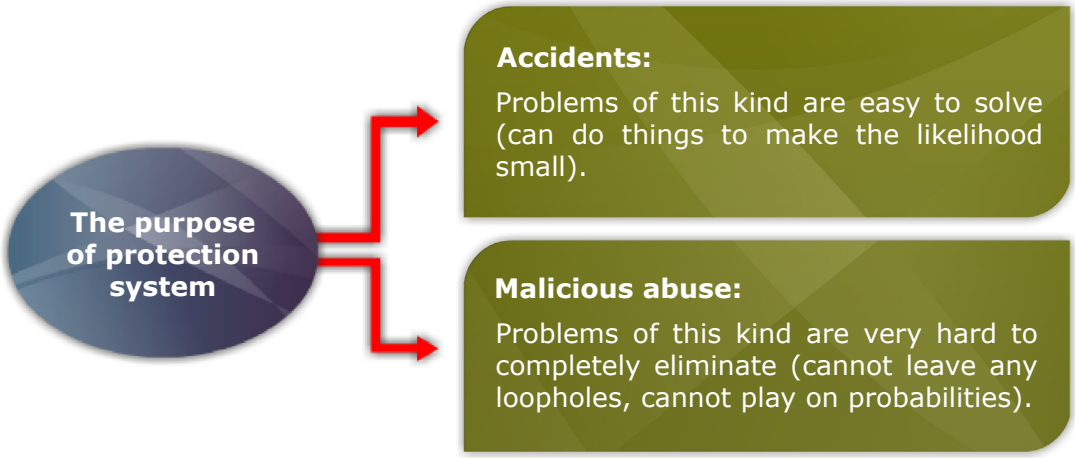


Figure 4.5: The purpose of protection system

There are three aspects to a protection mechanism as shown in Figure 4.6.

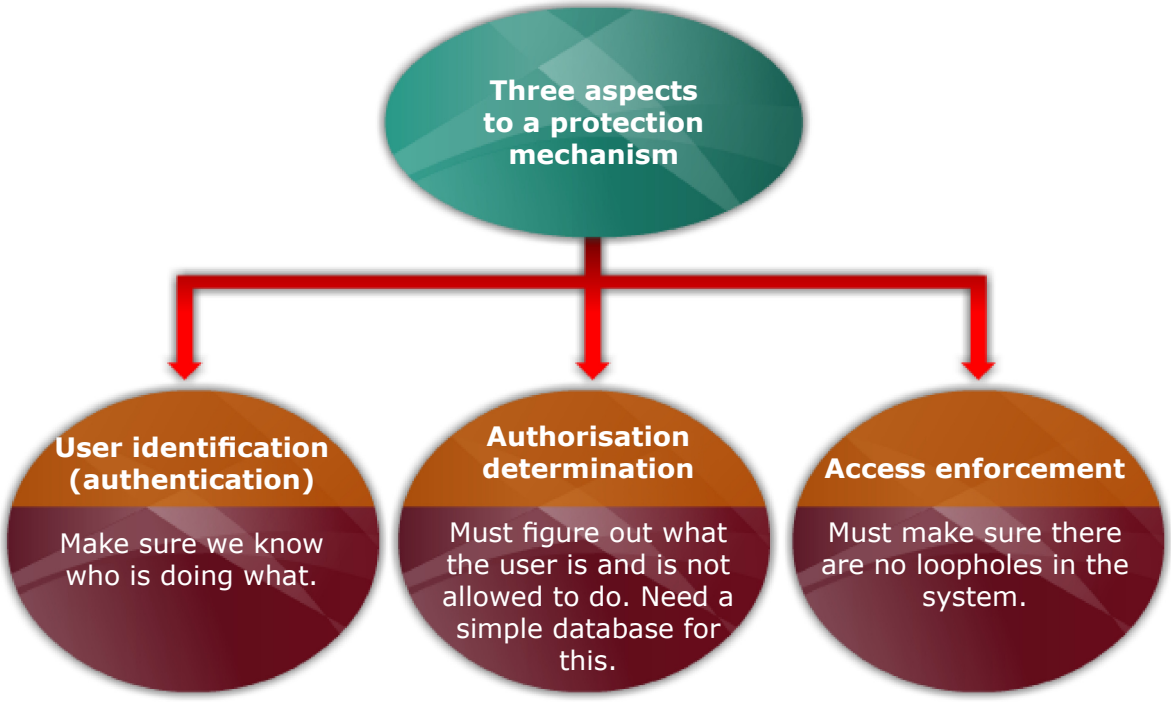


Figure 4.6: The three aspects to a protection mechanism

Even the slightest flaw in any of these areas may ruin the whole protection mechanism.

4.2.2 LAN Security

There are a few network security controls that can be implemented in order to protect from threats and vulnerabilities.

4.2.2.1 Encryption

Encryption techniques are used to safeguard information while it is stored within a network node or while it is in transit across communications media between nodes. Protection within a node is generally the less demanding of the two applications because the confined nature of the node facilitates physical protective measures. For transmission between nodes, there is generally substantial opportunity for data interception, so encryption techniques that provide security in the communications environment are very important to network security.

Encryption is a very powerful tool for providing privacy, authenticity, integrity and limited access to data. In network applications, encryption can be applied either between

two hosts or between two applications. Key distribution is always a problem with encryption. Encryption keys must be delivered to the sender and receiver in a secure manner.

(a) **Link Encryption**

In link encryption data is encrypted just before it is placed on the physical communications link. In this case, encryption occurs at layer 1 or 2 in the OSI model. Decryption occurs just as the communication enters the receiving computer. A model of link encryption is shown in Figure 4.7.

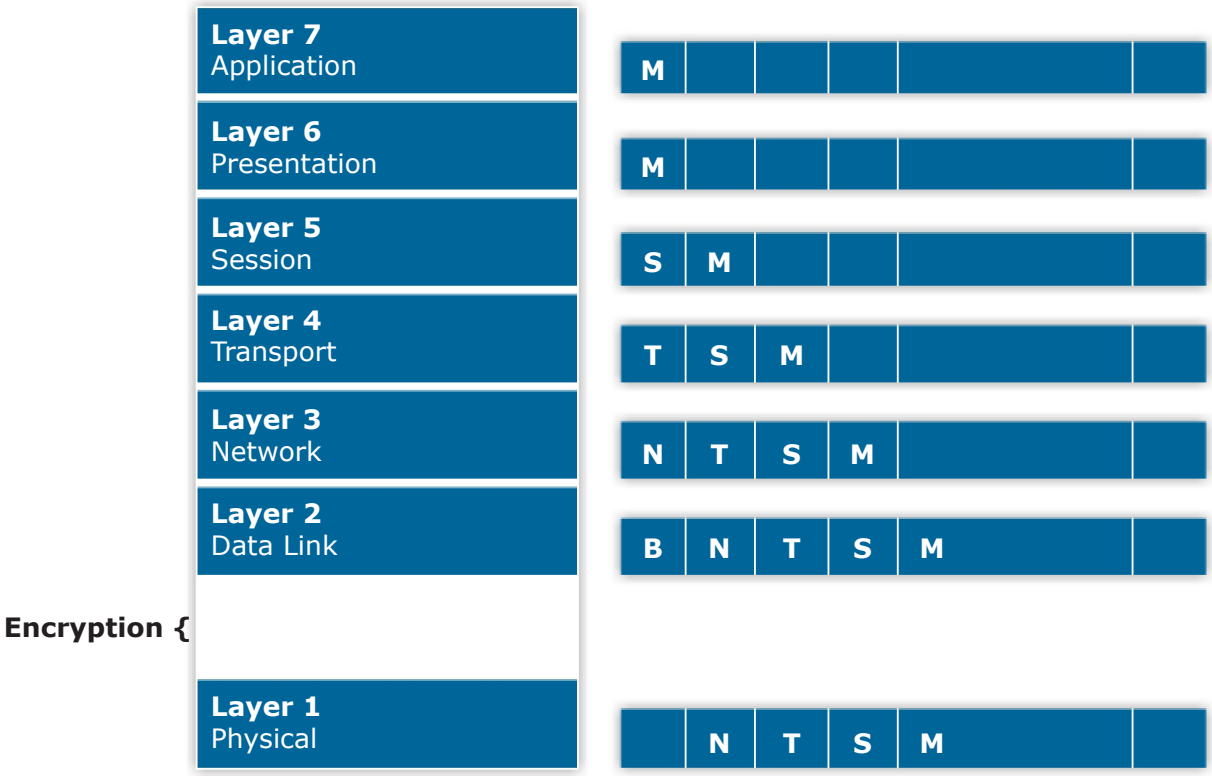


Figure 4.7: Model of link encryption

Encryption is used to convert a message (plaintext or clear text) into a "cryptogram" or ciphertext or a cipher. An encryption key is almost always used in encryption process in order to allow changes in the process and/or to allow secrecy, even if adversaries know the encryption algorithm. An algorithm for encryption and decryption is called a "cryptosystem". Encryption protects the message as it is in transit between two computers, but the message is in plaintext inside the hosts. Link encryption is especially vulnerable when a communication must pass through one or more additional hosts between sender and receiver as shown in Figure 4.8.

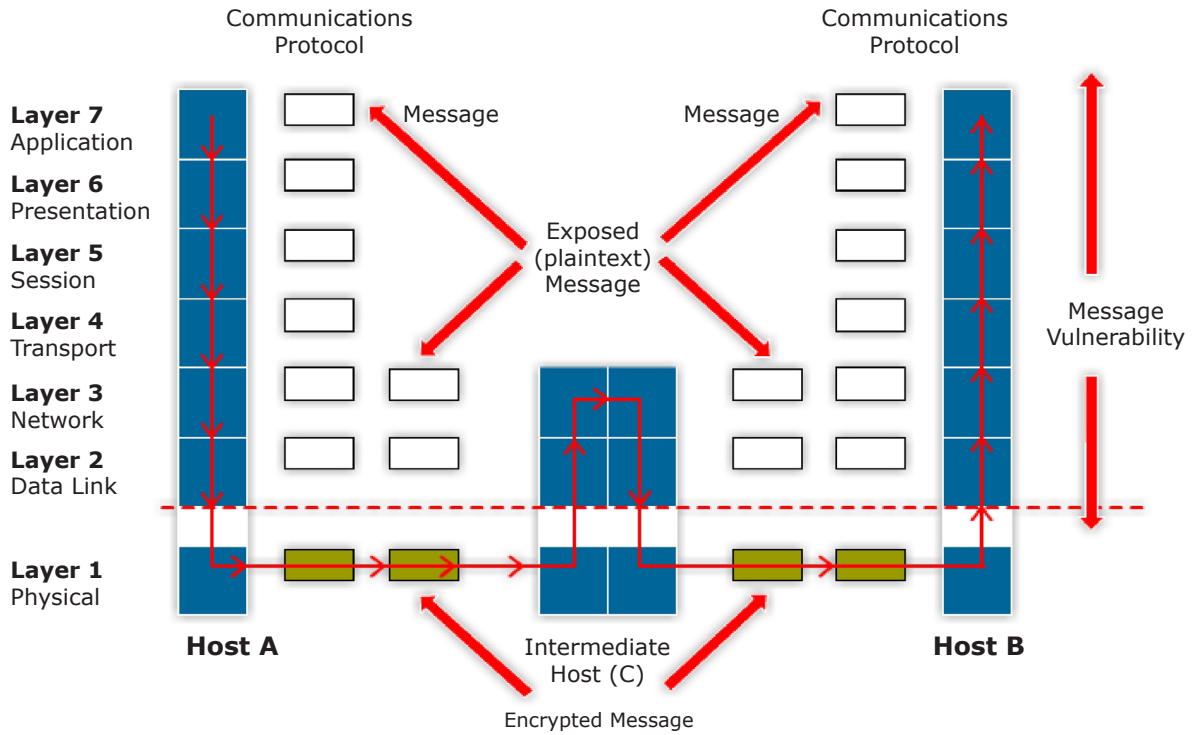


Figure 4.8: Link encryption with intermediate host

For example, there is no direct link between host A and B of Figure 4.8, but there is a link between A and C, and one between C and B. A message may be adequately protected by hosts A and B, and encryption protects the message along the links. However, the message is in the clear in host C, and that host may not be especially trustworthy. If node C is compromised, all messages passing through C are exposed.

Link encryption is invisible to the user. Encryption becomes a transmission service performed by a low-level network protocol layer, just like message routing or transmission error detection. A typical link encrypted message is shown in Figure 4.9.

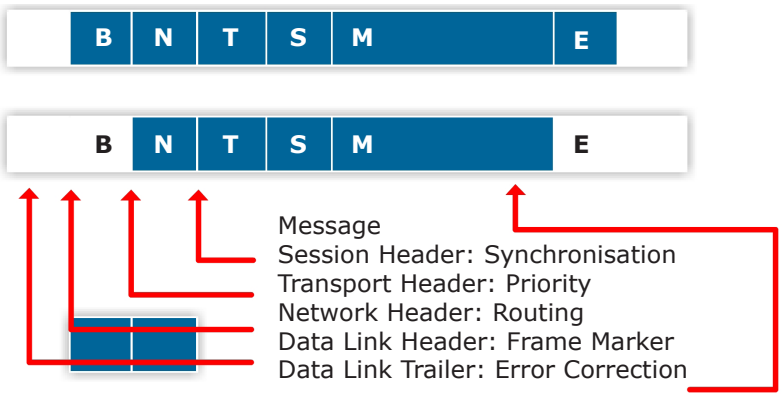


Figure 4.9: Messages under link encryption

There are devices that perform encryption quickly and reliably as a hardware function. In this case, link encryption is invisible to the operating system and the operator, too. Link encryption is an easy control to use if all hosts on a network are reasonably secure but the communications medium is shared with other users or is not secure. It is because link encryption is especially appropriate where the transmission line is the point of greatest vulnerability.

(b) **End-to-End Encryption**

End-to-end encryption provides security from one end of a transmission through the other. A hardware device between the user and the host can apply the encryption.

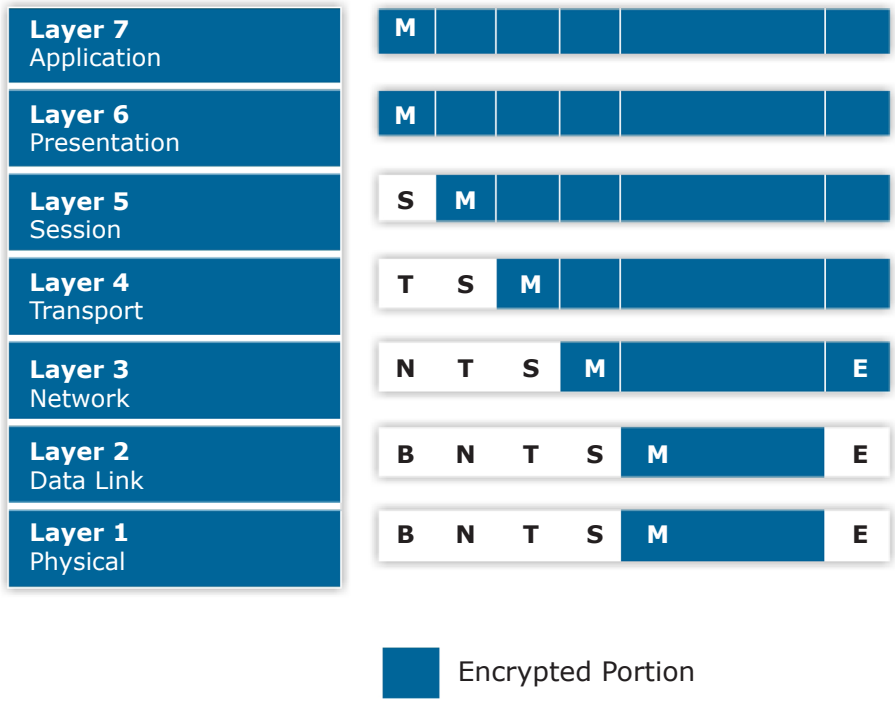


Figure 4.10: Model of end-to-end encryption

The encryption also can be done by software running on the host computer. In either case, the encryption is performed at the highest levels, either at layer 7 or layer 6 of the OSI model. Figure 4.10 shows a model of end-to-end encryption. The message is transmitted in encrypted form throughout the network since the encryption precedes all routing and transmission processing of the layer. So, the encryption covers potential flaws in lower layers in the transfer model.

Figure 4.11 shows a typical message using end to end encryption.

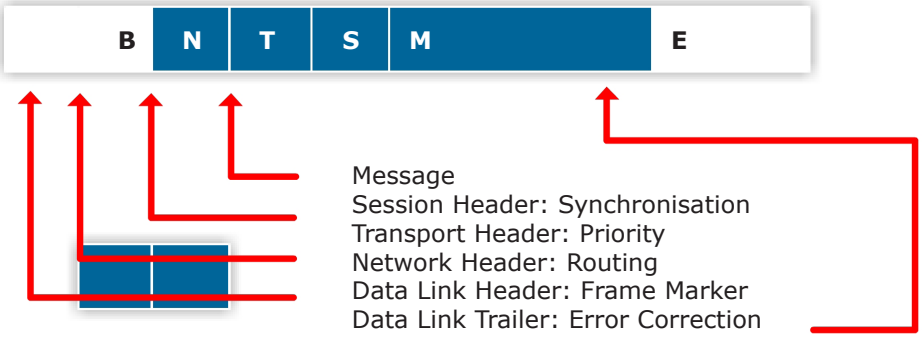


Figure 4.11: End-to-end encrypted message

Messages sent through several hosts are protected. The data content of the message is still encrypted as shown in Figure 4.12. Therefore, even though a message must pass through insecure node C on the path between A and B, the message is encrypted while in C.

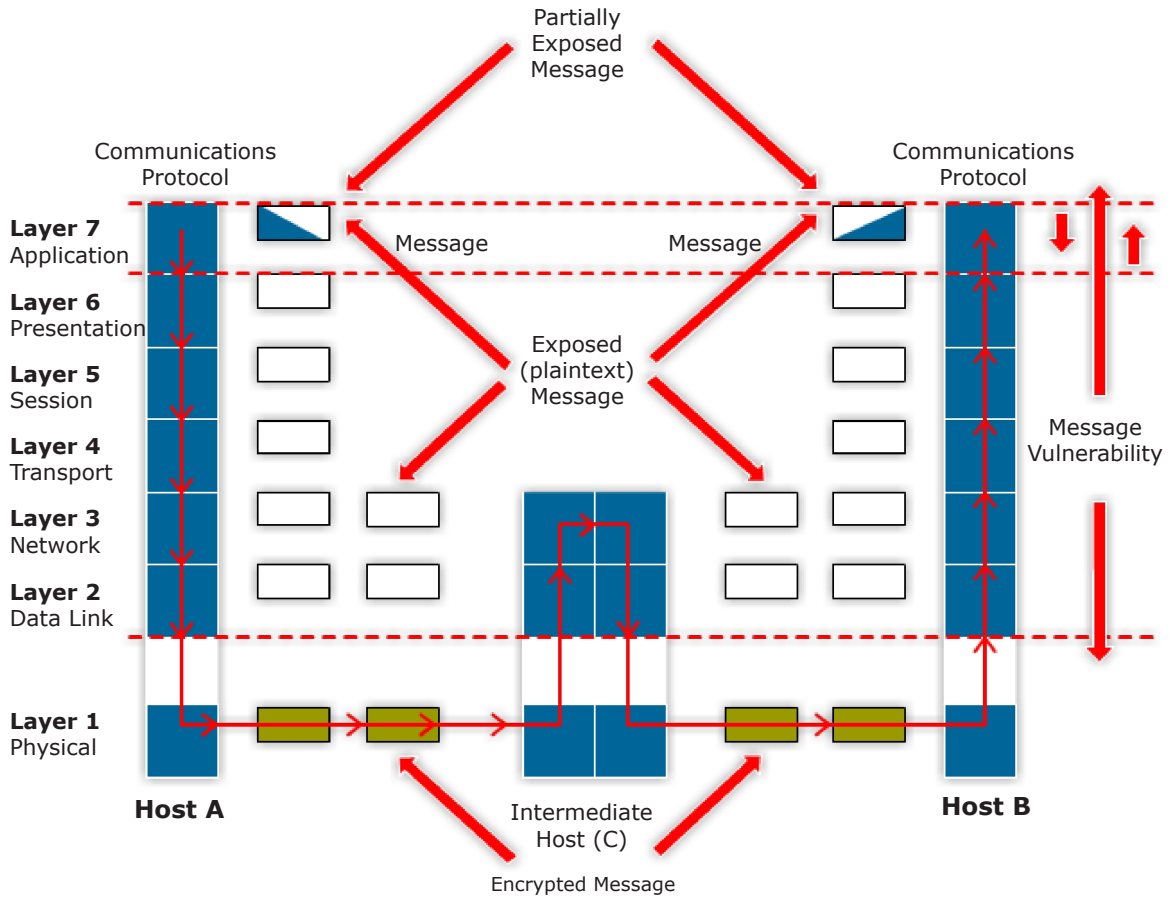


Figure 4.12: End-to-end encryption with intermediate host

(c) Comparison of Encryption Method

In many instances, however, the strength of encryption is adequate protection, considering the likelihood of the interceptor's breaking the encryption and the timeliness of the message. Table 4.3 shows the comparison between Link Encryption and End-to-End Encryption.

Table 4.3: Comparison between Link Encryption and End-to-End Encryption

Link Encryption	End-to-End Encryption
Security Within Hosts	
• Message exposed in sending host. • Message exposed in intermediate nodes.	• Message encrypted in sending host. • Message encrypted in intermediate nodes.
Role of User	
• Applied by sending host. • Invisible to user. • Host maintains encryption. • One facility for all users. • Can be done in hardware. • All or no messages encrypted.	• Applied by sending process. • User applies encryption. • User must find algorithm. • User selects encryption. • Software implementation. • User chooses to encrypt or not, for each message.
Implementation Concerns	
• Requires one key per host pair. • Provides node authentication.	• Requires one key per user pair. • Provides user authentication.

4.2.2.2 Access Control

Although encryption is especially good for protecting data within a network, access to data, programs and other resources of the network is also a serious concern in network security. Thus, in a network environment, access control must protect each single system of the network and also avoid allowing unauthorised users to pass through one system of a network to access other systems.

The goal of access control is to protect against unauthorised access to any resource. The term unauthorised access includes unauthorised use, unauthorised disclosure, unauthorised modification, unauthorised destruction and unauthorised issuing of commands. Access control is a means for enforcing authorisation. Two aspects of network access that can be considered are shown in Figure 4.13.

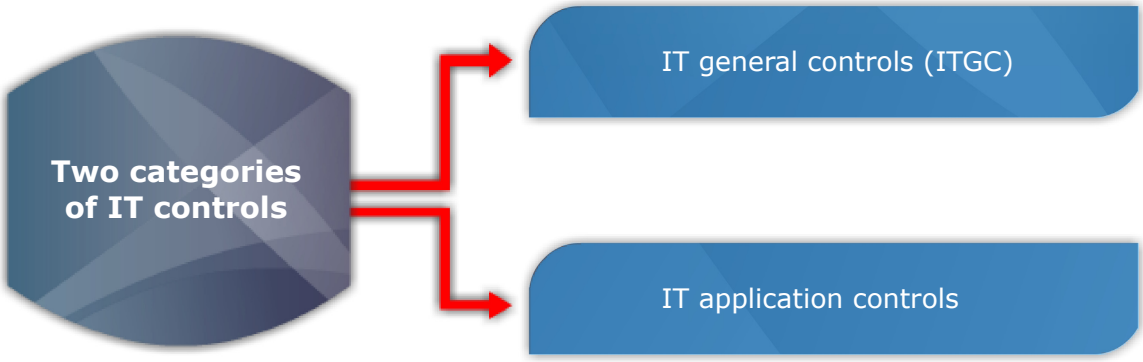


Figure 4.13: Two aspects of network access

(a) **Port Protection**

Dial-in port access is a serious vulnerability to a network system. User authentication is difficult enough in a single computing system, but it becomes far more difficult when users can dial in from a telephone; literally anywhere in the world (telephones are now available even in airplanes). Port protection is accomplished by several administrative and hardware techniques.

(b) **Automatic Call-Back**

An authorised user dials a computer system with an automatic call back system. After the user identifies him - or her, the computer breaks the communication line, effectively hanging up on the user. The computer then consults an internal table of telephone numbers and calls the user back at the predetermined number.

For example, if a person needed to access a computer from a terminal to his house, his home telephone number would be recorded on the list. This scheme works for people who expect to be at one number. If a person might be at more than one location, he could list all the telephone numbers with the computer as legitimate locations. When he dials, he identifies himself and gives the telephone number at which he expects to be called back. If the number he gives is one of the registered for him, the computer calls him back there and if not one of the registered, the computer issues a warning to the security officer.

(c) **Differentiated Access Rights**

Differentiated access rights can be useful for people such as representatives who travel to many locations. Limiting the points from which access is allowed can protect sensitive data. Sensitive accesses must be made when there is more difficult to compromise data or where it would be more noticeable if one were being forced to reveal the data.

On a network, users will access to sensitive objects can do so only by direct connection, not through another network host. This restriction reduces the threat of malicious hosts in a network.

(d) **Node Authentication**

A network node must be able to convince other nodes that is it authentic. It is not node of an impersonator masquerading as another node. Encryption is used to verify the identity of nodes. There is a possible exposure for an intruder could wait until node B had been accepted by node A even after authentication and also the intruder could tap the link between A and B and insert similar messages, which A would presume came from B.

(e) **User Authentication**

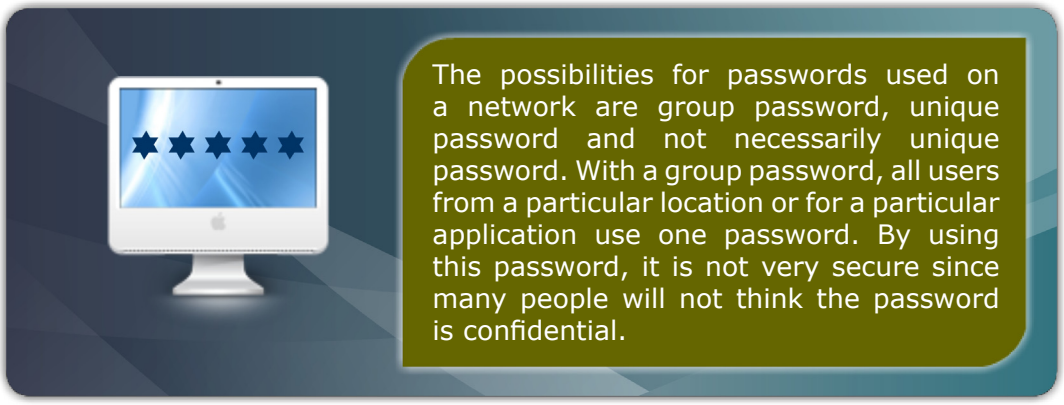
Authentication depends on two factors, which are some piece of secret, unforgettable data and a protocol for reliable transmission of that data. Although some password systems provide very little security, but there are some passwords systems that coupled with some form of encryption can enhance security dramatically.

Authentication mechanisms are divided into three categories:

- What you know, such as a password or an encryption key.
- What you posses, such as a token or a capability.
- Something about you, such as a picture or a fingerprint.

(f) **Password**

Passwords can offer reasonable security but choose a good password is the main point in security by using password. Refer to Chapter 2 to know how to choose a good password and the characteristics of that password.



In a unique password situation, each password is distinct from that of every other user. It means that no two system users have the same password. Therefore, one password establishes the user's identity and authenticates the user as well. Not necessarily unique password system commonly allowed each user chooses a password, but it is not required to be unique. Thus, two users may choose the same password and neither knows that someone else has the same password. This password can only be used for authentication but not for identification.

(g) Challenge-response System

Challenge-response systems are a technique where two machines can be effect of one-time passwords. They are essentially cryptosystems in which the host sends a message M and user replies with E(M). Both the message M and its encryption E(M) may be obtained but this loss will not reveal the encryption algorithm. The system presents a challenge to the user and judges the authenticity of the user by user's response. Figure 4.14 shows the process of challenge-response system.

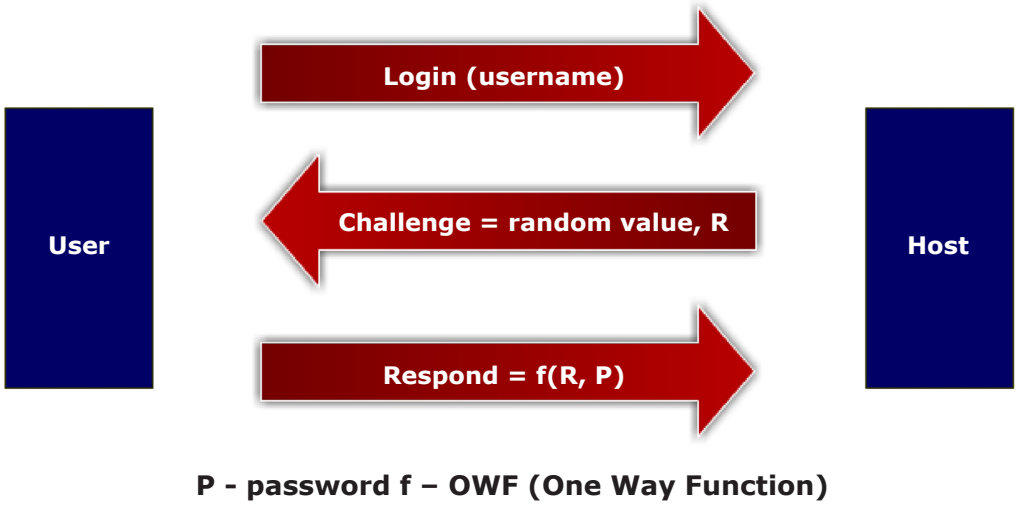


Figure 4.14: Challenge-response system process

As with regular cryptosystems, challenge-response systems are subject to two weaknesses, which are as following:

Even with several messages in plaintext and ciphertext, the encryption may still secure. However, the more plaintext or ciphertext becomes available about the encryption system, the more likely an interceptor is to be able to break the system.

With encryption systems is the possibility of replay of an old message. An unoriginal login program could masquerade as a system in order to capture a user's password.

4.2.3 Firewalls Security

Firewall is a process that filters all traffic between a protected or "inside" network and a less trustworthy or "outside" network. The purpose of firewall is to keep "bad" things outside a protected environment. Firewalls implement a security policy, which might be to prevent any access from outside. Alternatively, it might be to permit accesses only for certain users, or for certain activities.

4.2.3.1 Firewall Characteristics

Following are the lists of design goals for a firewall (see Figure 4.15).

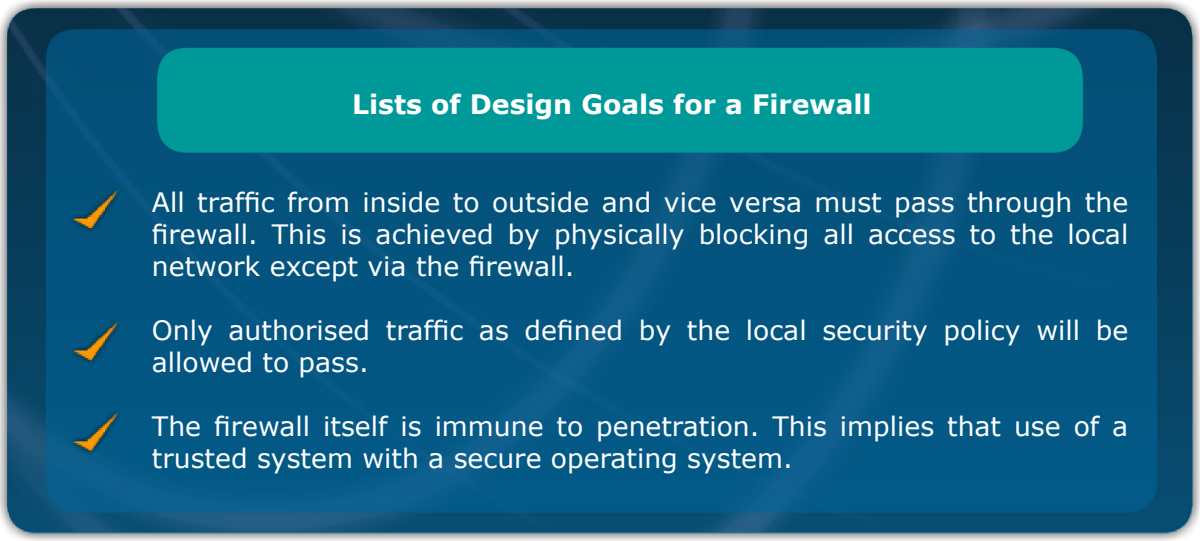


Figure 4.15: The lists of design goals for a firewall

The following Figure 4.16 shows the capabilities that are within the scope of a firewall (what one can expect from a firewall).

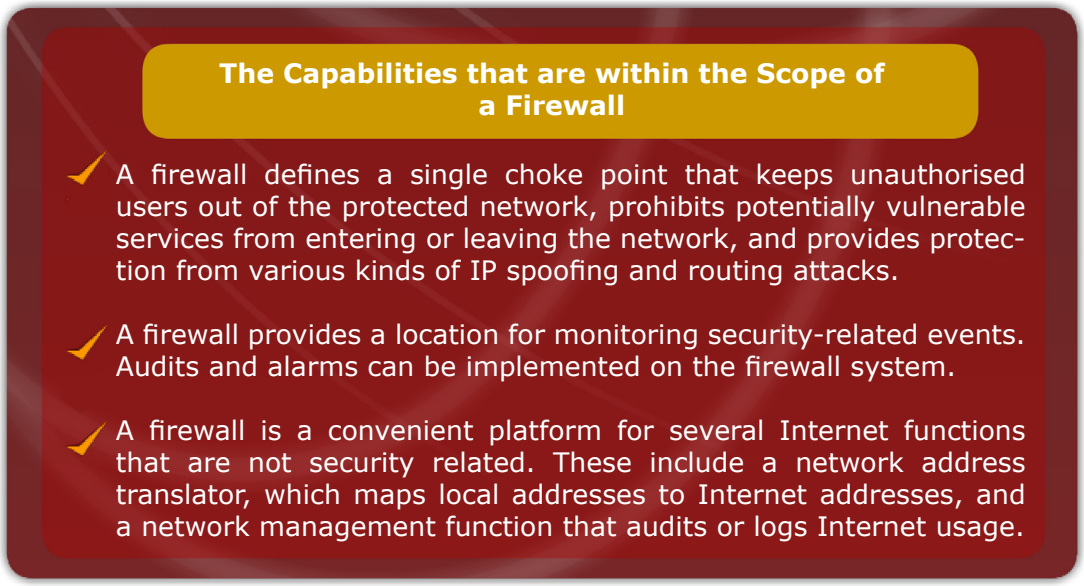


Figure 4.16: The capabilities that are within the scope of a firewall

Firewalls have their limitations, including the following where the firewall:

- Cannot protect against attacks that bypass the firewall.
- Does not protect against internal threats, such as a disgruntled employee or an employee who unwitting cooperates with an external attacker.
- Cannot protect against the transfer of virus-infected programs or files.

4.2.3.2 Types of Firewall

The term firewall is used rather loosely. Figure 4.17 displays three different things that are known as firewalls:

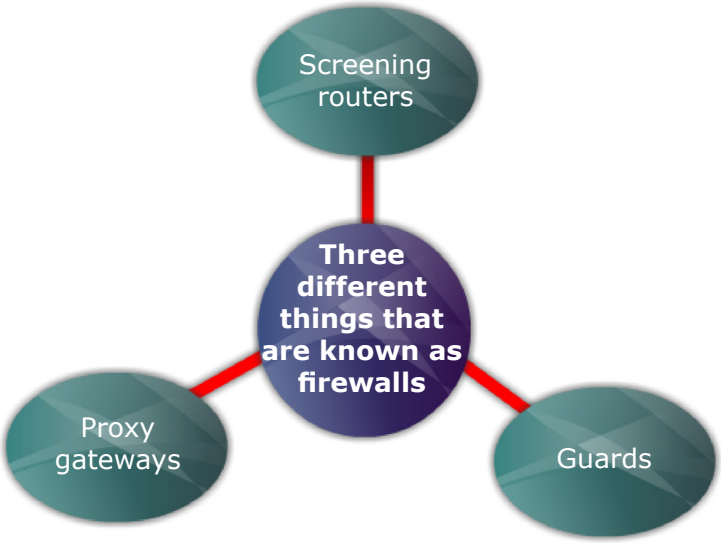


Figure 4.17: The three different things that are known as firewalls

From Figure 4.17, we will look into each of the category mentioned below.

(a) **Screening routers**

- A screening router is the simplest and in some situations, the most effective type of firewall.
- Screening routers can perform the very important service of ensuring the validity of inside addresses.
- A screening router might be configured to block all packets from the outside that claimed their source address was an inside address.
- A screening router can also control traffic by application.

(b) **Proxy gateways**

- A proxy gateway or also called a bastian host is a firewall that simulates the effects of an application. So that, the application will receive only requests to act properly.
- A proxy gateway is a two-headed piece of software: to the inside it looks as if it is the outside (destination) connection, while to the outside it responds just as the inside would.
- A proxy gateway runs pseudo-applications.
- A proxy gateway is a system identified by the firewall administrator as a critical strong point in the network's security.

(c) **Guards**

- A guard is a sophisticated proxy firewall.
- It receives protocol data units, interprets them, and passes through the same or different protocol data units that achieve either the same result or a modified result.
- The guard decides what services to perform on the user's behalf based on its available knowledge.

4.2.3.3 Comparison of Firewall Types

The differences between these three types of firewalls are shown in Table 4.4.

Table 4.4: Comparison among Three Types of Firewalls

Screening Router	Proxy Gateway	Guard
• Simplest. • Sees only addresses and service protocol type. • Auditing difficult. • Screens based on connection rules. • Complex addressing rules can make configuration tricky.	• Somewhat complex. • Sees full text of communication. • Can audit activity. • Screens based on behavior of proxies. • Simple proxies can substitute for complex addressing rules.	• Somewhat complex. • Sees full text of communication. • Can audit activity. • Screens based on behavior of proxies. • Simple proxies can substitute for complex addressing rules.

4.2.4 Antivirus Technology

The top computer threats are viruses and worms. Both these types of viral malware replicate themselves and can rapidly spread unless there is good anti-virus protection. For this reason, traditional anti-virus tools are fundamental to enterprise threat defense.

Good anti-virus applications must be able to protect computers against all types of viral threats and also be able to rapidly respond to new and emerging viral malware.

An effective anti-virus application must have a reliable scanning engine that can remove viral threats rapidly. There are several internationally recognised anti-virus certifications that can be used to verify the effectiveness of anti-virus software. Anti-virus applications must be regularly updated when new virus signatures are developed. Administrators can configure and manage anti-virus clients from a central location by using policies. Policies are an important tool that should be used, together with other simple deployment tools, so that anti-virus protection can be deployed automatically to clients across the network. Your defensive strategy will have the following components (see Figure 4.18).

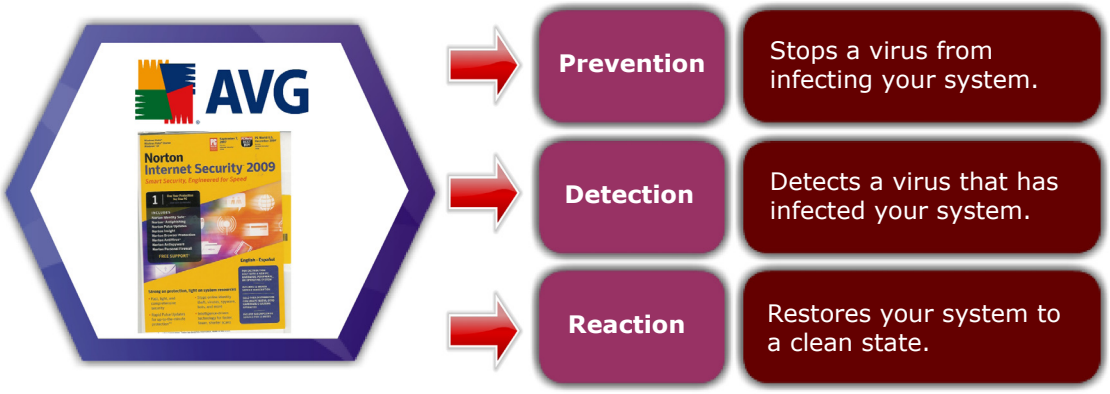


Figure 4.18: Defensive strategy that consists of the following components

Effective anti-virus applications should include the following components:

- **Reliable and comprehensive scanning engine**
  It is essential that anti-virus applications are able to remove viral threats rapidly and effectively. To help assess the effectiveness of anti-virus products, there are several internationally recognised detection and removal certifications. ICSA Labs issues certifications for anti-virus products that can detect and clean 100% of "in-the-wild" viruses.

  West Coast Labs certifications include specific Checkmarks for different types of malware detection and removal, such as Anti-Virus Level 1, Anti-Virus Level 2 and Trojan. Virus Bulletin has the "100% Award" for anti-virus products that remove all viruses during test. You can also carry out your own tests; for example, the European Expert Group for IT-Security, also known as Eicar, provides a downloadable anti-malware test file that you can use to test anti-virus software.

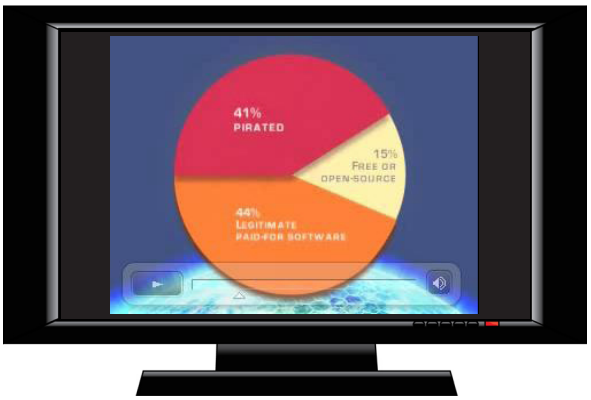
- **Regular signature and software updates**
  All anti-virus applications must be able to be updated quickly when new virus signatures are developed. Signature updates must be packaged so that updates can be rapidly deployed across all computers in an enterprise. The anti-virus software itself must also be able to be updated to meet new types of viral threats.

- **Policy-based management policies**
  It is an important tool that administrators can use to configure and manage anti-virus clients from a central location. Policies can be used to schedule updates and virus scans, manage alerts and set the level of protection required. The ability to use policy-based management is important for most enterprises, because all users and computers do not require the same settings for anti-virus protection.

- **Simple deployment tools**
  If multiple computers are installed across several physical locations, it is important to be able to rapidly deploy anti-virus protection by using automated methods.

It must also be simple to deploy software updates across the network and to identify any computers that have not been updated.

4.3 PIRACY AND ANTI-PIRACY TECHNIQUES



Source: http://www.youtube.com/watch?v=wNvDYXPWcsQ

Based from the video, define and provide an example of piracy in the world today.

4.3.1 What is Piracy?

Compared to literature, music and movies, computer software is a relatively new form of intellectual property. Nevertheless, software is protected under the very same laws that govern music, literature, movies and other copyrighted content. All software comes with a license agreement that specifically states the terms and conditions under which the software may be legally used.

Licenses vary from program to program and may authorise as few as one computer or individual to use the software or as many as several hundred network users to share the application across the system. It is important to read and understand the license accompanying the application to ensure that we have enough legal copies of the software for our organisation's needs. Making additional copies, or loading the software onto more than one machine, may violate copyright law and be considered piracy.

Use the internet do a research on piracy. Your research should include the effect on piracy to the economy and organisation. Provide an example based on your research. Share your findings in the LMS Forum.

4.3.2 Risks of Piracy

The losses suffered through software piracy directly affect the profitability of the software industry. Because of the money lost to pirates, publishers have fewer resources to devote to research and development of new products, have less revenue to justify lowering software prices and are forced to pass these costs on to their customers. Consequently, software publishers, developers, and vendors are taking serious actions to protect their revenues.

Using pirated software is also risky for users. Aside from the legal consequences of using pirated software, your organisation forfeits some practical benefits as well. Those who uses pirates software (see Figure 4.19).

- Increase the chances that the software will not function correctly or will fail completely;
- Forfeit access to customer support, upgrades, technical documentation, training, and bug fixes;
- Have no warranty to protect themselves;
- Increase their risk of exposure to a debilitating virus that can destroy valuable data;
- May find that the software is actually an outdated version, a beta (test) version, or a nonfunctional copy;
- Are subject to significant fines for copyright infringement; and
- Risk potential negative publicity and public and private embarrassment.

Figure 4.19: The effects of using pirated software

4.3.3 Types of Piracy

Many computer users have found themselves caught in the piracy trap, unaware they were doing anything illegal. To avoid such unpleasant surprises, it may be helpful to know the ten basic ways one can intentionally or unintentionally pirate software. It can be end-user piracy, reseller piracy or Bulletin board system piracy. There are ten types of piracy, which are shown in Figure 4.20, followed by description on each of the types.

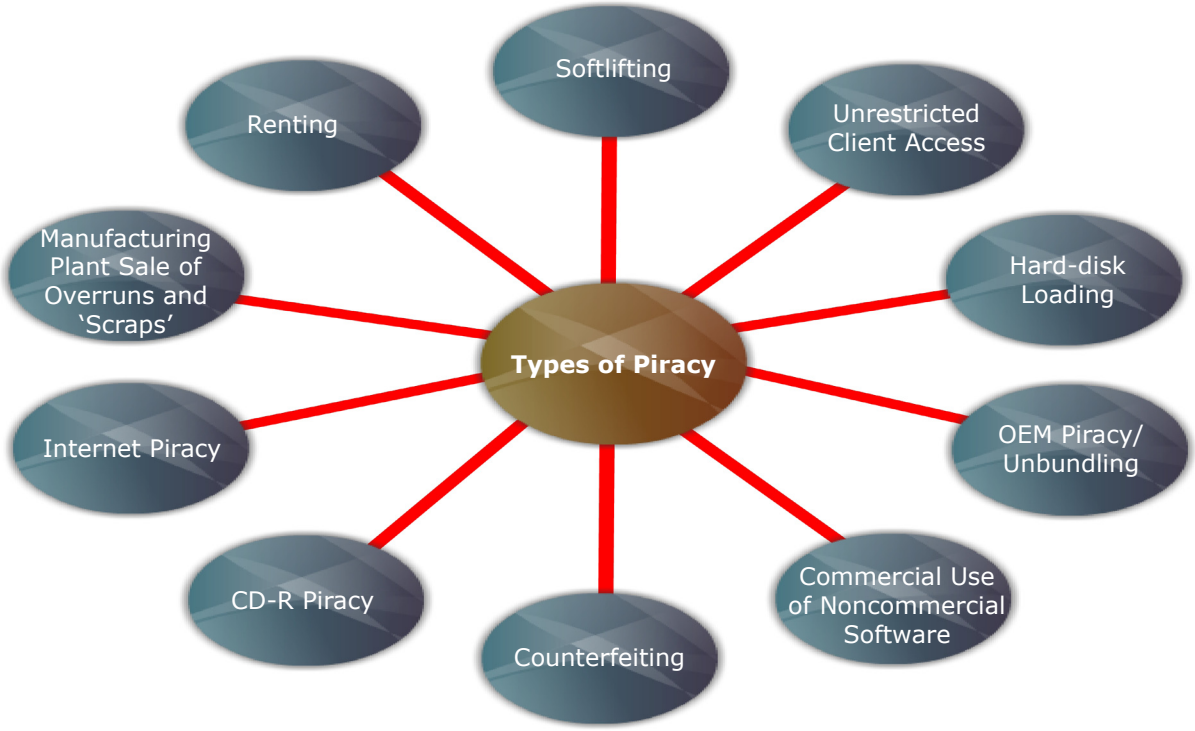


Figure 4.20: Types of piracy

1. Softlifting

Softlifting occurs when a person purchases a single licensed copy of a software program and loads it on several machines, in violation of the terms of the license agreement. Typical examples of softlifting include, "sharing" software with friends and co-workers and installing software on home/laptop computers if not allowed to do so by the license. In the corporate environment, softlifting is the most prevalent type of software piracy and perhaps, the easiest to catch.

2. Unrestricted Client Access

Unrestricted client access piracy occurs when a copy of a software program is copied onto an organisation's servers and the organisation's network "clients" are allowed to freely

access the software in violation of the terms of the license agreement. This is a violation when the organisation has a "single instance" license that permits installation of the software onto a single computer, rather than a client-server license that allows concurrent server-based network access to the software.

A violation also occurs when the organisation has a client-server license, the organisation is not enforcing user restrictions outlined in the lciense. For instance, when the license places a restriction on the number of concurrent users that are allowed access to that program and the organisation is not enforcing that number. Unrestricted client access piracy is similar to softlifting, in that it results in more employees having access to a particular program than is permitted under the license for that software. Unlike softlifting though, unrestricted client access piracy occurs when the software is loaded onto a company's server (not on individual machines) and clients are permitted to access the server-based software application through the organisation's network.

3. Hard-disk Loading

Hard-disk loading occurs when an individual or company sells computers preloaded with illegal copies of software. Often this is done by the vendor as an incentive to buy certain hardware. If you buy or rent computers with preloaded software, your purchase documentation and contract with the vendor must specify which software is preloaded and that these are legal, licensed copies. If it does not and the vendor is unwilling to supply you with the proper documentation, do not deal with that vendor.

4. OEM Piracy/Unbundling

Some software, known as OEM (original equipment manufacturer) software, is only legally sold with specified hardware. When these programs are copied and sold separately from the hardware, this is a violation of the distribution contract between the vendor and the software publisher. Similarly, the term "unbundling" refers to the act of selling software separately that is legally sold only when bundled with another package. Software programs that are marked "not for resale" are often bundled applications.

5. Commercial Use of Noncommercial Software

Using educational or other commercial-use-restricted software in violation of the software license is a form of software piracy. Software companies will often market special non-commercial software aimed at a particular audience. For example, many software companies sell educational versions of their software to public schools, universities and other educational institutions. The price of this software is often greatly reduced by the publisher in recognition of the educational nature of the institutions. Acquiring and using noncommercial software hurts not only the software publisher, but also the institution that was the intended recipient of the software.

6. Counterfeiting

Counterfeiting is the duplication and sale of unauthorised copies of software in such a manner as to try to pass off the illegal copy as if it were a legitimate copy produced or authorised by the legal publisher. Much of the software offered for bargain sale at non-trade computer shows is counterfeit software. SIIA estimates that at least 50% of the software sales that take place at computer shows throughout the United States involve counterfeit software.

7. CD-R Piracy

CD-R piracy is the illegal copying of software using CD-R recording technology. This form of piracy occurs when a person obtains a copy of a software program and makes a copy or copies and re-distributes them to friends or for re-sale. Although there is some overlap between CD-R piracy and counterfeiting, with CD-R piracy there may be no attempt to try to pass off the illegal copy as a legitimate copy - it may have hand-written labels and no documentation at all.

With CD recording equipment becoming relatively inexpensive, the software industry is being plagued by this new form of end-user piracy. Just a few years ago, so-called "compilation CDs" (illegal CD-ROMs containing many different software applications) were selling for $400-$500. With CD-R's becoming more available, the price has dropped to $20 and this making illegal software available to a greater number of people.

8. Internet Piracy

Internet piracy is the uploading of commercial software (i.e., software that is not freeware or public domain) on to the Internet for anyone to copy or copying commercial software from any of these services. Internet piracy also includes making available or offering for sale pirated software over the Internet.

Examples of this include the offering of software through an auction site, IM, IRC or a warez site. Incidences of Internet piracy have risen exponentially over the last few years. Internet piracy is discussed in greater detail below.

9. Manufacturing Plant Sale of Overruns and 'Scraps'

Software publishers routinely authorise CD manufacturing plants to produce copies of their software onto CD-ROM so that they can distribute these CD-ROMs to their authorised vendors for resale to the public. Plant piracy occurs when the plant produces more copies of the software than it was authorised to make, and then resells these unauthorised overruns. Piracy also occurs when the plant is ordered by the publisher

to destroy any CDs not distributed to its vendors, but the plant, in violation of these orders, resells those CDs that were intended to be scrapped. While most plants appear to be compliant, and there are compliance procedures in place, there have been several instances of these forms of piracy.

10. Renting

Renting software for temporary use, like you would a movie, was made illegal in the United States by the Software Rental Amendments Act of 1990 and in Canada by a 1993 amendment to the Copyright Act. As a result, rental of software is rare.

The ten types of piracy identified above are not mutually exclusive. There is often overlap between one type of piracy and another. For instance, numerous instances of OEM counterfeiting has occurs when OEM software is unbundled in order to be re-sold, and not only does the pirate sell the OEM software, but he also makes numerous illegal copies of the OEM software and sells them as counterfeits.

4.3.4 What is Anti-Piracy

Anti-piracy is a term used by some to describe the attempt to prevent copyright infringement, counterfeiting, and other violations of intellectual-property rights. It is a combined efforts of corporate associations, law enforcement agencies, and various world governments to combat copyright infringement relating to various types of creative works, such as software, music and films. These measures often come in the form of copy protection measures such as DRM (Digital Right Management).

4.3.4.1 Anti-Piracy Techniques

Some of the techniques that come together with the software are dongles, software keys, watermarks, encryption and Digital Right Management. Refer to Figure 4.21 for the illustration and description of each of the anti-piracy techniques.

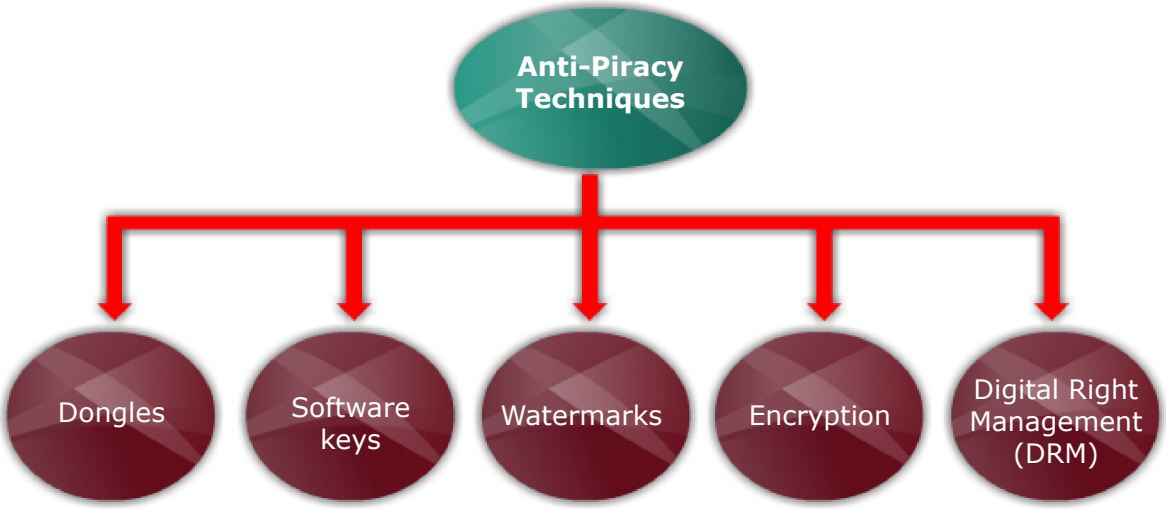
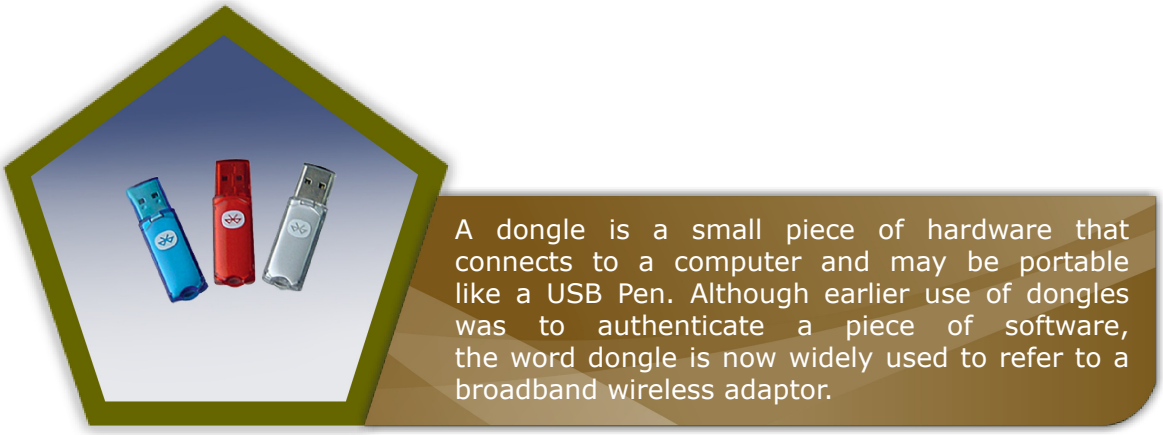


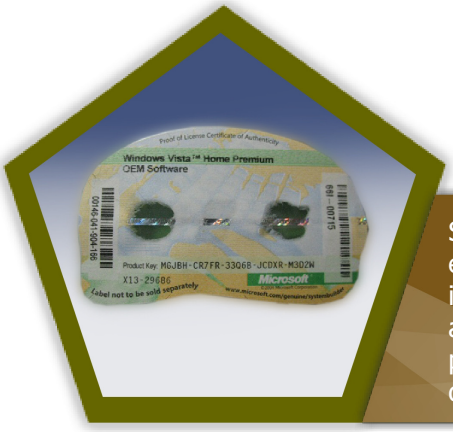
Figure 4.21: Anti-piracy techniques

(a) **Dongles**



Electrically the authentication dongles mostly appear as two-interface security tokens with transient data flow that does not interfere with other dongle functions and a pull communication that reads security data from the dongle. Without the dongle, the software will run only in a restricted mode, or not at all. Dongles are used by some proprietary vendors as a form of copy protection or digital rights management, because it is much harder to copy a dongle than to copy the software it authenticates. Despite being hardware, however, dongles are not a complete solution to the trusted client problem.

(b) **Software keys**



Software keys are used to secure data and equipment. It is generally a string of numbers that is used for identification purposes. It is either to allow access to the use of the equipment or to permit authorised printing, processing or copying data.

(c) **Watermarks**

Digital watermarks are unobtrusive features of media that are added during production or distribution. Digital watermarks involve data that is arguably steganographically embedded within the audio or video data.

Watermarks can be used for different purposes that may include:

- For recording the copyright owner;
- For recording the distributor;
- For recording the distribution chain; and
- For identifying the purchaser of the music.

Watermarks are not complete DRM mechanisms in their own right, but are used as part of a system for Digital Rights Management, such as helping provide prosecution evidence for purely legal avenues of rights management, rather than direct technological restriction. Some programs used to edit video and/or audio may distort, delete, or otherwise interfere with watermarks. Signal/modulator-carrier chromatography may also separate watermarks from original audio or detect them as glitches. Use of third party media players and other advanced programs render watermarking useless.

Additionally, comparison of two separately obtained copies of audio using simple,

home-grown algorithms can often reveal watermarks. New methods of detection are currently under investigation by both industry and non-industry researchers.

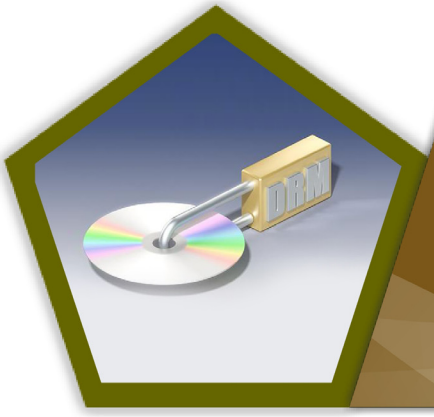
(d) **Encryption**

Encryption has long been used by militaries and governments to facilitate secret communication. Encryption is now commonly used in protecting information within many kinds of civilian systems.

For example, in 2007 the U.S. government reported that 71% of companies surveyed utilised encryption for some of their data in transit. Encryption can be used to protect data "at rest", such as files on computers and storage devices (e.g. USB flash drives). In recent years there have been numerous reports of confidential data such as customers' personal records being exposed through loss or theft of laptops or backup drives.

Encrypting such files at rest helps protect them should physical security measures fail. Digital rights management systems which prevent unauthorised use or reproduction of copyrighted material and protect software against reverse engineering are another different example of using encryption on data at rest.

(e) **Digital Rights Management (DRM)**



Digital rights management technologies attempt to control use of digital media by preventing access, copying or conversion to other formats by end users. Long before the arrival of digital or even electronic media, copyright holders, content producers, or other financially or artistically interested parties had business and legal objections to copying technologies.

Examples include: player piano rolls early in the 20th century, audio tape recording, and video tape recording (e.g. the "Betamax case" in the U.S.). Copying technology thus

exemplifies a disruptive technology.

The advent of digital media and analog/digital conversion technologies, especially those that are usable on mass-market general-purpose personal computers, has vastly increased the concerns of copyright-dependent organisations, especially within the music and movie industries. While analog media inevitably loses quality with each copy generation, and in some cases even during normal use, digital media files may be duplicated an unlimited number of times with no degradation in the quality of subsequent copies.

The advent of personal computers as household appliances has made it convenient for consumers to convert media (which may or may not be copyrighted) originally in a physical/analog form or a broadcast form into a universal, digital form (this process is called ripping) for location or timeshifting. This, combined with the Internet and popular file sharing tools, has made unauthorised distribution of copies of copyrighted digital media (so-called digital piracy) much easier.

SUMMARY

1. Protecting infrastructure from disaster has always been important for industry, government and society. However, the reliability and security of information and communication systems against disasters, both natural and man-made, are in uncertainty.
2. In OS security, the basis of protection is separation which keeping one user's objects separate from other users. The separation can be physical separation, temporal separation, logical separation and cryptographic separation.
3. In LAN security, There are a few network security controls that can be implement in order to protect from threats and vulnerabilities which are encryption, access control and authentication in distributed environments.
4. In firewall security, there are three types of firewall which are screening routers, proxy gateway and guards.
5. Some of the anti-piracy techniques that come together with the software are dongles, software keys, watermarks, encryption and digital rights management.

GLOSSARY

Defense	A means or method of defending or protecting.
Information Infrastructure	The entirety of IT elements that are part of a given infrastructure.
IT	Information Technology
Technical	Having special skill or practical knowledge.

DISCUSSION QUESTION

1. Explain briefly the differences between Link Encryption and End-to-End Encryption. Which methods are more secure to use.
2. What is the security impact of the unknown perimeter of a network? Does it matter to user A if the network is also accessible to user B to user C through a network shared with B and to user D through a network shared with C?
3. Explain briefly the process of Kerberos system and how it can supports authentication in distributed system.

REFERENCES

Charles P. Pfleeger (2003). *Security in Computing*. New Jersey, United States: Prentice Hall.

Federal Ministry of the Interior (2005). *National Plan for Information Infrastructure Protection*. http://www.en.bmi.bund.de/...Information__Infrastructure__Protection.../ National_Plan_for_Information_Infrastructure_Protection.pdf.

Matt Bishop (2003). *Computer Security: Art and Science*. Addison-Wesley.

SIIA (2009). *What is software piracy: The Piracy Problem*. http://www.spa.org/piracy/whatis.asp

http://en.wikipedia.org/