Debre Tabor Univesity

Faculty of Technology

Department of Electrical and Computer Engineering

Module Name:-Computer Network Security

Target group 4th year Computer stream students

Prepared by;- Misganaw.A

Approved by:- ECE quality Assurance

Date:-21/06/09

Contents page

I Like a confidencial.....

I Like a confidencial....

I Like a confidencial....

Chapter one

1. Overview of networking

A system of interconnected computers and computerized peripherals such as printers to computer, computer to computer,mobile to computer is called computer network. This interconnection among computers facilitates information sharing among them. Computers may connect to each other by either wired or wireless media.

1.1. Classification of computer network

Computer networks are classified based on the following various factors.

- Geographical span
- Administration
- Inter-connectivity
- Architecture

1.1.1. Geographical span

Geographically a network can be seen in one of the following categories:

- Personal area network
- Local area network
- Wide area network
- Metropolitan network

1.1.2. Inter-connectivity

Components of a network can be connected to each other differently in some fashion. By connected we mean either logically, physically, or both ways. Such connectivity are:

- Point to point connection
- Star connection
- Hybrid connection
- Ring connection
- Bus connection
- Mesh connection

1.1.3. Administration

From an administrator's point of view, a network can be private network which belongs a single autonomous system and cannot be accessed outside its physical or logical domain. A network can be public, which is accessed by all.

I Like a confidencial....

1.1.4. Network architecture

- ✧ Computer networks can be discriminated into various types such as Client-Server,peer-to-peer or hybrid, depending upon its architecture.
- ✧ There can be one or more systems acting as Server. Other being Client, requests the Server to serve requests. Server takes and processes request on behalf of Clients.
- ✧ Two systems can be connected Point-to-Point, or in back-to-back fashion. They both reside at the same level and called peers.
- ✧ There can be hybrid network which involves network architecture of both the above types.

1.2. Network application

Computer systems and peripherals are connected to form a network. They provide numerous advantages:

- ❖ Resource sharing such as printers and storage devices
- ❖ Exchange of information by means of e-Mails and FTP
- ❖ Information sharing by using Web or Internet
- ❖ Interaction with other users using dynamic web pages
- ❖ IP phones
- ❖ Video conferences
- ❖ Parallel computing
- ❖ Instant messaging

1.3. Inter network

A network of networks is called an inter network, or simply the internet. It is the largest network in existence on this planet. Internet is widely deployed on World Wide Web services using HTML linked pages and is accessible by client software known as Web Browsers. Internet is serving many proposes and is involved in many aspects of life. Some of them are:

Web sites

- ❖ E-mail
- ❖ Instant Messaging
- ❖ Blogging

I Like a confidencial...

- Social Media
- Networking
- Audio and Video Streaming
- Marketing
- Resource Sharing

1.4. Network LAN technology

Some of the various LAN technologies are the following:

- Ethernet
- Giga Ethernet
- Fast Ethernet
- Virtual LAN

1.5. Computer network model

One of the most example of computer network model is called ***OSI model*** and ***Internet model.***

1.5.1. OSI Model

Open System Interconnect is an open standard for all communication systems. OSI model is established by International Standard Organization (ISO). This model has seven layers which includes:

- Physical layer
- Transport layer
- Application layer
- Data link layer
- Session layer
- Network layer
- Presentation layer

1.5.2. Internet model

This is also known as internet suit, which contains four main layers:

- Application layer
- Internet layer
- Transport layer
- Link layer

1.6. Network services

This network service are implemented on application layer which contains the following network service type:

- Directory service
- File service

Like a confidencial....

- ❖ Communication service
- ❖ Application service

What is data?

Any object that can be processed or executed by a computer

Two states of data

- ◆ transmission state
- ◆ storage state

Review questions

1. list and describe types of network according to geographical span?
2. list and describe types of network according to inter connectivity span?
3. Define OSI model and write the different b/n OSI model and Internet model?
4. List the seven network layer and write there function?
5. Write the difference b/n Ethernet, fast Ethernet and Giga-Ethernet?
6. Write a clear explanation about four types of network services?
7. Write two types of data transmission method with its clear definition?
8. Define what does that mean error detection and error detection?
9. Write different types of switching that we use in networking?
10. Write different types of communication protocols and there application?

I Like a confidencial....

Chapter two

2. Introduction to computer and network security

2.1. Security definitions

Some basic security definitions are:

- Freedom from risk or danger; safety.
- Freedom from doubt, anxiety, or fear; confidence.
- Something that gives or assures safety, as:

A. A group or department of private guards: Call building security if a visitor acts suspicious.

B. Measures adopted by a government to prevent espionage, sabotage, or attack.

C. Measures adopted, as by a business or homeowner, to prevent a crime such as burglary or assault: Security was lax at the firm's smaller plant….etc.

Network security entails protecting the usability, reliability, integrity, and safety of network and data. Effective network security defeats a variety of threats from entering or spreading on a network.

security means preventing unauthorized access, use, alteration, and theft or physical damage to these resources.

2.2. The need of security

- For Protect vital information while still allowing access to those who need it

E.g. for Trade secrets, medical records, etc.

- Provide authentication and access control for resources

E.g: AFS

For Guarantee availability of resources

E.g: 5 9's (99.999% reliability)

Who is vulnerable to security attack?

I Like a confidencial....

- ✧ Financial institutions and banks
- ✧ Internet service providers
- ✧ Pharmaceutical companies
- ✧ Government and defense agencies
- ✧ Contractors to various government agencies
- ✧ Multinational corporations
- ✧ ANYONE ON THE Network

What things should be secured?

✧ First of all, is to check the physical security by setting control systems like motion alarms, door accessing systems, humidity sensors, temperature sensors. All these components decrease the possibility of a computer to be stolen or damaged by humans and environment itself.

✧ People having access to computer systems should have their own user id with password protection.

✧ Monitors should be screen saver protected to hide the information from being displayed when the user is away or inactive.

✧ Secure your network especially wireless, passwords should be used.

✧ Internet equipment as routers to be protected with password.

✧ Data that you use to store information which can be financial, or non-financial by encryption.

✧ Information should be protected in all types of its representation in transmission by encrypting it.

2.3. Computer Security - Terminologies

In this chapter, we will discuss about the different terminology used in Computer Security.

Unauthorized access – An unauthorized access is when someone gains access to a server, website, or other sensitive data using someone else's account details.

Hacker – Is a Person who tries and exploits a computer system for a reason which can be money, a social cause, fun etc.

Threat – Is an action or event that might compromise the security.

[Like a confidencial...

Vulnerability – It is a weakness, a design problem or implementation error in a system that can lead to an unexpected and undesirable event regarding security system.

Attack – Is an assault on the system security that is delivered by a person or a machine to a system. It violates security.

Antivirus or Antimalware – Is a software that operates on different OS which is used to prevent from malicious software.

Social Engineering – Is a technique that a hacker uses to stole data by a person for different for purposes by psychological manipulation combined with social scenes.

Virus – It is a malicious software that installs on your computer without your consent for a bad purpose.

Firewall – It is a software or hardware which is used to filter network traffic based on rules.

2.4. Computer network security objectives

The three main computer security objectives are:

- Identification
- Authentication and
- Access control

A. **Identification:**–something which identifies the user using user id

B. **Authentication:**– the process of verifying the identity user based on password,key, smart card, disk, finger print retinal scan and voice

The authentication may be categorized as ***general access authentication and functional authentication.***

I Like a confidencial....

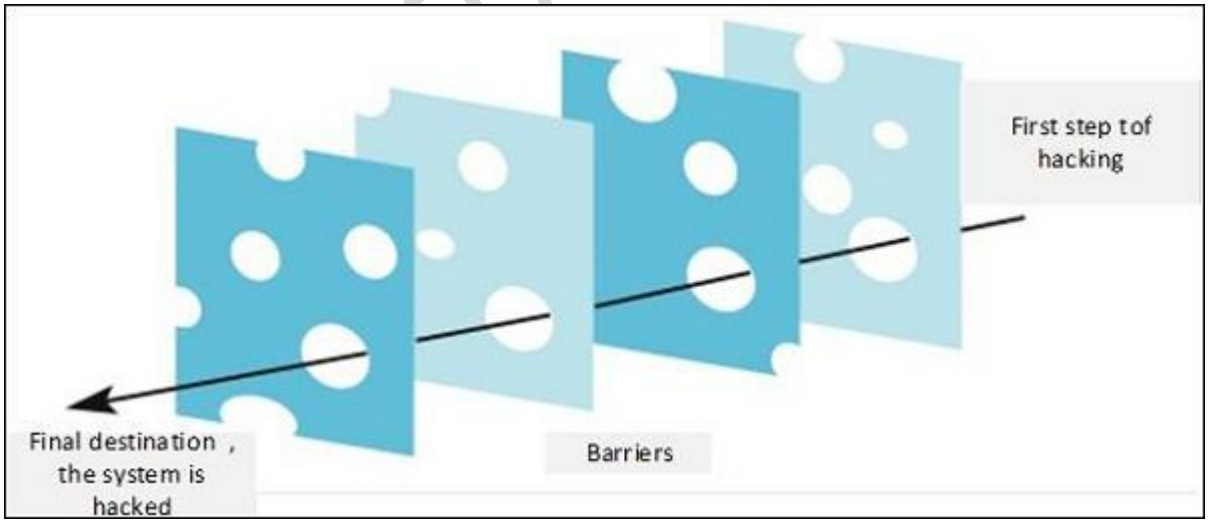
general access authentication:- to control weather a particular user has any type of access right to the element in in question usually we consider this in the form of user account.

functional authentication:- concerns with individual user right.e,g, can a user do once authenticated, can the user figure the device or only see the data.

2.5. Computer network security layers

In Computer Security, layers is a well-known practice which was taken from military techniques. The aim of this is to exhaust the attacker when he succeeds to penetrate the first layer of security by finding a hole, then he has to find a hole in the second layer and so on, until he arrives at the destination if he succeeds.

Following is an image which explains about Layer Security.



Let's see the best practices in a Layer type of Security –

Computer Application Whitelistening – The idea is to install just a restricted number of applications in your computers, which are useful as

well as are genuine.

Computer System Restore Solution – In case your computer is hacked and your files are damaged, you should have the possibility to again have access to your files. An example is Windows System Restore or Backup.

Computer and Network Authentication – The data that is accessed over the network is best to be provided only to the authorized users. Use usernames and passwords!!!

File, Disk and Removable Media Encryption – Generally a good practice is to encrypt hard disks or removable devices, the idea behind this is in case your laptop or your removable USB is stolen and it is plugged in another machine it cannot be read. A good tool for this is **Truecrypt**.

Remote Access Authentication – Systems which are accessed over the network is best to be provided only to the authorized users. Use usernames and passwords!!!

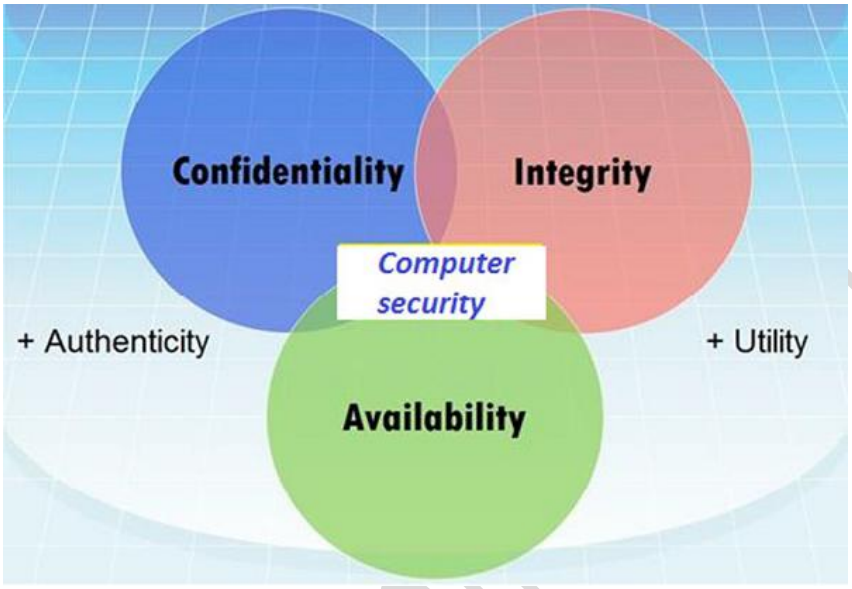
Network Folder Encryption – Again like the case of Network Authentication, if you have a network storage or a network folder shared, it is good to be encrypted to prevent any unauthorized user who is listening to the network to read the information.

Secure Boundary and End-To-End Messaging – Nowadays email or instant messaging is widely spread and it is the number one tool to communicate. It is better that the communication to be encrypted between the end users, a good tool for this is **PGP Encryption Tool**.

I like a confidencial...

2.6. Computer and network security elements

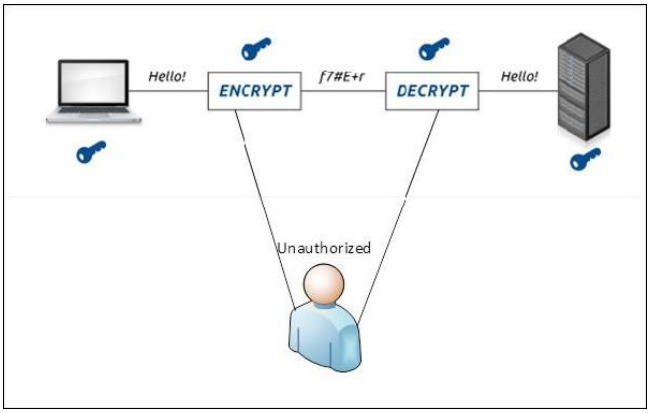
The three main elements which are ***confidentiality, integrity,*** and *availability* and the recently added ***authenticity*** and ***utility***



2.6.1. Confidentiality (Secrecy)

Confidentiality is the concealment of information or resources. Also, there is a need to keep information secret from other third parties that want to have access to it, so just the right people can access it. *Confidentiality Prevent/Detect/Deter improper disclosure of information*

The function of confidentiality is to protect precious business data from unauthorized persons. Confidentiality part of network security makes sure that the data is available only to the intended and authorized persons.



2.6.2. Integrity

Integrity is the trustworthiness of data in the systems or resources by the point of view of preventing unauthorized and improper changes. Generally, Integrity is composed of two sub-elements – data-integrity, which it has to do with the content of the data and authentication which has to do with the origin of the data as such information has values only if it is correct. *Integrity Prevent/Detect/Deter improper modification of information*

This goal means maintaining and assuring the accuracy and consistency of data. The function of integrity is to make sure that the data is reliable and is not changed by unauthorized persons.

2.6.3. Availability

Availability refers to the ability to access data of a resource when it is needed, as such the information has value only if the authorized people can access at right time. *Availability Prevent/Detect/Deter improper denial of access to services provided by the system*

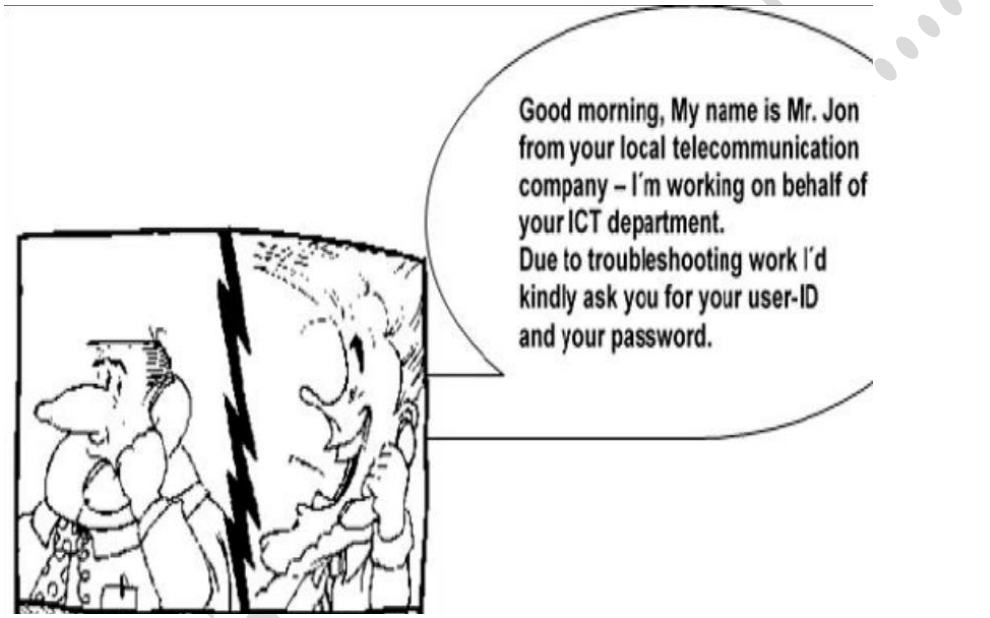
The function of availability in Network Security is to make sure that the data,

I Like a confidencial....

network resources/services are continuously available to the legitimate users, whenever they require it.

Do you know in all this digital world, what is the biggest hole or the weakest point of the security?

Answer. It is us, humans.



2.7. Potential lose due to security attack

The potential loses in this cyberspace are many even if you are using a single computer in your room. some examples that have a direct impact on you and on others –

Losing you data – If your computer has been hacked or infected, there is a big chance that all your stored data might be taken by the attacker.

Bad usage of your computer resources – This means that your network or computer can go in overload so you cannot access your genuine services or in a worst case scenario, it can be used by the hacker to attack another machine or network.

Reputation loss – Just think if your Facebook account or business email has been owned by a social engineering attack and it sends fake information to

your friends, business partners. You will need time to gain back your reputation.

Identity theft – This is a case where your identity is stolen (photo, name surname, address, and credit card) and can be used for a crime like making false identity documents.

Review questions

1. write an example for the three network security services I.e, confidentiality, availability and integrity?
2. Write the respective security attack at the three security services?
3. What is security in your perspective?
4. Suppose you have a facebook account unfortunately the account becomes block, in your opinion what thing trigger that your account going to unable to access by the user?
5. Suppose you want to block your flash disk that hold a huge data for other user, so by what mechanism this can be accomplished?

I Like a confidencial....

Chapter three

3. Computer security

3.1. Basic computer check list

There are some basic things that everyone of us in every operating system need to do:

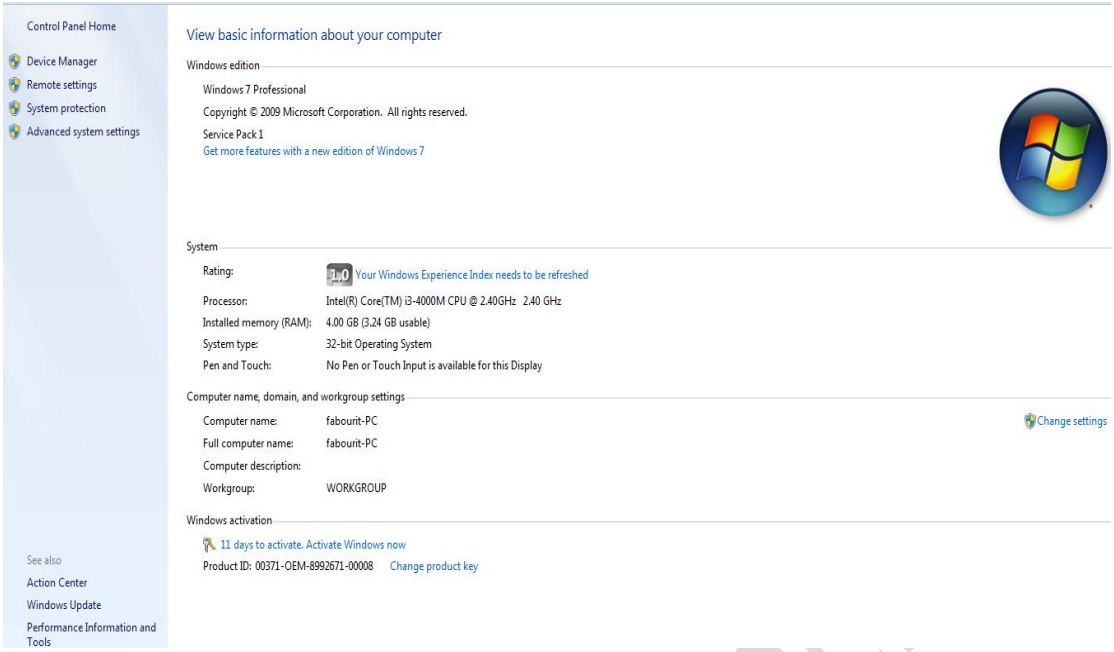
- Check if the user is password protected.
- Check if the operating system is being updated.
- Check if the antivirus or antimalware is installed and updated.
- Check for the unusual services running that consumes resources.
- Check if your monitor is using a screen saver.
- Check if the computer firewall is on or not.
- Check if you are doing backups regularly.
- Check if there are shares that are not useful.
- Check if your account has full rights or is restricted.
- Update other third party software's

3.2. Securing Operating System

Guidelines for securing windows OS

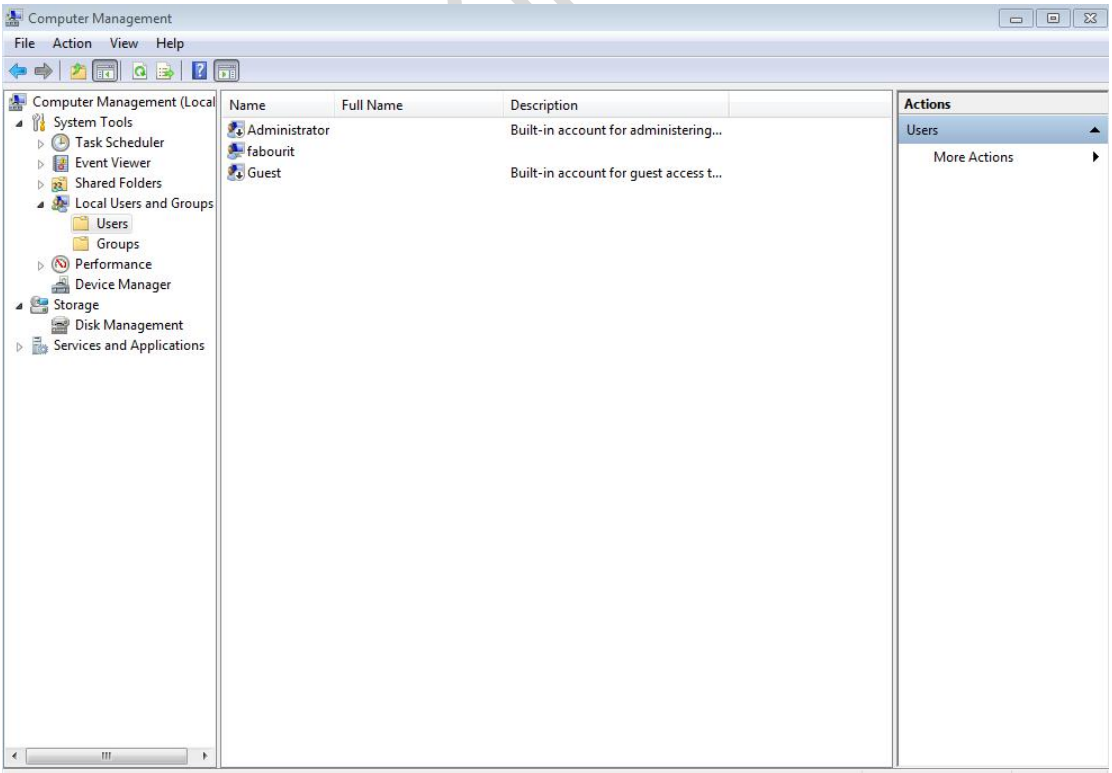
The Following are the list of guidelines for Windows Operating System Security. Use the licensed versions of Windows OS, not the cracked or pirated ones and activate them in order to take genuine updates.

I Like a confidencial....



3.2.1. Disable Unused Users

To do this, Right Click on *Computer – Manage – Local Users and Groups – Users, then disable* those users that are not required.

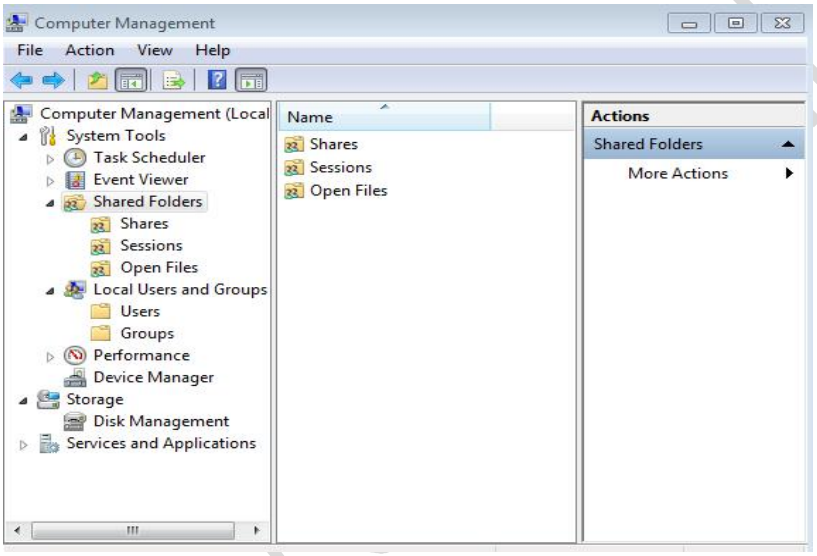


3.2.2. Disable unused shares

By default, Windows OS creates shares, please see the

following screen shot. You have to disable them and to do this, you follow –

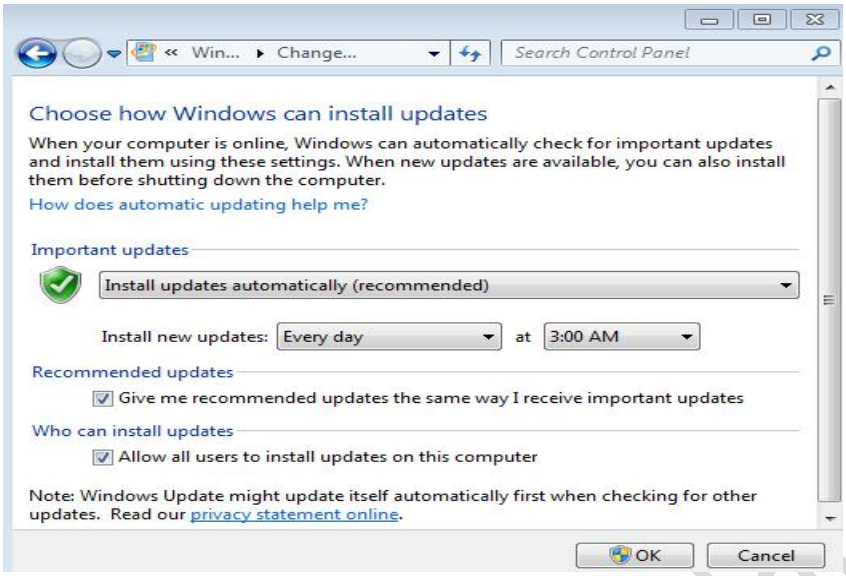
Right Click on *My Computer – Manage – Shared Folders – Right Click Stop Sharing.*



3.2.3. Update windows Os

It is recommended to do them automatically and periodically. To set this up,

go to Control Panel – System and Security – Windows Updates – OK



3.2.4. Adjust firewall setting

Put your Windows System Firewall up, this will block all the unauthorized services that make traffic. To set this up, go to *Control Panel – System and Security – Windows Firewall.*

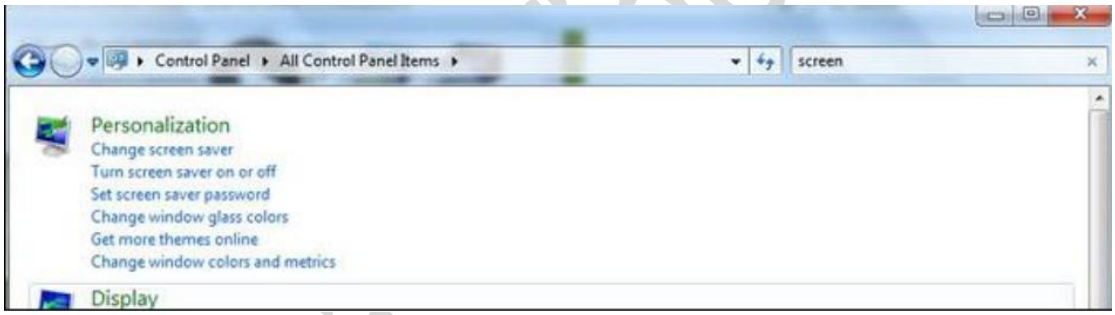
Confidencia.....

3.2.5.Install anti virus

Install a licensed anti virus and take updates, in the coming sections we will cover in detail about anti viruses. It is strongly recommended not to download from torrents and install cracked versions.

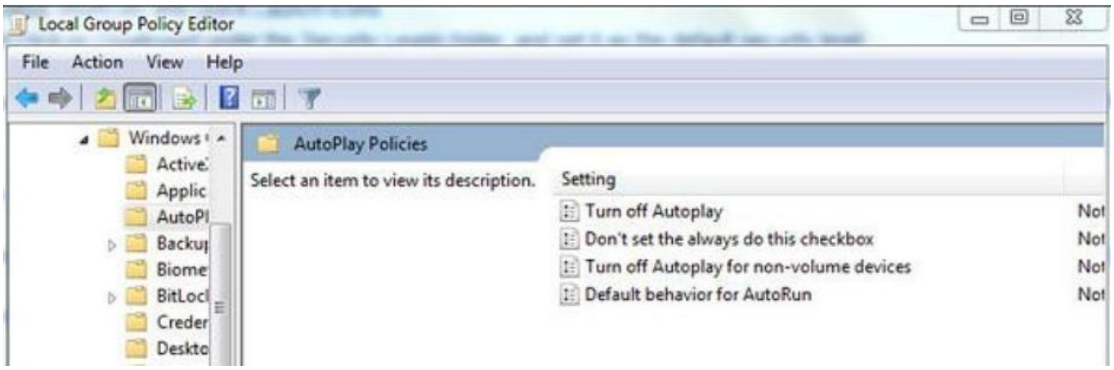
3.2.6. Password protected screen saver

You should always Configure a password protected Screen Saver. To set this up, please follow this path – *Control Panel – All Control Panel Items – Personalize – Turn Screen Saver on or off – Check "On resume, display logon Screen"*



3.2.7. Disable Auto play for Removable Media.

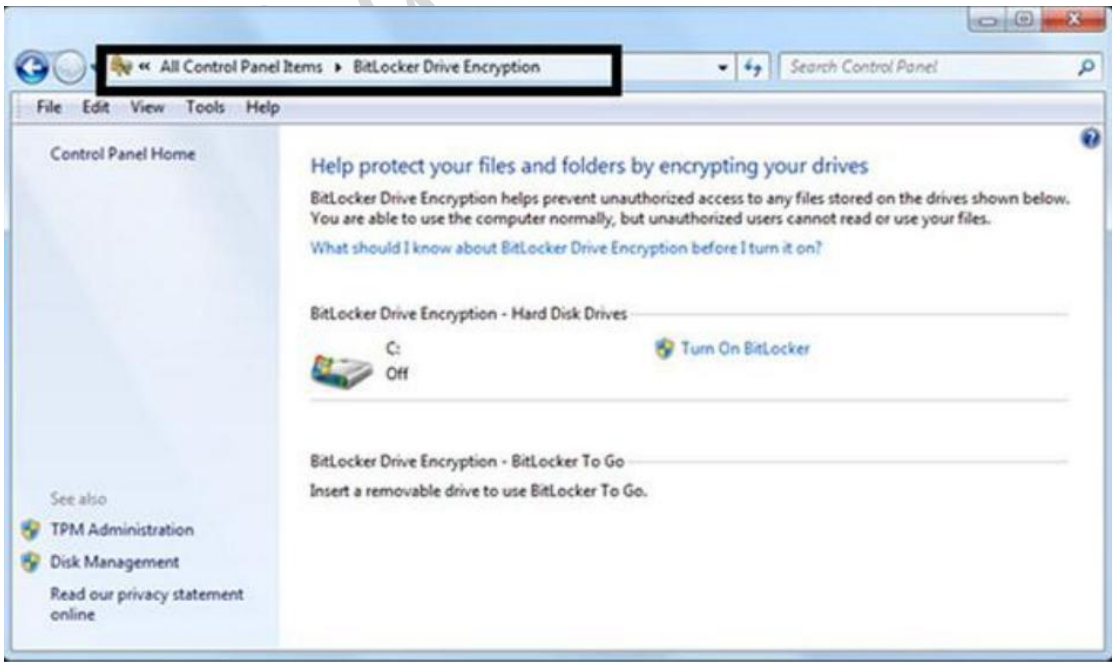
This blocks the viruses to run automatically from removable devices. To disable it go to – S*tart – on Search box type Edit Group Policy –Administrative Templates – Windows Components – Auto play Policy – Turn off Auto play – Enable – Ok*



Install only trusted internet explorer browsers like Internet explorer, Chrome or Mozilla Firefox and then update them regularly. Missing the updates can lead to possible hacking.

3.2.8. Enable the Bit Locker Drive Encryption

to encrypt hard drives, but it is only available in Windows & Ultimate and Upper Versions. To enable it follow the path: Start – Control Panel – System and Security – Bit Locker Drive Encryption



a confidencial....

3.2.9. Set Bios Password

This option differs based on different computer producers and we need to read manufacturer guidelines, this option secures your computer one layer upper in the OS.

3.3. Data backup

Why we need data backup?

The main purpose is to recover the lost data from an unpredictable event like deletion by mistake or file corruption which in many cases is caused by a virus or other unauthorized access.

3.3.1. Backup devices

Some of data backup device are as follows:

- CD and DVD, Blue-Rays
- Network attached storage
- Removable device
- Storage area network

3.3.2. Types of data backup

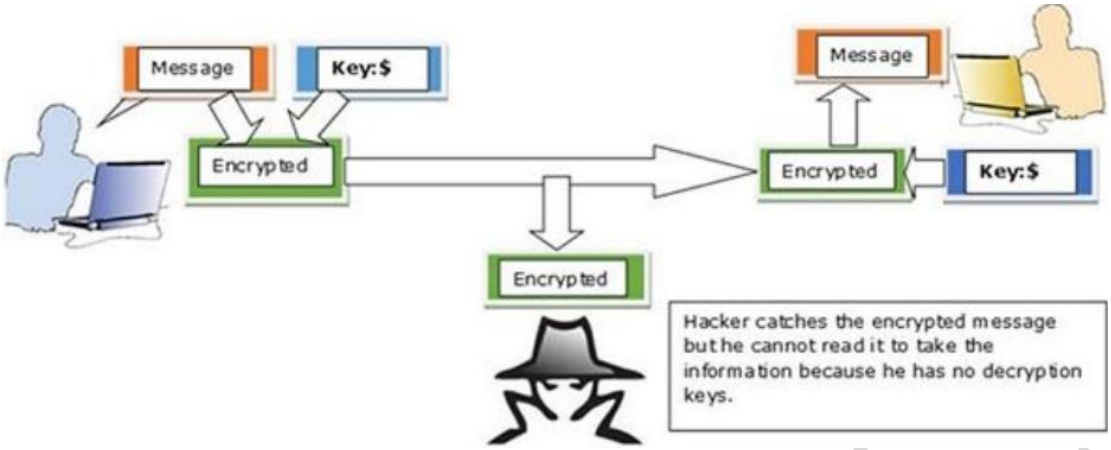
Computer data backup can be categorized based on location such as:

- Local backup
- Online backup

3.4. Encryption

Encryption is a transformed type of genuine information where only the authorized parties know how to read it, so in the worst case scenario if somebody has access to these files they would still not be able to understand the message in it.

I Like a confidencial...



3.5. Tools to encrypt document

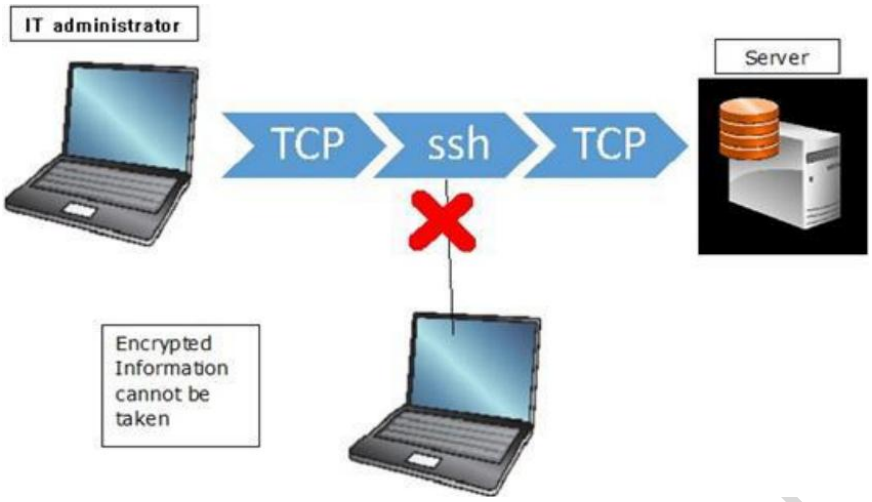
- Axcrypt:- you can download from –http://www.axantum.com/AxCrypt/Downloads.aspx
- GnuPG– It can be downloaded from– https://www.gnupg.org/download/index.html
- Windows BitLocker
- FileVault

How to see if the communication is secure?

Browsers give visual cues, such as a lock icon or a green bar, to help visitors know when their connection is secured. An example is shown in the following

Some example of encryption tool are security socket layer (SSL) and security shell (SSH)

I Like a confidencial....



Review questions

1. write the steps to enter into system password setting?
2. Write the steps to backup the data for further security?
3. Write the steps to delete unwanted file from the computer permanently?
4. Explain how encrypt the password into hash form?
5. Suppose while accessing your laptop unfortunately the pc become becomes freeze or very slow unlikely to he previous day, so what problem present with your computer?

I Like a confidencial....

Chapter four

4. Computer network Security and threat

4.1. General threat perceptions

- Network threatened by external running malicious scripts (Malware)
- Adversaries attempting access protected services, break into machines, snoop communications, collect statistics of transactions …
- Insiders and outsiders
- Disasters (natural and man-made)

4.2. Contributing factor for network security threat

Most of the time computer network security can face into vulnerability due to the following reason:

- Erroneous Program:- including Lack of prudent Software Engineering Practices, Complexity of software (millions of lines) and Urgently developed Components of The Shelf (COTS)
- The user (Systems should be User proof!):-Responsibility lies with the user (ignorance/non co-operation are problems), Security policy should convince the users
- Poor Administration:- including Configuration, backup procedures, constant updates, monitoring, disaster recovery …
- Hacking tools that can be found very easily by everyone just by Goggling and they are endless.
- Technology with the end-users
- has increased rapidly within these world, like internet bandwidth and computer processing speeds.
- Access to hacking information manuals
- Lack of awareness of threats and risks

I Like a confidencial....

of information systems

- Wide-open network policies
- Many Internet sites allow wide-open Internet access
- Vast majority of network traffic is unencrypted
- Lack of security in TCP/IP
- Complexity of security management and administration
- Exploitation of software bugs: e.g. Send mail bugs
- Cracker skills keep improving

4.3. Security attack

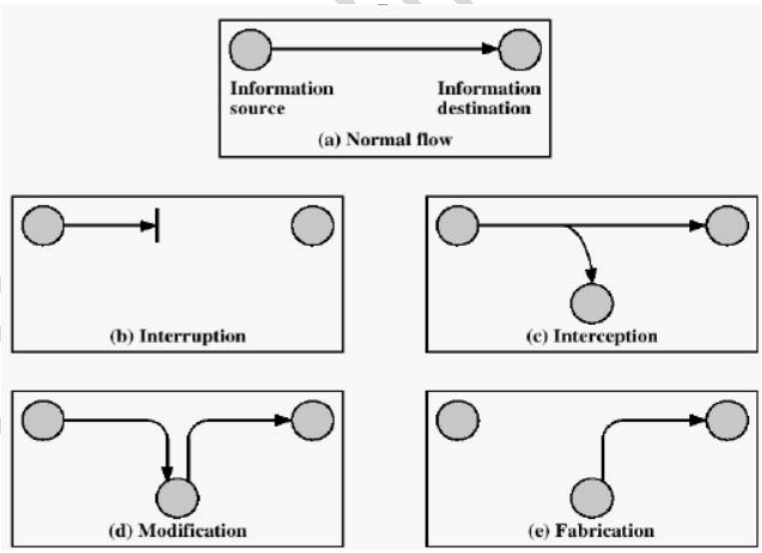
The following are common computer network security attacks:

Interruption:-this an attack that perform on the availability.

Interception:- an attack on confidentiality

Modification:- an attack on integrity

Fabrication:- an attack on authentication



4.4. Classification of security attack

Computer network security attack can be classified as passive and active security attack

1. **passive attacks** – eavesdropping on, or monitoring of, transmissions to:

- obtain message contents, or

- monitor traffic flows

2. **active attacks** – modification of data stream to:

- masquerade of one entity as some other: man-in-the-middle
- replay previous messages
- modify messages in transit
- denial of service

4.5. Security service

1. **Confidentiality:** protection of any information from being exposed to unintended entities.

- Information content
- Parties involved
- Where they are, how they communicate, how often, etc.

2. **Authentication:** assurance that an entity of concern or the origin of a communication is authentic - it's what it claims to be or from

3. **Integrity:** assurance that the information has not been tampered with or making sure message has not been altered

4. **Non-repudiation:** offer of evidence that a party is indeed the sender or a receiver of certain information

5. **Access control:** facilities to determine and enforce who is allowed access to what resources, hosts, software, network connections

5. **Security management:** facilities for coordinating users' service requirements and mechanism implementations throughout the enterprise network and across the internet

– Trust model

– Trust communication protocol

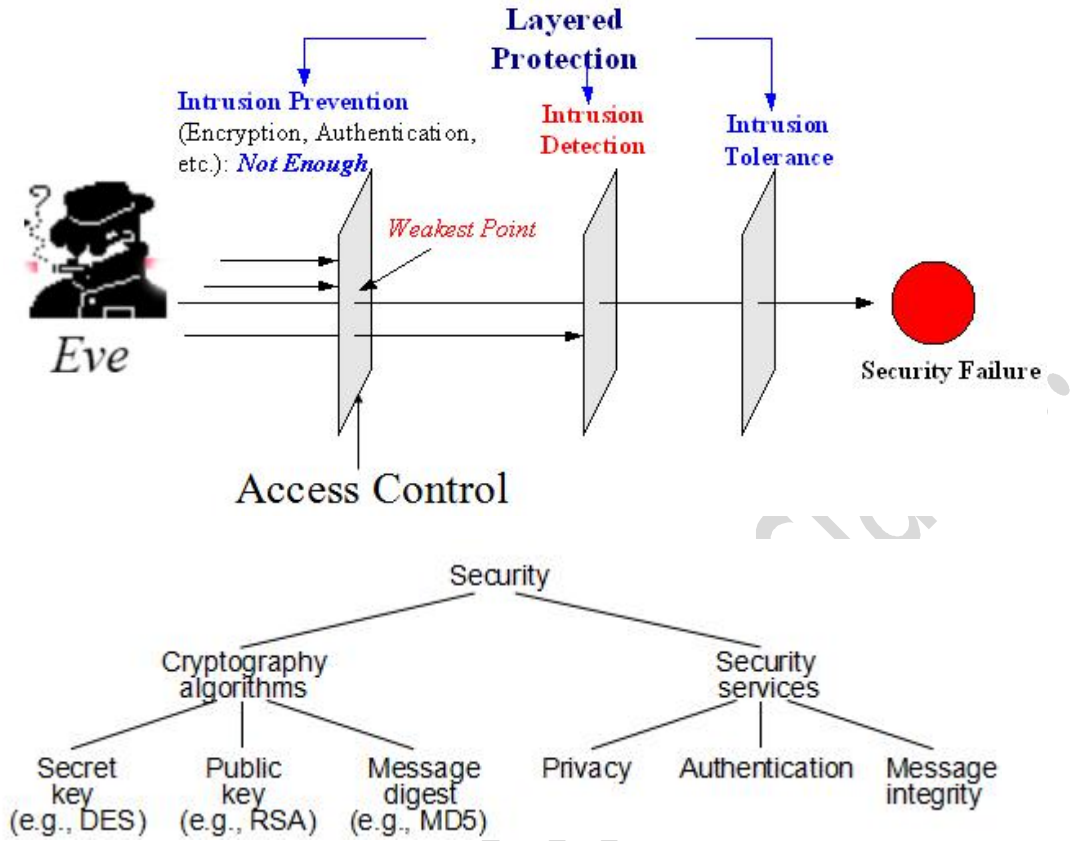
– Trust management infrastructure

4.6. Security mechanism

The following diagram describes the full concept that how we protect any network security

I Like a confidencial....

attack.



✧ **Cryptography functions :-** including Secret key (e.g., DES), Public key (e.g., RSA) Message digest (e.g., MD5)

✧ **Security services:-** including ***Privacy:*** preventing unauthorized release of information ***Authentication:*** verifying identity of the remote participant and ***Integrity:*** making sure message has not been altered

Secret key (Symmetric Key Ciphers)

In a symmetric-key cipher, both participants in a communication share the same key. In other words, if a message is encrypted using a particular key, the same key is required for decrypting the message.

Public key (Public Key Ciphers)

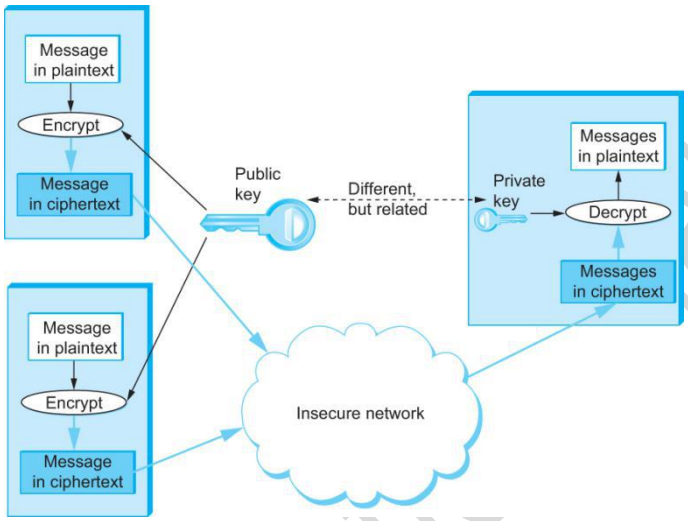
An alternative to symmetric-key ciphers is asymmetric, or public-key, ciphers.

✧ Instead of a single key shared by two participants, a public-key cipher uses a pair of related keys, one for encryption and a different one for decryption.

✧ The pair of keys is "owned" by just one participant.

✧ The owner keeps the decryption key secret so that only the owner can decrypt messages; that key is called the private key.

✧ The owner makes the encryption key public, so that anyone can encrypt messages for the owner; that key is called the public key.



Message digest

In this method, actual data is not sent; instead a hash value is calculated and sent. The other end user, computes its own hash value and compares with the one just received. If both hash values are matched, then it is accepted; otherwise rejected.

Privacy: preventing unauthorized release of information

Authentication: verifying identity of the remote participant

Integrity: assurance that the information has not been tampered with or making sure message has not been altered.

4.7. Basic security technique

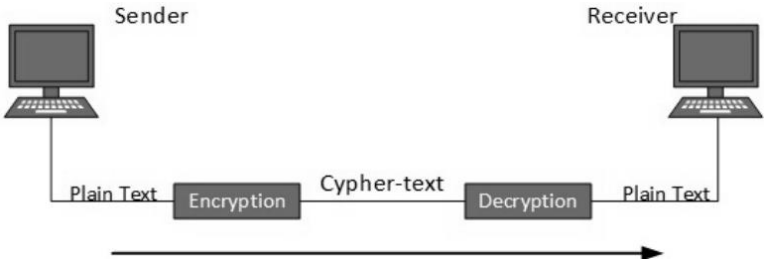
✧ Hashing

✧ Diffie-Hellman Key Exchange

✧ Symmetric Key Cryptography

✧ Public Key Cryptography

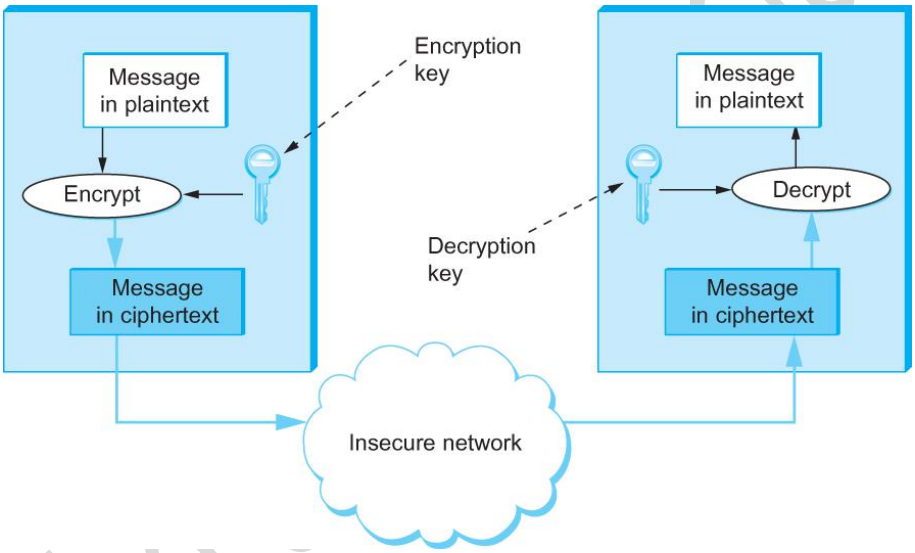
The most widely used technique is ***Cryptography***



Basically security may be ***hard ware security*** and **software security** including data file such as files and databases

4.8. Cryptographic building block

The first step is the cryptographic algorithms—ciphers and cryptographic hashes



The basic requirement for an encryption algorithm is that it turn plaintext into ciphertext in such a way that only the intended recipient—the holder of the decryption key—can recover the plaintext.

Principles of Ciphers

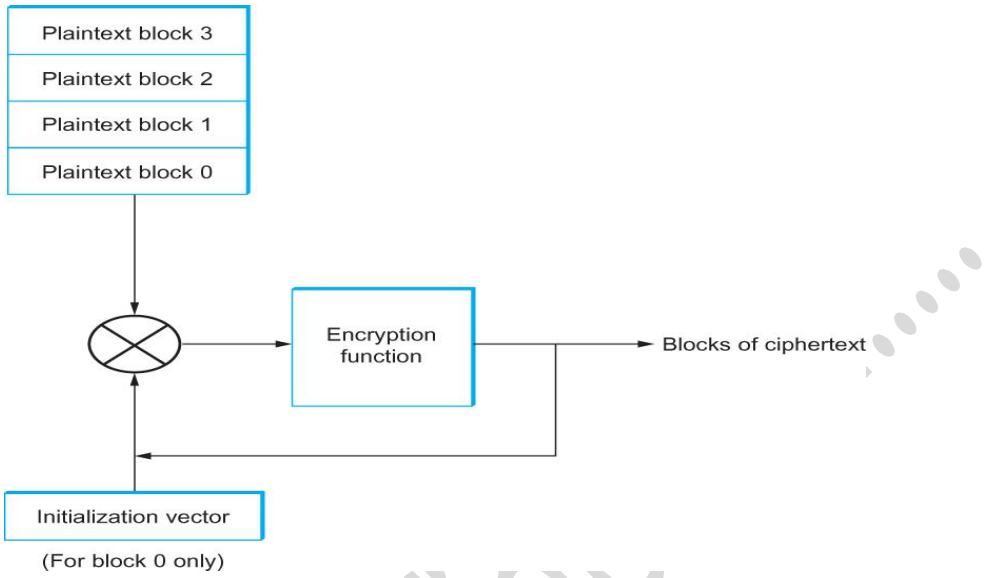
✧ Encryption transforms a message in such a way that it becomes unintelligible to any party that does not have the secret of how to reverse the transformation.

✧ The sender applies an encryption function to the original plaintext message, resulting in a ciphertext message that is sent over the network.

✧ The receiver applies a secret decryption function–the inverse of the encryption function–to recover the original plaintext.

Block Ciphers

A common mode of operation is cipher block chaining (CBC), in which each plaintext block is XORed with the previous block's ciphertext before being encrypted.



4.9. Common security attack and its counter measure

1. **Finding a way into the network.**– the best solution for this types of attack is firwall

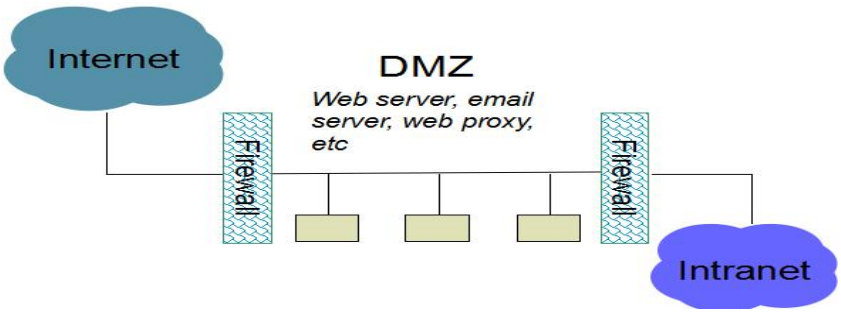
Firewall

A firewall is a hardware, software, or a combination of both that monitors and filters traffic packets that attempt to either enter or leave the protected private network.

- ✧ Firewall can be software or hardware
- ✧ The only point of access int the network

Most firewall perform two basic function

- ✧ Packet filtering based on accept or deny policy that is itself based on rules of the security policy.
- ✧ Application proxy gateways that provide services to the inside users and at the same time protect each individual host from the "bad" outside users.



2. **Exploiting software bugs, buffer overflows:-** the protection is using Intrusion Detection Systems

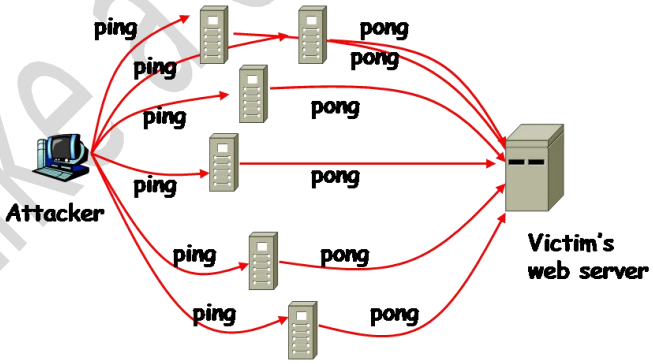
Intrusion Detection

Used to monitor for "suspicious activity" on a network means that Can protect against known software exploits, like buffer overflows.

3. Denial of services

Many different kinds of DoS attacks

- ✧ SYN flooding
- ✧ SMURF
- ✧ Distributed attacks
- ✧ Mini Case Study: Code-Red



The Solution for this type of attack isuse "SYN cookies"

- ✧ In response to a SYN, create a special "cookie" for the connection, and forget everything else
- ✧ Then, can recreate the forgotten information when the ACK comes in from a legitimate connection

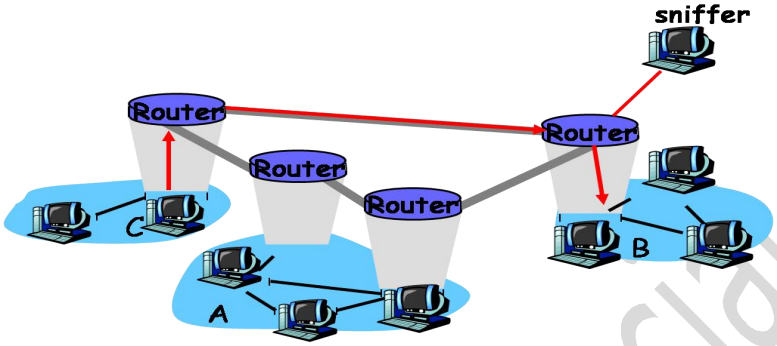
4. TCP Attack (TCB hijacking)

I Like a confidencial....

We can protect it by using IPSec which Provides source authentication and

5. packet sniffing

The solution or protection mechanism is using security protocol such as S***SL, HTTP, IPSec, FTP*** and other



6. **Cryptanalaysis**:-we can defend this using Use of longer keys and stronger encryption algorithm

7. Password pilfering

Methods to pilfer user password:

- ✧ Guessing
- ✧ Dictionary attacks
- ✧ Social engineering
- ✧ Password sniffing

Rules to help protect passwords from pilfering:

- ✧ Use long passwords, with a combination of letters, capital letters, digits, and other characters such as $,#,@. Do not use dictionary words, common names and dates.
- ✧ Do not reveal your passwords to anyone you do not know. Do not submit to anyone who acts as if he has authority. If you have to give out your password, do so face to face.
- ✧ Change passwords periodically and do not reuse old passwords.
- ✧ Do not use the same password for different accounts.
- ✧ Do not use remote login software that does not encrypt user passwords and other important personal information.
- ✧ Shred all discarded papers using a good paper shredder.
- ✧ Avoid entering any information in any popup window, and avoid clicking on links in suspicious emails.

Like a confidencial.....

8. **identity spoofing**:–there are four types of this type of security attack,thus are.
   - ✧ Man-in-the-middle attacks.
   - ✧ Message replays
   - ✧ Network spoofing attacks
   - ✧ Software exploitation attacks
9. **Buffer overflow exploiting**:– it can be defend using two methods
   - ✧ Coding: follow good programming practice; always add statements to check bounds when dealing with buffers
   - ✧ Compiling: insert a random canary value before a returned address

Review questions

1. write the explanation of SYN spoofing, intrusion detection and denial of service?
2. Describe man-in-middle attack, network spoofing and message relays?
3. Explain about identity spoofing and packet hijacking?
4. Explain about SSL, SSH, HTTP and FTP and there role on attack protection?
5. How to hardware firewall protect any attack in the networking area, and also how about software firewall?
6. How cryptanalysis attack our network explain with definition?
7. Define hashing and explain is application in security aspects?

I Like a confidencial....

Chapter five

5. Malwares and its protection

Malwares are self-replication programs that reproduce their own codes by attaching themselves to other executable codes. They operate without the permissions or knowledge of the computer users. Viruses or malwares like in real-life, in computers they contaminate other healthy files. Malwar can be categorize in three main types:

- Trojans and Rootkits
- Viruses
- Worms

Following are a couple of characteristics of any virus that infects our computers.

- ✧ They reside in a computer's memory and activates themselves while the program that is attached starts running
- ✧ They modify themselves after the infection phase like they source codes, extensions, new files, etc. so it is harder for an antivirus to detect them.
- ✧ They always try to hide themselves in the operating systems.
- ✧ It may delete important data from your computer to gain space for their processes.
- ✧ It may avoid detection by redirection of disk data.
- ✧ It may perform tasks by triggering an event with itself. For example,

I Like a confidencial....

this happens when in an infected computer pop-up tables etc., show up automatically on the screen.

- ✧ They are common in Windows and Mac OS because these operation systems do not have multiple file permissions and are more spread out.

5.1. Working process of malware and how to clean it

The following are some of the method that virus can attach themselves to the files:

- ✧ Start by themselves
- ✧ Transmit themselves by using non-executable files
- ✧ Infect other networks or computer

Investigating the virus process

The following are some of the tool that help us to investigate weather the virus start its process in our computer:

- ✧ fport.exe
- ✧ pslist.exe
- ✧ handle.exe
- ✧ netstat.exe

Detecting a computer error from virus infection

The following sign that will happens in our computer operation are due to virus infection:

- ✧ Your computer shows a pop-up or error tables.
- ✧ Freezes frequently.
- ✧ It slows down when a program or process starts.

I Like a confidencial....

✧ Third parties complain that they are receiving invitation in social media or via email by you.

✧ Files extensions changes appear or files are added to your system without your consent.

✧ Internet Explorer freezes too often even though your internet speed is very good.

✧ Your hard disk is accessed most of the time as you can see from the LED light on your computer case.

✧ OS files are either corrupted or missing.

✧ If your computer is consuming too much bandwidth or network resources this is the case of a computer worm.

Some recommendation to avoid virus

✧ Don't open any email attachment coming from unknown people or from known people that contain suspicious text.

✧ Don't accept invitation from unknown people on social media.

✧ Don't open URL sent by unknown people or known people that are in any weird form.

I Like a confidencial....

5.2. Antiviruses

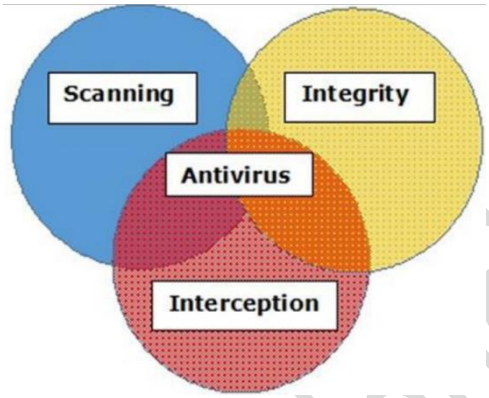
Antiviruse can protect our system from any malicious and unwanted infection using antivirus engine

5.2.1. Basic function of antivirus engine

All antivirus engines have three components to function accordingly. Thes

engine are:

- ✧ Scanning
- ✧ Integrity Checking
- ✧ Interception



5.2.1.Online virus testing

If the system administrator or any user does not have an antivirus installed or suspects a file that is infected. They would recommend to use the online testing antivirus engine which (according to me) is one of the best –https://virustotal.com/.

5.3. Free antivirus software

Avast:- it can be downloaded from https://www.avast.com/en-eu/index

AVG:- It can be downloaded from http://www.avg.com/us-en/free-antivirus-download.

Panda 2016:- it can be download form http://www.pandasecurity.com/usa/homeusers/downloads/

BiteDefender:- It can be downloaded from http://www.bitdefender.com/solutions/free.html

I like a confidential....

Microsoft Security essaential:- It can be downloaded from http://windows.microsoft.com/en-us/windows/securityessentials-download

5.4. Commercial antivirus

The best commercial antiviruses are:

- ✧ Kaspersky Anti-Virus
- ✧ Bitdefender Antivirus Plus 2016
- ✧ McAfee AntiVirus Plus (2016)
- ✧ Webroot SecureAnywhere Antivirus (2015)

Linux (MAC OS) can not affected by virus why?

Write the difference b/n virus, worm. Spay ware,Trojan horse and Zombie?

I Like a confidencial....

Chapter six

6. Security policies

6.1. Role of security policy in setting up protocols

Following are some pointers which help in setting u protocols for the security policy of an organization.

- ✧ Who should have access to the system?
- ✧ How it should be configured?
- ✧ How to communicate with third parties or systems?

Policies are divided in two categories

1) User policies
2) IT policies

IT police can be further categorized into the following:

- ✧ General Policies
- ✧ Server Policies
- ✧ Firewall Access and Configuration Policies
- ✧ Backup Policies
- ✧ VPN Policies

6.2. Structure of security policy

When you compile a security policy you should have in mind a basic structure in order to make something practical. Some of the main points which have to be taken into consideration are

- ✧ Description of the Policy and what is the usage for?

I Like a confidencial....

- ✧ Where this policy should be applied?
- ✧ Functions and responsibilities of the employees that are affected by this policy.
- ✧ Procedures that are involved in this policy.
- ✧ Consequences if the policy is not compatible with company standards.

6.3. types of security policy

- ✧ Permissive Policy
- ✧ Prudent Policy
- ✧ Acceptance User Policy
- ✧ User Account Policy
- ✧ Information Protection Policy
- ✧ Remote Access Policy .
- ✧ Firewall Management Policy
- ✧ Special Access Policy
- ✧ Network Policy
- ✧ Email Usage Policy
- ✧ Software Security Policy

6.4. Security checklist

we will use in order to educate users and IT staff too, when it comes to any security issues, they should come as natural expressions.

1. **Server room**
   - ✧ Server rack installed properly
   - ✧ Air conditioning present
   - ✧ Temperature monitoring and alarm system is in place
   - ✧ Automatic smoke/fire detection is available
   - ✧ Water entry prevention detector is available
   - ✧ Fire extinguisher is in place
2. **Business Critical Services**
   - ✧ Redundant power supplies are available

I Like a confidencial....

- ✧ RAID systems are available
- ✧ UPS systems are in place
- ✧ Emergency systems are in place
- ✧ Documentation is up to date
- ✧ Professional support is provided
- ✧ SLAs are signed
- ✧ Emergency plan is prepared

3. **Business Internet Account**

- ✧ Redundant lines
- ✧ Insurance for ICT equipment is available

4. **Information Systems**

- ✧ Server is installed according to the Setup Policies Manuals
- ✧ Standard GPOs are configured on the Server
- ✧ System security is done
- ✧ System documentation is up-to-date
- ✧ Data backup is configured properly and done regularly according to backup policies
- ✧ To check proper naming of all computers, network devices to be in line

with IT Policy

- ✧ Standard Whitelist Software to be aligned on all PCs
- ✧ All PCs in domain system
- ✧ Administrator privileges are taken from computer users
- ✧ Program privileges are on minimum needed level

5. **Information Security**

- ✧ Identity and access management is configured
- ✧ Data access possibilities are minimized to needed level
- ✧ Virus protection software is installed on each PC

6. **Human Factor**

- ✧ ICT System and email Usage Policy is rolled-out (should be checked as per the disciplinary safeguards)
- ✧ Staff awareness training is provided regularly
- ✧ Responsibilities are documented

7. **Maintenance of Information Systems**

- ✧ Security updates are installed on all PC's
- ✧ ICT internal alert and notification system is configured

Like a confidencial....

- ✧ Security update action plan is done
- ✧ Security update roll out plan is in place

8. General
   - ✧ Network IP address schema are in line
9. Network Security
   - ✧ Firewall access rules and open ports are compliant with the firewall policy
   - ✧ Protection of sensitive information is in place
   - ✧ Restriction of communication services is enabled
   - ✧ VPN is configured properly with the partners
   - ✧ WLAN security is enabled on all WIFI devices
   - ✧ Limited internet access is configured
   - ✧ BYOD regulations are implemented
10. Network Management
    - ✧ Bandwidth Management System is configured
    - ✧ Network Monitoring System is available
    - ✧ DRP files are up to date

I Like a confidencial....

I Like a confidencial....