MODULE I

Introduction: Overview of computer security, Security concepts, Need of Security- Threats- Deliberate software attacks, Deviation in quality of service, Attacks- malicious code, brute force, Timing attack, sniffers

Access Control Mechanisms - Access Control, Access control matrix, Access control in OS-Discretionary and Mandatory access control, Role-based access control, case study SELinux

OVERVIEW OF COMPUTER SECURITY

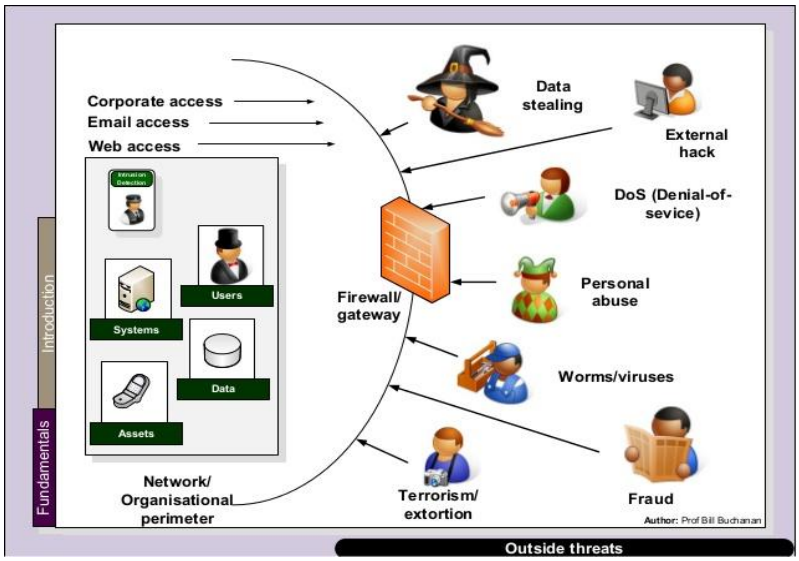
- A **computing system**: is a collection of hardware, software, data, and people that an organization uses to do computing tasks
- Computer security means protect our computing system

Main aspects are:

- Prevention:- Prevent your assets from being damaged
- Detection :- Detect when assets has been damage
- Reaction:- Recover your assets

Computer Security: - Ensuring the data stored in a computer cannot be read or compromised by an individual's without authorization.

- Most computer security measures involve data encryption and passwords.
- The purpose of computer security is to device ways to prevent the weaknesses from being



SECURITY CONCEPTS

Three Goals in Computing Security

Three goals of computer security are

1. Confidentiality
2. Integrity
3. Availability

•**Confidentiality**: ensures that computer-related assets are accessed only by authorized parties. Confidentiality is sometimes called secrecy or privacy.

-Difficult to ensure

- Easy to assess

Confidentiality is the ability to hide information from those people unauthorized to view it. It is perhaps the most obvious aspect of the CIA(Confidentiality, Integrity and Availability) triad when it comes to security; but correspondingly, it is also the one which is attacked most often.

Cryptography and Encryption methods are an example of an attempt to ensure confidentiality of data transferred from one computer to another.

A good example of methods used to ensure confidentiality is an account number or routing number when banking online.

Data encryption is a common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication is becoming the norm.

Other options include biometric verification and security tokens, key fobs or soft tokens.

In addition, users can take precautions to minimize the number of places where the information appears and the number of times it is actually transmitted to complete a required transaction.

Different approaches for achieving confidentiality are

- **Access control**: - specify who can access. One access control mechanism for preserving confidentiality is cryptography
- **Identification and Authentication**

Two concepts in confidentiality are

1. **Data Confidentiality**: - assures that confidential information is not disclosed to authorize individuals.
   - Only the people who are authorized to do so can gain access to sensitive data. Imagine your bank records.
   - You should be able to access them, of course, and employees at the bank who are helping you with a transaction should be able to access them, but no one else should.
2. **Privacy:** The right of individuals to hold information about themselves in secret, free from the knowledge of others

•**Integrity:** it means that assets can be modified only by authorized parties or only in authorized ways.

- Much difficult to measure

Two concepts in integrity are

1. **Data Integrity**:- Information and programs are changed only in authorized manner
2. **System Integrity**: - System performs its operation in unimpaired manner that means state of the system not changed.

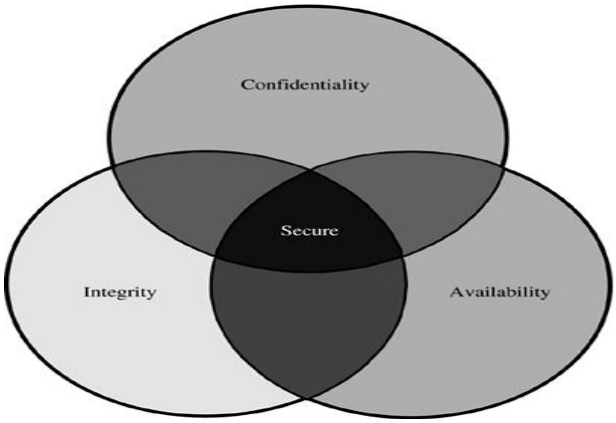
Integrity mechanisms fall into two classes: ***prevention*** **mechanisms and** ***detection*** **mechanisms**.

Prevention mechanisms seek to maintain the integrity of the data by blocking any unauthorized attempts to change the data or any attempts to change the data in unauthorized ways.

Detection mechanisms do not try to prevent violations of integrity; they simply report that the data's integrity is no longer trustworthy. The mechanisms may report the actual cause of the integrity violation (a specific part of a file was altered), or they may simply report that the file is now corrupt.

•**Availability:** it means that assets are accessible to authorized users in all time

- Availability applies both to data and to service.
- Failure to this goal (availability)is known as Denial of service.
- Availability is an important aspect of reliability as well as of system design because an unavailable system is at least as bad as no system at all



One of the challenges in building a secure system is finding the right balance among the goals, which often conflict.

Along with three objectives system should also ensure

1. **Authentication**: Computer system be able to verify identity of user.

   Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server.

   Users are usually identified with a user ID, and authentication is accomplished when the user provides a credential, for example a password, that matches with that user ID.

2. **Accountability**: Every individual who works with an information system should have specific responsibilities for information assurance.
3. **Non repudiation**: non-repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data. In other words, non-repudiation makes it very difficult to successfully deny who/where a message came from as well as the authenticity of that message.

Digital signatures can offer non-repudiation when it comes to online transactions, where it is crucial to ensure that a party to a contract or a communication can't deny the authenticity of their signature on a document or sending the communication in the first place.

In this context, non-repudiation refers to the ability to ensure that a party to a contract or a communication must accept the authenticity of their signature on a document or the sending of a message.

NEED OF SECURITY

Why is computer security important?

Computer security is important, primarily to keep your information protected. It's also important for your computer's overall health, helping to prevent viruses and malware and allowing programs to run more smoothly.

Security is needed due to following reason

1. Privacy:- It defines the right of individuals to hold information about themselves in secret, free from the knowledge of others
2. Accuracy: - Most of damages of data is caused by errors and omissions. An organization always needs accurate data for transaction processing, providing better service and making
3. Threats by dishonest employ
4. Computer Crimes:- When computer resources can be misused for unauthorized or illegal function
5. Threats for fire and Natural Disasters:- fire and natural disasters like floods, storms, lightening etc

THREATS

•A threat to a computing system is a set of circumstances that has the potential to cause loss or harm.

- A threat can be an object or person or other entity that represents a constant danger to an asset

•There are many threats to a computer system, including **human-initiated and computer- initiated ones.**

•A threat is blocked by control of vulnerability (Weakness of the system).

We can view any threat as being one of four

•An **interception** means that some unauthorized party has gained access to an asset. The outside party can be a person, a program, or a computing system.

•In an **interruption** is an asset of the system becomes lost, unavailable, or unusable.

•If an unauthorized party not only accesses but tampers with an asset, is called as a **modification**.

•An unauthorized party might create a **fabrication** of counterfeit objects on a computing system.

•The intruder may insert spurious transactions to a network communication system or add records to an existing database.

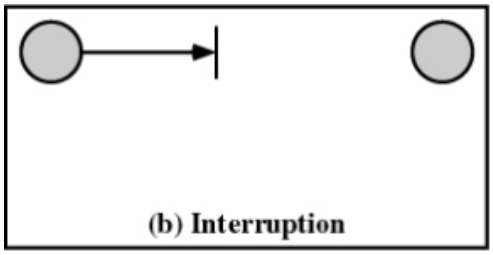
Kinds of threats

- **Interruption**

- An asset of the system is destroyed of becomes unavailable or unusable

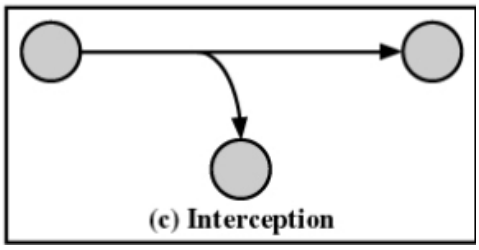
  – Attack on availability

- Destruction of hardware
- Cutting of a communication line
- Disabling the file management system



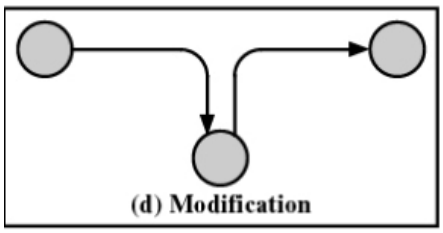
- Here the information being interrupted

- **Interception**
  - An unauthorized party gains access to an asset
  - Attack on confidentiality
  - Wiretapping to capture data in a network
  - Illicit copying of files or programs



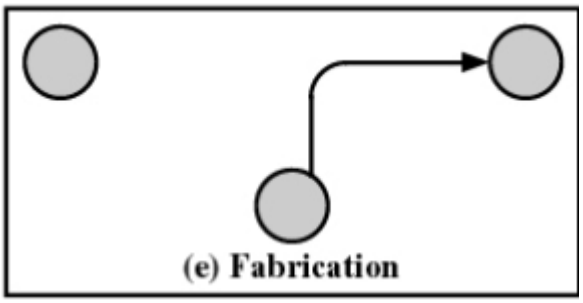
- There is a middleman or process or machine trying to intercept

- **Modification**
  - An unauthorized party not only gains access but tampers with an asset
  - Attack on integrity
  - Changing values in a data file
  - Altering a program so that it performs differently
  - Modifying the content of messages being transmitted in a network

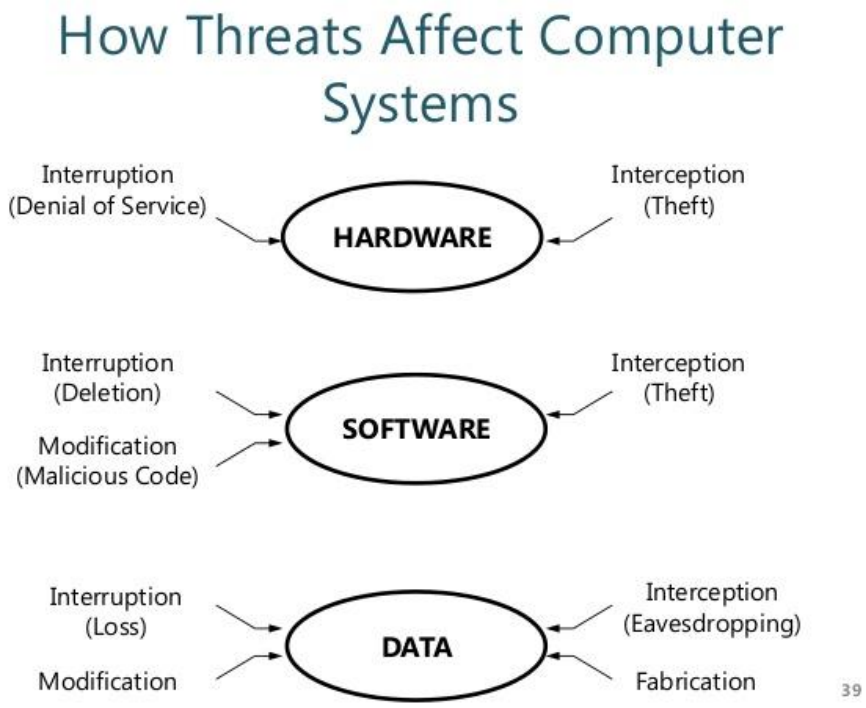


- Here middleman changes the data and send to the receiver

- **Fabrication**
  - An unauthorized party inserts counterfeit objects into the system
  - Attack on authenticity
  - Insertion of spurious messages in a network
  - Addition of records to a file



- Here sender not sends data to the receiver. Middleman fabricate the data



ATTACKS

- Attack is the process of gaining the access of data by unauthorized user.
- It is an Act or attack that exploit vulnerability(Weakness of the system)

Definition - What does Attack mean?

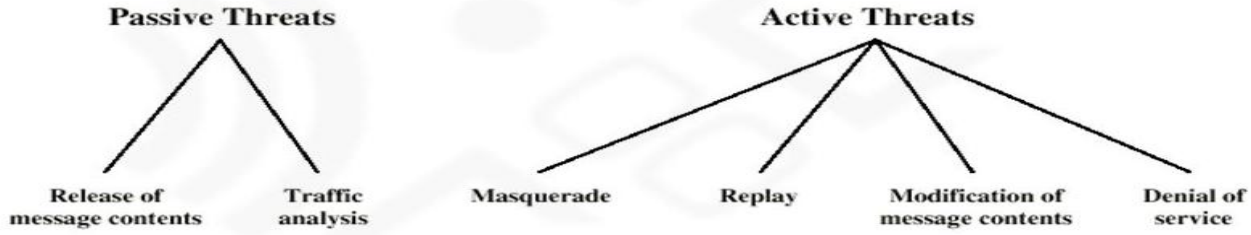
An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission. It happens to both individuals and organizations.

Two types of attacks are

1. Passive attack:-data just accessed by third party, no modification, does not affect system resources
2. Active attack:- data will be modified

Attack Categories

Generally attacks may be categorized in ***passive*** and ***active*** attacks. While passive attacks can be defined as read-only attacks, active attacks include data generation, modification, or destruction.



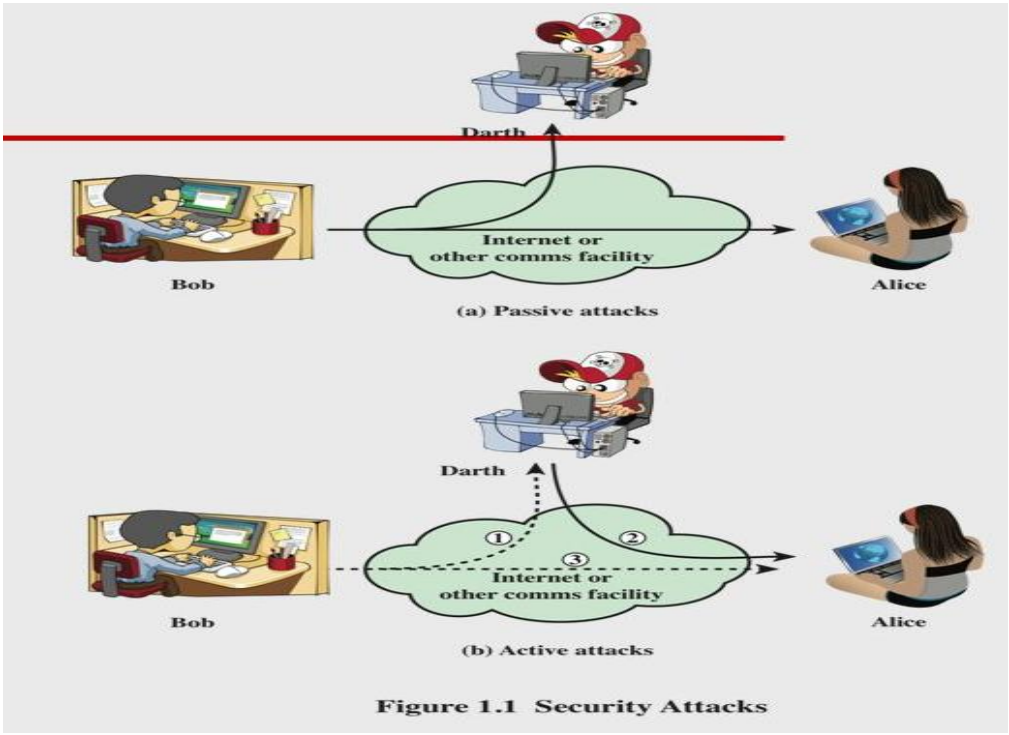


Figure 1.1 Security Attacks

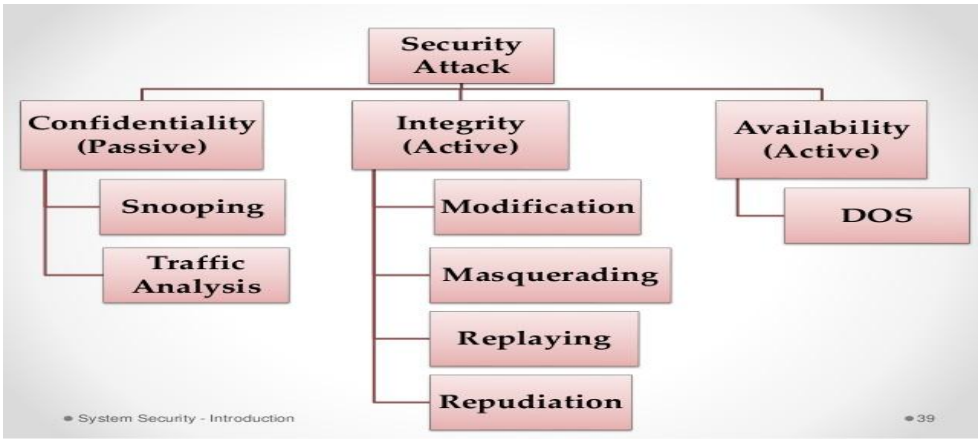
- **Passive Attacks**
  - **Release of message contents** for a telephone conversion, an electronic mail message, and a transferred file are subject to these threats
  - **Traffic analysis:-** By analyzing the traffic flow between sender and receiver third party access the data
- **Active Attacks**
  - **Masquerade** takes place when one entity pretends to be a different entity
  - **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect
  - **Modification** of messages means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect
  - **Denial of service** prevents or inhibits the normal use or management of communications facilities
    - Disable network or overload it with messages

Passive VS Active Attacks

Passive Attacks

- To obtain information that is being transmitted.
- E.g. Release of confidential information and Traffic analysis
- Difficult to detect
- Initiative to launch an active attack
- Interception
- Relieved by using encryption

- **Active Attacks**
  - Involve modification of the data stream or creation of a false stream
  - E.g. Masquerade, replay, message modification, denial of services
  - Potentially detected by security mechanisms
  - Interruption, Modification, Fabrication



1. **Masquerade attack**

Masquerade

A masquerade is a type of attack where the attacker act as an authorized user system in order to gain access to it or to gain greater privileges than they are authorized for.

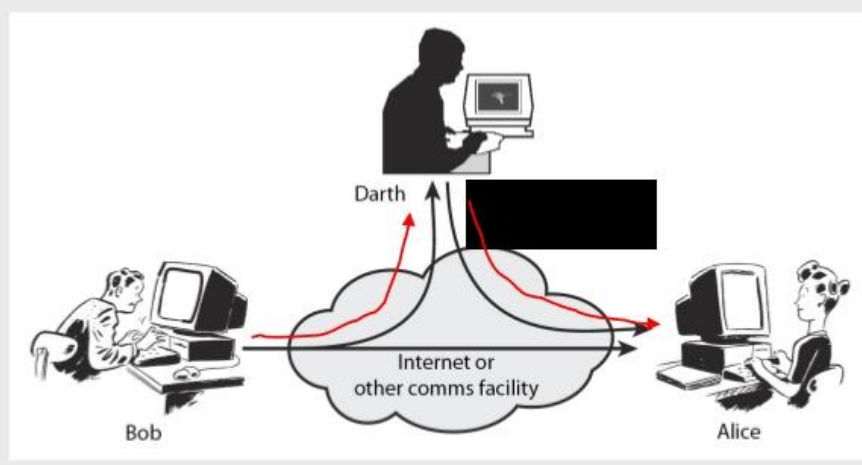
The third party sends the same message to the receiver and receiver receives it with the name of sender.

2. **Replay attack**

- Here receiver receives two messages. One from sender and another from third party.
- Receiver did not know which one is correct

3. **Data Modification attack**

- Modification is integrity violation.
- An unauthorized party not only gains access to but tampers with an asset.
- This is an attack on the integrity.
- Examples include changing values in a data file, altering a program so that it performs differently, and modifying the content of a message being transmitted in a network.

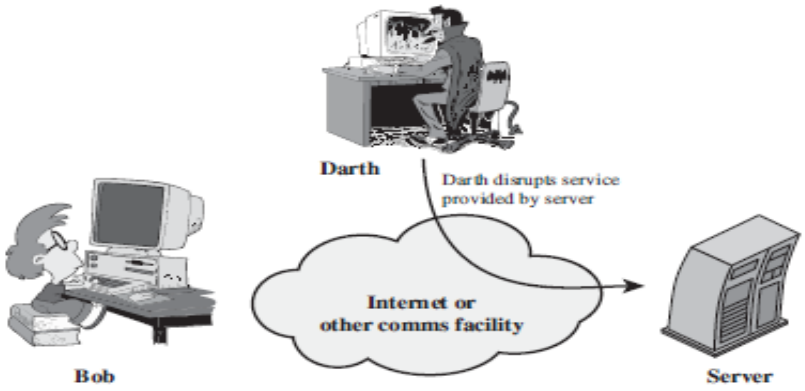


4. **Denial of Service**

- A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service.
- In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses.
- The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection.

- When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy.

- Here the third party interrupts (disrupts) the services sends by the server.
- Disruption of entire network either by disabling the network or by overloading it with message , so as to degrade performance



(d) Denial of service

-

MALICIOUS CODE (MALWARE)

- It is a software written into intentionally cause undesirable effect
- Can do anything that a normal program can do
- Designed to damage a computer system without owners concern
- Gets installed in your device and perform unwanted tasks
- Mainly designed to transmit information about your web browsing.
- It comes from different sources such as website, email, physical media etc
- In some cases it spreads itself to other computers though email or infected discs.

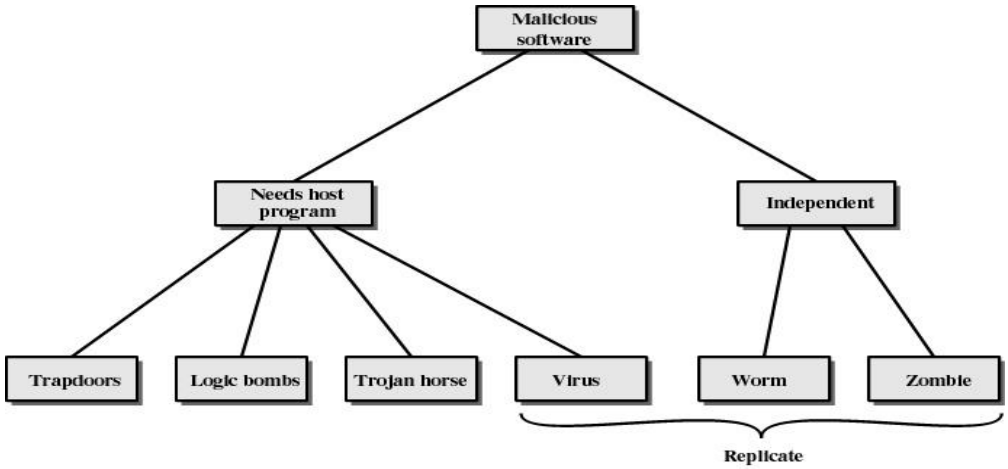


Figure 15.7 Taxonomy of Malicious Programs

- Malware or Malicious software is software designed to damage a computer system without the owner's concerns.

- Malicious software includes Virus, Worm, Trojan, Adware, Root kit, Spyware and many other unwanted software.

Common forms of malware

1. **Viruses**
   - Program that can "infect" other programs by modifying them
     - Modification includes copy of virus program
     - The infected program can infect other programs
   - A computer virus is a program code that can copy itself and infect a computer **without the permission of the user.**
   - It require user intervention
   - In order to replicate itself, a virus must be permitted to execute and write to memory.
   - For this reason, many viruses attach themselves to an executable files that may be part of legitimate programs. Some viruses change its own code by itself.
   - Viruses spread via network, floppy disk, CDs, USB drive.

Symptoms of a virus attack

- Changes file size.
- Change system date and time.
- Slow down the computer.
- Shut down computer unexpectedly.
- Take more time to boot computer.

2. **Worms**
   - It is a self-replicating computer program.
   - It uses a network to send copies of itself to other systems and it may do so **without any user intervention.**
   - Unlike a virus, it does not need to attach itself to an existing program.
   - Use network connections to spread form system to system

Properties of worm

- Electronic mail facility
  - A worm mails a copy of itself to other systems
- Remote execution capability
  - A worm executes a copy of itself on another system
- Remote log-in capability
  - A worm logs on to a remote system as a user and then uses commands to copy itself from one system to the other

3. **Trojan Horse**

   Useful program that contains hidden code that when invoked performs some unwanted or harmful function

Can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly

- User may set file permission so everyone has

Symptoms when Trojan horse affects the computer:

- Sending the user's important details to others.
- Changing or deleting data of the computer.
- Uploading and downloading data in an unauthorized way.
- Spreading malware such as viruses.
- Shutting down the computer unexpectedly.
- Unauthorized Software installation.

4. Trapdoor

A computer trapdoor, also known as a back door, provides a secret -- or at least undocumented -- method of gaining access to an application, operating system or online service.

- Entry point into a program that allows someone who is aware of trapdoor to gain access
- used by programmers to debug and test programs
  - Avoids necessary setup and authentication
  - Method to activate program if something wrong with authentication procedure

5. Logic Bomb

Code embedded in a legitimate program that is set to "explode" when certain conditions are met

- Presence or absence of certain files
- Particular day of the week

6. Spyware

• Software that is installed into a computer without the user's knowledge.

• Transmits information about the user's computer, and user activities over the Internet.

• Redirect to sites which spoil the culture and the computer.

Symptoms when Spy ware affects to your computer:

- Sending user's important data to others.
- Unauthorized Software installation.
- Redirect Web browser to dangerous web sites.
- Change Computer settings.
- Using anti-spyware we can minimize the damages.

7. Time Bomb

• This is simply some code on a computer which does not immediately trigger.

• Instead, it is set to cause it's damage at some point in the future.

• Usually Time bombs are designed to take revenge towards a company or an organization. E.g.: Sending messages such as "You are a great FOOL!!!!" on April first. OR "Am the vampire who suck ur blood" at 12 P.M

Differences: Virus, Trojan, Worm

1. Worms are programs that replicate themselves from system to system without the use of a host file.

2. This is in contrast to viruses, which requires the spreading of an infected host file.

3. A very important distinction between Trojan horse programs and true viruses is that they do not replicate themselves.

4. Another very important distinction between Trojan horse programs and worms or viruses is that Trojans need user activation of programs (Like: opening infected attach files)

DELIBERATE SOFTWARE ATTACKS

- Deliberate software attacks occur when an individual or group designs and use software to attack a system.
- Most of this software is referred to as malicious code or malicious software, or sometimes malware.
- These software components or programs are designed to damage, destroy, or deny service to the target systems.
- Some of the more common instances of malicious code are viruses and worms, Trojan horses, logic bombs, and back doors.

DEVIATIONS IN QUALITY OF SERVICE

- An organization's information system depends on the successful operation of many interdependent support systems, including power grids, telecom networks, parts suppliers, service vendors etc.
- Any one of these support systems can be interrupted by storms, employee illnesses, or other unforeseen events.
- The backup provider may be online and in service, but may be able to supply only a fraction of the bandwidth the organization needs for full service.
- This degradation of service is a form of availability disruption.

- Irregularities in Internet service, communications, and power supplies can dramatically affect the availability of information and systems.

Internet Service Issues

- In organizations that rely heavily on the Internet and the World Wide Web to support continued operations, Internet service provider failures can considerably undermine the availability of information.
- Many organizations have sales staff and telecommuters working at remote locations.
- When these offsite employees cannot contact the host systems, they must use manual procedures to continue operations.
- When an organization places its Web servers in the care of a Web hosting provider, that provider assumes responsibility for all Internet services as well as for the hardware and operating system software used to operate the Web site.
- These Web hosting services are usually arranged with an agreement providing minimum service levels known as a Service Level Agreement (SLA).
- When a service provider fails to meet the SLA, the provider may accrue fines to cover losses incurred by the client

Communications and Other Service Provider Issues

- Other utility services can affect organizations as well.
- Among these are telephone, water, wastewater, trash pickup, cable television, natural or propane gas, and custodial services.
- The loss of these services can impair the ability of an organization to function.
- For instance, most facilities require water service to operate an air-conditioning system.

Power Irregularities

- Irregularities from power utilities are common and can lead to fluctuations such as power excesses, power shortages, and power losses.
- This can pose problems for organizations that provide inadequately conditioned power for their information systems equipment
- A momentary low voltage or sag, or a more prolonged drop in voltage, known as a brownout, can cause systems to shut down or reset, or otherwise disrupt availability.
- Complete loss of power for a moment is known as a fault, and a more lengthy loss as a blackout.
- Because sensitive electronic equipment—especially networking equipment, computers, and computer-based systems—are vulnerable to fluctuations, controls should be applied to manage power quality. With small computers and network systems, quality power-conditioning options such as surge suppressors can smooth out spikes.
- The more expensive uninterruptible power supply (UPS) can protect against spikes and surges as well as against sags and even blackouts of limited duration.

BRUTE FORCE ATTACK

- Brute force attack is one in which hackers try a large number of possible keyword or password combinations to gain unauthorized access to a system or file
- Brute force attacks are often used to defeat a cryptographic scheme, such as those secured by passwords.
- Hackers use computer programs to try a very large number of passwords to decrypt the message or access the system
- Here attacker first gather information about user such as user full name, room no, vehicle no etc
- Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.
- A brute force attack is also known as brute force cracking or simply brute force.

Way of work

• A Brute Force Attack simply uses the cryptography algorithm.

• When we attempt to login and our page request is sent from the server to the client machine hackers are more active to access the account.

• They attempt all possible combinations to unlock it.

• There is a computer program that runs automatically to get the password.

The characteristics:-

- Need very high processing speed

- Produces many number of passwords for a particular user using permutations and combinations May take months years to crack the password

• It is a fairly simplistic attack that doesn't require a lot of work to setup or initiate.

Disadvantage:

- Hardware intensive : consume lots of processing power
- Extends the amount of time needed to crack the code by huge margin.

Password Length Guesses

2 characters = 3,844 guesses because of:

First character: lower case letters (26) + upper case letters (26) + numbers (10) = 62

Second character: same = 62

Total permutations = 62*62 = 3,844

How Can Prevent It?

- Password Length.
- Password Complexity.
- Limit Login Attempts.
- Using Captcha.
- Two Factor Authentication.

Password Length:

The first step towards Brute Force Attack prevention should be longer password length. Nowadays many websites and platforms enforce their users to create a password of certain length (8 – 16 characters).

Password Complexity:

Another important thing is to create a complex password. It is not recommended to create passwords like 'ilovemycountry' or 'password123456'; instead your password should consist of UPPERCASE and lowercase alphabets and should also have numbers and special characters. Complexity of the password delays the cracking process.

Limit Login Attempts:

Simple yet very powerful action is to limit the login attempts on your WordPress admin or any other admin panel for that matter. For example if your website receives five failed login attempts; it should block that IP for a certain period of time to stop further attempts being made.

Using Captcha:

Captchas are now commonly used in websites. They prevent bots from executing automated scripts mainly used in Brute Force attack. Installing captcha in your WordPress site is fairly easy.

Two Factor Authentication:

this adds a layer of security to the primary form of authentication. Two-factor security requires two forms of authentication

Other best practices are:

- Unique password for each account.
- Frequent password change.
- Avoid sharing credentials through insecure channels.

One example of a type of brute force attack is known as a **dictionary attack**, which might try all the words in a dictionary.

Credential recycling is a form of brute force attacks where usernames and passwords from previous attacks are used.

Hybrid Brute force attack is another form of attack, here attacker slightly modifies the dictionary words and peform attack.

SNIFFERS

A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets.

If the packets are not encrypted, a sniffer provides a full view of the data inside the packet.

Using a sniffer, an attacker can do any of the following:

- Analyze your network and gain information to eventually cause your network to crash or to become corrupted.
- Read your communications.

Sniffing motives:

- Getting username an passwords
- Stealing bank related/transaction related information
- Spying on email and chat messages
- Identity theft

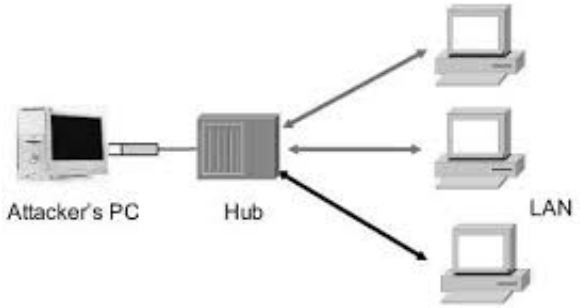
Types of Sniffing

There are two types of sniffing- **active and passive**. As the name suggests, active involves some activity or interaction by the attacker in order to gain information. In passive the attacker is just hiding dormant and getting the information.

Passive Sniffing:

This kind of sniffing occurs at the hub. A hub is a device that received the traffic on one port and then retransmits that traffic on all other ports.

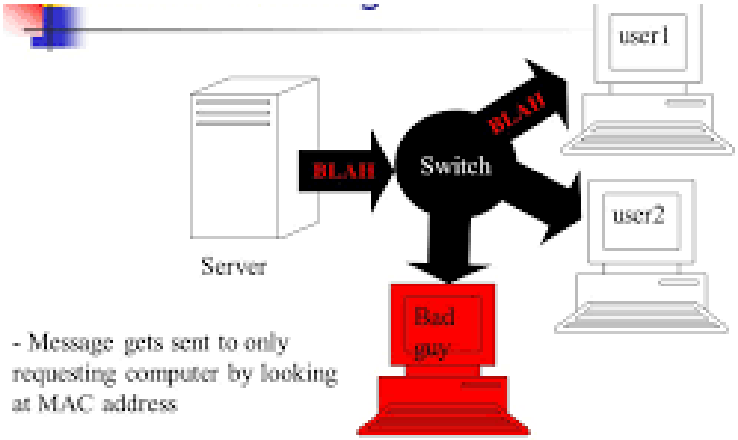
In this case, if a sniffer device is placed at the hub then all the network traffic can be directly captured by the sniffer. The sniffer can sit there undetected for a long time and spy on the network. Since hubs are not used these days much, this kind of attack will be an old-school trick to perform. Hubs are being replaced by switches and that is where active sniffing comes into the picture.



Active Sniffing:

A switch learns a CAM (Content Addressable Memory) table that has the MAC addresses of the destinations. Basis this table the switch is able to decide what network packet is to be sent where.

In active sniffing, the sniffer will flood the switch with bogus requests(fake request) so that the CAM table gets full. Once the CAM is full the switch will act as a switch and send the network traffic to all ports. Now, this is legitimate traffic that gets distributed to all the ports. This way the attacker can sniff the traffic from the switch.



Types of Sniffer Attacks

- **LAN Sniffing:** In this, the sniffer software is installed on the internal LAN to scan the entire network exhaustively. This helps to provide further information such as server inventory, live hosts, open ports etc.
- **Protocol Sniffing:** This method involves creating separate sniffers to carry out attacks on different network protocols. For instance, if a hacker sees UDP packets in a network, a separate sniffer is started to capture information.
- **ARP Sniffing:** The hackers steal all the important information related to the IP addresses and its associated MAC addresses. This data is further used to initiate packet spoofing attacks, ARP poisoning attacks or exploit vulnerabilities in the network router.
- **TCP Session Sniffing:** This is a basic sniffer attack in which the hackers get hold of the traffic between the source and destination IP address. They target details like service types, port numbers and TCP sequence numbers to create and control a fabricated TCP session.
- **Web Password Sniffing:** In these sniffer attacks, the hackers penetrate the HTTP sessions that do not use secure encryption. Following this, the user IDs and passwords can be stolen and used for malicious purposes.

Tips To Protect Against Sniffer Attacks

- Enable a WPA or WPA2 (Wi-Fi Protected Access) encryption for your router. Also, make sure you change its default password to limit access to your network. Use a long and secure password consisting of numbers, uppercase letters, lowercase letters and symbols.
- Use MAC filtering on your network. You must allow only trusted MAC addresses to access your private VPN, thus, reducing the chances of a sniffer spying on the network.
- Ensure that the important sites you use, particularly those that involve making financial transactions, have SSL (Secure Socket Layer) encryption. If a site is SSL enabled, it will have a URL beginning with HTTPS instead of HTTP.

TIMING ATTACKS

Basic idea: learn the system's secret by observing how long it takes to perform various computations

- It is a security exploit that allows an attacker to discover vulnerabilities (weakness of the system) in the security of computer or network system by studying how long it takes the system to respond to different inputs.
- Timing characteristics will vary depending upon encryption key because different systems take slightly different amount of time to process different inputs.

Typical goal: extract private key

- Extremely powerful because **isolation** doesn't help
  - Victim could be remote
  - Victim could be inside its own virtual machine
  - Keys could be in tamper-proof storage or smartcard
- Attacker wins simply by measuring response times

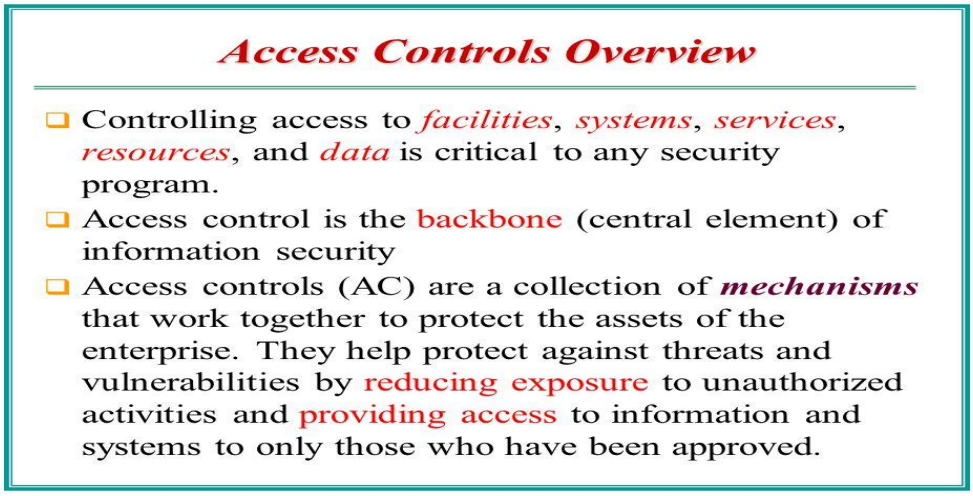
ACCESS CONTROL MECHANISMS

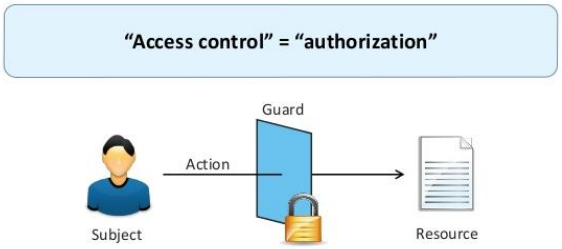
Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

Access control is restricting access to a system or system resources based on something other than the identity of the user

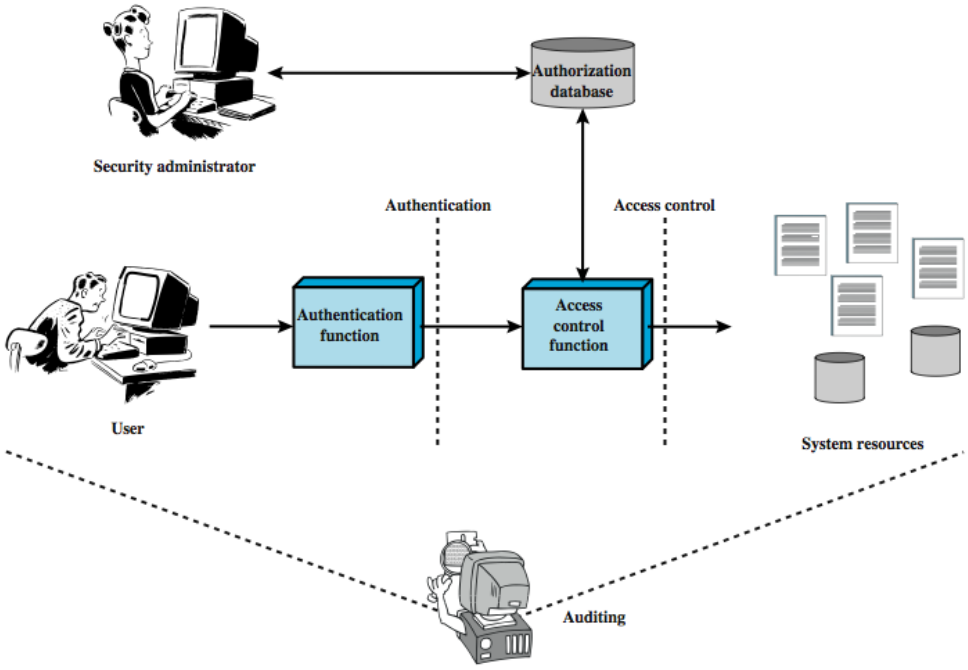
- Minimize the risk of unauthorized access

- "The prevention of unauthorized use of a resource, in an unauthorized manner"





–



Access control is the intermediate layer between malicious user and protected system

- Access control consists of four elements:
  - subjects,
  - objects,
  - operations,
  - a reference monitor
- Subjects are system users and groups of users while objects are files and resources such as memory, printers, and scanners including computers in a network.
- An access operation comes in many forms including Web access, server access, memory access, and method calls.
- The job of the reference monitor is to check on the hierarchy of rules that specify certain restrictions

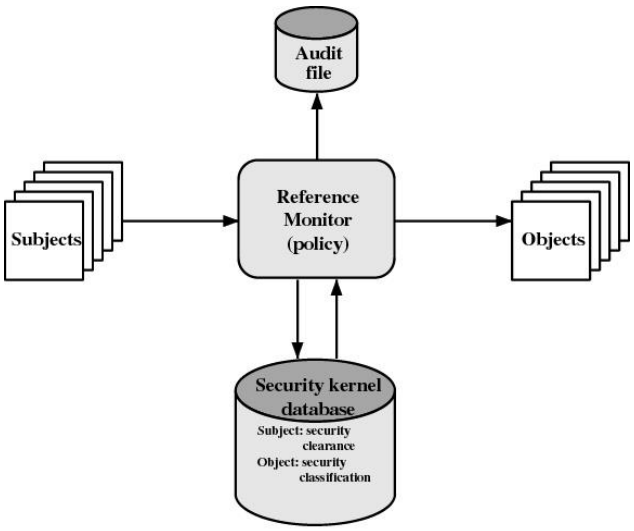


Figure 15.9 Reference Monitor Concept

- Whenever a subject requests to access an object, an access mode must be specified.
- There are two access modes:
  - **Observe** - in this mode, the subject may only look at the content of the object. This mode is the typical read in which a client process may request a server to read from a file.
  - **Alter** – in this mode, the subject may change the content of the object

For example a user, initiates an access request for a specified system resource, usually a passive object in the system such as a Web resource. The request goes to the reference monitor. The job of the reference monitor is to check on the hierarchy of rules that specify certain restrictions. A set of such rules is called an *access control list* (ACL).

The access control hierarchy is based on the URL path for a Web access, or file path for a file access such as in a directory. When a request for access is made, the monitor or server goes in turn through each ACL rule, continuing until it encounters a rule that prevents it from continuing and results in a request rejection or comes to the last rule for that resource, resulting into access right being granted.

- Access rights refer to the user's ability to access a system resource.
- There are four access rights:
  - *execute,*
  - *read,*
  - *append,*
  - *write.*
- The user is cautioned not to confuse access rights and access modes.
- The difference lies in the fact that you can perform any access right within each access mode.
- Access rights can be set individually on each system resource for each individual user and group.
- Who sets these rights? - The owner of the resource sets the access rights to the resource.
- In a global system, the operating systems own all system resources and therefore sets the access rights to those resources. However, the operating system allows folders and file owners to set and revoke access rights.

Access Control List

Access control list (ACL) refers to the permissions attached to an object that specify which users are granted access to that object and the operations it is allowed to perform.

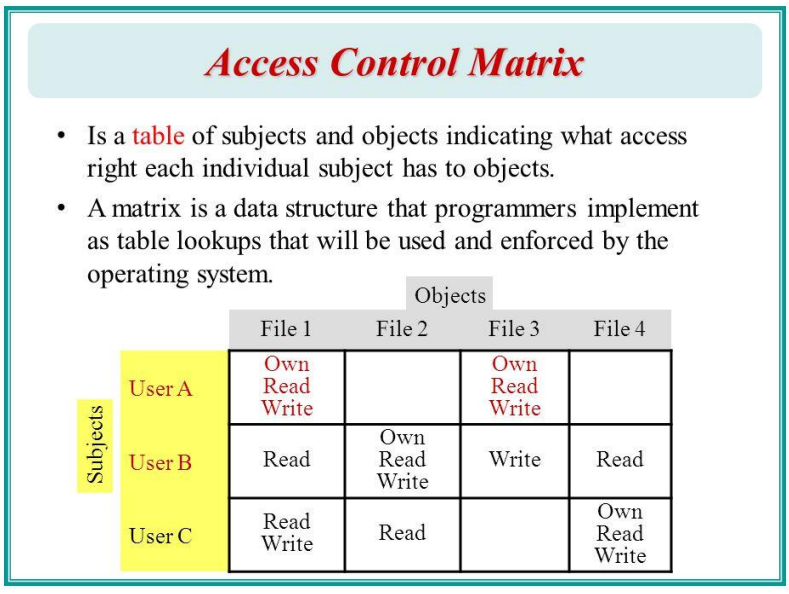
Each entry in an access control list specifies the subject and an associated operation that is permitted. File system ACL is a data structure that holds entries that specify individual user or group rights to system objects such as processes, files and programs. These entries are referred to as access control entities. Each system object is associated with a security attribute that identifies its access control list.

The ACL has an entry for each system user that defines the user's privileges, such as reading a file, writing to a file or executing a file.

When a subject requests an object in an ACL-based security model, the OS initially checks the ACL for an applicable entry to decide whether the requested operation is authorized. The ACL model is applicable to both individual entities and the collection of objects within the system hierarchy.

ACCESS CONTROL MATRIX

- All the information needed for access control administration can be put into a matrix with rows representing the subjects or groups of subjects and columns representing the objects.
- The access that the subject or a group of subjects is permitted to the object is shown in the body of the matrix.
- It is a table of subjects and objects indicating what actions individual subjects can take upon individual objects.
- For example, in the matrix in Figure, user B has permission to read in file R4.
- The entry access(i,j) defines the set of operations that a process executing in Subject i can invoke on Object j
- One feature of the access control matrix is its sparseness. Because the matrix is so sparse, storage consideration becomes an issue, and it is better to store the matrix as a list.



Implementation of Access control matrix

Access control can be implemented in three ways

1. Global table
2. Access lists for objects
3. Capability list for subjects

Global Table

The simplest implementation of the access matrix

Table consists of set of ordered triples<Subject, object, right set>

Whenever an operation M is executed on object(Oj) with subject(Si) then a global table is searched for triple <Si, Oj, Rk> If found, operation is allowed to continue otherwise it deny access

It has several disadvantage usually large thus cannot be kept in main memory.

Access lists for objects

Access Control Lists (ACLs)

• Focus on the object

ACLs ≡ columns of the access control matrix Oj <Si , Rk>

• ACL define all domain with non empty set of access rights for that object

• Access rights are often defined for groups of users

– Because individual subjects may create a huge list

Capability List

• Focus on the subject

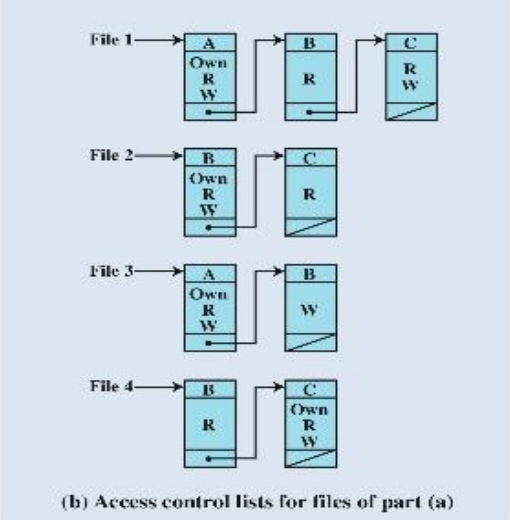
Capabilities list ≡ rows of the access control matrix

• Capability is pointer to the object, contain address of the object

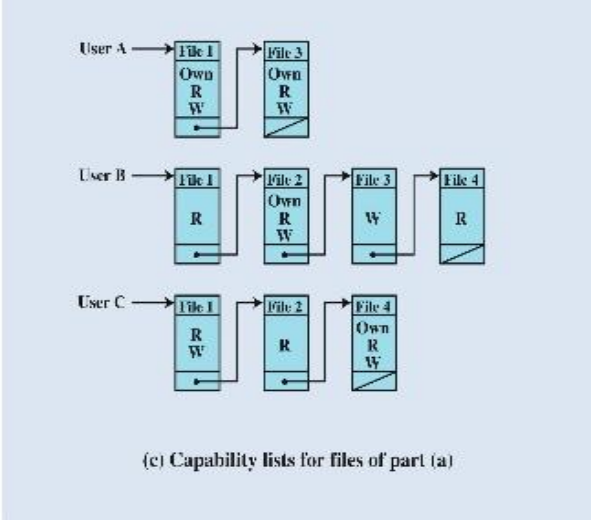
• Each domain has its capability list which contain list of capability together with operation allowed

• Capability list is itself a protected object

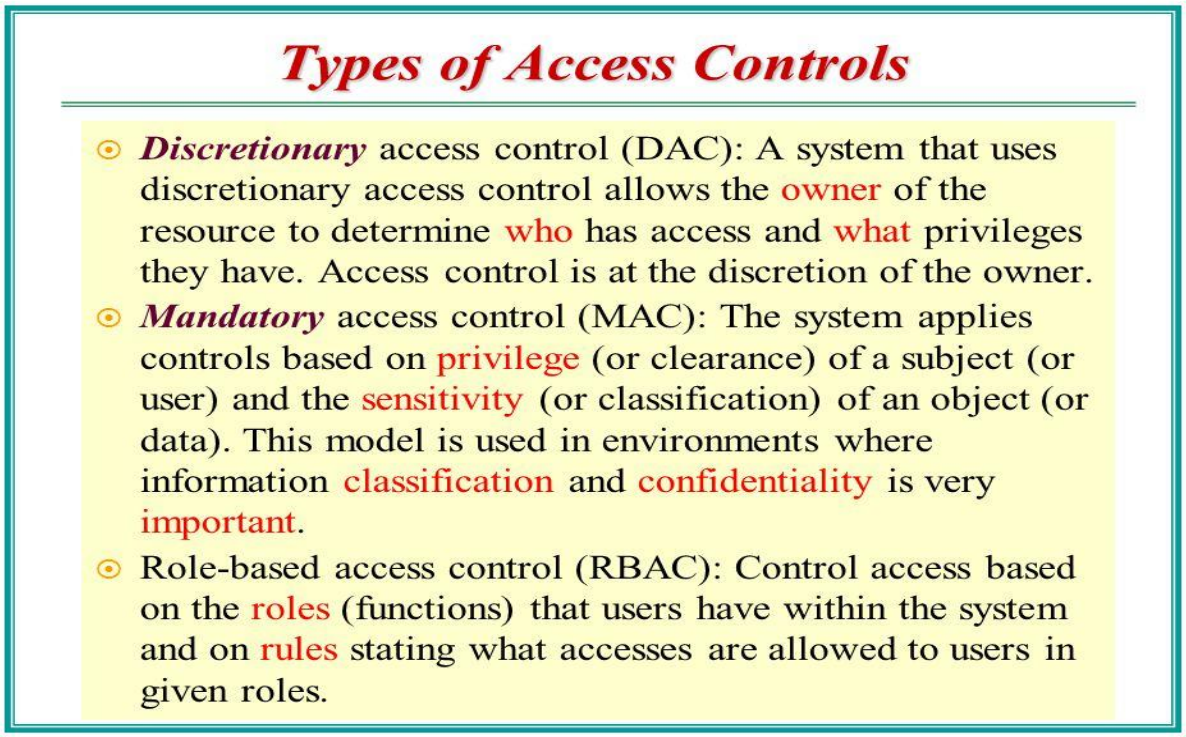
- Maintained by operating system
- Accessed by user only indirectly



(b) Access control lists for files of part (a)



(c) Capability lists for files of part (a)



Discretionary access control (DAC): based on the identity of the requestor and access rules

Permissions are set *at the discretion* of the resource owner

- Highly flexible policy, where permissions can be transferred
- Lack of central control makes revocation or changes difficult

Discretionary acces control in use

- Controlling access to files
  - E.g., Windows Access Control Lists (ACL), UNIX file handles
- Controlling the sharing of personal information
  - E.g.. Social networks

- This is a mechanism grants access privileges to users based on control policies that govern the access of subjects to objects using the subjects' **identity and authorization rules**.
- These mechanisms are discretionary in that **they allow subjects to grant other users authorization to access the data**.
- They are highly flexible, making them suitable for a large variety of application domains.
- However, the same characteristics that make them flexible also make them vulnerable to malicious attacks, such as Trojan Horses embedded in application programs.
- The reason is that discretionary authorization models do not impose any control on how information is propagated and used once it has been accessed by users authorized to do so.
- A general approach to DAC is Access Control Matrix (**Write Access Control Matrix also in this topic)**

Mandatory access control (MAC): based on comparing security labels with security clearances (mandatory: **one with access to a resource cannot pass to others**)

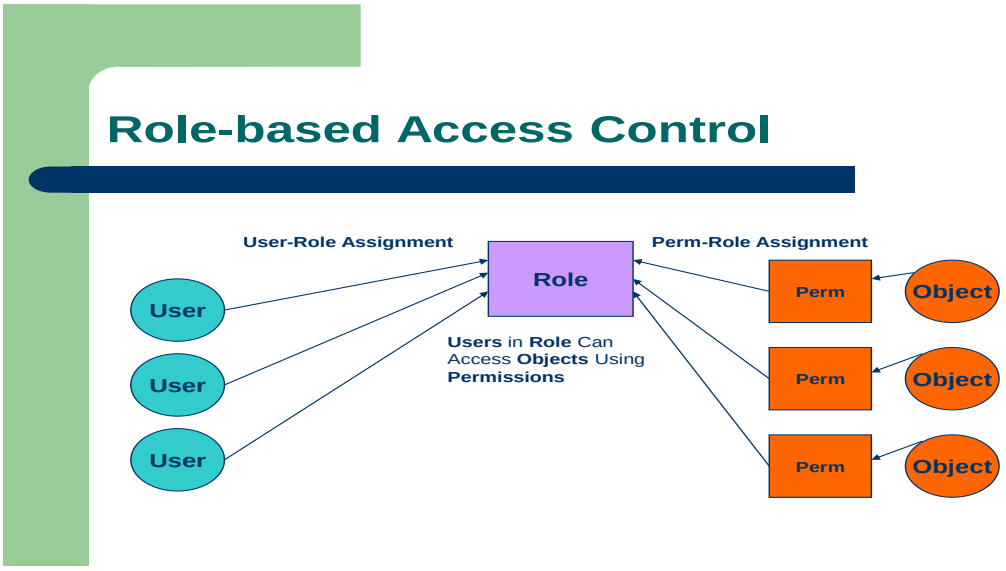
- Permissions are assigned by a central authority according to a central policy
  - Good fit within organizations with a strong need for central controls
  - Low flexibility and high management overhead
- Mandatory Access Control in use
  - Often linked to multi-level security systems -> see later on
    - E.g. Government-regulated secrecy systems, military applications
  - Modern operating systems, to separate applications and processes
    - E.g. Windows' *Mandatory Integrity Control*, SELinux, TrustedBSD

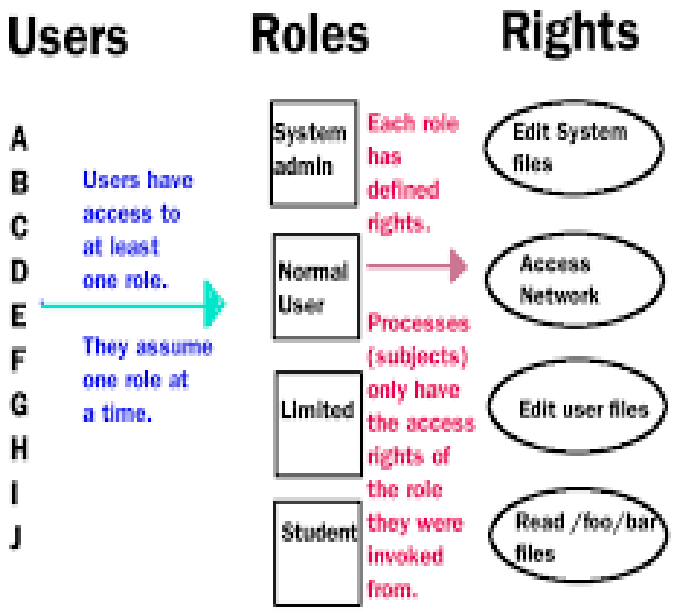
- Mandatory policies, unlike the discretionary ones seen above, ensure a high degree of protection in that they prevent any illegal flow of information through the **enforcement of multilevel security** by classifying the data and users into various security classes.
- They are, therefore, suitable for contexts that require structured but graded levels of security such as the military.
- However, mandatory policies have the drawback of being too rigid, in that they require a strict classification of subjects and objects in security levels, and are, therefore, applicable only to very few environments.

- opposite of DAC and is most restrictive access control model
- MAC assigns users' access controls strictly according to custodian's desires and user has no freedom to set any controls
- **two key elements to MAC**:
  - labels - every entity is an object (laptops, files, projects, and so on) and assigned classification label (confidential, secret, and top secret) while subjects assigned privilege label (a clearance)
  - levels - hierarchy based on labels is also used, both for objects and subjects (top secret higher level than secret)
- **major implementations**
  - lattice model - subjects and objects are assigned "rung" on lattice and multiple lattices can be placed beside each other
  - bell-lapadula - similar to lattice model but subjects may not create new object or perform specific functions on lower level objects
  - biba integrity model - goes beyond blp model and adds protecting data integrity and confidentiality
  - mandatory integrity control (mic) - based on biba model, mic ensures data integrity by controlling access to securable objects

Role-based access control (RBAC): based on user roles

- The changing size and technology of computer and communication networks are creating complex and challenging problems in the security management of these large networked systems.
- The changing technology and large numbers of users joining the networks are making the administration of systems extremely costly and prone to error when it is based solely on access control lists for each user on the system individually.
- System security in role-based access control (RBAC) is based on roles assigned to each user in an organization. For example, one can take on a role as a chief executive officer, a chief information officer, or chief security officer.
- A user may be assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. Access decisions are then based on the roles individual users have as part of an organization.
- The process of defining roles is based on a thorough analysis of how an organization operates and include input from a wide spectrum of users in an organization.
- Access rights are grouped by role name, and the use of resources is restricted to individuals authorized to assume the associated role.
- Users are granted membership into roles based on their competencies and responsibilities in the organization.
- The types of operations that a user is permitted to perform in the role he or she assumes are based on that user's role. User roles are constantly changing as the user changes responsibilities and functions in the organizations, and these roles can be revoked.
- Role associations can be established when new operations are instituted, and old operations can be deleted as organizational functions change and evolve.
- RBAC is also based on the concept of least *privilege* that requires identifying the user's job functions, determining the minimum set of privileges required to perform that function, and restricting the user to a domain with those privileges and nothing more.





OBJECTS

ROLES	R_1	R_2	R_n	F_1	F_2	P_1	P_2	D_1	D_2
R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R_2		control		write *	execute			owner	seek *
• • •									
R_n			control		write	stop			

Figure 4.8 **Access Control Matrix Representation of RBAC**

Access Control in Operating System

Access control for an operating system determines how the operating system implements accesses to system resources by satisfying the security objectives of integrity, availability, and secrecy. Such a mechanism authorizes subjects (e.g., processes and users) to perform certain operations (e.g., read, write) on objects and resources of the OS (e.g., files, sockets).

For example, in the case of an operating system, the subjects are users and the objects are files, programs, peripheral devices, etc.,

An Access Control Matrix is a table that maps the permissions of a set of subjects to act upon a set of objects within a system. The matrix is a two-dimensional table with subjects down the columns and objects across the rows. The permissions of the subject to act upon a particular object are found in the cell that maps the subject to that object.