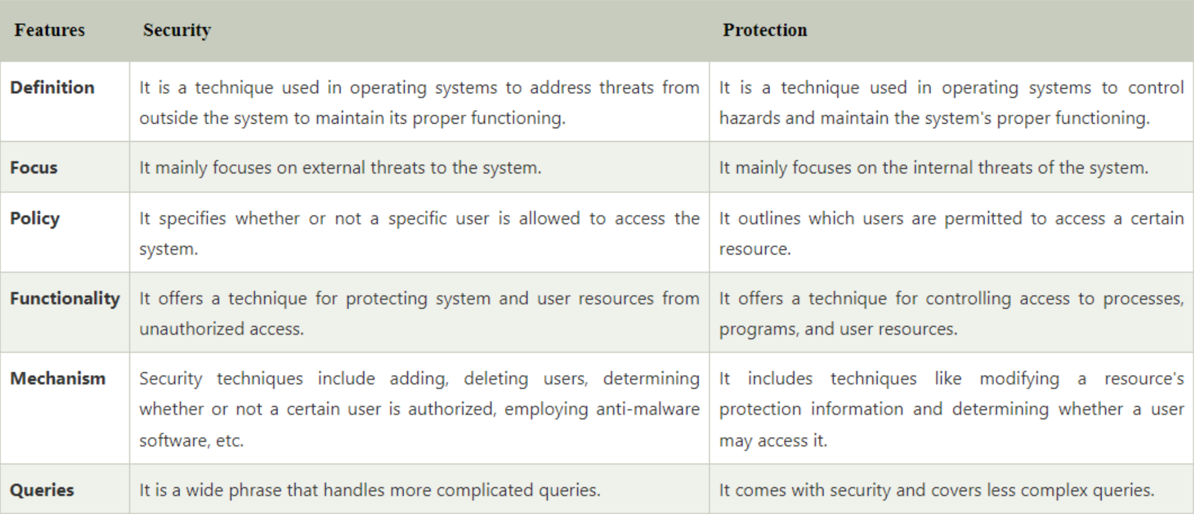
OPERATING SYSTEM – UNIT 3 – IMP QUES

Note: ** mean important

Q1. What is protection and security? and differentiate between them.

->



Features	Security	Protection
Definition	It is a technique used in operating systems to address threats from outside the system to maintain its proper functioning.	It is a technique used in operating systems to control hazards and maintain the system's proper functioning.
Focus	It mainly focuses on external threats to the system.	It mainly focuses on the internal threats of the system.
Policy	It specifies whether or not a specific user is allowed to access the system.	It outlines which users are permitted to access a certain resource.
Functionality	It offers a technique for protecting system and user resources from unauthorized access.	It offers a technique for controlling access to processes, programs, and user resources.
Mechanism	Security techniques include adding, deleting users, determining whether or not a certain user is authorized, employing anti-malware software, etc.	It includes techniques like modifying a resource's protection information and determining whether a user may access it.
Queries	It is a wide phrase that handles more complicated queries.	It comes with security and covers less complex queries.

____

**Q2. What is access matrix? How it is implemented?

->

Access Matrix is a security model of protection state in computer system. It is represented as a matrix.

Access matrix is used to define the rights of each process executing in the domain with respect to each object.

The rows of matrix represent domains and columns represent objects. Each cell of matrix represents set of access rights which are given to the processes of domain means each entry (i, j) defines the set of operations that a process executing in domain Di can invoke on object Oj.

<u>There are various methods of implementing the access matrix in the operating system. These methods are as follows:</u>

1. **<u>Global Table</u>**

It is the most basic access matrix implementation. A set of ordered triples **<domain, object, rights-set>** is maintained in a file. When an operation **M** has been performed on an object Oj within domain Di, the table is searched for a triple **<Di, Oj, Rk>.** The operation can proceed if this triple is located; otherwise, an exception (or error) condition has arrived. This implementation has various drawbacks. The table is generally large and cannot be stored in the main memory, so additional input and output are required.

2. **Access Lists for Objects**

   Every access matrix column may be used as a single object's access list. It is possible to delete the blank entries. For each object, the resulting list contains ordered pairs **<domain, rights-set>** that define all domains for that object and a nonempty set of access rights.

   We may start by checking the default set and then find the access list. If the item is found, we enable the action; if it isn't, we verify the default set. If M is in the default set, we grant access. Access is denied if this is not the case, and an extraordinary scenario arises.

3. **Capability Lists for Domains**

   A domain's capability list is a collection of objects and the actions that can be done on them. A capacity is a name or address that is used to define an object. If you want to perform operation M on object **Oj,** the process runs operation M, specifying the capability for object **Oj.** The simple possession of the capability implies that access is allowed.

   In most cases, capabilities are separated from other data in one of two ways. Every object has a tag to indicate its type as capability data. Alternatively, a program's address space can be divided into two portions. The programs may access one portion, including the program's normal instructions and data. The other portion is a capability list that is only accessed by the operating system.

4. **Lock-Key Mechanism**

   It is a compromise between the access lists and the capability lists. Each object has a list of locks, which are special bit patterns.

   On the other hand, each domain has a set of keys that are special bit patterns. A domain-based process could only access an object if a domain has a key that satisfies one of the locks on the object. The process is not allowed to modify its keys.

**Q3. Define program threats and system threats in OS.

->

Program threats

Operating system's processes and kernel do the designated task as instructed. If a user program made these process do malicious tasks, then it is known as **Program Threats**. One of the common examples of program threat is a program installed in a computer which can store and send user credentials via network to some hacker.

Following is the list of some well-known program threats.

- **Trojan Horse** − Such program traps user login credentials and stores them to send to malicious user who can later on login to computer and can access system resources.
- **Logic Bomb** − Logic bomb is a situation when a program misbehaves only when certain conditions met otherwise it works as a genuine program. It is harder to detect.
- **Virus** − Virus as name suggest can replicate themselves on computer system. They are highly dangerous and can modify/delete user files, crash systems. A virus is generally a small code embedded in a program. As user accesses the program, the virus starts getting embedded in other files/ programs and can make system unusable for user.

System threats

System threats refers to misuse of system services and network connections to put user in trouble. System threats can be used to launch program threats on a complete network called as program attack. System threats creates such an environment that operating system resources/ user files are misused. Following is the list of some well-known system threats.

- **Worm** − Worm is a process which can choked down a system performance by using system resources to extreme levels. A Worm process generates its multiple copies where each copy uses system resources, prevents all other processes to get required resources. Worm processes can even shut down an entire network.

**Q4. Explain Man-in-the-middle attack, Session hijacking, phishing attack, Masquerade attack.

->

Man in the middle (MITM) attack

A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.

The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications, SaaS businesses, e-commerce sites and other websites where logging in is required.

Session Hijacking

The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. A session token is normally composed of a string of variable width and it could be used in different ways, like in the URL, in the header of the http requisition as a cookie, in other parts of the header of the http request, or yet in the body of the http requisition.

The Session Hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server.

Phishing attack

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

Masquerade Attack

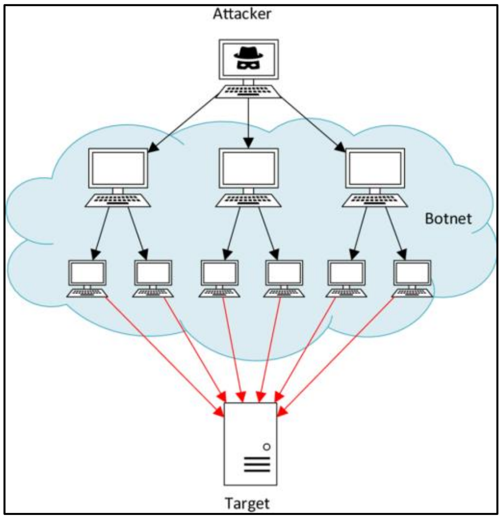
A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack.

**Q5. What is DDOS attack? How does it work? How to prevent it?

->

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic.



How does it work

Individual devices are referred to as bots (or zombies), and a group of bots is called a botnet. Once a botnet has been established, the attacker is able to direct an attack by sending remote instructions to each bot.

When a victim's server or network is targeted by the botnet, each bot sends requests to the target's IP address, potentially causing the server or network to become overwhelmed, resulting in a denial-of-service to normal traffic.

Because each bot is a legitimate Internet device, separating the attack traffic from normal traffic can be difficult.

How to prevent it

It can be prevented by following:

- Blackhole routing
- Rate limiting
- Web application firewall
- Anycast network diffusion

**Q6. Client Server architecture? Explain RPC (remote procedure call).

->

The client-server architecture refers to a system that hosts, delivers, and manages most of the resources and services that the client requests. In this model, all requests and services are delivered over a network, and it is also referred to as the networking computing model or client server network.

Advantages and Disadvantages of Client-Server Architecture

Advantages:

- It's a centralized system that keeps all the data and its controls in one place
- It brings a high level of scalability, organization, and efficiency
- It's cost-efficient, especially in terms of maintenance
- It allows data recovery

Disadvantages:

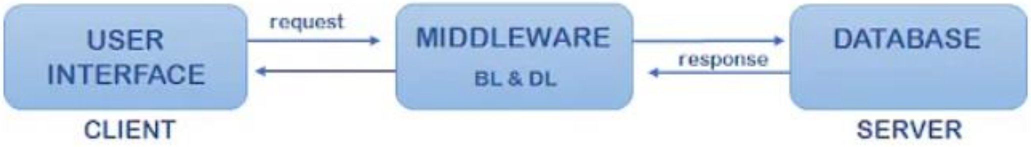
- The server is vulnerable to Denial of Service (DoS) attacks
- It's expensive to start up and initially implement
- If a critical server goes down, the clients are dead in the water
- The setup is prone to phishing and Man in the Middle (MITM) attacks

Three tier Client Server architecture

The three-tier client-server architecture consists of a presentation tier known as the User Interface layer, an application tier called the Service layer, and a data tier comprising the database server. Three-tier architecture can be divided into three parts:

- Presentation layer (or Client Tier): This layer takes care of the User Interface.
- Application layer (or Business Tier): This layer handles the detailed processing.
- Database layer (or Data Tier): This layer stores the information.

The Client system controls the Presentation layer; the Application server looks after the Application layer, and the Server system supervises the Database layer.



Remote Procedure Call

Remote Procedure Call is a software communication protocol that one program can use to request a service from a program located in another computer on a network without having to understand the network's details. RPC is used to call other processes on the remote systems like a local system. A procedure call is also sometimes known as a *function call* or a *subroutine call*.

RPC uses the client-server model. The requesting program is a client, and the service-providing program is the server.

When program statements that use the RPC framework are compiled into an executable program, a stub is included in the compiled code that acts as the representative of the remote procedure code. When the program is run and the procedure call is issued, the stub receives the request and forwards it to a client runtime program in the local computer. The first time the client stub is invoked, it contacts a name server to determine the transport address where the server resides.

**Q7. Differentiate between loosely coupled and tightly coupled.

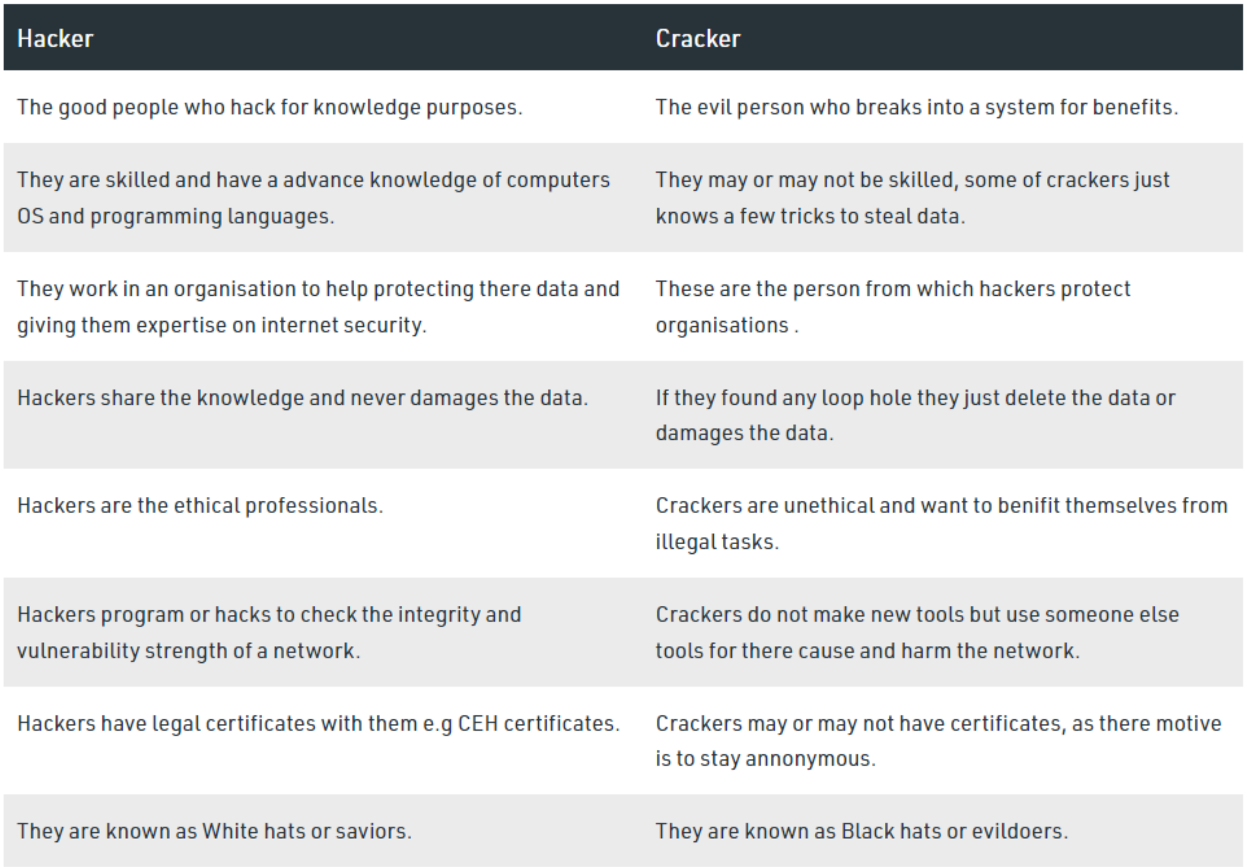
->

Loosely coupled	**Tightly coupled**
There is distributed memory in loosely coupled multiprocessor system.	There is shared memory, in tightly coupled multiprocessor system.

Loosely Coupled Multiprocessor System has low data rate.	Tightly coupled multiprocessor system has high data rate.
The cost of loosely coupled multiprocessor system is less.	Tightly coupled multiprocessor system is more costly.
In loosely coupled multiprocessor system, modules are connected through **Message transfer system** network.	While there is PMIN, IOPIN and ISIN networks.
In loosely coupled multiprocessor, Memory conflicts don’t take place.	While tightly coupled multiprocessor system have memory conflicts.
Loosely Coupled Multiprocessor system has low degree of interaction between tasks.	Tightly Coupled multiprocessor system has high degree of interaction between tasks.
In loosely coupled multiprocessor, there is direct connection between processor and I/O devices.	While in tightly coupled multiprocessor, IOPIN helps connection between processor and I/O devices.
Applications of loosely coupled multiprocessor are in distributed computing systems.	Applications of tightly coupled multiprocessor are in parallel processing systems.

Q8. Differentiate between hacker and cracker.

->

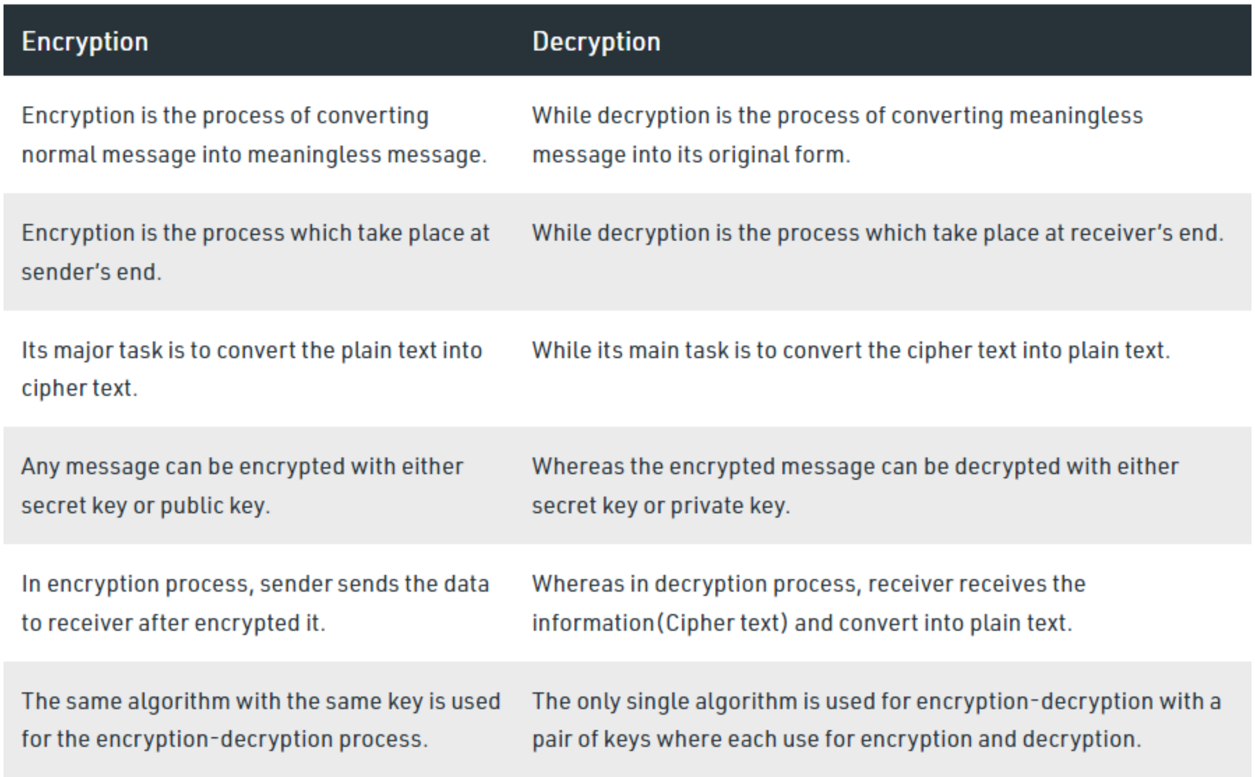


Hacker	Cracker
The good people who hack for knowledge purposes.	The evil person who breaks into a system for benefits.
They are skilled and have a advance knowledge of computers OS and programming languages.	They may or may not be skilled, some of crackers just knows a few tricks to steal data.
They work in an organisation to help protecting there data and giving them expertise on internet security.	These are the person from which hackers protect organisations .
Hackers share the knowledge and never damages the data.	If they found any loop hole they just delete the data or damages the data.
Hackers are the ethical professionals.	Crackers are unethical and want to benifit themselves from illegal tasks.
Hackers program or hacks to check the integrity and vulnerability strength of a network.	Crackers do not make new tools but use someone else tools for there cause and harm the network.
Hackers have legal certificates with them e.g CEH certificates.	Crackers may or may not have certificates, as there motive is to stay annonymous.
They are known as White hats or saviors.	They are known as Black hats or evildoers.

Q9. What is cryptography and state difference between encryption and decryption.

->

Cryptography is technique of securing information and communications through use of codes so that only those people for whom the information is intended can understand it and process it. Thus, preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.



Encryption	Decryption
Encryption is the process of converting normal message into meaningless message.	While decryption is the process of converting meaningless message into its original form.
Encryption is the process which take place at sender's end.	While decryption is the process which take place at receiver's end.
Its major task is to convert the plain text into cipher text.	While its main task is to convert the cipher text into plain text.
Any message can be encrypted with either secret key or public key.	Whereas the encrypted message can be decrypted with either secret key or private key.
In encryption process, sender sends the data to receiver after encrypted it.	Whereas in decryption process, receiver receives the information(Cipher text) and convert into plain text.
The same algorithm with the same key is used for the encryption-decryption process.	The only single algorithm is used for encryption-decryption with a pair of keys where each use for encryption and decryption.