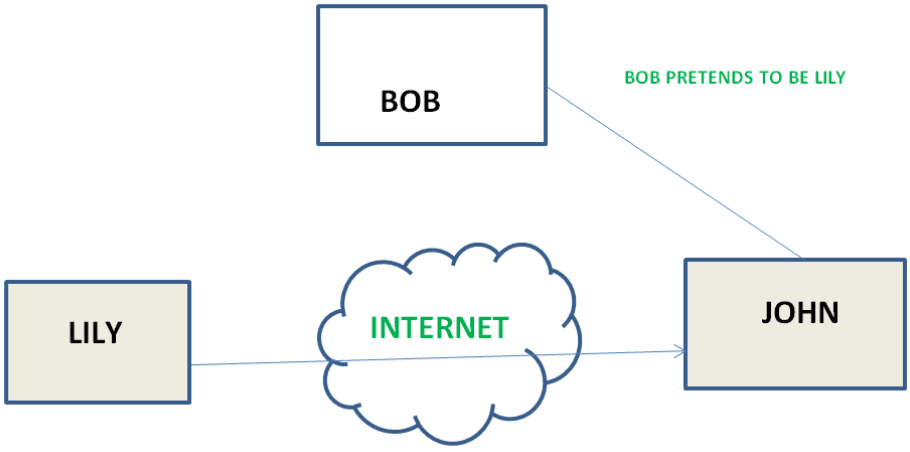
Attacks

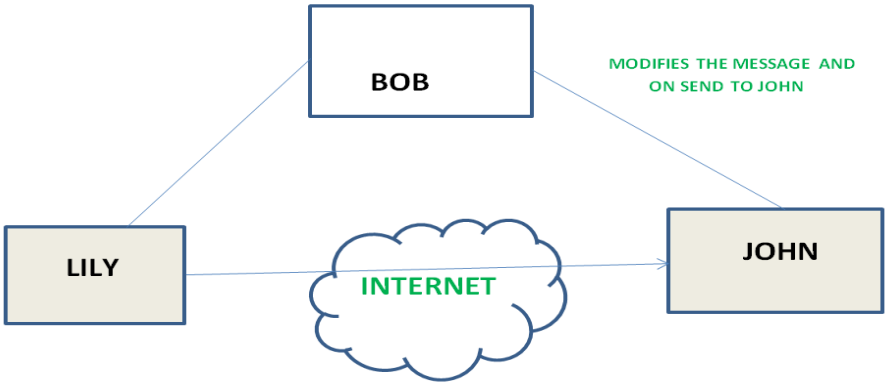
- Passive attacks
  - Interception
    - Release of message contents
    - Traffic analysis
- Active attacks
  - Interruption, modification, fabrication
    - Masquerade
    - Replay
    - Modification
    - Denial of service

***ACTIVE ATTACKS*:** An Active attack attempts to alter system resources or effect their operations. Active attack involve some modification of the data stream or creation of false statement. Types of active attacks are as following:

1. **Masquerade –**
   Masquerade attack takes place when one entity pretends to be different entity. A Masquerade attack involves one of the other form of active attacks.



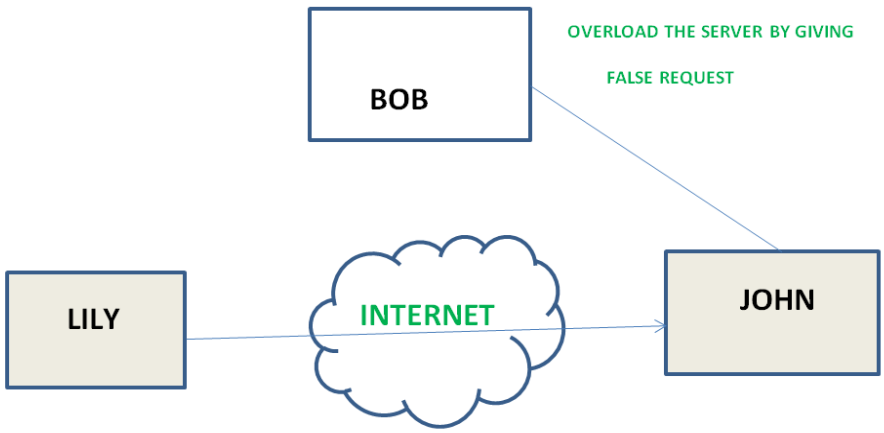
2. **Modification of messages –**
   It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorised effect. For example, a message meaning "Allow JOHN to read confidential file X" is modified as "Allow Smith to read confidential file X".



.

3. **Replay –**
   It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.
4. **virus(explained later)**

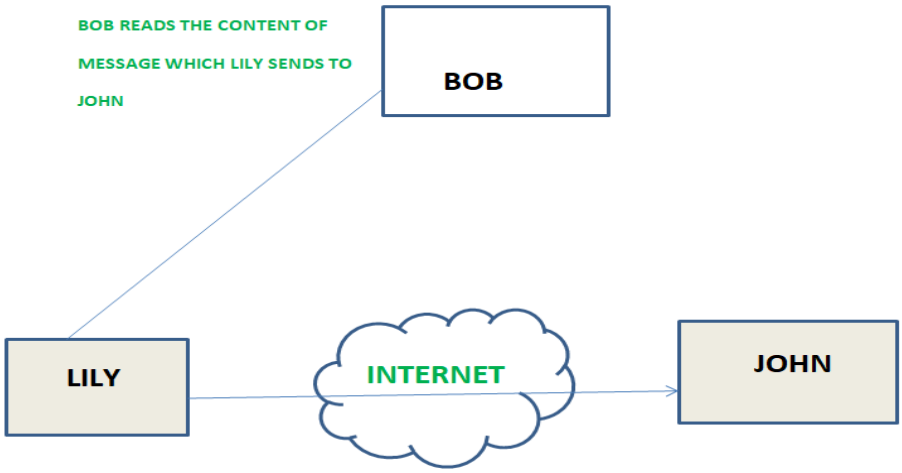
5. **Denial of Service –**
   It prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network wither by disabling the network or by overloading it by messages so as to degrade performance.



6. **Rootkit-**
   rootkits might be the most dangerous, both in the damage they can cause and the difficulty you might have in finding and removing them.Rootkits are a type of malware that are designed so that they can remain hidden on your computer. But while you might not notice them, they are active. Rootkits give cybercriminals the ability to remotely control your computer.Rootkits can contain a number of tools, ranging from programs that allow hackers to steal your passwords to modules that make it easy for them to steal your credit card or online banking information. Rootkits can also give hackers the ability to subvert or disable security software and track the keys you tap on your keyword, making it easy for criminals to steal your personal information

***PASSIVE ATTACKS*:** A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted. Types of Passive attacks are as following:

1. **The release of message content –**
   Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



2. **Traffic analysis –**
   Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message.
   The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.
3. **Eavesdropping**-An eavesdropping attack, which are also known as a sniffing or snooping attack, is an incursion where someone tries to steal information that computers, smartphones, or other devices transmit over a network. An eavesdropping attack takes advantage of unsecured network communications to access the data being sent and received. Eavesdropping attacks are difficult to detect because they do not cause network transmissions to appear to be operating abnormally.

SOME OTHER KIND OF COMPUTER NETWORK ATTACKS

1. PHISHING

Phishing is the crime of deceiving people into sharing sensitive information like passwords and credit card numbers. As with real fishing, there's more than one way to reel in a victim, but one phishing tactic is the most common. Victims receive a malicious email or a text message that imitates (or "spoofs") a person or organization they trust, like a coworker, a bank, or a government office. When the victim opens the email or text, they find a scary message meant to overcome their

better judgement by filling them with fear. The message demands that the victim go to a website and take immediate action or risk some sort of consequence.

If users take the bait and click the link, they're sent to an imitation of a legitimate website. From here, they're asked to log in with their username and password credentials. If they are gullible enough to comply, the sign-on information goes to the attacker, who uses it to steal identities, pilfer bank accounts, and sell personal information on the black market.

2. BOTNET

It is a network of private computers which are a victim of malicious software. The attacker controls all the computers on the network without the owner's knowledge. Each computer on the network is considered as zombies as they serve the purpose of spreading and infecting a large number of devices or as guided by the attacker.

3. SOCIAL ENGINEERING

Social engineering is the art of manipulating users of a computing system into revealing confidential information that can be used to gain unauthorized access to a computer system. The term can also include activities such as exploiting human kindness, greed, and curiosity to gain access to restricted access buildings or getting the users to installing backdoor software.

4. BACKDOOR

A backdoor is a means to access a computer system or encrypted data that bypasses the system's customary security mechanisms .A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes. However, attackers often use backdoors that they detect or install themselves as part of an exploit. In some cases, a worm or virus is designed to take advantage of a backdoor created by an earlier attack

5. VIRUS AND ITS TYPES

Virus is a computer program or software that connect itself to another software or computer program to harm computer system. When the computer program runs attached with virus it perform some action such as deleting a file from the computer system. Virus can't be controlled by remote.

WORM

Worms is also a computer program like virus but it does not modify the program. It replicate itself more and more to cause slow down the computer system. Worms can be controlled by remote.

TROJAN

Trojan Horse does not replicate itself like virus and worms. It is a hidden piece of code which steal the important information of user. For example, Trojan horse software observe the e-mail ID and password while entering in web browser for logging.

Difference between Virus, Worm and Trojan Horse:

VIRUS	WORM	TROJAN HORSE
Virus is a software or computer program that connect itself to another software or computer program to harm computer system.	Worms replicate itself to cause slow down the computer system.	Trojan Horse rather than replicate capture some important information about a computer system or a computer network.
Virus replicates itself.	Worms are also replicates itself.	But Trojan horse does not replicate itself.
Virus can't be controlled by remote.	Worms can be controlled by remote.	Like worms, Trojan horse can also be controlled by remote.
Spreading rate of viruses are moderate.	While spreading rate of worms are faster than virus and Trojan horse.	And spreading rate of Trojan horse is slow in comparison of both virus and worms.

The main objective of virus to modify the information.	The main objective of worms to eat the system resources.	The main objective of Trojan horse to steal the information.

Virus Detection

The most fundamental method of detection of virus is to check the functionality of your computer system; a virus affected computer does not take command properly.

However, if there is antivirus software in your computer system, then it can easily check programs and files on a system for virus signatures.

Virus Preventive Measures

Let us now see the different virus preventive measures. A computer system can be protected from virus through the following –

- Installation of an effective antivirus software.
- Putting highly secured Passwords.
- Use of Firewalls.

Most Effective Antivirus

Following are the most popular and effective antivirus from which you can choose one for your personal computer –

- McAfee Antivirus Plus
- Symantec Norton Antivirus
- Avast Pro Antivirus

FIREWALLS

A firewall is a network security system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented as both hardware and software, or a combination of both. Network firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the

firewall, which examines each message and blocks those that do not meet the specified security criteria.

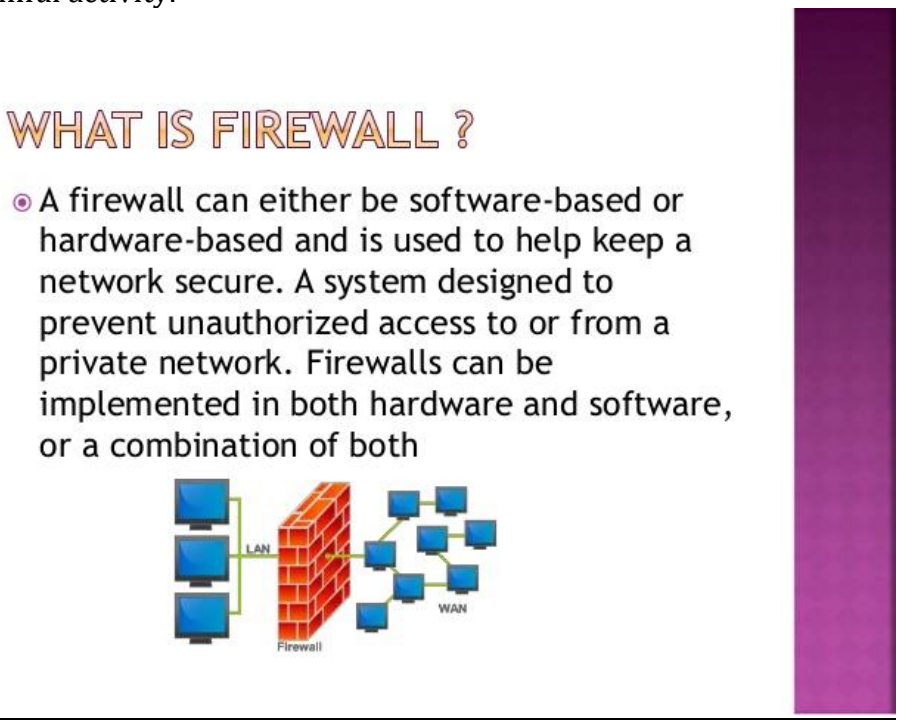
Hardware and Software Firewalls

Firewalls can be either hardware or software but the ideal configuration will consist of both. In addition to limiting access to your computer and network, a firewall is also useful for allowing remote access to a private network through secure authentication certificates and logins.

Hardware firewalls can be purchased as a stand-alone product but are typically found in broadband routers, and should be considered an important part of your system security and network set-up. Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, a business networking firewall solution is available.

Software firewalls are installed on your computer, like any software program, and you can customize it; allowing you some control over its function and protection features. A software firewall will protect your computer from outside attempts to control or gain access your computer.

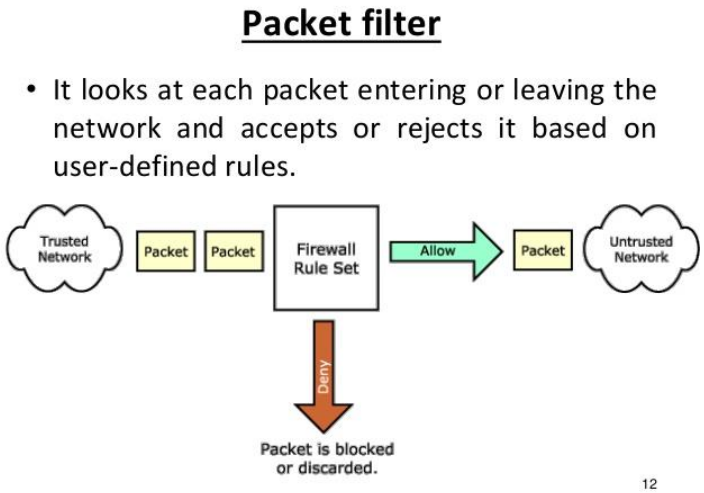
Firewalls may also be a component of your computer's operating system. For example, Windows Firewall is a Microsoft Windows application that notifies users of any ***suspicious*** activity. The app can detect and block viruses, worms, and hackers from harmful activity.



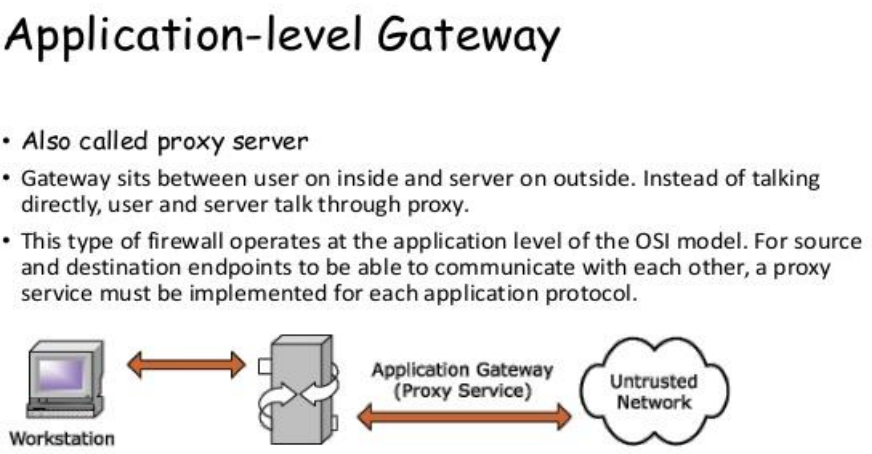
TYPES OF FIREWALLS:

1. **Packet Filters –**
   It works in the **network layer** of the OSI Model. It applies a set of rules (based on the contents of IP and transport header fields) on each packet and based on the outcome, decides to either forward or discard the packet.
   For example, a rule could specify to block all incoming traffic from a certain IP address or disallow all traffic that uses UDP protocol. If there is no match with any predefined rules, it will take default action. The default action can be to 'discard all packets' or to 'accept all packets'.

   Security threats to Packet Filters:
   1. **IP address Spoofing:**
      In this kind of attack, an intruder from the outside tries to send a packet towards the internal corporate network with the source IP address set equal to one of the IP address of internal users.
      Prevention:
      Firewall can defeat this attack if it discards all the packets that arrive at the incoming side of the firewall, with source IP equal to one of the internal IPs.
   2. **Source Routing Attacks:**
      In this kind of attack, the attacker specifies the route to be taken by the packet with a hope to fool the firewall.
      Prevention:
      Firewall can defeat this attack if it discards all the packets that use the option of source routing aka path addressing.
   3. **Tiny Fragment Attacks:**
      Many times, the size of the IP packet is greater than the maximum size allowed by the underlying network such as Ethernet, Token Ring etc. In such cases, the packet needs to be fragmented, so that it can be carried further. The attacker uses this characteristic of TCP/IP protocol. In this kind of attack, the attacker intentionally creates fragments of the original packet and send it to fool the firewall.
      Prevention:
      Firewall can defeat this attack if it discards all the packets which use the TCP protocol and is fragmented. *Dynamic Packet Filters* allow incoming TCP packets only if they are responses to the outgoing TCP packets.



2. **Application Gateways –**
   It is also known as **Proxy server**. It works as follows:
   1. **Step-1:** User contacts the application gateway using a TCP/IP application such as HTTP.
   2. **Step-2:** The application gateway asks about the remote host with which the user wants to establish a connection. It also asks for the user id and password that is required to access the services of the application gateway.
   3. **Step-3:** After verifying the authenticity of the user, the application gateway accesses the remote host on behalf of the user to deliver the packets.



3. **Stateful Inspection Firewalls –**
   It is also known as 'Dynamic Packet Filters'. It keeps track of the state of active connections and uses this information to decide which packets to allow through it, i.e., it adapts itself to the current exchange of information, unlike the normal packet filters/stateless packet filters, which have hardcoded routing rules.
4. **Circuit-Level Gateways –**
   It works at the **session layer** of the OSI Model. It is the advanced variation of *Application Gateway*. It acts as a virtual connection between the remote host and the internal users by creating a new connection between itself and the remote host. It also changes the source IP address in the packet and puts its own address at the place of source IP address of the packet from end users. This way, the IP addresses of the internal users are hidden and secured from the outside world.

CRYPTOGRAPHIC PROTOCOLS

- ***INTRODUCTION TO SSH***

Secure Shell (SSH) is a cryptographic protocol and interface for executing network services, shell services and secure network communication with a remote computer. Secure Shell enables two remotely connected users to perform network communication and other services on top of an unsecured network. It was initially a Unix-based command but is now supported on Windows-based systems as well.

SSH consists of the following steps

HANDSHAKE--AUTHENTICATION--DATA EXCHANGE

- ***SFTP***
  Secure File Transfer Protocol (SFTP) is a secure version of File Transfer Protocol (FTP), which facilitates data access and data transfer over a Secure Shell (SSH) data stream. It is part of the SSH Protocol. It supports the full security and authentication functionality of SSH.SFTP has pretty much replaced legacy **FTP** as a file transfer protocol, and is quickly replacing **FTP/S**. It provides all the functionality offered by these protocols, but more securely and more reliably, with easier configuration. There is basically no reason to use the legacy protocols any more.

  SFTP also protects against **password sniffing** and **man-in-the-middle attacks**. It protects the integrity of the data using encryption and cryptographic hash functions, and autenticates both the server and the user.

- ***HTTPS***
  The "S" in HTTPS stands for "Secure". It's the secure version of the standard "hypertext transfer protocol" your web browser uses when communicating with website,When you connect to a website with regular HTTP, your browser looks up the IP address that corresponds to the website, connects to that IP address, and assumes it's connected to the correct web server. Data is sent over the connection in clear text. An eavesdropper on a Wi-Fi network, your internet service provider, or government intelligence agencies like the NSA can see the web pages you're visiting and the data you're transferring back and forth.

HTTPS is much more secure than HTTP. When you connect to an HTTPS-secured server—secure sites like your bank's will automatically redirect you to HTTPS—your web browser checks the website's security certificate and verifies it was issued by a legitimate certificate authority. This helps you ensure that, if you see "https://bank.com" in your web browser's address bar, you're actually connected to your bank's real website. The company that issued the security certificate vouches for them. Unfortunately, certificate authorities sometimes issue bad certificates and the system breaks down. Although it isn't perfect, though, HTTPS is still much more secure than HTTP.

When you send sensitive information over an HTTPS connection, no one can eavesdrop on it in transit. HTTPS is what makes secure online banking and shopping possible.