Business Law III
By Prof. Kiran Marwade

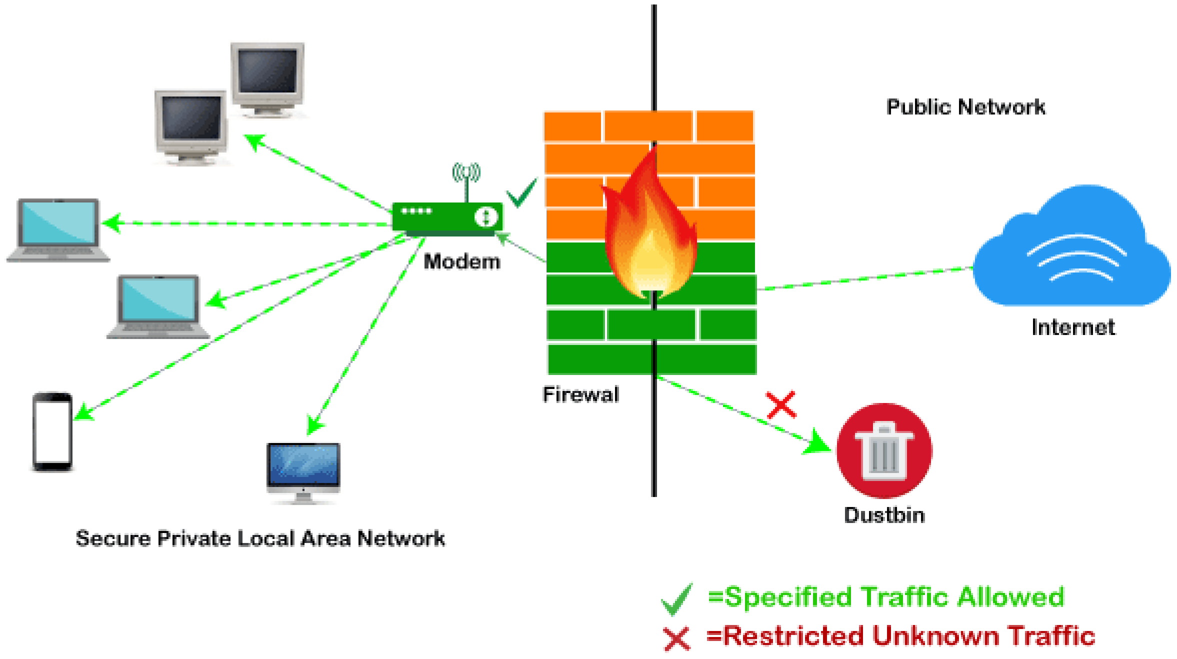
UNIT 3
Security Tools and Technology and Services

Firewall: A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organisation’s previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall’s main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

How does a firewall work?

A firewall system analyzes network traffic based on predefined rules. It then filters the traffic and prevents any such traffic coming from unreliable or suspicious sources. It only allows incoming traffic that is configured to accept.

Typically, firewalls intercept network traffic at a computer's entry point, known as a port. Firewalls perform this task by allowing or blocking specific data packets (units of communication transferred over a digital network) based on predefined security rules. Incoming traffic is allowed only through trusted IP addresses, or sources.


Public Network
Modem
Internet
Firewal
Dustbin
Secure Private Local Area Network
✓ =Specified Traffic Allowed
✗ =Restricted Unknown Traffic

Types of Firewalls

- **Packet filtering**
  A small amount of data is analyzed and distributed according to the filter's standards.
- **Proxy service**
  Network security system that protects while filtering messages at the application layer.
- **Stateful inspection**
  Dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall.
- **Next Generation Firewall (NGFW)**
  Deep packet inspection Firewall with application-level inspection.

Denial of Services (Dos):

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

How does a DoS attack work?

The primary focus of a DoS attack is to oversaturate the capacity of a targeted machine, resulting in denial-of-service to additional requests.

Buffer overflow attacks: An attack type in which a memory buffer overflow can cause a machine to consume all available hard disk space, memory, or CPU time. This form of exploit often results in sluggish behaviour, system crashes, or other deleterious server behaviours, resulting in denial-of-service.

Flood attacks: By saturating a targeted server with an overwhelming amount of packets, a malicious actor is able to oversaturate server capacity, resulting in denial-of-service. In order for most DoS flood attacks to be successful, the malicious actor must have more available bandwidth than the target.

Digital Signature:

A digital signature is an electronic, encrypted, stamp of authentication on digital information such as email messages, macros, or electronic documents. A signature confirms that the information originated from the signer and has not been altered.

Digital signature assurances

The following terms and definitions show what assurances are provided by digital signatures.

- **Authenticity** The signer is confirmed as the signer.
- **Integrity** The content has not been changed or tampered with since it was digitally signed.
- **Non-repudiation** Proves to all parties the origin of the signed content. Repudiation refers to the act of a signer denying any association with the signed content.
- **Notarization** Signatures in Microsoft Word, Microsoft Excel, or Microsoft PowerPoint files, which are time stamped by a secure time-stamp server, under certain circumstances, have the validity of a notarization.

To make these assurances, the content creator must digitally sign the content by using a signature that satisfies the following criteria:

- The digital signature is valid.
- The certificate associated with the digital signature is current (not expired).
- The signing person or organization, known as the publisher, is trusted.
  Important: Signed documents, which have a valid timestamp, are considered to have valid signatures, regardless of the age of the signing certificate.
- The certificate associated with the digital signature is issued to the signing publisher by a reputable certificate authority (CA).

  https://youtu.be/TmA2QWSLSPg

Digital Signature Certificate: The Information Technology Act, 2000 has provisions for use of Digital Signatures on the documents submitted in electronic form in order to ensure the security and authenticity of the documents filed electronically. This is a secure and authentic way to submit a document electronically. As such, all filings done by the companies/LLPs under MCA21 e-Governance programme are required to be filed using Digital Signatures by the person authorised to sign the documents.

- 1 Legal Warning:
  You can use only the valid Digital Signatures issued to you. It is illegal to use Digital Signatures of anybody other than the one to whom it is issued.
- 2 Certification Agencies:
  Certification Agencies are appointed by the office of the Controller of Certification Agencies (CCA) under the provisions of IT Act, 2000. There are a total of eight Certification Agencies authorised by the CCA to issue Digital Signature Certificates (DSCs). The details of these Certification Agencies are available on the portal of the Ministry Certifying Authorities
- 3 Class of DSCs:
  The Ministry of Corporate Affairs has stipulated a Class-II or above category signing certificate for e-Filings under MCA21. A person who already has the specified DSC for any other application can use the same for filings under MCA21 and is not required to obtain a fresh DSC.
- 4 Validity of Digital Signatures:
  The DSCs are typically issued with one year validity and two year validity. These are renewable on expiry of the period of initial issue.
- 5 Costing/ Pricing of Digital Signatures:
  It includes the cost of medium (a UBS token which is a one time cost), the cost

of issuance of DSC and the renewal cost after the period of validity. The company representatives and professionals required to obtain DSCs are free to procure the same from any one of the approved Certification Agencies as per the MCA portal. The issuance costs in respect of each Agency vary and are market driven.

However, for the guidance of stakeholders, the Ministry has obtained the costs of issuance of DSCs at the consumer end from the Certification Agencies. The costs as intimated by them are as under:

- 6 Obtain Digital Signature Certificate
  • Digital Signature Certificate (DSC) Applicants can directly approach Certifying Authorities (CAs) with original supporting documents, and self-attested copies will be sufficient in this case
  • DSCs can also be obtained, wherever offered by CA, using Aadhar eKYC based authentication, and supporting documents are not required in this case
  • A letter/certificate issued by a Bank containing the DSC applicant’s information as retained in the Bank database can be accepted. Such letter/certificate should be certified by the Bank Manager

Packet sniffer: Packet sniffing is the practice of gathering, collecting, and logging some or all packets that pass through a computer network, regardless of how the packet is addressed. In this way, every packet, or a defined subset of packets, may be gathered for further analysis. You as a network administrator can use the collected data for a wide variety of purposes like monitoring bandwidth and traffic.

A packet sniffer, sometimes called a packet analyzer, is composed of two main parts. First, a network adapter that connects the sniffer to the existing network. Second, software that provides a way to log, see, or analyse the data collected by the device.

How does packet sniffing work?

A network is a collection of nodes, such as personal computers, servers, and networking hardware that are connected. The network connection allows data to be transferred between these devices. The connections can be physical with cables, or wireless with radio signals. Networks can also be a combination of both types.

As nodes send data across the network, each transmission is broken down into smaller pieces called packets. The defined length and shape allows the data packets to be checked for completeness and usability. Because a network's infrastructure is common to many nodes, packets destined for different nodes will pass through numerous other nodes on the way to their destination. To ensure data is not mixed up, each packet is assigned an address that represents the intended destination of that packet.

A packet's address is examined by each network adapter and connected device to determine what node the packet is destined for. Under normal operating conditions, if a node sees a packet that is not addressed to it, the node ignores that packet and its data.

Packet sniffing ignores this standard practice and collects all, or some of the packets, regardless of how they are addressed.

There are two main types of packet sniffers:

- Hardware Packet Sniffers
  A hardware packet sniffer is designed to be plugged into a network and to examine it. A hardware packet sniffer is particularly useful when attempting to see traffic of a specific network segment. By plugging directly into the physical network at the appropriate location, a hardware packet sniffer can ensure that no packets are lost due to filtering, routing, or other deliberate or inadvertent causes. A hardware packet sniffer either stores the collected packets or forwards them on to a collector that logs the data collected by the hardware packet sniffer for further analysis.
- Software Packet Sniffers
  Most packet sniffers these days are of the software variety. While any network interface attached to a network can receive every bit of network traffic that flows by, most are configured not to do so. A software packet sniffer changes this configuration so that the network interface passes all network traffic up the stack. This configuration is known as *promiscuous mode* for most network adapters. Once in promiscuous mode, the functionality of a packet sniffer becomes a matter of separating, reassembling, and logging all software packets that pass the interface, regardless of their destination addresses. Software

packet sniffers collect all the traffic that flows through the physical network interface. That traffic is then logged and used according to the packet sniffing requirements of the software.

SSL: SSL stands for Secure Sockets Layer and, in short, it's the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems, preventing criminals from reading and modifying any information transferred, including potential personal details. The two systems can be a server and a client (for example, a shopping website and browser) or server to server (for example, an application with personal identifiable information or with payroll information). It does this by making sure that any data transferred between users and sites, or between two systems remain impossible to read. It uses encryption algorithms to scramble data in transit, preventing hackers from reading it as it is sent over the connection. This information could be anything sensitive or personal which can include credit card numbers and other financial information, names and addresses.

How does it Work?

The primary purpose of SSL is to provide a secure transport-layer connection between two endpoints, the server and the client. This connection is typically between a website server and the client's browser, or a mail server and the client's email application, such as Outlook.

SSL comprises two separate protocols:

1. The Handshake protocol authenticates the server(and optionally the client), negotiates crypto suites, and generates the shared key.
2. The Record protocol isolates each connection and uses the shared key to secure communications for the remainder of the session.

HTTPS: Hypertext transfer protocol secure (HTTPS) is the secure version of HTTP, which is the primary protocol used to send data between a web browser and a website. HTTPS is encrypted in order to increase security of data transfer. This is particularly important when users transmit sensitive data, such as by logging into a bank account, email service, or health insurance provider.

Any website, especially those that require login credentials, should use HTTPS. In modern web browsers such as Chrome, websites that do not use HTTPS are marked differently than those that are. Look for a green padlock in the URL bar to signify the webpage is secure.

How does HTTPS work?

HTTPS uses an encryption protocol to encrypt communications. The protocol is called Transport Layer Security (TLS), although formerly it was known as Secure Sockets Layer (SSL). This protocol secures communications by using what's known as an asymmetric public key infrastructure. This type of security system uses two different keys to encrypt communications between two parties:

1. The private key - this key is controlled by the owner of a website and it's kept, as the reader may have speculated, private. This key lives on a web server and is used to decrypt information encrypted by the public key.
2. The public key - this key is available to everyone who wants to interact with the server in a way that's secure. Information that's encrypted by the public key can only be decrypted by the private key.

Pen Register: A "pen register" is defined as "a device or process which records or decodes dialling, routing, addressing, or signalling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication

CERT: A computer emergency response team (CERT) is an expert group that handles computer security incidents. Alternative names for such groups include computer emergency readiness team and computer security incident response team (CSIRT). A more modern representation of the CSIRT acronym is Cyber Security Incident Response Team

The name "Computer Emergency Response Team" was first used in 1988 by the CERT Coordination Center (CERT-CC) at Carnegie Mellon University (CMU). The term CERT is registered as a trade and service mark by CMU in multiple countries worldwide. CMU encourages the use of Computer Security Incident Response Team (CSIRT) as a generic term for the handling of computer security incidents.

The Community Emergency Response Team (CERT) Program educates people about disaster preparedness for hazards that may impact their area and trains them in basic disaster response skills, such as fire safety, light search and rescue, team organization, and disaster medical operations

CERT-In Objectives

CERT-In works towards the goal of enhancing cyber security in India. With this goal, this organization has defined its objectives as follows:

- Prevention of cyber attacks that target the country’s cyber space
- Responding to cyber attacks to minimize damage and reducing recovery time to ultimately minimize the national vulnerability to cyber attacks
- Enhancing the level of cyber awareness among citizens

Functions of CERT-In

The functions of CERT-In have been assigned by the Information Technology (Amendment) Act 2008:

1. CERT-In collects, analyzes, and shares information on cyber incidents taking place in India.
2. Forecasts and alerts about cyber incidents.
3. Takes emergency measures to handle cyber security incidents.
4. Plays a major role in the coordination of cyber incident response activities.
5. Issues guidelines and advisories in relation to information security best practices and procedures, prevention, and reporting of cyber incidents.
6. Any other functions that relate to cyber security as prescribed.