CYBER SECURITY – WEEK 1

SYLLABUS

Protecting your personal data
- Online identity
- Where is your data ?
- Smart devices
- What do attackers want ?
- Identity theft
- Protecting your organization data
- Traditional data
- Cloud; IoT; Big data
- Types of data
- Sensitive and non-sensitive data
- Personal data, PII data
- Data classification
- Ex: Govt. of India classification of data
- Unclassified
- Restricted
- Confidential
- Secret
- Top secret

Recap –
Topology
OSI Model
TCP/IP Model
Internet protocols
Network resources
Router and Firewall, Hub, switch – security issues
Basic Network terminologies

PROTECTING YOUR PERSONAL DATA

Protecting your personal data online is crucial for maintaining your privacy and security.

10ways to enhance data protection are:

1. **USE STRONG PASSWORD:** Create complex passwords using a mix of letters, numbers and symbols. Avoid using the same password for multiple accounts.
2. **ENABLE TWO FACTOR AUTHENTICATION[2FA]:** Add an extra layer of security by enabling 2FA on your accounts. This typically involves receiving a code on your phone in addition to entering your password.
3. **KEEP SOFTWARE UPDATED :** Regularly update your OS, apps and antivirus software to protect against the latest security threats.
4. **BE CAUTIOUS WITH PUBLIC WIFI :** Avoid accessing sensitive information over public WiFi networks. Use a Virtual Private Networks(VPN) if necessary to encrypt your internet connections. Don't do your online shopping and banking at local café(when you use a shared computer or a business wifi connection, you don't know how secure the network really is. So use your own device and secure network instead.
5. **LIMIT SOCIAL MEDIA SHARING :** Be mindful of the personal information you share on social media. Adjust your privacy settings to control who can see your posts.
6. **USE SECURE BROWSERS :** choose browsers that offer privacy features, such as blocking tracking cookies and providing secure connections.
7. **ENCRYPTING THE DATA:** Using encryption tools to protect sensitive files and communications.
8. **BEWARE OF PHISHING SCAMS:** Treat unexpected email messages or links with caution, especially if they ask for personal details. Confirm the sender's identity before clicking on links or downloading attachments.
9. **REGULARLY BACK UP YOUR DATA:** Keep regular backups of your important data to recover it. Incase of data loss or a ransomware attack.
10. **MONITOR YOUR ACCOUNTS:** Regularly review your bank statements, credit reports and online accounts for any suspicious activity. Setup alerts to notify you of any unusual transactions or changes.

ONLINE IDENTITY:

An online identity is defined as an identity that a person establish in an online platform such as social Networks.

An online identity exists for everyone who uses the web, regardless of whether they have social media or online accounts.

Eg :

Selecting user name : first name : jane last name : doe year of birth: 1990 and sector : IT

jane.doe

j.doe12

jdoe

jdoe1990

jdoe.IT

Choose the right one

When choosing a username, it's important not to reveal any personal information. It should be something appropriate and respectful and should not lead strangers to think you are an easy target for cybercrimes or unwanted attention.

Some other useful tips to help you generate your username:

- Don't use your full name or parts of your address or phone number.
- Don't use your email username.
- Don't use the same username and password combination, especially on financial accounts.
- Don't choose a super-odd username and then reuse it again and again — it makes you easier to track.
- Don't choose a username that gives clues to your passwords such as a series of numbers/letters or the first part of a two-part phrase, such as knock-knock or starlight, or the department in which you work, such as IT.

- Do choose a username that's appropriate for the type of account, i.e., business, social or personal.

YOUR DATA :

Personal data describes any information about you, including your name, social security number, driver license number, date and place of birth, your mother's maiden name, and even pictures or messages that you exchange with family and friends.

Cybercriminals can use this sensitive information to identify and impersonate you, infringing on your privacy and potentially causing serious damage to your reputation.

Medical records

- Every time you visit the doctor, personal information regarding your physical and mental health and wellbeing is added to your electronic health records (EHRs). Since the majority of these records are saved online, you need to be aware of the medical information that you share and these records go beyond the bounds of the doctor's office.
- For example, many fitness trackers collect large amounts of clinical data such as your heart rate, blood pressure and blood sugar levels, which is transferred, stored and displayed via the cloud. Therefore, you should consider this data to be part of your medical records.

Education records

- Educational records contain information about your academic qualifications and achievements.
- However, these records may also include your contact information, attendance records, disciplinary reports, health and immunization records as well as any special education records including individualized education programs (IEPs).

Employment and financial records

- Employment data can be valuable to hackers if they can gather information on your past employment, or even your current performance reviews.
- Your financial records may include information about your income and expenditure. Your tax records may include paychecks, credit card statements, your credit rating and your bank account details.
- All of this data, if not safeguarded properly, can compromise your privacy and enable cybercriminals to use your information for their own gain.

WHERE IS YOUR DATA ?

Example :

Only yesterday, you shared a couple of photos of your first day on the job with a few of your close friends. But that should be OK, right?

- You took some photos at work on your mobile phone. Copies of these photos are now available on your mobile device.
- You shared these with five close friends, who live in various locations across the world.
- All of your friends downloaded the photos and now have copies of your photos on their devices.
- One of your friends was so proud that they decided to post and share your photos online. The photos are no longer just on your device. They have in fact ended up on servers located in different parts of the world and people whom you don't even know now have access to your photos.

Some more examples :

Medical billing :

- Following an appointment, the doctor will update your medical record.
- For billing purposes, this information may be shared with the insurance company.
- In such cases, your medical record, or part of it, is now accessible at the insurance company.

SHOPPING(STORE LOYALTY):

- Store loyalty cards may be a convenient way to save money on your purchases.
- However, the store is using this card to build a profile of your purchasing behavior, which it can then use to target you with special offers from its marketing partners.

SMART DEVICES:

- Consider how often you use your computing devices to access your personal data. Unless you have chosen to receive paper statements, you probably access digital copies of bank account statements via your bank's website. And when paying a bill, it's highly likely that you've transferred the required funds via a mobile banking app.
- But besides allowing you to access your information, computing devices can now also generate information about you.
- Wearable technologies such as smartwatches and activity trackers collect your data for clinical research, patient health monitoring, and fitness and wellbeing tracking. **As the global fitness tracker market grows, so also does the risk to your personal data.**

WHAT DO HACKERS WANT?

Hackers have various motivations depending on their objectives, skills, and the nature of the attack.

- **Financial gain:** Seeking to make money through illegal means.
- **Data Theft :** Stealing sensitive or valuable information Intellectual
- **Property Theft:** Stealing proprietary information or trade secrets.
- **Political or Social Activism :** Pursuing causes or influencing public opinion.
- **Cyber Warfare:** Conducting attacks for national security purposes.
- **Reputation Damage:** damaging an individual or organization's public image

IDENTITY THEFT:

Not content with stealing your money for short-term financial gain, cybercriminals are invested in the long-term gain of identity theft.

Eg:

1. **Medical theft**

- Rising medical costs have led to an increase in medical identity theft, with cybercriminals stealing medical insurance to use the benefits for themselves.
- Where this happens, any medical procedures carried out in your name will then be saved in your medical records.

2. **Banking**

- Stealing private data can help cybercriminals access bank accounts, credit cards, social profiles and other online accounts.
- Armed with this information, an identity thief could file a fake tax return and collect the refund.
- They could even take out loans in your name and ruin your credit rating (and your life as well).

WHO ELSE WANTS YOUR DATA?

It's not just criminals who seek your personal data.

Your Internet service provider (ISP)

Your ISP tracks your online activity and, in some countries, they can sell this data to advertisers for a profit.

Advertisers

Targeted advertising is part of the Internet experience. Advertisers monitor and track your online activities such as shopping habits and personal preferences and send targeted ads your way.

Search engines and social media platforms

These platforms gather information about your gender, geolocation, phone number and political and religious ideologies based on your search histories and online identity. This information is then sold to advertisers for a profit.

Websites you visit

Websites use cookies to track your activities in order to provide a more personalized experience. But this leaves a data trail that is linked to your online identity that can often end up in the hands of advertisers!

PROTECTING YOU ORGANIZATIONAL DATA

Types of Organizational Data

1. Traditional Data
2. Internet of Things (IoT) and Big Data

1. TRADITIONAL DATA

Traditional data is typically generated and maintained by all organizations, big and small. It includes the following:

- **Transactional data** such as details relating to buying and selling, production activities and basic organizational operations such as any information used to make employment decisions.
- **Intellectual property** such as patents, trademarks and new product plans, which allows an organization to gain economic advantage over its competitors. This information is often considered a trade secret and losing it could prove disastrous for the future of a company.
- **Financial data** such as income statements, balance sheets and cash flow statements, which provide insight into the health of a company.

INTERNET OF THINGS (IOT) AND BIG DATA

- IoT is a large network of physical objects, such as sensors, software and other equipment. All of these **'things'** are **connected to the Internet**, with the ability to collect and share data.

- And given that **storage options are expanding through the cloud** and **virtualization**, it's no surprise that the emergence of IoT has led to an exponential growth in data, creating a new area of interest in technology and business called **'Big Data.'**

TYPES OF DATA :

Sensitive Data

Data that must **be protected from unauthorized access** due to its confidential nature. This data could lead to risks such as identity theft, financial loss, or damage to an individual's or organization's reputation if exposed.

Eg : Personal Identification Information (PII), Financial Records, Health Information

Non-Sensitive Data

Data that does not pose significant risks if exposed and does not require special protection measures.

Eg: Public Information, Company Announcements, Basic Statistics

PERSONAL DATA AND PII DATA

Personal data refers to any information that relates to an identified or identifiable individual. It encompasses a broad range of data that can be used to directly or indirectly identify a person.

Name**, Contact Information Address, Date of Birth, Gender, Employment Details, Educational Background**

PERSONALLY IDENTIFIABLE INFORMATION (PII)

PII is a subset of personal data that includes any information that can be used alone or with other data to identify an individual. It specifically refers to data that can directly lead to the identification of a person.

Full Name**,** Social Security Number**,** Driver's License Number**,** Financial Information**,** Health Information**,** Credit Card Details

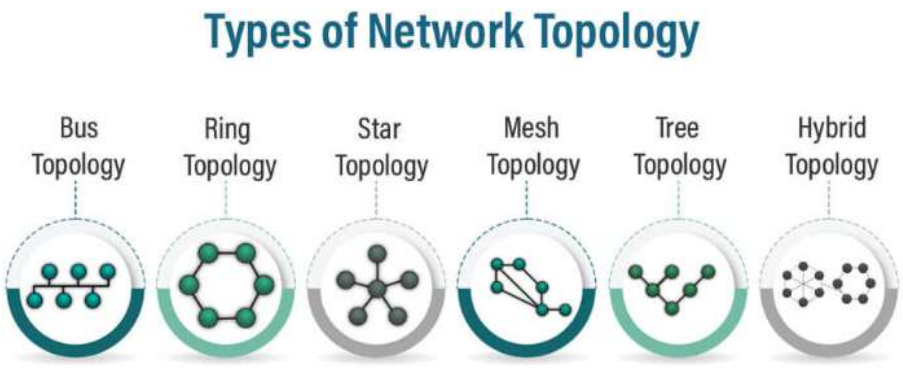
DATA CLASSIFICATION EXAMPLE: GOVERNMENT OF INDIA

- The Government of India employs a comprehensive data classification framework to manage, protect, and regulate data.
- This framework is structured around various data classification levels, which guide how sensitive information should be handled.

Classification Level	Definition	Examples	Security Measures
Unclassified	Information that is public or does not require special protection.	Government websites, Public announcements	General public access
Confidential	Sensitive information that should be protected from unauthorized access.	Personal records, Financial documents	Encryption, Access Controls, Confidentiality agreements
Secret	Highly sensitive information that requires stringent protection.	National security details, Sensitive diplomatic communications	Strong encryption, Restricted access, Regular audits
Top Secret	Extremely sensitive information that, if disclosed, could severely impact national security.	Classified intelligence reports, Strategic military information	Highest level of security, Secure facilities, Strict access control

TOPOLOGY :

Network topology refers to the arrangement of different elements (links, nodes, etc.) in a computer network.



Bus Topology

- All devices are connected to a single central cable, called the bus or backbone.
- **Advantages**:
  - Easy to implement and extend.
  - Requires less cable length than other topologies.
- **Disadvantages**:
  - Limited cable length and number of stations.
  - A failure in the main cable will cause the entire network to go down.
  - Difficult to troubleshoot.

Ring Topology

- Each device is connected to exactly two other devices, forming a circular pathway for signals.
- **Advantages**:
  - Data is transferred quickly without a collision.
  - Simple protocols for data transmission.
- **Disadvantages**:
  - A failure in any cable or device breaks the loop and can take down the entire network.
  - Troubleshooting can be difficult.

Star Topology

- All devices are connected to a central hub. The hub acts as a repeater for data flow.
- **Advantages**:
  - Easy to install and manage.
  - Failure of one link doesn't affect the rest of the network.
  - Easy to detect faults and to remove parts.
- **Disadvantages**:
  - Requires more cable length than a bus topology.
  - If the central hub fails, the whole network is inoperable.

Mesh Topology

- Every device is connected to every other device in the network.
- **Advantages**:
  - Provides high redundancy and reliability.
  - Data can be transmitted simultaneously from different devices.
- **Disadvantages**:
  - Expensive and complex to install and configure.
  - Requires a lot of cabling and I/O ports.

Tree Topology

- A hybrid topology that combines characteristics of star and bus topologies. It has a root node, and all other nodes are connected in a hierarchy.
- **Advantages**:
  - Easy to expand and manage.
  - Fault isolation is easy.
- **Disadvantages**:
  - If the backbone fails, the entire network segments fail.
  - More difficult to configure and wire than star or bus topologies.

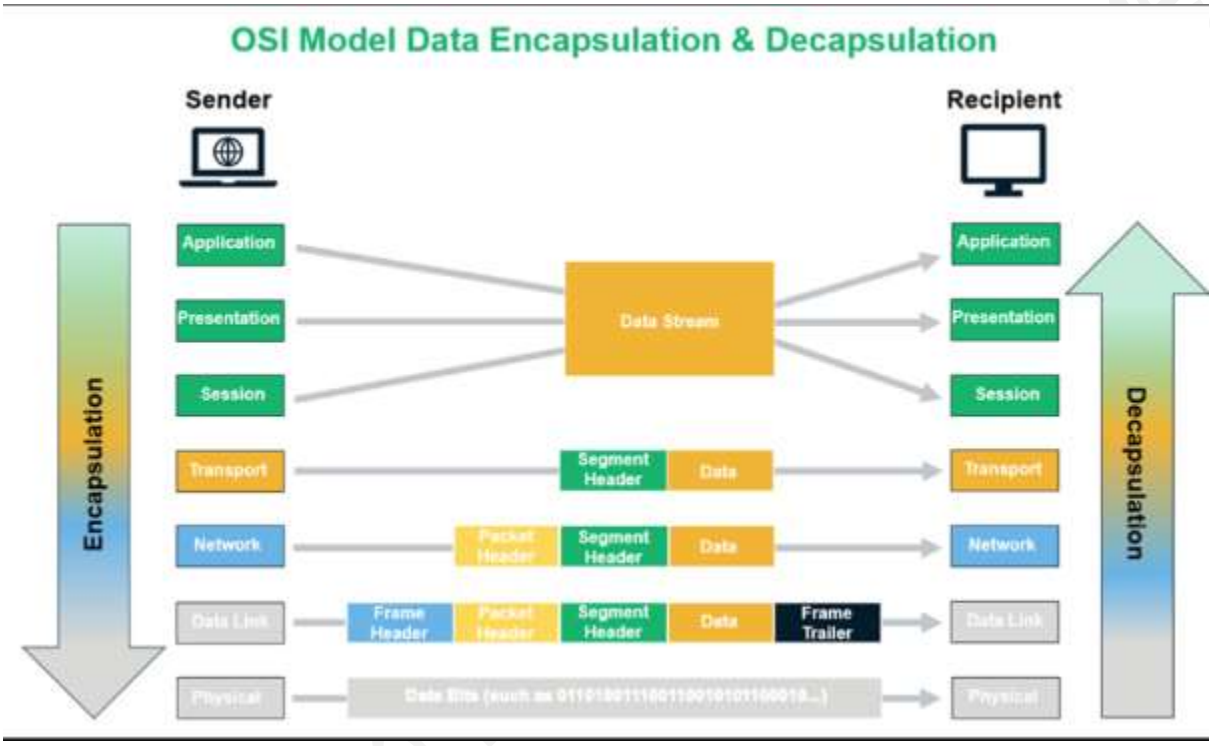
Hybrid Topology

- A combination of two or more different types of topologies.
- **Advantages**:
  - Offers flexibility and scalability.
  - Optimizes the strengths and minimizes the weaknesses of the combined topologies.
  - **Disadvantages**: Can be complex and costly to design and maintain.

OSI MODEL :

The OSI (Open Systems Interconnection) model is a conceptual framework used to understand and implement networking protocols. The model is divided into seven layers, each responsible for different aspects of data communication.

OSI Model Layers



1. **Physical Layer (Layer 1)**
    - **Function**: Deals with the physical connection between devices and the transmission and reception of raw binary data over a physical medium.
    - **Components**: Cables, switches, network interface cards (NICs), and other hardware.
    - **Protocols/Standards**: Ethernet, USB, Bluetooth, IEEE 802.11 (Wi-Fi).
2. **Data Link Layer (Layer 2)**
    - **Function**: Responsible for node-to-node data transfer and error detection/correction. It also handles MAC addresses and organizes data into frames.
    - **Components**: Switches, bridges, and NICs.

- **Protocols/Standards**: Ethernet, PPP, HDLC, MAC, ARP.

3. **Network Layer (Layer 3)**
   - **Function**: Manages logical addressing and routing of data packets across the network. It determines the best path for data to travel from source to destination.
   - **Components**: Routers.
   - **Protocols/Standards**: IP (Internet Protocol), ICMP, OSPF, RIP, BGP.
4. **Transport Layer (Layer 4)**
   - **Function**: Ensures reliable data transfer between end systems, providing error checking and data flow control. It can establish, manage, and terminate connections.
   - **Components**: Gateways, firewalls.
   - **Protocols/Standards**: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).
5. **Session Layer (Layer 5)**
   - **Function**: Manages sessions between applications. It establishes, maintains, and terminates connections between local and remote applications.
   - **Components**: APIs, sockets.
   - **Protocols/Standards**: NetBIOS, RPC, PPTP.
6. **Presentation Layer (Layer 6)**
   - **Function**: Translates data between the application layer and the network. It handles data encryption, compression, and translation.
   - **Components**: Gateways, firewalls.
   - **Protocols/Standards**: SSL/TLS, JPEG, GIF, ASCII.
7. **Application Layer (Layer 7)**
   - **Function**: Provides network services directly to end-users or applications. It facilitates communication between software applications and lower layers of the OSI model.
   - **Components**: Application software, network services.
   - **Protocols/Standards**: HTTP, FTP, SMTP, DNS, POP3, IMAP.

Data Encapsulation Process

When data is transmitted over a network, it goes through a process called encapsulation, where each layer adds its own header to the data. Here's how it works:

1. **Application Layer**: The data starts at the application layer as a message.
2. **Presentation Layer**: The message is formatted, encrypted, or compressed if needed.
3. **Session Layer**: A session is established, and session information is added.
4. **Transport Layer**: The data is segmented, and a transport layer header (e.g., TCP or UDP) is added.
5. **Network Layer**: The segments are encapsulated into packets with an IP header.
6. **Data Link Layer**: The packets are encapsulated into frames with a MAC header and trailer.
7. **Physical Layer**: The frames are converted into bits and transmitted over the physical medium.

Data Decapsulation Process

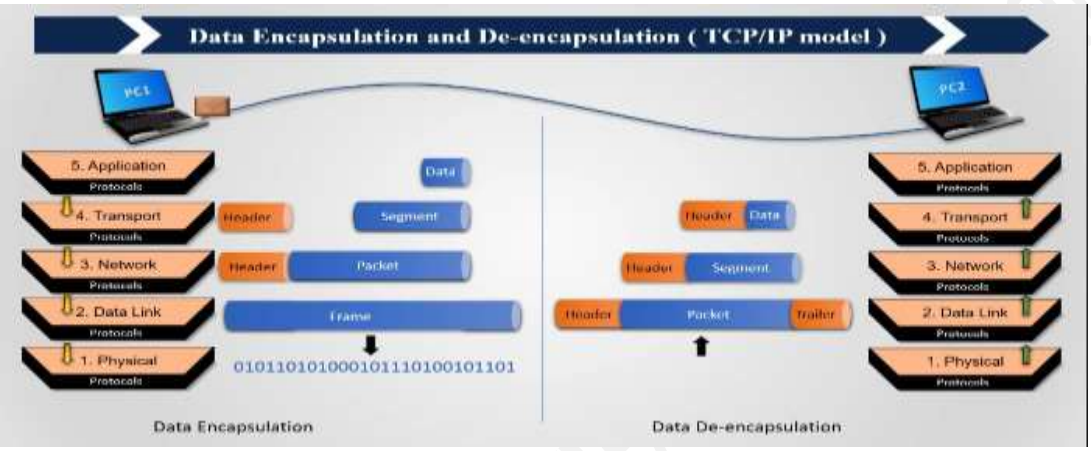
When data is received, it undergoes the reverse process called decapsulation:

1. **Physical Layer**: The bits are received and converted into frames.
2. **Data Link Layer**: The frames are checked for errors, and the MAC header is removed.
3. **Network Layer**: The IP header is removed, and the packets are reassembled.
4. **Transport Layer**: The segments are reassembled, and the transport layer header is removed.
5. **Session Layer**: The session information is processed.
6. **Presentation Layer**: The data is decrypted, decompressed, or translated as needed.
7. **Application Layer**: The message is delivered to the application.

TCP/IP MODEL :

The TCP/IP model (Transmission Control Protocol/Internet Protocol) is a simplified framework used to understand and implement network communications. It was developed by the Department of Defense (DoD) and is widely used for Internet communications. The TCP/IP model consists of four layers, each responsible for different aspects of data communication.

TCP/IP Model Layers



1. **Network Interface Layer (Link Layer)**
    - **Function**: Corresponds to the OSI model's physical and data link layers. It deals with the physical transmission of data over a network medium and handles hardware addressing.
    - **Components**: Ethernet cables, switches, network interface cards (NICs), and other physical devices.
    - **Protocols/Standards**: Ethernet, Wi-Fi (IEEE 802.11), ARP (Address Resolution Protocol).
2. **Internet Layer**
    - **Function**: Corresponds to the OSI model's network layer. It manages logical addressing and routing of data packets across different networks. It determines the best path for data to travel from source to destination.
    - **Components**: Routers.
    - **Protocols/Standards**: IP (Internet Protocol), ICMP (Internet Control Message Protocol), IGMP (Internet Group Management Protocol).
3. **Transport Layer**

- **Function**: Corresponds to the OSI model's transport layer. It ensures reliable data transfer between end systems, providing error checking, data flow control, and retransmission of lost data. It can establish, manage, and terminate connections.
- **Components**: Gateways, firewalls.
- **Protocols/Standards**: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

4. **Application Layer**

   - **Function**: Combines the functions of the OSI model's session, presentation, and application layers. It provides network services directly to end-users or applications. It facilitates communication between software applications and lower layers of the TCP/IP model.
   - **Components**: Application software, network services.
   - **Protocols/Standards**: HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System), Telnet, SSH, POP3, IMAP.

Data Encapsulation and Decapsulation

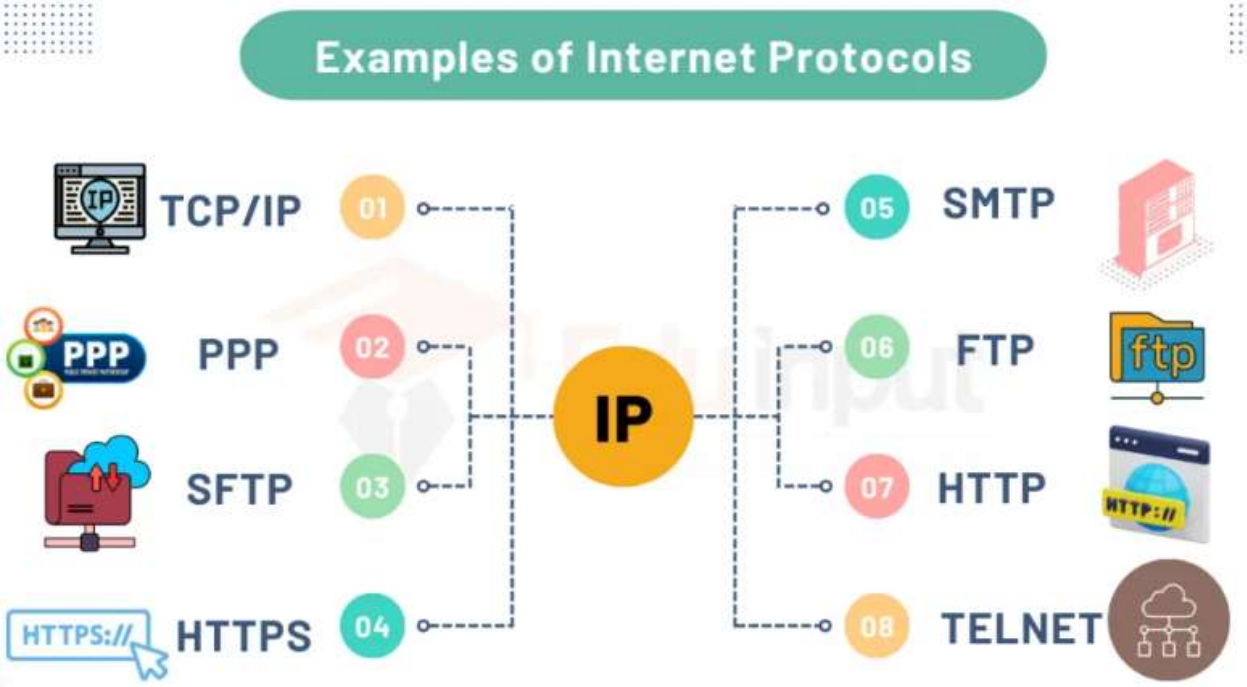
In the TCP/IP model, data encapsulation occurs as follows:

1. **Application Layer**: The data starts as a message in the application layer.
2. **Transport Layer**: The message is segmented, and a transport layer header (e.g., TCP or UDP) is added, creating a segment.
3. **Internet Layer**: The segment is encapsulated into a packet with an IP header.
4. **Network Interface Layer**: The packet is encapsulated into a frame with a MAC header and trailer.
5. **Physical Transmission**: The frame is converted into bits and transmitted over the physical medium.

In the receiving end, data decapsulation occurs in the reverse order, stripping headers at each layer until the original message is delivered to the application layer.

INTERNET PROTOCOLS

Internet protocol (IP) is a specific network protocol that is used to route data across the internet. It is responsible for addressing and routing data. TCP, UDP, HTTP, and FTP are a few examples of internet protocols.



Here's the updated table with serial numbers:

S.No	Protocol	Full Form	Function	Responsibility
1	**HTTP**	Hyper Text Transfer Protocol	Defines how messages are formatted and transmitted for web communication.	Facilitates the transfer of web pages and other resources.
2	**HTTPS**	Hyper Text Transfer Protocol Secure	Secure version of HTTP, encrypts data for secure web communication.	Ensures secure data transmission over the internet.
3	**FTP**	File Transfer Protocol	Transfers files between a client and a server.	Manages file uploading and downloading.
4	**SMTP**	Simple Mail Transfer Protocol	Sends and relays outgoing emails between mail servers.	Handles the sending of emails.

S.No	Protocol	Full Form	Function	Responsibility
5	**IMAP**	Internet Message Access Protocol	Retrieves emails from a server, allowing users to view and manipulate them as if stored locally.	Manages email retrieval and storage on the server.
6	**POP3**	Post Office Protocol version 3	Retrieves emails from a server, typically downloading them for local storage.	Downloads emails from the server for local access.
7	**DNS**	Domain Name System	Translates domain names to IP addresses, facilitating easier web navigation.	Resolves domain names to IP addresses.
8	**TCP**	Transmission Control Protocol	Provides reliable, ordered, and error-checked delivery of data between applications.	Ensures reliable data transmission between devices.
9	**UDP**	User Datagram Protocol	Offers a faster, simpler transmission model without guaranteeing delivery, order, or error checking.	Facilitates low-latency, loss-tolerating data transmission.
10	**IP**	Internet Protocol	Routes packets of data from the source to the destination across networks.	Determines the path for data packets to reach their destination.
11	**ICMP**	Internet Control Message Protocol	Sends error messages and operational information, such as ping requests.	Diagnoses network communication issues and reports errors.
12	**ARP**	Address Resolution Protocol	Resolves IP addresses to MAC addresses.	Maps IP addresses to physical MAC addresses.
13	**RARP**	Reverse Address Resolution Protocol	Maps MAC addresses to IP addresses.	Resolves MAC addresses to IP addresses.
14	**SNMP**	Simple Network	Manages and monitors	Monitors and

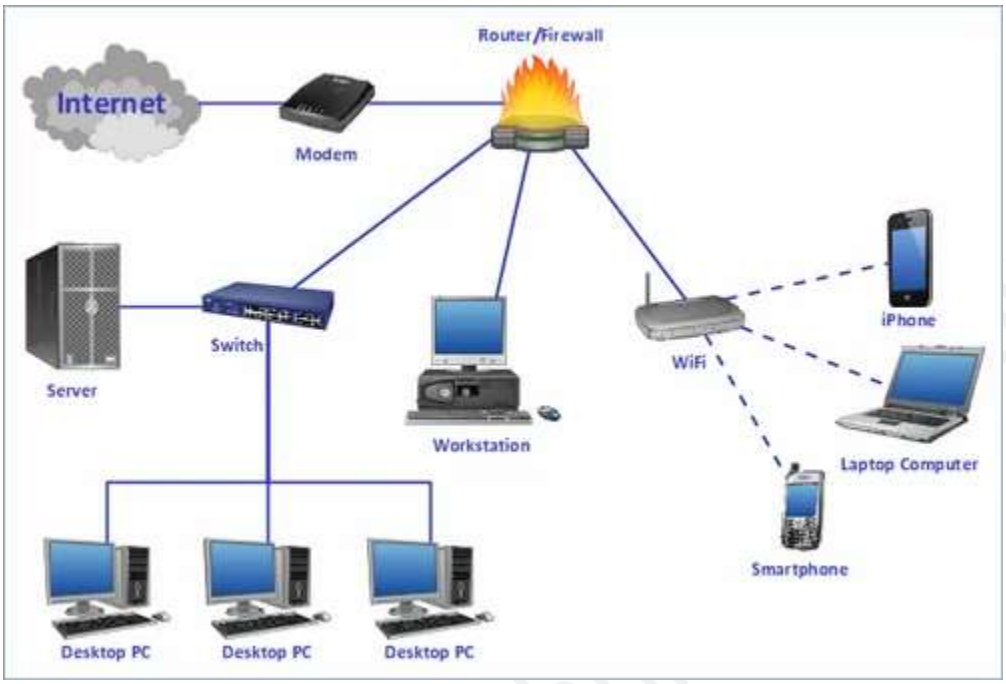
S.No	Protocol	Full Form	Function	Responsibility
		Management Protocol	network devices and their functions.	controls network devices.
15	**NTP**	Network Time Protocol	Synchronizes clocks of computer systems over networks.	Ensures accurate timekeeping across network devices.
16	**TELNET**	Telecommunications Network	Provides interactive text-based communication using a virtual terminal connection.	Allows remote access to network devices.
17	**SSH**	Secure Shell	Provides secure access to remote computers with encrypted communication.	Ensures secure remote login and command execution.
18	**SIP**	Session Initiation Protocol	Initiates, maintains, and terminates real-time communication sessions like VoIP calls.	Manages the setup and control of communication sessions.
19	**LDAP**	Lightweight Directory Access Protocol	Accesses and maintains distributed directory information services over an IP network.	Manages directory services and user authentication.
20	**BGP**	Border Gateway Protocol	Manages how packets are routed across the internet through the exchange of routing and reachability information.	Determines the best paths for data transmission across networks.

NETWORK RESOURCES :

S.No	Network Resource	Function	Responsibility
1	**Router**	Forwards data packets between networks, directing traffic to its destination.	Manages traffic between different networks and directs data to the appropriate path.
2	**Switch**	Connects devices within a network and forwards data based on MAC addresses.	Ensures data is sent only to the intended recipient within the network.
3	**Firewall**	Monitors and controls network traffic based on security rules.	Protects the network from unauthorized access and various types of cyber threats.
4	**Modem**	Modulates and demodulates signals for internet connectivity.	Provides internet access by converting digital data to analog signals and vice versa.
5	**Access Point**	Provides wireless connectivity to devices within a network using Wi-Fi.	Extends the range of a wired network to wireless devices.
6	**Network Interface Card (NIC)**	Connects a computer or device to a network.	Enables communication between devices on a network.
7	**Hub**	Connects multiple devices in a network but sends data to all devices.	Facilitates basic data transfer in a network without intelligent data forwarding.
8	**Server**	Provides resources, data, services, or applications to other devices.	Hosts applications, data, and services for network clients.
9	**DNS Server**	Translates domain names into IP addresses.	Resolves human-readable domain names to machine-readable IP addresses.
10	**VPN (Virtual Private Network)**	Creates a secure, encrypted connection over a public network.	Provides secure remote access to a private network over the internet.
11	**Load Balancer**	Distributes incoming network traffic across multiple servers.	Ensures reliability and performance by balancing the load among servers.
12	**Proxy Server**	Acts as an intermediary	Provides anonymity, security,

S.No	Network Resource	Function	Responsibility
		between client devices and other servers.	and content filtering.
13	**Network Cable**	Physical medium that connects devices in a network.	Enables data transmission through wired connections.
14	**Content Delivery Network (CDN)**	Delivers web content and resources from distributed servers.	Improves access speed and reliability for end-users.
15	**Bandwidth Analyzer**	Measures and analyzes network bandwidth usage.	Monitors network performance and identifies bandwidth issues.
16	**Network Storage**	Centralized storage solutions for data storage and management.	Provides shared access to data and ensures data availability.
17	**Bandwidth Management**	Tools and techniques to allocate and optimize bandwidth usage.	Ensures fair and efficient use of network bandwidth.
18	**DHCP Server**	Automatically assigns IP addresses to devices on the network.	Manages dynamic IP address allocation and configuration.
19	**Intrusion Detection System (IDS)**	Monitors network traffic for suspicious activities.	Detects potential threats and network policy violations.
20	**Intrusion Prevention System (IPS)**	Analyzes network traffic for threats and takes action to prevent intrusions.	Protects the network by blocking detected threats and vulnerabilities.

Router and Firewall, Hub, switch – security issues



Device	Definition	Security Issue	Description	Solutions
Router	A networking device that forwards data packets between computer networks, creating an overlay network.	Default Credentials	Many routers come with default usernames and passwords that are easily exploitable.	Change default usernames and passwords
		Outdated Firmware	Failure to update router firmware can leave vulnerabilities open to exploitation.	Keep firmware up-to-date
		Weak Encryption	Using weak encryption protocols (e.g., WEP) makes it easier for attackers to intercept data.	Use strong encryption protocols (e.g., WPA3)
		Remote	Enabled remote	Limit access and

Device	Definition	Security Issue	Description	Solutions
		Management	management interfaces can be accessed by attackers if not secured.	disable if not needed
		Open Ports	Unnecessarily open ports can be entry points for attackers.	Close unnecessary ports
Firewall	A network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.	Misconfiguration	Incorrectly configured firewalls can allow unauthorized traffic or block legitimate traffic.	Ensure proper configuration and regular audits
		Policy Bypass	Complex rules and policies might be improperly enforced, leading to security loopholes.	Simplify and regularly review rules
		Outdated Software	Firewalls that are not updated may have vulnerabilities that can be exploited.	Keep software up-to-date
		Logging and Monitoring	Insufficient logging and monitoring can delay detection of breaches.	Implement robust logging and monitoring
Hub	A basic networking device that connects multiple Ethernet	Lack of Security Features	Hubs do not filter or secure traffic, making all connected	Replace with switches where possible

Device	Definition	Security Issue	Description	Solutions
	devices, making them act as a single network segment.		devices susceptible to sniffing.	
		Broadcast Traffic	All data packets are sent to every device on the network, increasing interception risk.	Use network segmentation
Switch	A networking device that connects devices on a computer network by using packet switching to forward data to the destination device.	MAC Flooding	Attackers can flood the switch with fake MAC addresses, causing it to send data to all ports.	Implement port security and rate limiting
		VLAN Hopping	Improper VLAN configuration can allow attackers to send packets to unauthorized VLANs.	Proper VLAN configuration and tagging
		Port Security	Lack of port security can lead to unauthorized devices connecting to the network.	Limit the number of devices per port
		Spanning Tree Protocol (STP) Attacks	STP can be manipulated to alter the network topology and cause disruptions.	Use STP security features (e.g., BPDU Guard)

BASIC NETWORK TERMINOLOGIES :

Term	Definition
Network	A group of two or more computer systems linked together to share resources and information.
LAN (Local Area Network)	A network that spans a relatively small area, typically within a single building or campus.
WAN (Wide Area Network)	A network that covers a broad area, such as multiple buildings or cities, often using leased telecommunication lines.
Protocol	A set of rules and conventions for communication between network devices. Examples include TCP/IP, HTTP, FTP.
IP Address	A unique identifier assigned to each device on a network to facilitate communication.
Subnet	A subdivision of an IP network that segments a network into smaller, more manageable pieces.
Gateway	A device that acts as an entrance to another network, often used to connect different networks.
DNS (Domain Name System)	A system that translates human-readable domain names into IP addresses.
DHCP (Dynamic Host Configuration Protocol)	A network protocol that automatically assigns IP addresses and other network configuration parameters to devices on a network.
MAC Address	A unique identifier assigned to a network interface card for communication on the physical network segment.
Router	A device that forwards data packets between computer networks, directing traffic on the Internet.
Switch	A networking device that connects devices within a network and uses packet switching to forward data.
Hub	A basic networking device that connects multiple Ethernet devices, making them act as a single network segment.
Firewall	A network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
VLAN (Virtual Local Area Network)	A logical subdivision of a network that allows devices in different physical locations to communicate as if they were on the same LAN.
Bandwidth	The maximum rate of data transfer across a given path,

Term	Definition
	usually measured in bits per second (bps).
Latency	The time it takes for a data packet to travel from the source to the destination, typically measured in milliseconds (ms).
Throughput	The actual rate at which data is successfully transmitted over a network, often measured in bits per second (bps).
Packet	A unit of data transmitted over a network, including both the data being sent and control information for routing.
Network Topology	The physical or logical arrangement of network devices and how they communicate, such as star, ring, and mesh topologies.
ISP (Internet Service Provider)	A company that provides individuals and organizations access to the Internet.
VPN (Virtual Private Network)	A secure network connection over the Internet that provides remote access to a private network.
SSID (Service Set Identifier)	The name of a wireless network, used to identify and connect to it.
Network Interface Card (NIC)	A hardware component that connects a computer to a network, either wired or wireless.
QoS (Quality of Service)	A set of technologies that manage network traffic to ensure the performance of critical applications.

Syllabus

Introduction and Basic concepts of cyber security

What is Cyber security, Security principles
CIA, AAA
Vulnerability, Threat, Risk, attack and Impact on People, Process and Technology
McCumbers Cube

Cyber Security

- Brief history and types
    - Infrastructure, network, cloud, IOT, application.
- Purpose and Importance
- Challenges
- Applications

How does cyber security work?

Hackers

Who are they?
What is not hacking
Types of hackers
Hacking methodologies
Purpose

Activity: Stuxnet - a case study

Introduction and Basic concepts of cyber security

WHAT IS CYBER SECURITY, SECURITY PRINCIPLES

Cyber security is the ongoing **effort to protect individuals, organizations and governments from digital attacks** by protecting networked systems and data from unauthorized use or harm.

Personal

On a personal level, you need to safeguard your identity, your data, and your computing devices.

Organizational

At an organizational level, it is everyone's responsibility to protect the organization's reputation, data and customers.

Government

As more digital information is being gathered and shared, its protection becomes even more vital at the government level, where national security, economic stability and the safety and wellbeing of citizens are at stake.

SECURITY PRINCIPLES OF CYBERSECURITY

The Cyber Security Principles are a set of guiding principles developed for improving the online security of Internet users. They protect and provide strategic guidance against cyber threats or malicious security breaches.

These cyber security principles are grouped into five functions:

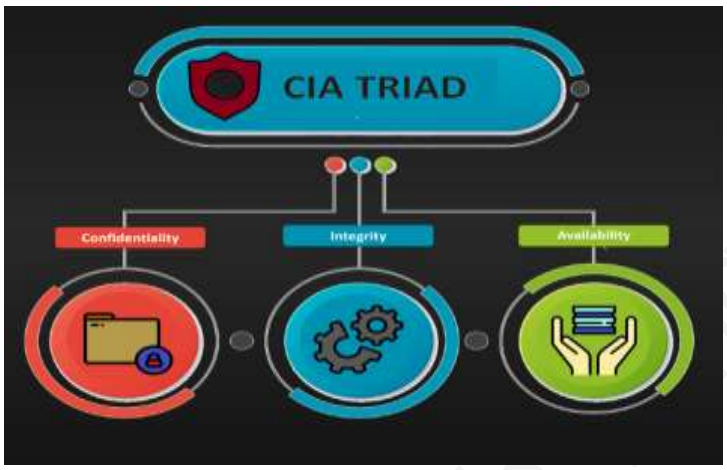
GOVERN: Develop a strong cyber security culture.
IDENTIFY: Identify assets and associated security risks.
PROTECT: Implement controls to manage security risks.
DETECT: Detect and analyse cyber security events to identify cyber security incidents.
RESPOND: Respond to and recover from cyber security incidents.

The 10 Cyber Security Principles are:

1. **Economy of Mechanism:** Keep the design as simple and small as possible to reduce complexity and potential vulnerabilities.
2. **Fail-Safe Defaults:** Default to a secure state in case of failure, ensuring access is denied unless explicitly granted.
3. **Complete Mediation:** Ensure that every access to every resource is checked for authorization to prevent unauthorized access.
4. **Open Design:** Security should not depend on the secrecy of the design; transparency allows for community review and improvement.
5. **Separation of Privilege:** Use multiple conditions to achieve access, reducing the risk of a single point of failure.
6. **Least Privilege:** Limit access to the minimum necessary for users and systems to complete their tasks.
7. **Least Common Mechanism:** Minimize shared resources to reduce potential vulnerabilities and information leakage.
8. **Psychological Acceptability:** Security mechanisms should be easy to use and not hinder access, encouraging proper usage.
9. **Work Factor:** The cost and difficulty of breaching security should exceed the potential reward, matching security measures to asset value.
10. **Compromise Recording:** Record attempts at unauthorized access to understand attack patterns and improve security measures.

What is the CIA triad (confidentiality, integrity and availability)?

The CIA triad refers to confidentiality, integrity and availability, describing a model designed to guide policies for information security (infosec) within an organization.



1. **Confidentiality.**

- Confidentiality is similar to privacy and prevents sensitive information from unauthorized access and threats
- Data is usually classified according to how harmful it would be if it fell into the wrong hands.

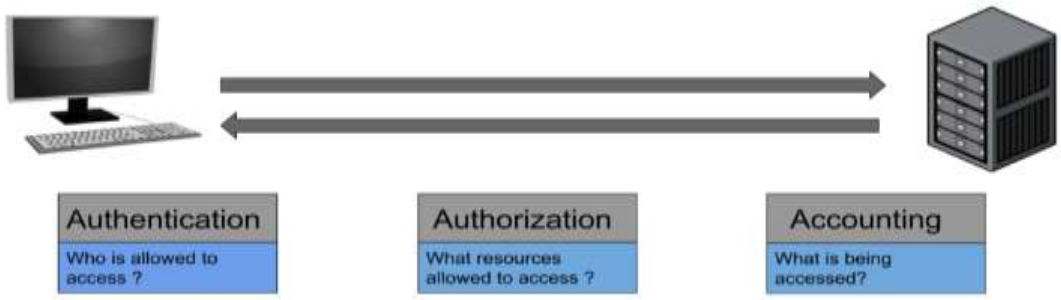
2. **Integrity.**

- The consistency, accuracy and trustworthiness of data must be maintained over its entire lifecycle.
- Data should not be changed while it is being sent, and there should be steps to stop people without permission from changing it — for ex, a data breach.

3. **Availability.**

- It means that the right person should always be able to access the data and information, whenever they need it.

Authentication, Authorization, and Accounting (AAA) in Cyber Security :



Authentication

- Authentication is the process of verifying a user's identity to ensure(make sure) it is real before giving them access.

- It includes checking identity proofs like usernames, passwords and biometrics (such as fingerprints or face scans),

Authorization

- Authorization is the process of deciding what an authenticated user, device, or system is allowed to do or access.

- Authorization occurs after authentication and controls what an authenticated user is allowed to do or access based on their roles and permissions.

Accounting

- Accounting (or auditing) involves the systematic recording and analysis of user activities and resource usage to monitor compliance, detect anomalies, and support security investigations.
- Accounting focuses on documenting what users do within the system, including their login times, resource access, and changes made.

- This process provides the necessary data for security audits, compliance checks, and investigations into suspicious or unauthorized activities.

THREAT

- A cyber threat is a malicious act that seeks to steal or damage data or discompose the digital network or system.
- Threats can also be defined as the possibility of a successful cyber attack to get access to the sensitive data of a system unethically.
- Examples of threats include **computer viruses**, **Denial of Service (DoS) attacks**, **data breaches**, and even sometimes **dishonest employees**.

Types of Threat

Threats could be of three types, which are as follows:

1. **Intentional-** Malware, phishing, and accessing someone's account illegally, etc. are examples of intentional threats.
2. **Unintentional-** Unintentional threats are considered human errors, for example, forgetting to update the firewall or the anti-virus could make the system more vulnerable.
3. **Natural-** Natural disasters can also damage the data, they are known as natural threats.

Impact on People :

- **Awareness & Training:** People may need to be trained to recognize vulnerabilities.
- **Errors & Negligence:** Human errors can create or overlook vulnerabilities.

Impact on Process :

- **Security Procedures:** Weak processes can lead to unaddressed vulnerabilities.
- **Compliance:** Vulnerabilities can lead to non-compliance with security standards.

Impact on Technology

- **System Integrity:** Vulnerabilities can compromise functionality and security.

- **Updates & Patches:** Technology must be updated to address vulnerabilities.

VULNERABILITY:

- In cybersecurity, a vulnerability is a flaw in a system's design, security procedures, internal controls, etc., that can be exploited by cybercriminals.
- In some very rare cases, cyber vulnerabilities are created as a result of cyberattacks, not because of network misconfigurations. Even it can be caused if any employee anyhow downloads a virus or a social engineering attack.

Types of Vulnerability

Vulnerabilities could be of many types, based on different criteria, some of them are:

1. **Network-** Network vulnerability is caused when there are some flaws in the network's hardware or software.
2. **Operating system-** When an operating system designer designs an operating system with a policy that grants every program/user to have full access to the computer, it allows viruses and malware to make changes on behalf of the administrator.
3. **Human-** Users' negligence can cause vulnerabilities in the system.
4. **Process-** Specific process control can also cause vulnerabilities in the system.

Impact on People :

- **Awareness:** Recognition of potential threats.
- **Training:** Training to recognize and counteract threats.

Impact on Process :

- **Incident Handling:** Processes for managing and responding to threats.
- **Security Measures:** Protection against threats.

Impact on Technology

- **Defenses:** Building technology defenses.
- **Updates:** Regular updates to handle threats.

Risk:

- Cyber risk is a potential consequence of the loss or damage of assets or data caused by a cyber threat.
- Risk can never be completely removed, but it can be managed to a level that satisfies an organization's tolerance for risk.
- So, our target is not to have a risk-free system, but to keep the risk as low as possible.
- Cyber risks can be defined with this simple formula- **Risk = Threat + Vulnerability**. Cyber risks are generally determined by examining the threat actor and type of vulnerabilities that the system has.

Types of Risks

There are two types of cyber risks, which are as follows:

1. External- External cyber risks are those which come from outside an organization, such as cyberattacks, phishing, ransomware, DDoS attacks, etc.
2. Internal- Internal cyber risks come from insiders. These insiders could have malicious intent or are just not be properly trained.

Impact on People :

- **Responsibility:** Managing and mitigating risks
- **Training:** Training for effective risk management.

Impact on Process :

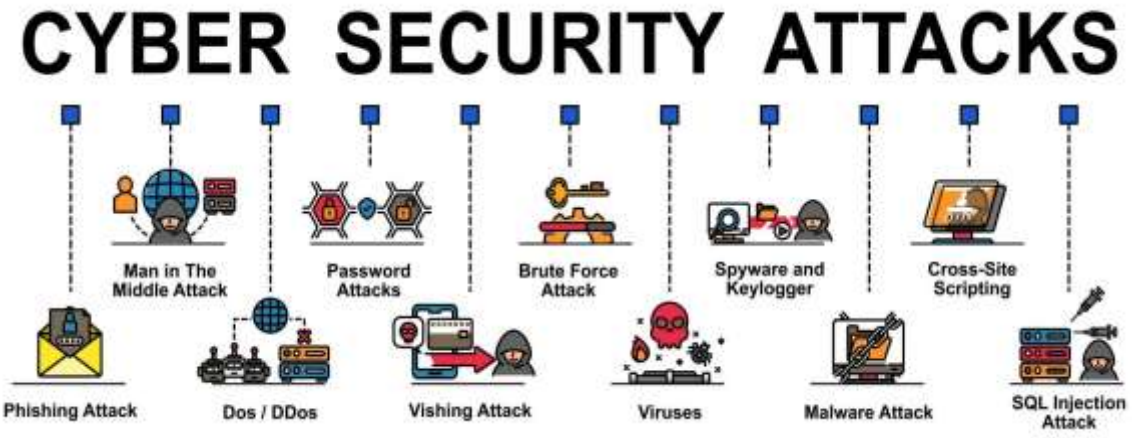
- **Risk Management:** Identification, assessment, and mitigation of risks.
- **Decision Making:** Influences strategic and operational decisions.

Impact on Technology

- **Resilience:** Ensuring technology systems are robust.
- **Mitigation:** Addressing risks and vulnerabilities.

ATTACK:

- An **attack** is a deliberate and malicious action taken by a **threat actor** to exploit vulnerabilities in a system, network, or application with the intent to cause harm, disrupt services, or steal information.
- Attacks are strategic efforts aimed at compromising the **confidentiality**, **integrity**, or **availability** of information or systems.



1. **Phishing Attack**:

   - A fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising as a trustworthy entity in electronic communication.

2. **Man In The Middle Attack**:

   - A type of attack where the attacker secretly intercepts and relays messages between two parties who believe they are directly communicating with each other.

3. **Dos / DDoS**:

   - Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks involve overwhelming a network or service with a flood of internet traffic to make it unavailable to its intended users.

4. **Vishing Attack**:

   - A type of phishing attack conducted via voice communication, where attackers attempt to trick individuals into revealing personal information over the phone.

5. **Password Attacks**:

- Attacks aimed at obtaining passwords to gain unauthorized access to systems and data. Common methods include brute force, dictionary attacks, and password cracking.

6. **Brute Force Attack**:

- A trial-and-error method used to decode encrypted data such as passwords by trying all possible combinations until the correct one is found.

7. **Viruses**:

- Malicious software programs that, when executed, replicate by inserting copies of themselves into other computer programs, data files, or the boot sector of the hard drive.

8. **Spyware and Keylogger**:

- Malicious software designed to spy on the user's activities and capture sensitive information, such as keystrokes, without the user's knowledge.

9. **Malware Attack**:

- Malicious software intended to damage, disrupt, or gain unauthorized access to computer systems. This includes viruses, worms, trojans, ransomware, etc.

10. **Cross-Site Scripting (XSS)**:

- A type of security vulnerability typically found in web applications that allows attackers to inject malicious scripts into webpages viewed by other users.

11. **SQL Injection Attack**:

- A code injection technique that exploits vulnerabilities in an application's software by inserting malicious SQL statements into an entry field for execution.

Impact on People

1. **Stress and Anxiety**: Employees may feel stressed or anxious due to data breaches or personal information exposure.
2. **Loss of Trust**: Customers and employees might lose trust in the organization.
3. **Disrupted Work**: Attacks can halt operations, making it hard for people to do their jobs.
4. **Training Needs**: More training might be needed to prevent future attacks.

Impact on Processes

1. **Operational Disruption**: Attacks can stop business processes and affect service delivery.
2. **Legal Issues**: Data breaches can lead to legal trouble and fines.
3. **Policy Changes**: Organizations may need to update their procedures to fix vulnerabilities.
4. **Financial Impact**: Recovering from an attack can be costly, and downtime can lead to revenue loss.

Impact on Technology

1. **System Damage**: Attacks can damage systems and cause data loss.
2. **Improved Security**: Organizations often invest in better security measures after an attack.
3. **Adoption of New Tools**: New technologies may be used to better defend against future attacks.
4. **Regular Updates**: Keeping systems updated to fix security gaps becomes a priority.

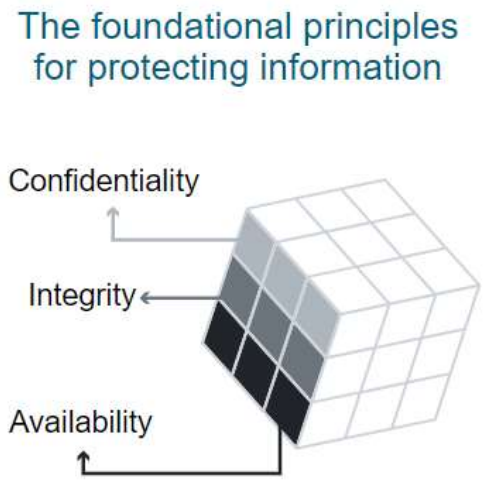
MCCUMBERS CUBE

The McCumber Cube is a model framework created by John McCumber in 1991 to help organizations establish and evaluate information security plans by considering all of the related factors that impact them.

This security model has three dimensions:

1. The foundational principles for protecting information systems.
2. The protection of information in each of its possible states.
3. The security measures used to protect data.

1. The foundational principles for protecting information systems.

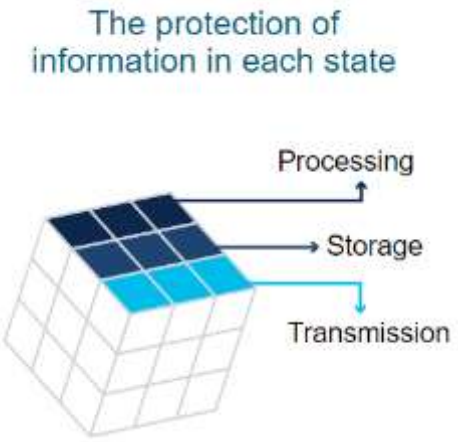


1. **Confidentiality**
   - It is a set of rules that prevents sensitive information from being disclosed to unauthorized people, resources and processes.
   - Methods to ensure confidentiality include **data encryption**, **identity proofing** and **two factor authentication**.

2. **Integrity**
   - It ensures that system information or processes are protected from intentional or accidental modification.
   - One way to ensure integrity is to use a **hash function** or **checksum**.

3. **Availability**
    - It means that authorized users are able to access systems and data when and where needed and those that do not meet established conditions, are not.
    - This can be achieved by **maintaining equipment**, **performing hardware repairs**, **keeping operating systems and software up to date**, and **creating backups**.

2. **The protection of information in each of its possible states.**



- **Processing** refers to data that is being used to perform an operation such as updating a database record (data in process).
- **Storage** refers to data stored in memory or on a permanent storage device such as a hard drive, solid-state drive or USB drive (data at rest).
- **Transmission** refers to data traveling between information systems (data in transit).

3. **The security measures used to protect data.**

- **Awareness, training and educatio** mean that the organization informs its people about security threats and teaches them how to keep the system safe.

- **Technology** refers to the software- and hardware-based solutions designed to protect information systems such as firewalls, which continuously monitor your network in search of possible malicious incidents.

- **Policy and procedure** refers to the administrative controls that provide a foundation for how an organization implements information assurance, such as incident response plans and best practice guidelines.

CYBER SECUIRITY

BREIF HISTORY:

Early Beginnings (1960s-1970s)

1. **Initial Concerns**: Cybersecurity began as a concept in the 1960s when researchers realized the potential for computers to be used for malicious purposes.
2. **First Attacks**: The first recorded instance of a cybersecurity breach occurred in the early 1970s when a researcher named Bob Thomas created a program called "Creeper" that could move across ARPANET (the precursor to the internet), leaving a trail of messages. Ray Tomlinson, who later developed email, created "Reaper," a program designed to delete Creeper, marking the first known example of antivirus software.

The Birth of Modern Cybersecurity (1980s)

3. **Viruses and Malware**: In the 1980s, personal computers became more widespread, and so did malicious software. The first PC virus, "Brain," was created in 1986 by two Pakistani brothers.
4. **Legislation**: The Computer Fraud and Abuse Act (CFAA) was enacted in the United States in 1986 to address computer-related crimes.
5. **Security Organizations**: The formation of the Computer Emergency Response Team (CERT) in 1988 by DARPA following the Morris Worm attack highlighted the need for coordinated responses to cybersecurity incidents.

Development of Security Protocols (1990s)

6. **Encryption Standards**: The development of encryption standards, such as SSL (Secure Sockets Layer), began in the 1990s to secure online communications.
7. **Firewalls and Antivirus Software**: As the internet grew, so did the development of security technologies like firewalls and antivirus software to protect individual and corporate systems.
8. **Notable Attacks**: The 1990s saw significant cybersecurity incidents, such as the Melissa virus in 1999, which spread rapidly via email, causing substantial disruptions.

The Internet Age (2000s)

9. **Sophistication of Attacks**: Cyber attacks became more sophisticated and targeted. The early 2000s saw the rise of advanced persistent threats (APTs) and organized cybercrime.
10. **Legislation and Standards**: Governments and organizations developed more comprehensive cybersecurity regulations and standards, such as the Payment Card Industry Data Security Standard (PCI DSS) in 2004.
11. **High-Profile Breaches**: Major breaches, including the 2005 breach of TJX Companies and the 2007 Estonia cyberattacks, demonstrated the vulnerability of even large, well-resourced organizations.

Modern Era (2010s-Present)

12. **State-Sponsored Attacks**: The 2010s saw an increase in state-sponsored cyber attacks, such as the Stuxnet worm targeting Iran's nuclear facilities.
13. **Ransomware and Cyber Espionage**: Ransomware attacks, like WannaCry in 2017, and cyber espionage activities became more prevalent.
14. **Advanced Security Measures**: Organizations adopted more advanced security measures, including multi-factor authentication (MFA), intrusion detection systems (IDS), and security information and event management (SIEM) systems.
15. **Legislation and Compliance**: New regulations like the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States aimed to enhance data protection and privacy.

TYPES OF CYBER SECURITY:

1. Network Security

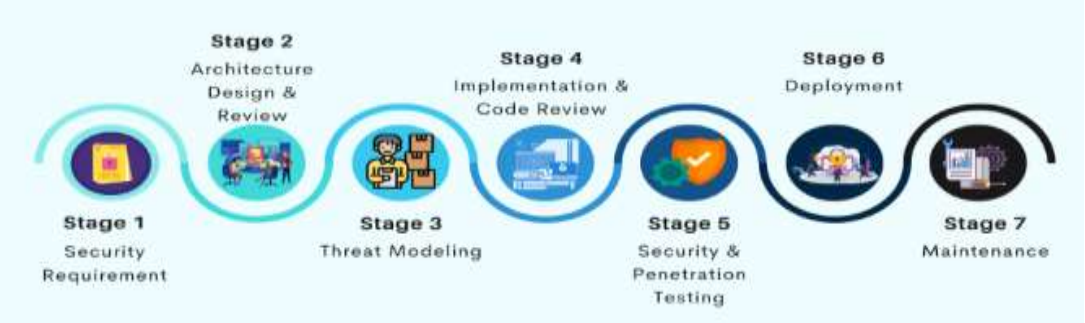
- Network security involves **protecting the integrity, confidentiality, and availability of computer networks and data using both hardware and software technologies.**
- It includes measures such as **firewalls, intrusion detection systems, and virtual private networks (VPNs)** to prevent unauthorized access and misuse.
- Regular network monitoring and vulnerability assessments are essential to identify and mitigate potential threats.

2. IoT Security

- IoT security focuses on **safeguarding Internet of Things devices and the networks they connect to from cyber threats.**
- It involves implementing **encryption, secure authentication methods,** and **regular firmware updates** to protect against **unauthorized access and vulnerabilities.**
- With the growing number of IoT devices, robust security measures are crucial to prevent attacks that could compromise sensitive data and disrupt services.

3. Application Security

- Application security aims **to protect software applications from threats throughout their lifecycle, from development to deployment** and beyond.
- This involves **incorporating security practices in the software development process**, such as **code reviews, penetration testing, and secure coding standards.**
- Continuous monitoring and updating of applications are essential to address emerging vulnerabilities and ensure the integrity and confidentiality of data.



4. **Disaster Recovery**

- Disaster recovery **involves creating plans and processes to restore and maintain critical IT functions after a cyberattack, natural disaster, or other catastrophic events.**
- Key components **include regular data backups, offsite storage, and a well-defined recovery plan** that outlines the steps to resume operations.
- Testing the disaster recovery plan periodically is essential **to ensure its effectiveness and to make necessary adjustments** based on new threats and changes in the IT environment.

5. **Information Security**

- Information security is **the practice of protecting sensitive information from unauthorized access, disclosure, alteration, and destruction.**
- It **encompasses a range of strategies and technologies, including encryption, access controls, and data masking,** to safeguard **both digital and physical information.**
- Following rules with regulatory standards and continuous monitoring are crucial to maintaining the security and integrity of information within an organization.

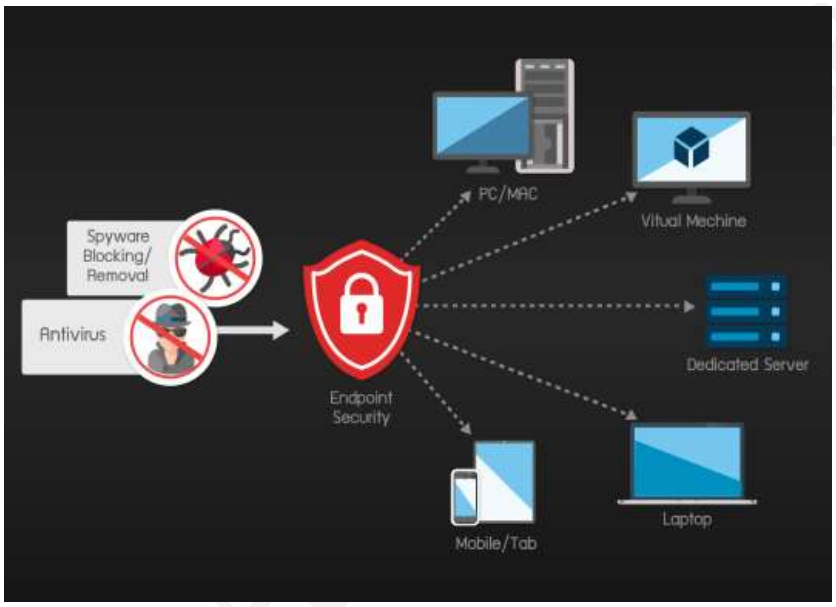
6. **Cloud Security**

- Cloud security means protecting data, applications, and services that are stored or used on the internet (cloud) from hackers, threats, or unauthorized access.
  - It includes measures such **as encryption, identity and access management (IAM), and multi-factor authentication** to ensure secure cloud environments.

7. Endpoint Security

{End-user devices are the devices that people use directly to work, access data, or connect to the internet. such as:- Mobile, Laptops, Desktop computer, Tablet, etc..}

- Endpoint security(focuses on) /(means) **protecting end-user devices, such as desktops, laptops, and mobile devices, from cyber threats.**
  - Essential measures include **deploying anti-virus software, endpoint detection and response (EDR) solutions, and mobile device management (MDM) systems.**
  - Regular updates and patches, along with user education on safe practices, are critical to maintaining robust endpoint security and preventing breaches.



PURPOSE OF CYBER SECURITY :

1. **Protecting Confidentiality:**
   - Cybersecurity measures safeguard sensitive information from unauthorized access and disclosure.
   - Ensuring data privacy is critical for personal information, financial records, and proprietary business data.
2. **Maintaining Integrity:**
   - Cybersecurity ensures that data remains accurate and unaltered during storage or transmission.
   - Protecting the integrity of information prevents data breaches and tampering, ensuring reliable and trustworthy data.
3. **Ensuring Availability:**
   - Cybersecurity aims to maintain the availability of information and resources to authorized users when needed.
   - It involves protecting systems from disruptions, such as denial-of-service attacks, to ensure continuous operation.
4. **Defending Against Cyber Threats:**
   - Cybersecurity strategies are designed to detect, prevent, and respond to cyber threats, including malware, phishing, ransomware, and other attacks.
   - Effective defense mechanisms reduce the risk of cyber incidents and minimize potential damage.
5. **Compliance(following rules) and Legal Requirements:**
   - Organizations must adhere to various regulatory standards and legal requirements related to data protection and cybersecurity.
   - Compliance ensures that businesses avoid legal penalties and maintain trust with stakeholders.
6. **Building Trust and Reputation:**
   - Robust cybersecurity practices build trust with customers, partners, and employees by demonstrating a commitment to protecting their data.
   - Maintaining a strong security posture helps preserve an organization's reputation and competitive edge.
7. **Supporting Business Continuity:**
   - Cybersecurity is integral to business continuity planning, ensuring that operations can continue during and after a cyber incident.
   - It includes disaster recovery plans and backup strategies to restore critical functions quickly.
   -

8. **Enhancing Overall Security Measures:**
    - Cybersecurity involves a proactive approach to identifying vulnerabilities and implementing controls to mitigate risks.
    - Continuous improvement of security measures helps organizations stay ahead of emerging threats and adapt to the evolving cyber landscape.

IMPORTANCE OF CYBER SECURITY

1. **Protection of Sensitive Data**: Cybersecurity safeguards personal, financial, and business information from unauthorized access and breaches. This protection is crucial for maintaining privacy and preventing identity theft.
2. **Prevention of Financial Loss**: Effective cybersecurity helps avoid costs related to data breaches and cyber-attacks, such as legal fees, fines, and loss of revenue. It also protects against financial instability caused by security incidents.
3. **Maintaining Business Continuity**: Ensuring cybersecurity allows businesses to operate smoothly without interruptions from cyber incidents. It also supports quick recovery and minimizes downtime, preserving overall operational efficiency.
4. **Compliance(following rules) with Regulations**: Cybersecurity practices adhere to legal and industry standards for data protection. Compliance helps avoid legal penalties and demonstrates a commitment to safeguarding user and client information.
5. **Safeguarding National Security**: Cybersecurity protects critical infrastructure and national interests from cyber threats and espionage. This protection is essential for maintaining the security of vital services and national security.

CHALLENGES IN CYBER SECURITY

1. **Cloud Attacks**:

- Cloud attacks involve unauthorized access to cloud-based systems, leading to data breaches and loss of sensitive information.
- These attacks exploit vulnerabilities in cloud infrastructure, often targeting misconfigured services and weak authentication mechanisms.

2. **Ransomware Attacks**:

- Ransomware attacks encrypt a victim's data, demanding a ransom payment for the decryption key.
- These attacks can cripple businesses and individuals by locking them out of their critical data and systems until the ransom is paid.

3. **IoT Attacks (Internet of Things)**:

- IoT attacks exploit vulnerabilities in connected devices, such as smart home gadgets and industrial sensors, to gain unauthorized access or disrupt services.
- These devices often lack robust security measures, making them prime targets for hackers looking to infiltrate networks or cause disruptions.

4. **Phishing Attacks**:

- Phishing attacks deceive individuals into providing sensitive information, such as passwords or credit card numbers, by posing as legitimate entities.
- These attacks typically use emails, messages, or fake websites to trick users into divulging their personal data, leading to identity theft and financial losses.

5. **Insider Attacks**:

- Insider attacks occur when employees or trusted individuals misuse their access to company systems and data for malicious purposes.
- These attacks can be particularly damaging as insiders often have privileged access and knowledge, making it easier to bypass security measures and cause significant harm.

APPLICATIONS OF CYBER SECURITY

1. **Network Security**:

- Protects computer networks from intrusions and cyber threats using firewalls, intrusion detection systems, and encryption. Ensures the integrity and confidentiality of data during transmission.

2. **Information Security**:

- Safeguards data by maintaining its confidentiality, integrity, and availability with encryption, access controls, and data masking. Protects sensitive information from unauthorized access and breaches.

3. **Application Security**:

- Ensures software applications are secure throughout their lifecycle by conducting security testing, code reviews, and using secure coding practices. Prevents exploitation of application vulnerabilities.

4. **Endpoint Security**:

- Secures individual devices such as computers and smartphones from cyber threats with antivirus software and endpoint detection and response (EDR) tools. Protects data on devices through encryption and secure access.

5. **Cloud Security**:

- Protects data, applications, and services hosted in the cloud with identity and access management (IAM) and continuous monitoring. Ensures secure configuration and protection of cloud environments.

6. **Mobile Security**:

- Secures mobile devices and the data they store or access by using mobile device management (MDM) solutions and app vetting. Ensures safe connections through secure Wi-Fi and encryption.

7. **IoT Security**:

- Protects Internet of Things (IoT) devices and networks from cyber threats using strong authentication and regular firmware updates. Enhances security in IoT ecosystems through network segmentation.

8. **Operational Technology (OT) Security**:

- Secures industrial systems and critical infrastructure from cyber attacks with specialized measures for SCADA and ICS systems. Ensures the safety and reliability of OT environments.

9. **Identity and Access Management (IAM)**:

- Manages user identities and access to resources using multi-factor authentication (MFA) and role-based access controls (RBAC). Ensures secure and controlled access to enterprise systems.

10. **Security Operations and Incident Response**:

- Monitors and responds to security incidents in real-time using security information and event management (SIEM) systems and threat intelligence. Employs incident response teams to address breaches promptly.

HOW DOES CYBER SECURITY WORK?

1. **Identify**:

   - Identify and assess potential security risks and vulnerabilities within the organization's systems and networks.
   - Conduct regular risk assessments and asset inventories to understand what needs protection.

2. **Protect**:

   - Implement safeguards and measures to protect critical infrastructure and data from cyber threats.
   - Use technologies like firewalls, encryption, and access controls to secure systems and information.

3. **Detect**:

   - Continuously monitor systems and networks to detect suspicious activities and potential security breaches.
   - Employ tools like intrusion detection systems (IDS) and security information and event management (SIEM) to identify threats in real-time.

4. **Respond**:

   - Develop and execute response plans to address and mitigate the impact of detected security incidents.
   - Coordinate with incident response teams to investigate and manage the aftermath of security breaches.

5. **Recover**:

   - Implement recovery plans to restore systems and data affected by security incidents to normal operation.
   - Conduct post-incident analysis to improve future resilience and update security strategies.

HACKERS:

Who are they?

Hackers are individuals or groups who use their technical skills to gain unauthorized access to systems, networks, and data.

What is not hacking?

Activities that do not involve unauthorized access or manipulation of computer systems and data. Here are some examples:

1. **Legal Use of Technology**: Using software or systems as intended by the developers and within the terms of service or licensing agreements.

2. **System Administration**: Managing and maintaining computer systems and networks within an organization, including configuring security settings and performing updates, as long as it's done with proper authorization.

3. **Programming**: Writing code or developing software that adheres to ethical standards and legal guidelines.

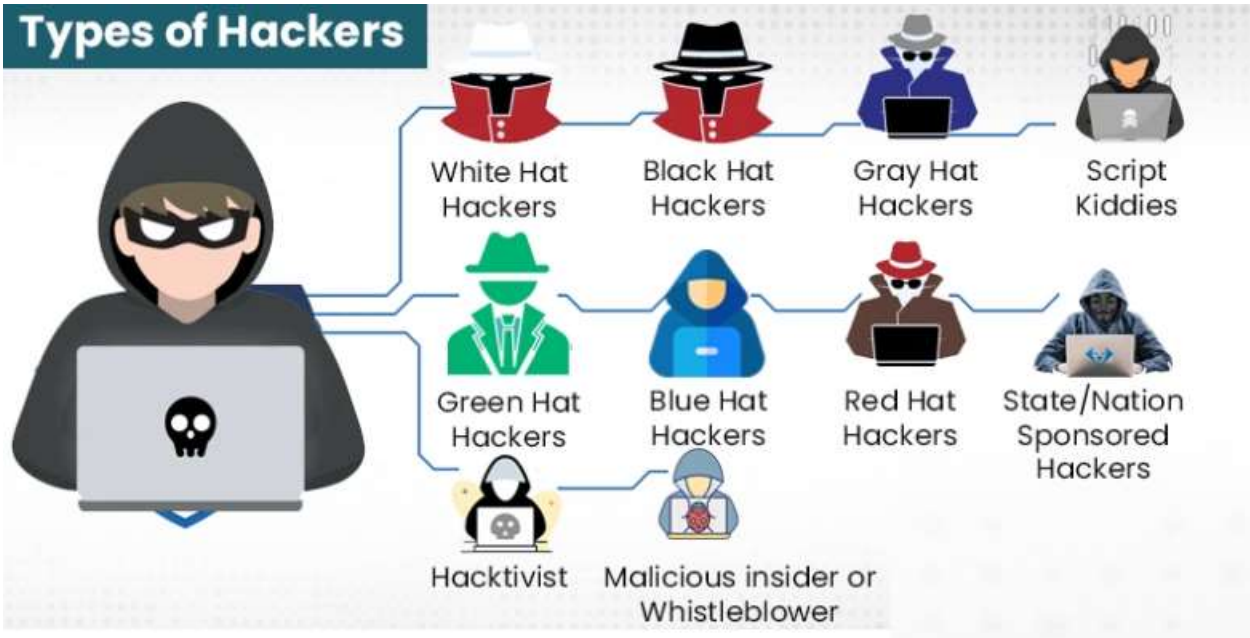
4. **Penetration Testing (Ethical Hacking)**: Conducting authorized security assessments to identify and fix vulnerabilities, typically performed with the consent of the system owner.

5. **Cybersecurity Research**: Studying and analyzing security threats and vulnerabilities in a responsible manner, often to improve defenses and protect systems, provided it's done legally and ethically.

6. **Data Analysis and Statistics**: Analyzing data sets to extract meaningful insights without accessing systems or data without permission.

7 **Social Engineering (If Done Ethically)**: Studying or educating others about the psychological manipulation of people to gain information or access, as long as it's done with consent and for educational purposes.

TYPES OF HACKERS



1. White Hat Hackers

- These hackers are professionals in the field of cybersecurity but in an ethical way.
- They hold certifications in this field and work for the government and multiple organizations.
- Their main aim is to assist these entities in strengthening their cybersecurity.
- They bridge the gap in their network and fill up the visible loopholes.
- They identify weaknesses and work on them to avoid threats in the future.
- The rules and regulations are something they abide by all the time.

2. Black Hat Hackers

- These hackers are the right opposite of the white hat hackers.
- They are computer experts who break into the networks without authorization with the wrong intention.
- The practice of threatening may differ according to knowledge but they all count as cybercrimes.
- The motive may be to steal money, data, or identity for unethical use.

3. Gray Hat Hackers

- These hackers fall between black and white hackers.
- They don't hold an authorized certificate but are experts in the field.
- Their intention for hacking is usually personal and led by monetary gains.

- They get into the network for experimenting and have a very casual approach to the process.
- The only main factor that differentiates them is their motive behind the hacking.

4. Script Kiddies

- The amateur hackers who follow scripts by other hackers to get into a network refer to script kiddies.
- These are mostly young adults who try to get into the field with little knowledge of hacking.
- A denial of service attack is the most common technique they use by flooding the network with traffic.

5. Green Hat Hackers

- These hackers are mere learners who are trying to learn the process of hacking from the base.
- They are sincere towards their skill and want to follow the ethical way of learning.
- They follow the footsteps of white hat hackers to get experience.

6. Blue Hat Hackers

- They are like script kiddies but don't want to learn the process at all.
- These hackers enter the field with the intent to gain popularity.
- They are not necessarily dangerous because there is a lack of knowledge.

7. Red Hat Hackers

- They are like white hackers when it comes to their intentions.
- They work to save companies from threats and attacks. But unlike white hackers, they cross the rules and regulations to protect the company.
- They become ruthless in such situations and thus refer to Eagle-Eyed Hackers.

8. State/Nation Sponsored Hackers

- These are hackers sponsored by the government to find confidential information about certain matters.

- These matters are mostly national security-related. The sourcing of information may be from companies, individuals, or even other country's base.
- These hackers only report to government officials with everything.

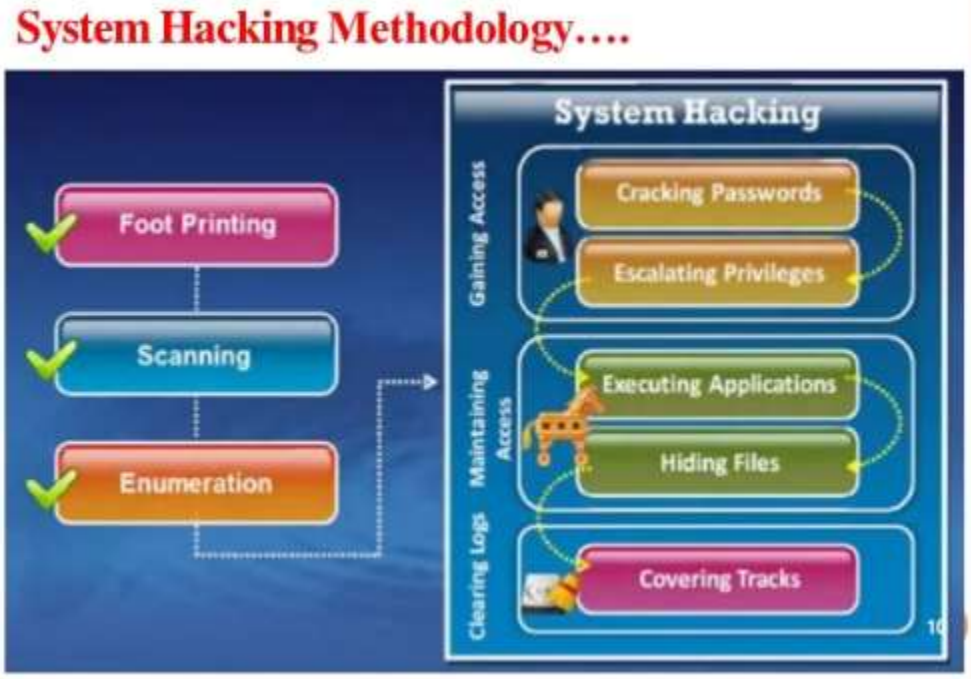
9. Hacktivist

- Hackers who work individually or in groups to get access to the government's website refers to hacktivists.
- They work with unethical intentions to exploit confidential information for personal, political, or social motives.

10. Malicious insider Hackers

- These people work inside an organization as normal employees but with an ulterior motive.
- They misuse confidential information and undertake illegal activities within the organization.
- The reason behind this may be personal or led by money.

HACKING METHODOLOGIES AND PURPOSES



Footprinting and Information Gathering:

- This initial phase involves collecting as much information as possible about the target. Hackers use public sources, social engineering, and network scanning tools to gather data on the target's network structure, systems, employees, and security measures.

Scanning and Enumeration:

- In this phase, hackers actively probe the target's systems to discover live hosts, open ports, services, and potential vulnerabilities. Tools like Nmap or Nessus are often used to perform network scans and vulnerability assessments, providing detailed information about the target's infrastructure.

Gaining Access:

- Using the information gathered from the previous steps, hackers exploit identified vulnerabilities to gain unauthorized access to the target system. This might involve techniques such as exploiting software flaws, performing SQL injection attacks, or using phishing schemes to trick users into revealing their credentials.

Maintaining Access:

- Once access is gained, hackers aim to maintain their presence on the compromised system. They achieve this by installing backdoors, rootkits, or other malicious software that allows them to control the system remotely and retain access even if the initial vulnerability is patched.

Covering Tracks:

- To avoid detection and prolong their access, hackers take steps to cover their tracks. This involves modifying or deleting logs, hiding malicious files, and using obfuscation techniques to erase evidence of their activities and ensure their presence remains unnoticed.

PURPOSE OF HACKING

- The purpose of hacking can vary widely, but it often includes financial gain through activities like theft or fraud, as well as spying for stealing sensitive information or state secrets.
- Some hackers engage in hacktivism to promote political or social causes by disrupting services or leaking information.
- Others hack out of curiosity or to demonstrate their technical skills and gain recognition within the hacking community.
- Ethical hackers, on the other hand, aim to identify and fix vulnerabilities to improve security.
- Additionally, hacking can be motivated by personal revenge or the desire to disrupt operations and cause financial or reputational damage.

SYLLABUS

Analyzing a Cyber Attack

Types of Malwares

Spyware
Malware
Backdoor
Ransomware
Scareware
Rootkit
Virus
Trojan horse
Worms

Symptoms of attack

Methods of Infiltration

-Social Engineering
Pretexting
Tailgating
Something for something (quid pro quo)

-Denial-of-Service and DDoS

-Botnet

-On the Path attack

-SEO Poisoning

-Wi-Fi Password Cracking

-Password Attacks
Password spraying
Dictionary attack
Brute force
-Password Cracking Times Rainbow
Traffic interception

-Advanced Persistent Threats

Security Vulnerability and Exploits

Hardware Vulnerabilities
Meltdown and Spectre

Software Vulnerabilities
Categorizing Software Vulnerabilities
Software updates

ANALYZING A CYBER ATTACK

Analyzing a cyber-attack involves a systematic process to understand the specifics of the attack, including how it happened, its impact, and how to prevent future occurrences.

Objectives of Cyber Attack Analysis

1. **Identify the nature of the attack**: Determine the type of cyber attack and the techniques used by the attackers.
2. **Assess the impact**: Understand the extent of damage or data breach caused by the attack.
3. **Find the root cause**: Determine how the attackers gained access and exploited vulnerabilities.
4. **Prevent future attacks**: Develop measures to improve security and prevent similar attacks in the future.

MALWARE :

- Cybercriminals use many different types of malicious software, or malware, to perform illegal activities.
- Malware is any kind of code or program that can steal data, bypass access controls.

Some of the most common malware

1. **SPYWARE**

- Spyware secretly watches what you do online, It can steal your personal data, monior your device record everything you type, including passwords or banking info.
- It changes your device's security settings to do this.
- Spyware often comes with real-looking software or Trojan viruses.

2. ADWARE

- Adware shows you unwanted ads, usually on your browser. It often comes with free software.
- You'll notice it when lots of pop-up ads appear.
- Sometimes, adware is bundled with spyware too.

3. BACKDOOR

- Backdoor malware secretly skips the login process and gives hackers remote access to your system.
- Hackers can then control your computer and give commands from far away.
- It runs in the background and is hard to detect.

4. RANSOMWARE

- Ransomware is a kind of malicious software that encrypts your files or entire system, making them inaccessible.
- They ask for money to decrypt your system, data, and files.
- It often spreads through phishing emails or weak security in software.

5. SCAREWARE

- Scareware is a kind of malware. it tries to scare you by showing fake warnings or messages, like system is at risk.
- Scareware scares you so that you click or install something harmful.
- If you click on it or install it your system gets infected.

6. ROOTKIT

- This malware is designed to modify the operating system to create a backdoor, which attackers can then use to access your computer remotely.
- Most rootkits take advantage of software vulnerabilities to gain access to resources that normally shouldn't be accessible (privilege escalation) and modify system files.
- Rootkits can also modify system forensics and monitoring tools, making them very hard to detect.
- In most cases, a computer infected by a rootkit has to be wiped and any required software reinstalled.

7. VIRUS

- A virus is a type of computer program that, when executed, replicates and attaches itself to other executable files, such as a document, by inserting its own code.
- Most viruses require end-user interaction to initiate activation and can be written to act on a specific date or time.
- Viruses can be relatively harmless, such as those that display a funny image. Or they can be destructive, such as those that modify or delete data.
- Viruses can also be programmed to mutate in order to avoid detection. Most viruses are spread by USB drives, optical disks, network shares or email.

8. TROJAN HORSE

- This malware carries out malicious operations by masking its true intent. It might appear legitimate but is, in fact, very dangerous.
- Trojans exploit your user privileges and are most often found in image files, audio files or games.
- Unlike viruses, Trojans do not self-replicate but act as a decoy to sneak malicious software past unsuspecting users.

9. WORMS

- This is a type of malware that replicates itself in order to spread from one computer to another.
- Unlike a virus, which requires a host program to run, worms can run by themselves.
- Other than the initial infection of the host, they do not require user participation and can spread very quickly over the network.
- Worms share similar patterns: They exploit system vulnerabilities, they have a way to propagate themselves, and they all contain malicious code (payload) to cause damage to computer systems or networks.
- Worms are responsible for some of the most devastating attacks on the Internet. In 2001, the Code Red worm had infected over 300,000 servers in just 19 hours.

SYMPTOMS OF MALWARE ATTACKS

Regardless of the type of malware a system has been infected with, there are some common symptoms to look out for. These include:

1. An increase in central processing unit (CPU) usage, which slows down your device.
2. Your computer freezing or crashing often.
3. A decrease in your web browsing speed.
4. Unexplainable problems with your network connections.
5. Modified or deleted files
6. The presence of unknown files, programs or desktop icons.
7. Unknown processes running.
8. Programs turning off or reconfiguring themselves.
9. Emails being sent without your knowledge or consent.

INFILTRATION IN CYBER SECURITY

What is infiltration in cybersecurity?

Infiltration in cybersecurity refers to a malicious attack or breach that involves gaining unauthorized access to a computer network, system, or application.

How do cyber attackers infiltrate a system?

Cyber attackers infiltrate a system by exploiting vulnerabilities in the software, hardware, or human error such as phishing scams, social engineering tactics, and weak passwords.

What are the consequences of infiltration?

Infiltration could lead to data theft, financial loss, system crashes, and damage to a company's reputation. It could also result in identity theft, ransomware attacks, and loss of business continuity.

METHODS OF INFILTRATION IN CYBER SECURITY

1. Social Engineering
2. Denial-of-Service
3. Distributed DoS
4. Botnet
5. On-Path Attacks
6. SEO Poisoning
7. Wi-Fi Password Cracking
8. Password Attacks
9. Cracking Times
10. Advanced Persistent Threats

1. SOCIAL ENGINEERING:

- Social engineering is the manipulation of people into performing actions or divulging confidential information.
- Social engineers often rely on people's willingness to be helpful, but they also prey on their weaknesses.

- For example, an attacker will call an authorized employee with an urgent problem that requires immediate network access and appeal to the employee's vanity or greed or invoke authority by using name-dropping techniques in order to gain this access.
- **some common types of social engineering attacks.**

a. Pretexting

- This is when an attacker calls an individual and lies to them in an attempt to gain access to privileged data.
- For example, pretending to need a person's personal or financial data in order to confirm their identity.

b. Tailgating

- This is when an attacker quickly follows an authorized person into a secure, physical location.

c. Something for something (quid pro quo)

- This is when an attacker requests personal information from a person in exchange for something, like a free gift.

2. DENIAL-OF-SERVICE

- Denial-of-Service (DoS) attacks are a type of network attack that is relatively simple to carry out, even by an unskilled attacker.
- A DoS attack results in some sort of interruption of network service to users, devices or applications.
- **The two main types of DoS attacks:**

1. Overwhelming quantity of traffic

- This is when a network, host or application is sent an enormous amount of data at a rate which it cannot handle.
- This causes a slowdown in transmission or response, or the device or service to crash.

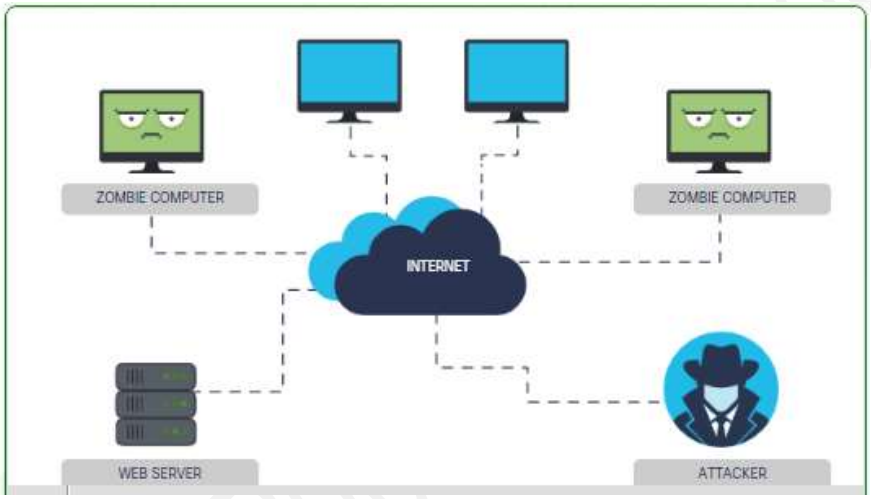
2. Maliciously formatted packets

- A packet is a collection of data that flows between a source and a receiver computer or application over a network, such as the Internet.
- When a maliciously formatted packet is sent, the receiver will be unable to handle it.
- For example, if an attacker forwards packets containing errors or improperly formatted packets that cannot be identified by an application, this will cause the receiving device to run very slowly or crash.

3. DISTRIBUTED DoS

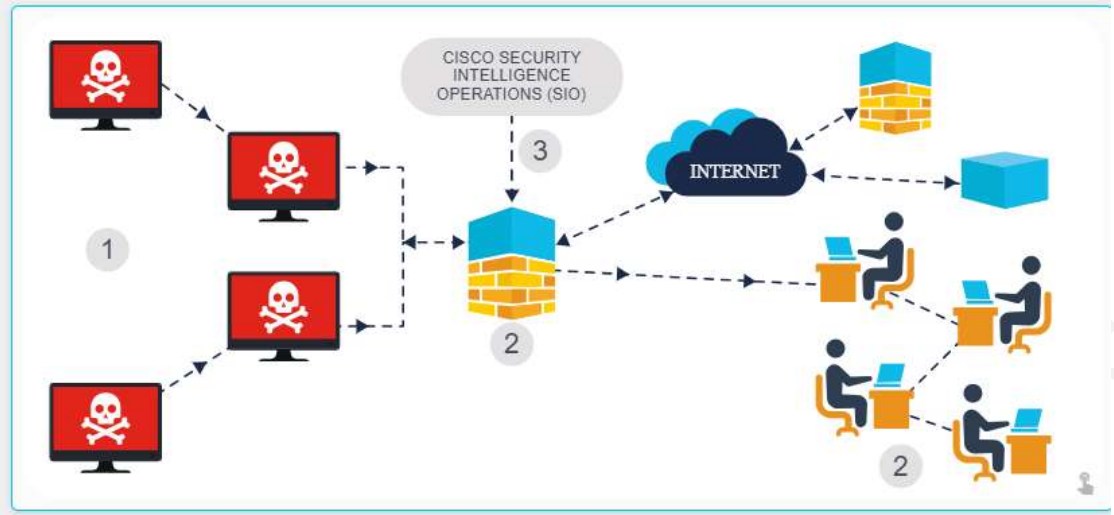
A Distributed DoS (DDoS) attack is similar to a DoS attack but originates from multiple, coordinated sources. For example:

- An attacker builds a network (botnet) of infected hosts called zombies, which are controlled by handler systems.
- The zombie computers will constantly scan and infect more hosts, creating more and more zombies.
- When ready, the hacker will instruct the handler systems to make the botnet of zombies carry out a DDoS attack.



4. BOTNET

- A bot computer is typically infected by visiting an unsafe website or opening an infected email attachment or infected media file.
- A botnet is a group of bots, connected through the Internet, that can be controlled by a malicious individual or group.
- It can have tens of thousands, or even hundreds of thousands, of bots that are typically controlled through a command and control server.
- These bots can be activated to distribute malware, launch DDoS attacks, distribute spam email, or execute brute-force password attacks. Cybercriminals will often rent out botnets to third parties for nefarious purposes.
- Many organizations. like Cisco, force network activities through botnet traffic filters to identify any botnet locations.



1. Infected bots try to communicate with a command and control host on the Internet.
2. The Cisco Firewall botnet filter is a feature that detects traffic coming from devices infected with the malicious botnet code.
3. The cloud-based Cisco Security Intelligence Operations (SIO) service pushes down updated filters to the firewall that match traffic from new known botnets.
4. Alerts go out to Cisco's internal security team to notify them about the infected devices that are generating malicious traffic so that they can prevent, mitigate and remedy these.

5. ON-PATH ATTACKS

- On-path attackers intercept or modify communications between two devices, such as a web browser and a web server, either to collect information from or to impersonate one of the devices.
- This type of attack is also referred to as a man-in-the-middle or man-in-the-mobile attack.

- A MitM attack happens when a cybercriminal takes control of a device without the user's knowledge.
- With this level of access, an attacker can intercept and capture user information before it is sent to its intended destination.
- These types of attacks are often used to steal financial information.
- There are many types of malware that possess MitM attack capabilities.

- A variation of man-in-middle, MitMo is a type of attack used to take control over a user's mobile device.
- When infected, the mobile device is instructed to exfiltrate user-sensitive information and send it to the attackers.
- ZeuS is one example of a malware package with MitMo capabilities.
- It allows attackers to quietly capture two-step verification SMS messages that are sent to users.

6. SEO POISONING

- Search engine optimization or SEO which, in simple terms, is about improving an organization's website so that it gains greater visibility in search engine results.

- Search engines such as Google work by presenting a list of web pages to users based on their search query. These web pages are ranked according to the relevancy of their content.
- While many legitimate companies specialize in optimizing websites to better position them, attackers take advantage of popular search terms and use SEO to push malicious sites higher up the ranks of search results. This technique is called SEO poisoning.
- The most common goal of SEO poisoning is to increase traffic to malicious sites that may host malware or attempt social engineering.

7. WI-FI PASSWORD CRACKING

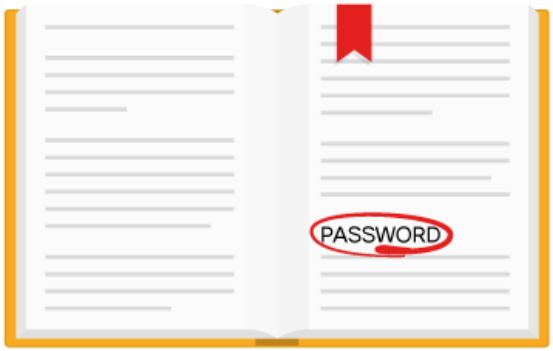
- Some use brute-force attacks, testing possible password combinations to try and guess a password.
- Others are able to identify unencrypted passwords by listening in and capturing packets sent on the network. This is called network sniffing.
- If the password is encrypted, they may still be able to reveal it using a password cracking tool.

8. PASSWORD ATTACKS

- Entering a username and password is one of the most popular forms of authenticating to a web site. Therefore, uncovering your password is an easy way for cybercriminals to gain access to your most valuable information.
- **Some of the common password security attacks.**
  1. **Password spraying:**

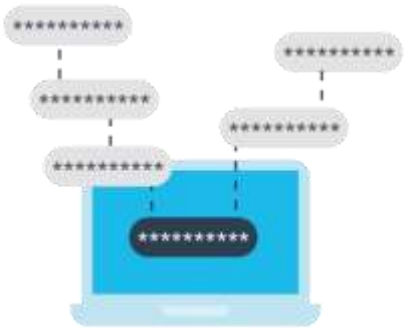
- This technique attempts to gain access to a system by 'spraying' a few commonly used passwords across a large number of accounts.
- For example, a cybercriminal uses 'Password123' with many usernames before trying again with a second commonly-used password, such as 'qwerty.'
- This technique allows the perpetrator to remain undetected as they avoid frequent account lockouts.

  2. **Dictionary attacks**



- A hacker systematically tries every word in a dictionary or a list of commonly used words as a password in an attempt to break into a password-protected account.

3. Brute-force attacks



- The simplest and most commonly used way of gaining access to a password-protected site, brute-force attacks see an attacker using all possible combinations of letters, numbers and symbols in the password space until they get it right.

4. Rainbow attacks

- Passwords in a computer system are not stored as plain text, but as hashed values (numerical values that uniquely identify data).
- A rainbow table is a large dictionary of precomputed hashes and the passwords from which they were calculated.
- Unlike a brute-force attack that has to calculate each hash, a rainbow attack compares the hash of a password with those stored in the rainbow table.
- When an attacker finds a match, they identify the password used to create the hash.

5. Traffic interception

- Plain text or unencrypted passwords can be easily read by other humans and machines by intercepting communications.

- If you store a password in clear, readable text, anyone who has access to your account or device, whether authorized or unauthorized, can read it.

9. CRACKING TIMES

It looks as if the hackers are trying everything to crack private Wi-Fi password. We have to make sure that the password is strong enough to withstand their attack!

Brute-force attacks require attackers to try all possible combinations of letters and numbers until they get it right.

How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

10. ADVANCED PERSISTENT THREATS

- Attackers also achieve infiltration through advanced persistent threats (APTs) — a multi-phase, long term, stealthy and advanced operation against a specific target.
- For these reasons, an individual attacker often lacks the skill set, resources or persistence to perform APTs.
- Due to the complexity and the skill level required to carry out such an attack, an APT is usually well-funded and typically targets organizations or nations for business or political reasons.
- Its main purpose is to deploy customized malware on one or more of the target's systems and remain there undetected.

SECURITY VULNERABILITY AND EXPLOITS

- **Security vulnerabilities** are any kind of **software or hardware defect**.
- A program written to take advantage of a known vulnerability is referred to as an **exploit**.
- A **cybercriminal** can use an exploit against a vulnerability to carry out an attack, the goal of which is to gain access to a system, the data it hosts or a specific resource.

HARDWARE VULNERABILITIES

- Hardware vulnerabilities are most often the result of hardware design flaws.
    - For example, the type of memory called RAM basically consists of lots of capacitors (a component which can hold an electrical charge) installed very close to one another.

- However, it was soon discovered that, due to their close proximity, changes applied to one of these capacitors could influence neighbor capacitors.
- Based on this design flaw, an exploit called **Rowhammer** was created. By repeatedly accessing (hammering) a row of memory, the **Rowhammer** exploit triggers electrical interferences that eventually corrupt the data stored inside the RAM.

MELTDOWN AND SPECTRE

- Google security researchers discovered Meltdown and Spectre, two hardware vulnerabilities that affect almost all **central processing units (CPUs)** released since **1995** within **desktops, laptops, servers, smartphones, smart devices and cloud services**.

- Attackers exploiting these vulnerabilities can read all memory from a **given system (Meltdown)**, as well as data handled by **other applications (Spectre)**.

- **The Meltdown and Spectre vulnerability exploitations** are referred to as side-channel attacks (information is gained from the implementation of a computer system).

- They have the ability to compromise large amounts of memory data because the attacks can be run multiple times on a system with very little possibility of a crash or other error.

- **Hardware vulnerabilities** are specific to device models and are not generally exploited through **random compromising attempts**.

- While hardware exploits are more common in **highly targeted attacks**, **traditional malware protection** and **good physical security** are sufficient protection for the everyday user.

SOFTWARE VULNERABILITIES

- Software vulnerabilities are usually introduced by errors in the operating system or application code.
- **SYNful Knock vulnerability discovered in Cisco Internetwork Operating System (IOS) in 2015.**

- The **SYNful Knock vulnerability** allowed attackers to gain control of enterprise-grade routers, such as the legacy Cisco ISR routers, from which they could monitor all network communication and infect other network devices.

- This vulnerability was introduced into the system when an altered IOS version was installed on the routers.

- To avoid this, you should always verify the integrity of the downloaded IOS image and limit the physical access of such equipment to authorized personnel only.

CATEGORIZING SOFTWARE VULNERABILITIES

Most software security vulnerabilities fall into several main categories.

1. BUFFER OVERFLOW

- Buffers are memory areas allocated to an application.
- A vulnerability occurs when data is written beyond the limits of a buffer.
- By changing data beyond the boundaries of a buffer, the application can access memory allocated to other processes.
- This can lead to a system crash or data compromise, or provide escalation of privileges.

2. NON-VALIDATED INPUT

- Programs often require data input, but this incoming data could have malicious content, designed to force the program to behave in an unintended way.
- For example, consider a program that receives an image for processing. A malicious user could craft an image file with invalid image dimensions. The maliciously crafted dimensions could force the program to allocate buffers of incorrect and unexpected sizes.

3. RACE CONDITIONS

- This vulnerability describes a situation where the output of an event depends on ordered or timed outputs.
- A race condition becomes a source of vulnerability when the required ordered or timed events do not occur in the correct order or at the proper time.

4. WEAKNESSES IN SECURITY PRACTICES

- Systems and sensitive data can be protected through techniques such as **authentication, authorization and encryption.**
- Developers should stick to using **security techniques and libraries** that have **already been created, tested and verified and should not attempt to create their own security algorithms**. These will only likely introduce new vulnerabilities.

5. ACCESS CONTROL PROBLEMS

- Access control is the process of controlling who does what and ranges from **managing physical access** to **equipment to dictating** who has access to a resource, such as a file, and what they can do with it, such as read or change the file. Many security vulnerabilities are created by the improper use of access controls.
- Nearly all access controls and security practices can be overcome if an attacker has physical access to target equipment.
- For example, no matter the permission settings on a file, a hacker can bypass the operating system and read the data directly off the disk. Therefore, to protect the machine and the data it contains, physical access must be **restricted, and encryption techniques must be used to protect data from being stolen or corrupted.**

SOFTWARE UPDATES

- The goal of software updates is to stay current and avoid exploitation of vulnerabilities.
- Microsoft, Apple and other operating system producers release patches and updates almost every day and applications such as web browsers, mobile apps and web servers are often updated by the companies or organizations responsible for them.
- Despite the fact that organizations put a lot of effort into finding and patching software vulnerabilities, new vulnerabilities are discovered regularly.
- That's why some organizations use third party security researchers who specialize in finding vulnerabilities in software, or actually invest in their own penetration testing teams dedicated to search, find and patch software vulnerabilities before they can get exploited.
- Google's Project Zero is a great example of this practice. After discovering a number of vulnerabilities in various software used by end users, Google formed a permanent team dedicated to finding software vulnerabilities.

Syllabus

Defence in depth

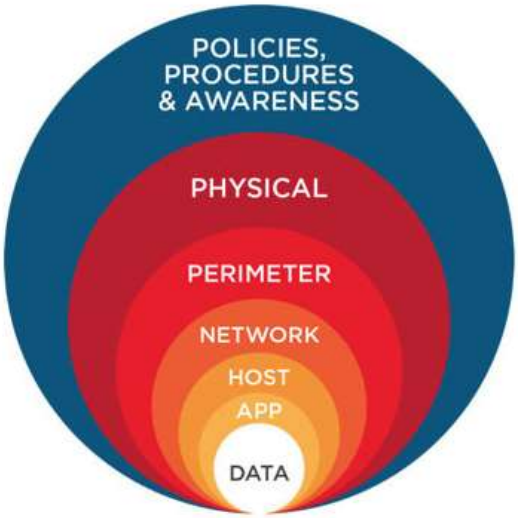
- What is defence in depth
- Layers
- Needs for Defence in depth
- Examples
- Host encryption
- Anti-virus
- Firewall
- E-Mail gateway
- Password management
- Honeypot
- Multi Factor Aut

DEFENSE IN DEPTH

WHAT IS DEFENSE IN DEPTH?

- "Defense in depth" is a cybersecurity strategy that involves using multiple layers of security controls to protect information and systems.
- The idea is to create a series of barriers, so if one layer of defense is breached, there are additional layers still in place to prevent further penetration.

LAYERS IN DEFENSE IN DEPTH:



The 7 layers of defense of depth are:

1. Policies, procedures, and awareness
2. Physical security
3. Perimeter defense
4. Internal network security
5. Host security
6. Application security
7. Data security

1. **Policies, Procedures, and Awareness**
    - This layer involves establishing organizational guidelines and protocols to manage cybersecurity effectively.
    - It includes training employees to recognize and respond to security threats.
2. **Physical Security**
    - Physical security measures protect hardware and facilities from unauthorized access and damage.
    - This includes using locks, surveillance cameras, and access control systems.
3. **Perimeter Defense**
    - The perimeter layer involves securing the boundary between an organization's internal network and external networks.
    - Firewalls and intrusion detection systems are commonly used to monitor and filter incoming and outgoing traffic.
4. **Internal Network Security**
    - Network security focuses on protecting data as it travels across internal and external networks.
    - Techniques such as encryption, secure communication protocols, and network segmentation are used to safeguard data integrity and confidentiality.
5. **Host Security**
    - Host security involves securing individual devices and servers within a network.
    - This includes using antivirus software, regular system updates, and host-based intrusion detection systems.
6. **Application Security**
    - Application security ensures that software applications are designed and maintained to resist attacks.
    - This involves practices such as secure coding, regular security testing, and patch management.
7. **Data Security**
    - Data security focuses on protecting information from unauthorized access, alteration, and destruction.

- Encryption, access controls, and data loss prevention techniques are employed to secure sensitive information.

The needs for a defense-in-depth strategy:

1. **Comprehensive Protection**: To address a wide range of threats and vulnerabilities, ensuring that if one layer is compromised, others remain intact.
2. **Layered Security**: To implement multiple layers of defense, such as physical security, network security, and application security, each providing a unique protective measure.
3. **Risk Mitigation**: To reduce the overall risk of cyber attacks by providing redundant security measures that can detect and respond to breaches effectively.
4. **Threat Detection and Response**: To enhance the ability to detect, contain, and mitigate attacks through a combination of preventive and reactive security measures.
5. **Regulatory Compliance**: To meet legal and regulatory requirements by implementing comprehensive security controls that protect sensitive data and maintain privacy.
6. **Business Continuity**: To ensure that critical systems and data remain secure and available, minimizing downtime and disruption in the event of a security incident.

EXAMPLES :

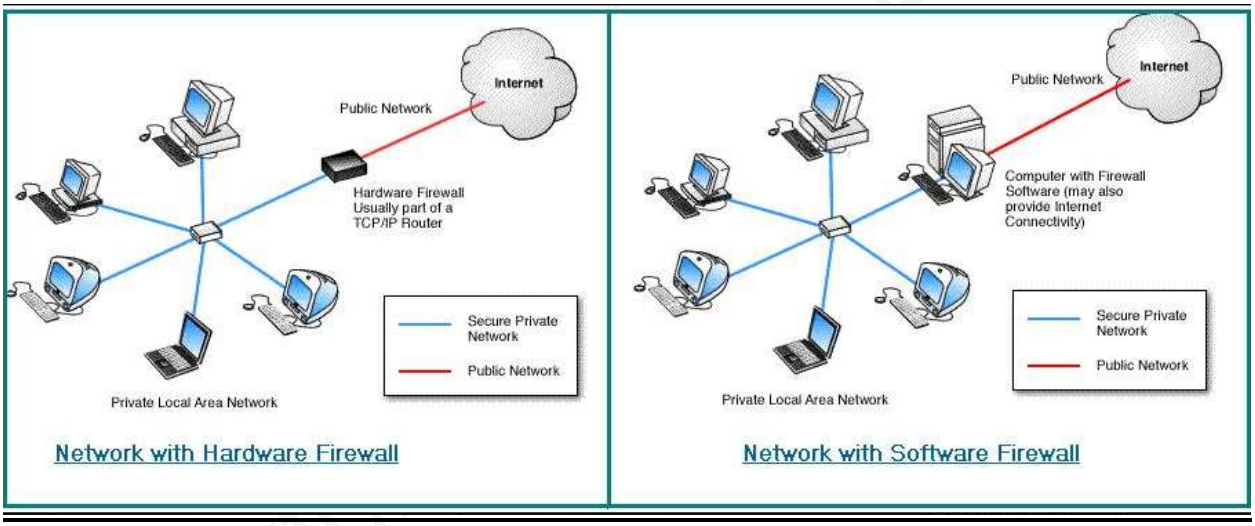
HOST ENCRYPTION:

- Host encryption in cybersecurity involves encrypting data stored on a computer or server to protect it from unauthorized access.
- This can be done through full disk encryption, which secures the entire drive, or file-level encryption, which targets specific files or folders.
- The encryption process converts data into an unreadable format, requiring a decryption key to access it.
- Proper key management is essential to maintain security and ensure data can be decrypted when needed. Overall, host encryption is crucial for protecting sensitive information and adhering to data protection regulations.

ANTIVIRUS

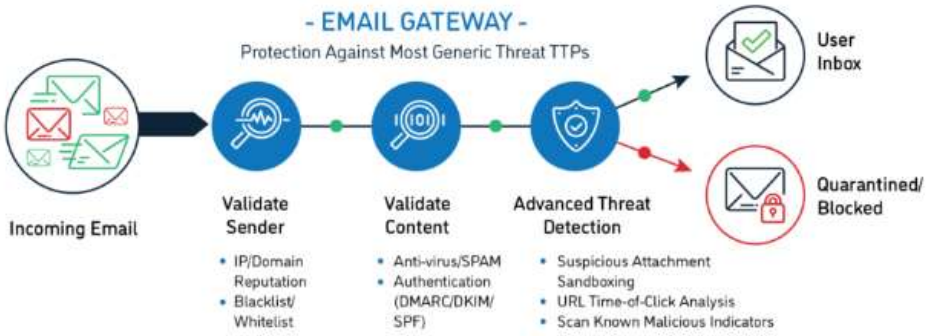
- Antivirus software is a type of program designed to detect, prevent, and remove malicious software, such as viruses, worms, trojans, and spyware, from a computer system.
- It works by scanning files and programs for known threats, using virus definitions and detective methods to identify and neutralize potential threats.
- Antivirus software often includes additional features like real-time protection, firewall capabilities, and system optimization tools.
- Regular updates are crucial to keep the software effective against new and evolving threats. Proper use of antivirus software helps protect your computer from security breaches and data loss.

FIREWALL



- Firewalls are network security systems designed to monitor and control incoming and outgoing network traffic based on predetermined security rules.
- They act as a barrier between a trusted internal network and untrusted external networks, such as the internet, to prevent unauthorized access and potential threats.
- Firewalls can be hardware-based, software-based, or a combination of both.
- They work by filtering traffic, blocking or allowing data packets based on specific criteria.
- Proper configuration and management of firewalls are essential for maintaining network security and protecting sensitive data.

EMAIL GATEWAY



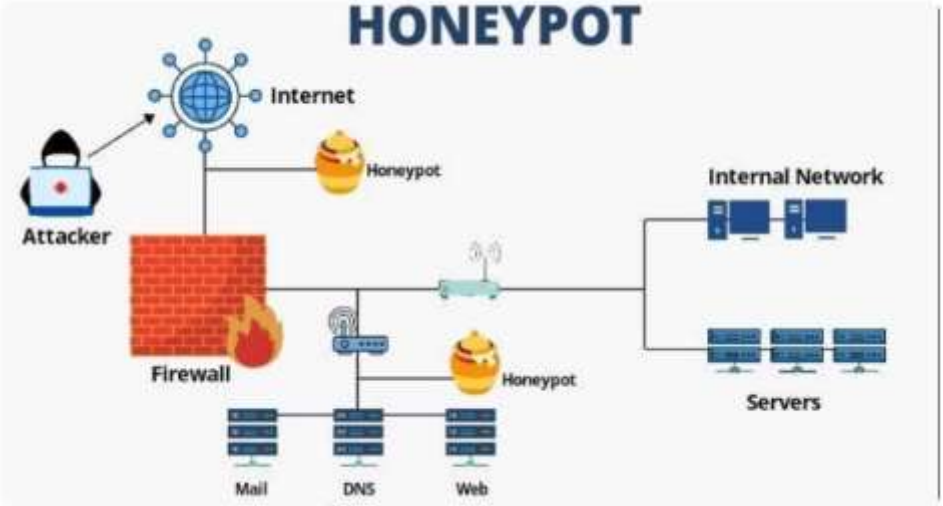
- An email gateway is a security solution that filters and manages email traffic between a company's internal network and the external internet.
- It helps protect against threats such as spam, phishing, malware, and other malicious content by scanning incoming and outgoing emails.
- Email gateways can enforce policies related to email use, data loss prevention, and encryption.
- They are typically used to ensure that only legitimate and safe emails reach users while blocking potentially harmful or unwanted messages.
- Effective email gateways are crucial for maintaining email security and protecting sensitive information.

PASSWORD MANAGEMENT IN CYBERSECURITY

1. **Create Strong Passwords:** Use complex passwords with a mix of letters, numbers, and symbols to make them harder to guess or crack.
2. **Use Unique Passwords:** Avoid reusing passwords across multiple accounts to prevent a single breach from compromising multiple accounts.
3. **Employ Password Managers:** Use password management tools to securely store, encrypt, and organize passwords, reducing the risk of forgetting or mismanaging them.
4. **Enable Multi-Factor Authentication (MFA):** Add an extra layer of security by requiring a second form of verification, such as a text message or authentication app.
5. **Regularly Update Passwords:** Change passwords periodically and immediately update them if a breach is suspected.

6. **Avoid Predictable Information:** Refrain from using easily guessable information, such as birthdays or common words, in your passwords.
7. **Educate Users:** Provide training on best practices for creating and managing passwords to enhance overall security awareness.
8. **Implement Password Policies:** Enforce guidelines for password strength and change intervals within an organization to standardize security practices.
9. **Monitor for Breaches:** Use tools to monitor if passwords have been exposed in data breaches and take immediate action to change affected passwords.
10. **Secure Password Storage:** Ensure that passwords are stored securely, using encryption and access controls to prevent unauthorized access.

What is a Honeypot?



- A Honeypot is **a network-attached system used as a trap for cyber-attackers** to detect and study the tricks and types of attacks used by hackers.
- It acts as a potential target on the internet and informs the defenders about any unauthorized attempt at the information system.
- Honeypots are mostly used by large companies and organizations involved in cybersecurity.
- It helps cybersecurity researchers to learn about the different types of attacks used by attackers.

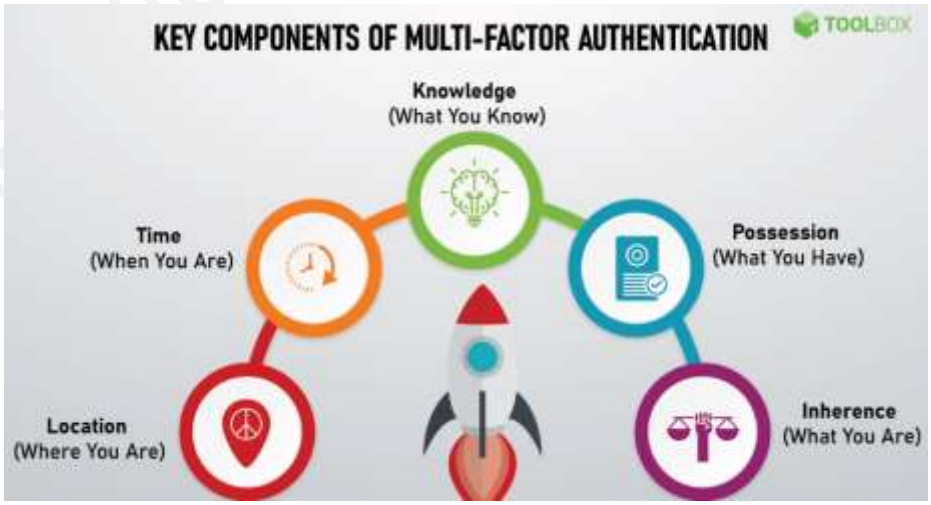
- It is suspected that even cybercriminals use these honeypots to **decoy(a fake asset that mimics a legitimate part of an organization's IT infrastructure)** researchers and spread wrong information.
- The cost of a honeypot is generally high because it requires specialized skills and resources to implement a system such that it appears to provide an organization's resources while still preventing attacks at the backend and access to any production system.

WHAT IS MULTI-FACTOR AUTHENTICATION?

- Multi-factor authentication (MFA) is a layered authentication approach of granting access to an application, account, or device.
- The first level is usually the traditional username and password procedure.
- The next levels of authentication can range from OTP emails to biometric-based methods such as fingerprint scanning and facial recognition.

There are two levels of multi-factor authentication:

1. **Device-level or system-level MFA:** This type of authentication is implemented while logging on to a device or system itself.
2. **Application-level MFA:** This type of authentication is implemented at a specific application or functional level. For example, sending an OTP to a mobile phone when a logged-in user tries to change the account password.



1. **Knowledge (What You Know)** Knowledge refers to the password, a security question, or a PIN that ideally only the user knows. It is usually the first level of authentication and is the most widely used one.
2. **Possession (What You Have)** This authentication is based on something that the user has, such as a mobile phone, a SIM card, a smart card, or a key fob. Therefore, even if a hacker gains access to the password, they also need to access one of these possessions to penetrate the system successfully.
3. **Inherence (What You Are)** This authentication is based on unique biological traits such as fingerprints, iris of the eye, and facial features. This typically requires reader hardware, a database, and software to process for authentication.
4. **Location (Where You Are)** This refers to the location from which the user's request to access has come in. It uses the IP address of the request and the user's geolocation if available.
5. **Time (When You Are)** This is based on the time of the user's access request. For example, if the employee's work hours are between 9 to 5 p.m., and they haven't granted access to log in after that, the request is denied.

SYLLABUS

Protecting Your Computing Devices

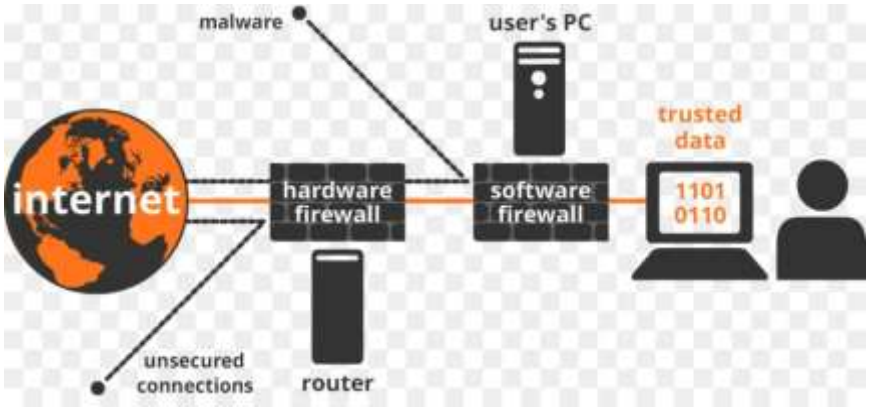
turn the firewall on
install antivirus and antispyware
manage your operating system and browser
set up password protection.

PROTECTING YOUR COMPUTING DEVICES

Your computing devices are the portal to your online life, storing a lot of your personal data. Therefore, it's important to protect the security of your devices.

Some top tips on how to protect the security of your devices :

1. TURN THE FIREWALL:



- You should use at least one type of firewall (either a software firewall or a hardware firewall on a router) to protect your device from unauthorized access.
- The firewall should be turned on and constantly updated to prevent hackers from accessing your personal or organization data.

2. INSTALL ANTIVIRUS AND ANTISPYWARE

- Malicious software, such as viruses and spyware, are designed to gain unauthorized access to your computer and your data.
- Once installed, viruses can destroy your data and slow down your computer. They can even take over your computer and broadcast spam emails using your account.
- Spyware can monitor your online activities, collect your personal information or produce unwanted pop-up ads on your web browser while you are online.
- To prevent this, you should only ever download software from trusted websites. However, you should always use antivirus software to provide another layer of protection.
- This software, which often includes antispyware, is designed to scan your computer and incoming email for viruses and delete them.
- Keeping your software up to date will protect your computer from any new malicious software that emerges.

3. MANAGE YOUR OPERATING SYSTEM AND BROWSER

- Hackers are always trying to take advantage of vulnerabilities that may exist in your operating system (such as Microsoft Windows or macOS) or web browser (such as Google Chrome or Apple Safari).

- Therefore, to protect your computer and your data, you should set the security settings on your computer and browser to medium level or higher.

- You should also regularly update your computer's operating system, including your web browser, and download and install the latest software patches and security updates from the vendors.

4. SET UP PASSWORD PROTECTION

- All of your computing devices, including PCs, laptops, tablets and smartphones, should be password protected to prevent unauthorized access.
- Any stored information, especially sensitive or confidential data, should be encrypted. You should only store necessary information on your mobile device, in case it is stolen or lost.
- Remember, if any one of your devices is compromised, the criminals may be able to access all of your data through your cloud storage service provider, such as iCloud or Google Drive.

SYLLABUS

Data Maintenance

Using free tools

Backup Your Data

How Do You Delete Your Data Permanently?

Tools

Who owns your data?

Terms of service

Understand the term; what are you agreeing to?

The data use policy

Privacy settings

Before you sign up protect your data

Activity: Check terms of service of the popular application you use on your phone and check their data sharing policy, access to device etc.

Safeguarding Your Online Privacy

Two Factor Authentication

Open Authorization

Social Sharing

Email and Web Browser Privacy

Activity: Discover your own risky online behavior

Scenario 1: posting private info on social media

Scenario 2: What password you choose when creating new account for social service

Scenario 3: Using public Wi-Fi

Scenario 4: Using trial version of the software

Activity: Check if your password is compromised

Note :Use Have I been pwned

DATA MAINTENANCE

Data maintenance in cybersecurity involves ensuring that data is accurate, consistent, and secure throughout its lifecycle.

What Is Encryption?

- Encryption is the process of converting information into a form in which unauthorized parties cannot read it.
- Only a trusted, authorized person with the secret key or password can decrypt the data and access it in its original form.

- Note that the encryption itself does not prevent someone from intercepting the data. It can only prevent an unauthorized person from viewing or accessing the content. In fact, some criminals may decide to simply encrypt your data and make it unusable until you pay a ransom.

How Do You Encrypt Your Data?

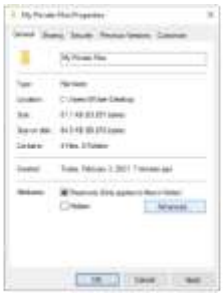
- Software programs are used to encrypt files, folders and even entire drives.
- **Encrypting File System (EFS)** is a Windows feature that can encrypt data.
- It is directly linked to a specific user account and only the user that encrypts the data will be able to access it after it has been encrypted using EFS.

Encrypt data using EFS in all Windows versions.

- **STEP 1:** Select one or more files or folders.

- **STEP 2:** Right click the selected data and go to 'Properties.'

- **STEP 3:** Find and click 'Advanced.'



- **STEP 4:** Select the 'Encrypt contents to secure data' check box.

- **STEP 5:** Files and folders that have been encrypted with EFS are displayed in green as shown here.

BACK UP YOUR DATA

- Having a backup may prevent the loss of irreplaceable data.
- To back up data properly, you will need an additional storage location for the data and you must copy the data to that location regularly.

Some of these additional storage locations.

Home network : Storing your data locally means that you have total control of it.

Secondary location: You could copy all of your data to a network attached storage device (NAS), a simple external hard drive or maybe even back up important folders on thumb drives, CDs, DVDs or tapes. In this scenario, you are the owner of the data and you are totally responsible for the cost and maintenance of the storage device equipment.

The cloud: You could subscribe to a cloud storage service, like Amazon Web Services (AWS). The cost of this service will depend on the amount of storage space you need, so you may need to be more selective about what data you back up. You will have access to your backup data as long as you have access to your account.

How Do You Delete Your Data Permanently?

Have you ever had to delete data or get rid of a hard drive? If so, did you take any precautions to safeguard the data to keep it from falling into the wrong hands?

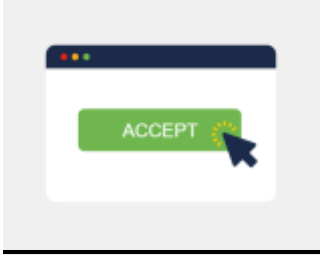
what you should do to ensure you delete your files securely and permanently.

- To erase data so that it is no longer recoverable, it must be overwritten with ones and zeroes multiple times, using tools specifically designed to do just that. SDelete from Microsoft claims to have the ability to remove sensitive files completely. Shred for Linux and Secure Empty Trash for Mac OS X claim to provide a similar service.

- The only way to be certain that data or files are not recoverable is to physically destroy the hard drive or storage device. Many criminals have taken advantage of files thought to be impenetrable or irrecoverable!

WHO OWNS YOUR DATA?

1. **Terms of Service:**
    - The Terms of Service, also known as Terms of Use or Terms and Conditions, is a legally binding contract that governs the rules of the relationship between you, the service provider and others who use the service.

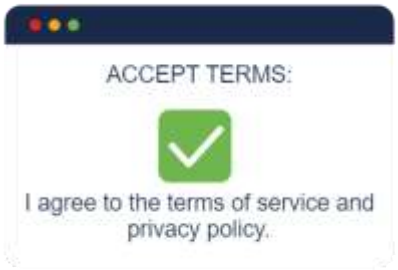


2. Understand the Terms

The Terms of Service will include a number of sections, from user rights and responsibilities to disclaimers and account modification terms.

- The data use policy outlines how the service provider will collect, use and share your data.
- The privacy settings allow you to control who sees information about you and who can access your profile or account data.
- The security policy outlines what the company is doing to secure the data it obtains from you.

3. What Are You Agreeing To?



4. The Data Use Policy

The data use policy of the company you used to set up the account states that for any content you publish: "you grant us a non-exclusive, transferable, sub-licensable, royalty-free, and worldwide license to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content (consistent with your privacy and application settings)".

It means that while you are the owner of the content, the company could re-use any content you have shared for any purposes.

5. Privacy Settings

As you didn't set the privacy settings before you accepted the terms, default settings were applied.

Accepting the default privacy settings usually means that anyone can see information about you and access your profile.

6. Before You Sign Up

What factors should you consider before you sign up to an online service?.

- Have you read the Terms of Service?
- What are your rights regarding your data?
- Can you request a copy of your data?
- What can the provider do with the data you upload?
- What happens to your data when you close your account?

7. Protect Your Data

You must always take appropriate action to protect your data and safeguard your account.

SAFEGUARDING YOUR ONLINE PRIVACY

1. **Two Factor Authentication**

- Popular online services, such as Google, Facebook, Twitter, LinkedIn, Apple and Microsoft, use two factor authentication to add an extra layer of security for account logins.
- Besides your username and password or personal identification number (PIN), two factor authentication requires a second token to verify your identity. This may be a:
    - physical object such as a credit card, mobile phone or fob
    - biometric scan such as a fingerprint or facial and voice recognition
    - verification code sent via SMS or email.

Even with two factor authentication, hackers can still gain access to online accounts through phishing attacks, malware and social engineering.

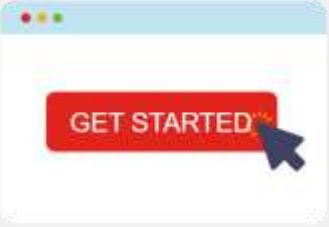
2. **Open Authorization**

Open authorization (OAuth) is an open standard protocol that allows you to use your credentials to access third-party applications without exposing your password.

EXAMPLE:

You are looking forward to registering for Cisco's 'Cybersecurity Essentials,' the next course in this series, to help you develop your career. But you must be logged into the eLearning portal to do so.

You can't remember your login details, but that's OK. The portal gives you the option of logging in using your credentials from a social media website such as Facebook or via another account such as Google.



So instead of having to reset your login details, you log into the eLearning portal using your existing social media accounts and register for your next course with ease. You can't wait to get started!

3. **Social Sharing**

- You decide to update your new job position on your social networks. When doing so, one of the sites asks you to update your profile information to ensure you receive the content that you really don't want to miss!

Email and Web Browser Privacy

These problems can be minimized by enabling the in-private browsing mode on your web browser. Many of the most commonly used web browsers have their own name for private browser mode:

Microsoft Internet Explorer: InPrivate

Google Chrome: Incognito

Mozilla Firefox: Private tab or private window

Safari: Private browsing

- When private mode is enabled, cookies — files saved to your device to indicate what websites you've visited — are disabled.
- Therefore, any temporary internet files are removed and your browsing history is deleted when you close the window or program.
- This may help to prevent others from gathering information about your online activities and trying to entice you to buy something with targeted ads.

Even with private browsing enabled and cookies disabled, companies are constantly developing new ways of fingerprinting users in order to track their online behavior. For example, some intermediary devices, like routers, can gather information about a user's web surfing history.