Cyber offenses & Cybercrime

- There are many methods and tools used by criminals tools to locate the vulnerabilities of their target. The criminals target can be an individual and/or an organization.
- Criminals plan two types of attacks against the target. They are passive and active attacks. In the active attacks criminals alter the system (i.e., computer network) and in passive attacks they try to gain information about the target.
    - Active attacks may have an effect on the integrity, availability, and authenticity of data.
    - Passive attacks cause breaches of confidentiality.
    - Active and passive attacks are also categorized as inside and outside attack.
- If an attack is originated within the security perimeter of an organization then it is an inside attack. Usually an insider who gains the access to more resources than expected attempts this attack.
- If an attack is attempted by a source outside the security perimeter then this attack is known as passive attack. The attacker can be an insider or outsider who is indirectly connected with the organization. The attack is attempted through the Internet or a remote access connection.

☸How criminal plan the attacks:

Phases involved in planning Cybercrime The phases involved in planning cybercrime are as follows :

1. Reconnaissance
2. Scanning and scrutinizing collected Information
3. Launching an attack

1. Reconnaissance

Reconnaissance (investigation or inspection) is the preliminary phase in which the hacker gathers information about the target before planning to launch an attack and is completed in phases before exploring system vulnerabilities. One of the phases is dumpster diving.

During this phase the hackers find important information such as old passwords, names of important employees (such as head of network department) and performs an active investigation on how the information flows through the organization and how the organization performs the functions.

Foot printing also provides information about the domain names, system names, active TCP and UDP services and passwords. The hacker can also use a search engine to extract information about the organization and use the information of current employees for impersonation.

The information is collected in two phases:

a. Passive attack
b. Active attack

A) Passive Attacks:

In passive attack the attacker collect the information about the target without individual for company's knowledge. For example, an attacker keep watch on an employee at what time is entering the building and leaving the premises attacker can also keep watch internet search for by using Google name get the information about an individual. The attacker can also monitor the network traffic for the emails sent using the monitoring tools. Attacker can get the General information from the following ways. Attacker can get the information from the following ways or using the following tools.

(i) **Search engines** - Searching the information about an employee on search engines like Google and Yahoo search engines.

(ii) (ii) **Social websites** - By Surfing the social websites like Facebook Instagram, Orkut etc an attacker and get the information about an individual.

(iii) (iii) **Organization website** - The organizational websites also provide personal information about the employees like their contact details email addresses etc. An attacker can also get the information from blogs, press releases, newsgroup about the company.

(iv) (iv) **Job posting** : An attacker can go through the job posting in a particular job profile for a technical person who gives information about the type of Technology, it means, the server and infrastructure devices the company is using on its network.

(v) (v) **Network sniffing** : In this attack, the attacker gives the information about the internet protocol address ranges, hidden servers or networks and other services on the system or network. The attacker monitors the flow of data check at what time certain transactions are taking place and where the traffic is going.

(vi) (vi) **People search** : It gives details about personal information like date of birth, residential address, contact number, etc.

B) Active Attacks – An active attack includes examining the system or network to find individual hosts to affirm the data (IP addresses, working framework type and form, and administrations on the system) accumulated in the passive attack stage.

Active reconnaissance can give confirmation to an attacker about security measures set up, however the procedure can likewise expand the opportunity of being gotten or raise a doubt.

2 Scanning and Scrutinizing Gathered Information

Scanning is a key step to examine intelligently while gathering information about the target. The objectives of scanning are as follows:

(i) **Port scanning:** Identify open/close ports and services.
(ii) **Network scanning:** Understand IP Addresses and related information about the computer network systems.
(iii) **Vulnerability scanning:** Understand the existing weaknesses in the system.

The scrutinizing phase is always called "enumeration" in the hacking world. The objective behind this step is to identify:

(i) The valid user accounts or groups;
(ii) Network resources and/or shared resources
(iii) OS and different applications that are running on the OS.

3 Attack (Gaining and Maintaining the System Access):

After the scanning and enumeration, the attack is launched using the following steps:

(i) Crack the password
(ii) Exploit he password
(iii) Execute the malicious command/applications;
(iv) Hide the files (if required);
(v) Cover the tracks - delete the access logs, so that there is no trail illicit activity.

☮Social engineering:

- Social engineering is a manipulation technique that exploits human error to obtain private information or valuable data.
- In cybercrime, the human hacking scams entice unsuspecting users to disclose data, spread malware infections, or give them access to restricted systems.
- Attacks can occur online, in-person, and by other interactions.
- Social engineering scams are based on how people think and act.

The stages of the social engineering attack cycle are below:

- Prepare by gathering background information on a large group.
- Infiltrate by building trust, establishing a relationship or starting a conversation.
- Establish the victim once more to confront the attack with confidence and weakness.
- Once the user takes the desired action, release it.

☯Step Social Engineering:

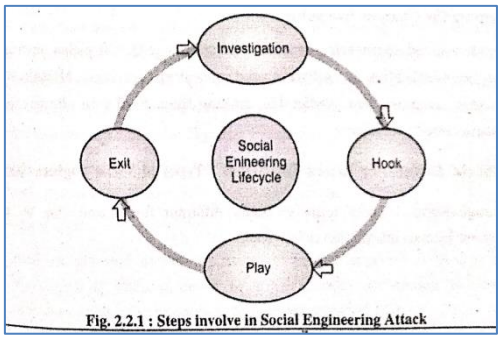


Fig. 2.2.1 : Steps involve in Social Engineering Attack

Step 1 : Investigation

- Preparing Ground for Attack.
- Identifying the victims.
- Gathering Background information.
- Selecting attack method.

Step 2: Hook : Deceiving the victims(s) to gain a foothold.

- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Step 3 : Play : Obtaining the information over a period of time.

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

Step 4 : Exit : Closing the interaction, ideally without arousing suspicion.

- Removing all traces of malware.
- Covering Track.
- Brining the Charade to a natural end.

❁Classification of Social Engineering:

1. Human-Based Social Engineering:

It needs interaction with humans; it means person-to-person contact and then retrieving the desired information. People use human based social engineering techniques in different ways; the top popular methods are:

- **Impersonating an employee or valid user:** "Impersonating an employee or valid user" is a social engineering technique that involves pretending to be a legitimate employee or authorized user in order to gain unauthorized access or manipulate individuals into revealing sensitive information or performing actions they normally wouldn't.

- **Posing as an important user**: Posing as an important user" is a social engineering technique that involves pretending to be a high-ranking or influential individual within an organization or online environment. This technique leverages authority, credibility, and the perception of importance to manipulate others into providing sensitive information, granting access, or performing actions they normally wouldn't.

- **Using a third person**: Using a third person" is a social engineering technique where an attacker communicates with a target individual while impersonating a third-party individual, such as a colleague, friend, or authority figure. This technique leverages the trust and familiarity that the target has with the third party to manipulate them into revealing sensitive information, performing actions, or making decisions that benefit the attacker's objectives.

- **Calling technical support:** Calling technical support" is a social engineering technique where an attacker poses as a legitimate technical support representative to manipulate individuals into revealing sensitive information, granting access to systems, or performing actions that compromise security. This technique leverages the target's trust in technical support personnel and their willingness to provide assistance.

- **Shoulder surfing**: Shoulder surfing" is a social engineering technique where an attacker observes or eavesdrops on a target individual while they are entering sensitive information, such as passwords, PINs, or confidential data. The attacker gains unauthorized access to the information by physically looking over the target's shoulder or using visual surveillance techniques.

- **Dumpster diving**: "Dumpster diving" is a social engineering technique where an attacker searches through physical trash, recycling bins, or discarded materials to retrieve valuable information. This technique involves retrieving documents, papers, electronic devices, or other items that contain sensitive or confidential information, which can be exploited for malicious purposes.

2. Computer –Based Social Engineering:

Computer-based social engineering uses computer software that attempts to retrieve the desired information.

- **Fake E-mails:** Fake emails" refer to phishing emails, which are a common type of social engineering technique. Phishing emails are fraudulent messages that impersonate legitimate individuals, organizations, or entities to deceive recipients into revealing sensitive information, clicking on malicious links, or downloading malicious attachments.

- **E-mail attachments**: "Email attachments" are files that are sent along with an email message. While email attachments are a convenient way to share documents, images, and other files, they can also be used as a vector for cyberattacks and social engineering techniques. Attackers often use malicious email attachments to deliver malware, viruses, or other harmful content to recipients' devices.

- **Pop-up windows**: "Pop-up windows" are small graphical user interface elements that appear on top of the current browser window or application interface. While pop-up windows can serve legitimate purposes, such

as displaying additional information or alerts, they can also be used in social engineering attacks to deceive users and manipulate their behaviour.

3.Mobile - based se:

- **Publish malicious app**: "Publishing malicious app" refers to a social engineering technique where an attacker creates and distributes mobile applications (apps) that appear legitimate but contain malicious code. These malicious apps are designed to deceive users into installing them on their devices, leading to various forms of cyberattacks or unauthorized access.

- **Repackaging legitimate app:** "Repackaging legitimate app" is a social engineering technique where an attacker takes a legitimate and popular mobile application (app), modifies it to include malicious code, and then distributes the modified version as if it were the original app. This technique exploits users' trust in well-known apps to trick them into installing and using the malicious version.

- **Using fake security apps**: "Using fake security apps" is a social engineering technique where an attacker creates and distributes mobile applications (apps) that claim to provide security features, such as antivirus or anti-malware protection, but are actually malicious or ineffective. These fake security apps are designed to deceive users into installing them on their devices, leading to various forms of cyberattacks or unauthorized access.

Prev:

- **Email hijacking is rampant**. Hackers, spammers, and social engineers taking over control of people's email accounts (and other communication accounts) has become rampant. Once they control someone's email account they prey on the trust of all the person's contacts. Even when the sender appears to be someone you know, if you aren't expecting an email with a link or attachment check with your friend before opening links or downloading.
- **Beware of any download.** If you don't know the sender personally AND expect a file from them, downloading anything is a mistake.
- **Foreign offers are fake**. If you receive email from a foreign lottery or sweepstakes, money from an unknown relative, or requests to transfer funds from a foreign country for a share of the money it is guaranteed to be a scam.
- **Set your spam filters to high.** Every email program has spam filters. To find yours, look under your settings options, and set these high–just remember to check your spam folder periodically to see if legitimate email has been accidentally trapped there. You can also search for a step-by-step guide to setting your spam filters by searching on the name of your email provider plus the phrase 'spam filters'.
- **Secure your computing devices.** Install anti-virus software, firewalls, email filters and keep these up-to-date. Set your operating system to automatically update, and if your smartphone doesn't automatically update, manually update it whenever you receive a notice to do so. Use an anti-phishing tool offered by your web browser or third party to alert you to risks.

✳Cyberstalking:

In Cyber Stalking, a cyber criminal uses the internet to consistently threaten somebody.

This crime is often perpetrated through email, social media, and the other online medium.

Cyber Stalking can even occur in conjunction with the additional ancient type of stalking, wherever the bad person harasses the victim offline.

Social media, blogs, image sharing sites and lots of different ordinarily used online sharing activities offer cyber Stalkers with a wealth of data that helps them arrange their harassment.

It includes actions like false accusations, fraud, information destruction, threats to life and manipulation through threats of exposure.

Examples of how Cyberstalking might take place:

- Posting offensive, suggestive, or rude comments online
- Sending threatening, lewd, or offensive emails or messages to the victim
- Joining the same groups and forums as the victim
- Releasing the victim's confidential information online
- Tracking all online movements of the victim through tracking devices
- Using technology for blackmailing or threatening the victim
- Excessively tagging the victim in irrelevant posts

❌Types of Cyber Stalking:

Webcam Hijacking: Internet stalkers would attempt to trick you into downloading and putting in a malware-infected file that may grant them access to your webcam. the method is therefore sneaky that it's probably you wouldn't suspect anything strange.

Observing location check-ins on social media: In case you're adding location check-ins to your Facebook posts, you're making it overly simple for an internet stalker to follow you by just looking through your social media profiles.

Catfishing: Catfishing happens via social media sites, for example, Facebook, when internet stalkers make counterfeit user-profiles and approach their victims as a companion of a companion.

Visiting virtually via Google Maps Street View: If a stalker discovers the victim's address, then it is not hard to find the area, neighbourhood, and surroundings by using Street View. Tech-savvy stalkers don't need that too.

Installing Stalkerware: One more method which is increasing its popularity is the use of Stalkerware. It is a kind of software or spyware which keeps track of the location, enable access to text and browsing history, make an audio recording, etc. And an important thing is that it runs in the background without any knowledge to the victim.

Looking at geotags to track location: Mostly digital pictures contain geotags which is having information like the time and location of the picture when shot in the form of metadata. Geotags comes in the EXIF format embedded into an image and is readable with the help of special apps. In this way, the stalker keeps an eye on the victim and gets the information about their whereabouts.

Protective Measures:

- Develop the habit of logging out of the PC when not in use.
- Remove any future events you're close to attending from the social networks if they're recorded on online approaching events and calendars.
- Set strong and distinctive passwords for your online accounts.
- Cyber Stalkers can exploit the low security of public Wi-Fi networks to snoop on your online activity. Therefore, avoid sending personal emails or sharing your sensitive info when connected to an unsecured public Wi-Fi.
- Make use of the privacy settings provided by the social networking sites and keep all info restricted to the nearest of friends.
- Do a daily search on the internet to search out what information is accessible regarding you for the public to check.

Bot nets:

- Bot: " an automated program for doing some particular task, often over a network"
- A botnet (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet.
- Any such computer is referred to as a zombie - in effect, a computer "robot" or "bot" that serves the wishes of some master spam or virus originator.
- Most computers compromised in this way are home-based.
- According to a report from Russian-based Kaspersky Labs, botnets -- not spam, viruses, or worms -- currently pose the biggest threat to the Internet.

Working:

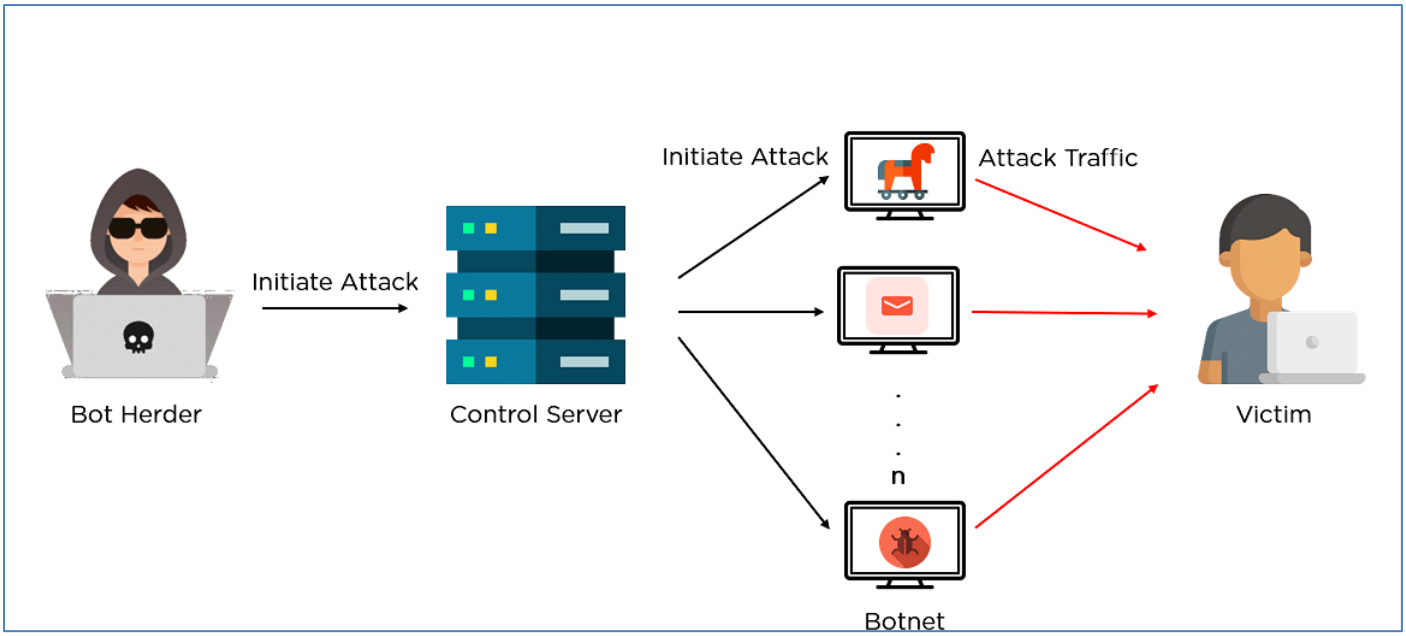
Prepping the Botnet Army: The first step in creating a botnet is to infect as many connected devices as possible, to ensure that there are enough bots to carry out the attack. It uses the computing power of the infected devices for tasks that remain hidden to the device owners. However, the fraction of bandwidth taken from a single machine isn't sufficient, and hence the Botnet combines millions of devices to carry out large-scale attacks. This way, it creates bots either by exploiting security gaps in software or websites or phishing emails. They often deploy botnets through a trojan horse virus.

Establishing the connection: Once it hacks the device, as per the previous step, it infects it with a specific malware that connects the device back to the central botnet server. This way, it connects all the devices within the botnet network, and they are ready to execute the attack. A bot herder uses command programming to drive the bot's actions.

Launching the attack: Once infected, a bot allows access to admin-level operations like gathering and stealing user data, reading and writing system data, monitoring user activities, performing DDoS attacks, sending spam, launching brute force attacks, crypto mining, and so on.

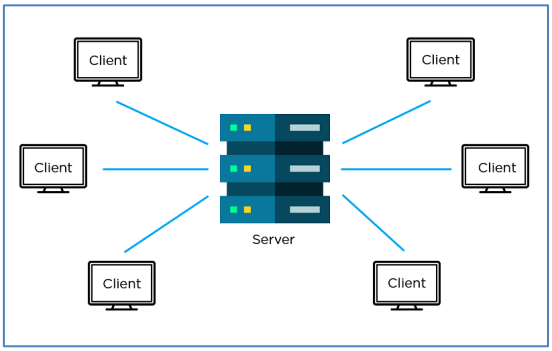
Botnet structure| architecture :

(i) 1 client-server model
(ii) 2. peer to peer



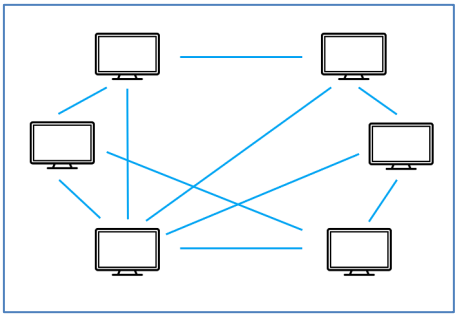
The client-server model

The client-server model is a traditional model that operates with the help of a command and control (C&C) server and communication protocols like IRC. For example, IRC or Internet Relay Chat sends automated commands to the infected bot devices.



P2P

Instead of using C&C servers, we have the P2P approach. Here, controlling infected bots involves a peer-to-peer network that relies on a decentralized approach. As seen in the above image, bots are topologically interconnected and act as both C&C servers and clients. Today, hackers adopt this approach to avoid detection and single-point failure.



How to Protect Yourself from Botnets:

(i) **Improve all user passwords for smart devices**. Using complex and long passwords will help your devices stay safer than weak and short passwords. Such as 'pass12345.

(ii) **Avoid buying devices with weak security**. While this isn't always easy to spot, many cheap smart home gadgets tend to prioritize user convenience over security. Research reviews on a product's safety and security features before buying.

(iii) **Update admin settings and passwords across all your devices**. You'll want to check all possible privacy and security options on anything that connects device-to-device or to the internet. Even smart refrigerators and Bluetooth-equipped vehicles have default manufacturer passwords to access their software systems. Without updates to custom login credentials and private connectivity, hackers can breach and infect each of your connected devices.

(iv) **Be wary of any email attachments**. The best approach is to completely avoid downloading attachments. When you need to download an attachment, carefully investigate, and verify the sender's email address. Also, consider using antivirus software that proactively scans attachments for malware before you download.

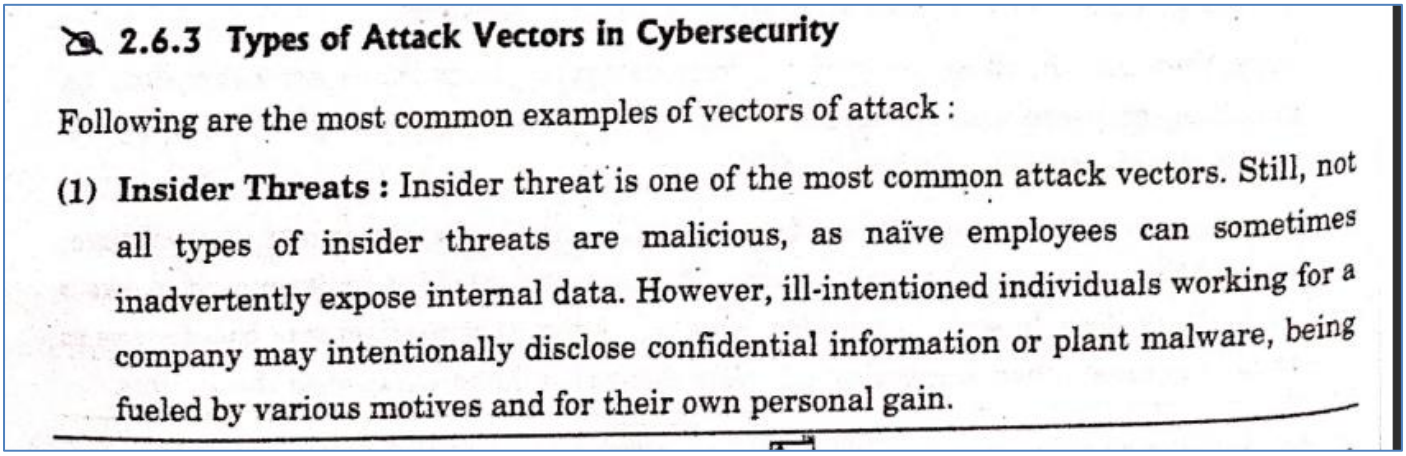
(v) **Never click links in any message you receive**. Texts, emails, and social media messages can all be reliable vehicles for botnet malware. Manually entering the link into the address bar will help you avoid DNS cache poisoning and drive-by downloads. Also, take an extra step to search for an official version of the link.

(vi) **Install effective anti-virus software**. A strong internet security suite will help to protect your computer against Trojans and other threats. Be sure to get a product that covers all your devices, including Android phones and tablets.

Attack vector:

An attack vector is a method or pathway used by a hacker to access or penetrates the target system. Hackers steal information, data and money from people and organizations by investigating known attack vectors and attempting to exploit vulnerabilities to gain access to the desired system.

- Attack vectors enable hackers to exploit system vulnerabilities, including the human element.
- Attack vectors include viruses, e-mail attachments, Web pages, pop-up windows, instant messages, chat rooms, and deception. All of these methods involve programming (or, in a few cases, hardware), except deception, in which a human operator is fooled into removing or weakening system defenses.



2.6.3 Types of Attack Vectors in Cybersecurity

Following are the most common examples of vectors of attack :

(1) **Insider Threats :** Insider threat is one of the most common attack vectors. Still, not all types of insider threats are malicious, as naïve employees can sometimes inadvertently expose internal data. However, ill-intentioned individuals working for a company may intentionally disclose confidential information or plant malware, being fueled by various motives and for their own personal gain.

(2) **Phishing :** Phishing is merely one of many hats that social engineering wears. It involves manipulation tactics adopted by a malicious individual whose ultimate purpose is to trick employees into clicking on suspicious links, opening malware-infected email attachments, or giving away their login credentials.

The most insidious subtype of phishing is spear phishing, where very specific employees are observed in great detail only to be targeted later on by cybercriminals. This phenomenon is also part of the rising threat of Business Email Compromise (BEC), a highly sophisticated practice that can devastate companies of all sizes.

(3) **Business partners :** Third-party organizations can also become major vectors of attack in cybersecurity. Some of the biggest security incidents and data breaches have been caused by vendors. Supply chain attacks are a common way for attackers to target a vendor's customers. This is the reason why organizations large and small together with their business partners must foster a culture where cybersecurity best practices are shared and mutual transparency is demonstrated.

(4) **Weak or compromised login credentials :** Should your employees' authentication credentials be too weak or become comprised, they may turn out to be an attacker's surefire way to gain unauthorized access to your IT systems.

Usernames and passwords are the most popular form of authentication that can easily be abused through phishing, data leaks, and credential-stealing malware, giving intruders free access to your workers' accounts.

(5) **Ransomware / Malware :** Ransomware continues to be a highly lucrative business for cybercriminals. Given its huge profits, it's no surprise that ransomware has even developed into a "business" model – Ransomware as a Service. This allows it to become easily accessible even to people with rather poor technical skills but determined to profit from vulnerable users.

At the same time, the huge palette of other existing types of malware can facilitate the infiltration of malicious hackers inside your organization – think about worms, trojans, rootkits, adware, spyware, file-less malware, bots, and many more.

2.6.4 Protect Devices from Common Attack Vectors

GQ. How to Protect Devices from Common Attack Vectors ?

- Install and use security solutions that can detect and block spam, malware, and malicious links so these cannot be compromised.

- Regularly download and apply patches to your devices and the applications installed on them, so these will have fewer or even no vulnerabilities that bad guys can exploit.
- Stay abreast of the latest cybersecurity news and updates. Anyone can be a victim of a cyber attack, so it is always best to be aware of threats and prepared to protect against them. Keep in mind that prevention is still better than cure.
- For organizations, conduct regular security training for employees because attackers often employ very clever social engineering tricks to trick them into getting into your networks.
- Educate the employee to recognize the signs of phishing, BEC, how to create their passwords based on your internal password policy and avoid the most common password mistakes, identify different types of malware, and learn how to report cybersecurity incidents and potential threats.

☁Cloud computing

Cloud computing means storing and accessing the data and programs on remote servers that are hosted on the internet instead of the computer's hard drive or local server. Cloud computing is also referred to as Internet-based computing, it is a technology where the resource is provided as a service through the Internet to the user. The data which is stored can be files, images, documents, or any other storable document.

Some operations which can be performed with cloud computing are –

- Storage, backup, and recovery of data
- Delivery of software on demand
- Development of new applications and services
- Streaming videos and audio

☁Types of Cloud

There are the following 5 types of cloud that you can deploy according to the organization's needs-

- **Public Cloud:** Computing resources are owned and operated by a third-party cloud service provider and are made available to the general public. Examples include AWS, Azure, and Google Cloud.
- **Private Cloud:** Computing resources are used exclusively by a single organization. This can be managed on-premises or by a third-party provider.
- **Hybrid Cloud:** Combines public and private cloud environments, allowing data and applications to be shared between them. It provides greater flexibility and optimization of existing infrastructure.

Service Models:

- **Infrastructure as a Service (IaaS):** Provides virtualized computing resources over the internet. Users can rent virtual machines, storage, and network infrastructure.
- **Platform as a Service (PaaS):** Offers a platform that allows users to develop, run, and manage applications without dealing with the complexities of underlying infrastructure.
- **Software as a Service (SaaS):** Delivers software applications over the internet on a subscription basis. Users can access applications without the need for installation or maintenance.

🍀Benefits of Cloud Computing:

- **Cost Efficiency**: Users pay for the resources they consume, avoiding the upfront costs and complexity of owning and maintaining physical infrastructure.
- **Scalability**: Cloud resources can be easily scaled up or down to accommodate changes in demand, providing flexibility and cost savings.
- **Flexibility and Accessibility**: Cloud services can be accessed from anywhere with an internet connection, allowing for increased flexibility and collaboration.
- **Automatic Updates**: Service providers handle software updates and maintenance, ensuring that users have access to the latest features and security patches.

types of attack in Cloud computing

Cloud computing, while offering numerous benefits, introduces its own set of security challenges. Various types of attacks can target cloud environments. Here are some common types of attacks in cloud computing:

1. **Data Breach:**

    - **Unauthorized Access:** Attackers gain unauthorized access to sensitive data stored in the cloud, potentially through weak credentials or compromised user accounts.
    - **Data Interception:** Intercepting data during transmission between the user and the cloud service, exploiting vulnerabilities in encryption or communication protocols.

2. **Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks:**

    - **Service Disruption:** Overwhelming cloud resources with traffic to disrupt or degrade service availability, making applications and services unavailable to legitimate users.

3. **Man-in-the-Middle (MitM) Attacks:**

    - **Interception of Communication:** Attackers intercept and potentially alter communications between users and the cloud service, leading to data manipulation or theft.

4. **Insecure Interfaces and APIs:**

    - **Exploiting Weak Interfaces:** Attackers exploit vulnerabilities in cloud service interfaces and APIs, potentially gaining unauthorized access or manipulating data.

5. **Insider Threats:**

    - **Malicious Insiders:** Authorized users with malicious intent can misuse their privileges to access or manipulate data.
    - **Unintentional Insider Threats:** Users may unintentionally expose sensitive data or misconfigure security settings, leading to security incidents.

6. **Eavesdropping:**

    - **Unauthorized Monitoring:** Attackers monitor network traffic or communication within the cloud to gain insights into sensitive information.

7. **Malware Injection:**

    - **Introducing Malicious Code:** Injecting malware into cloud-based applications or services, which can lead to data theft, disruption, or unauthorized access.

8. **Credential Theft:**

    - **Phishing and Social Engineering:** Tricking users into revealing their login credentials, leading to unauthorized access to cloud accounts.
    - **Keylogging:** Recording keystrokes to capture sensitive information, including usernames and passwords.

Proliferation of Mobile and Wireless Devices:

Today, incredible advances are being made for mobile devices. The trend is for smaller devices and more processing power. A few years ago, the choice was between a wireless phone and a simple PDA. Now the buyers have a choice between high-end PDAs with integrated wireless modems and small phones with wireless Web-browsing capabilities. A long list of options is available to the mobile users. A simple hand-held mobile device provides enough computing

power to run small applications, play games and music, and make voice calls. A key driver for the growth of mobile technology is the rapid growth of business solutions into hand-held devices.

As the term "mobile device" includes many products. We first provide a clear distinction among the key terms: mobile computing, wireless computing and hand-held devices. Figure below helps us understand how these terms are related. Let us understand the concept of mobile computing and the various types of devices.

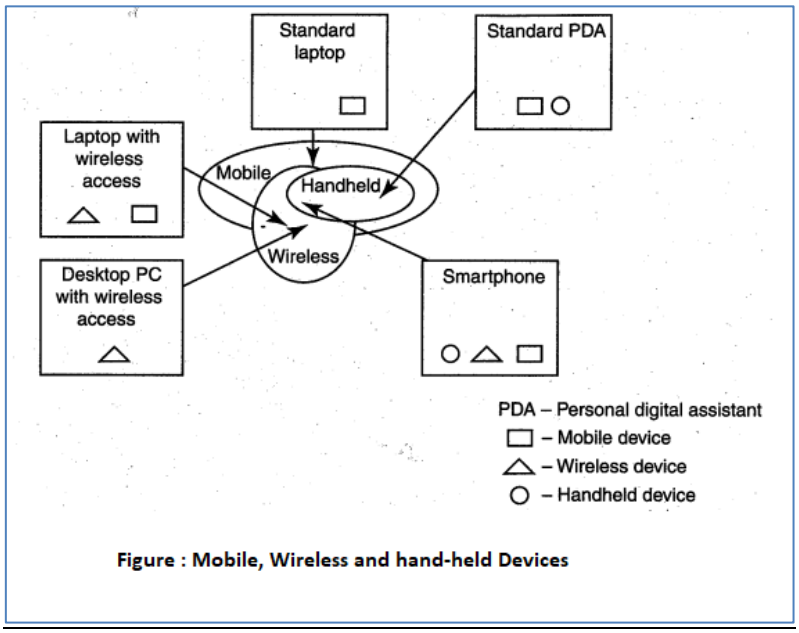


Figure : Mobile, Wireless and hand-held Devices

Mobile computing is "taking a computer and all necessary files and software out into the field." Many types of mobile computers have been introduced since 1990s. They are as follows:

1. **Portable computer:** It is a general-purpose computer that can be easily moved from one place to another, but cannot be used while in transit, usually because it requires some "setting-up" and an AC power source.

2. **Tablet PC:** It lacks a keyboard, is shaped like a slate or a paper notebook and has features of a touchscreen with a stylus and handwriting recognition software. Tablets may not be best suited for applications requiring a physical keyboard for typing, but are otherwise capable of carrying out most tasks that an ordinary laptop would be able to perform.

3. **Internet tablet**: It is the Internet appliance in tablet form. Unlike a Tablet PC, the Internet tablet does not have much computing power and its applications suite is limited. Also it cannot replace a general-purpose computer. The Internet tablets typically feature an MP3 and video player, a Web browser, a chat application and a picture viewer.

4. **Personal digital assistant (PDA**): It is a small, usually pocket-sized, computer with limited functionality. It is intended to supplement and synchronize with a desktop computer, giving access to contacts, address book, notes, E-Mail and other features.

5. **Ultramobile** (PC): It is a full-featured, PDA-sized computer running a general-purpose operating system (OS).

6. **Smartphone**: It is a PDA with an integrated cell phone functionality. Current Smartphones have a wide range of features and installable applications.

7. **Carputer**: It is a computing device installed in an automobile. It operates as a wireless computer, sound system, global positioning system (GPS) and DVD player. It also contains word processing software and is Bluetooth compatible.

8. **Fly Fusion Pentop computer**: It is a computing device with the size and shape of a pen. It functions as a writing utensil, MP3 player, language translator, digital storage device and calculator.

💳 Credit Card Frauds in Mobile and Wireless Computing Era:

The use of electronic credit cards made the process a lot faster. The terminals could dial banks automatically and verify the cards electronically in a matter of a few seconds. However, the magnetic medium of data storage on credit cards proved to have many problems. The magnetic strips can only hold a limited amount of information; also the information on the strips is easy to read with the right electronic devices even easy to copy and erase.

2.10.1 Elements of Credit Card Fraud

- Debit card fraud is thus committed when a person,
  (1) Fraudulently obtains, takes, signs, uses, sells, buys, or forges someone else's credit or debit card or card information;
  (2) Uses his or her own card with the knowledge that it is revoked or expired or that the account lacks enough money to pay for the items charged; and
  (3) Sells goods or services to someone else with knowledge that the credit or debit card being used was illegally obtained or is being used without authorization.
- Theft, the most obvious form of credit card fraud, can happen in a variety of ways, from low tech dumpster diving to high tech hacking. A thief might go through the trash to find discarded billing statements and then use your account information to buy things.
- A retail or bank website might get hacked, and your card number could be stolen and shared. Perhaps a dishonest clerk or waiter takes a photo of your credit card and uses your account to buy items or create another account.

2.10.2 Types of Credit Card Fraud

GQ. What are the Types of Credit Card Fraud ?

(1) **Lost or stolen cards :** It is relatively common one, and should be reported immediately to minimize any damages.

(2) **Account Takeover :** When a cardholder without knowing gives personal information to a fraudster, who then contacts the cardholder's bank, reports a lost card and change of address, and obtains a new card in the soon-to-be victim's name.

(3) **Clone :** When a card is "cloned" from another and then used to make purchases. In Asia Pacific, 10% to 15% of fraud results from malpractices such as card skimming but this number has significantly dropped from what it was a couple of years prior, largely due to the many safety features put in place for payment cards, such as EMV chip.

(4) **Never received :** When a new or replacement card is stolen from the mail, never reaching its rightful owner.

(5) **Fraudulent Application :** When a fraudster uses another person's name and information to apply for and obtain a credit card.

(6) **Multiple Imprint :** When a single transaction is recorded multiple times on old-fashioned credit card imprint machines known as "knuckle busters".

(7) **Collusive Merchants :** When merchant employees work with fraudsters to defraud banks.

Prevention

Following are some of fraud protection practices include :

- Don't give your account number to anyone on the phone unless you've made the call to a company you know to be reputable. If you've never done business with them before, do an online search first for reviews or complaints.
- Carry your cards separately from your wallet. It can minimize your losses if someone steals your wallet or purse. And carry only the card you need for that outing.
- During a transaction, keep your eye on your card. Make sure you get it back before you walk away.
- Never sign a blank receipt. Draw a line through any blank spaces above the total.
- Save your receipts to compare with your statement.
- Open your bills promptly or check them online often and reconcile them with the purchases you have made.
- Report any questionable charges to the card issuer.
- Notify your card issuer if your address changes or if you will be traveling.

⏭ 2.11 SECURITY CHALLENGES POSED BY MOBILE DEVICES

GQ. What are the Security Challenges Posed by Mobile Devices?

- Mobility brings two main challenges to cybersecurity: first, on the hand-held devices, information is being taken outside the physically controlled environment and second remote access back to the protected environment is being granted.

- As the number of mobile device users increases, two challenges are presented: one at the device level called "micro challenges" and another at the organizational level called "macro-challenges."
- Some well-known technical challenges in mobile security are: managing the registry settings and configurations, authentication service security, cryptography security, Lightweight Directory Access Protocol (LDAP) security, remote access server (RAS) security, media player control security, networking application program interface (API), security etc.

(1) **Physical Security :** Physical security is often a second thought when it comes to information security. Every year thousand of mobile phones are lost, and nearly all who found lost devices tried to access the information on the phone. Even temporarily misplacing a phone can put sensitive data at risk.

(2) **Multiple User Logging :** Mobile phones have come a long way, but they are still not versatile machines like computers. Multiple users on mobile devices still have trouble in opening unique protected accounts. Customizable 3rd party solutions are available, but it's much safer when phones are not shared.

(3) **Secure Data Storage :** Mobile phones need good file encrypting for strong security. Without the proper encryption, not only are personal documents up for grabs, but also passwords to bank, credit card and even business apps.

(4) **Mobile Browsing :** Perhaps one of the best features of mobile devices is the ability to browse the web on the go, but this also opens up the mobile phones to security risks. The problem is that users cannot see the whole URL or link, much less verify whether the link or URL is safe. That means that users could easily browse their way into a phishing-related attack.

(6) **System Updates :** Updates and patches designed to fix issues in mobile devices are not quite as cut and dry as with PCs. Mobile devices vendors often release updates and patches, but unfortunately carriers don't always stream them due to commercial or bureaucratic reasons.

(7) **Mobile Device Coding Issues :** Sometimes developers make honest mistakes, inadvertently creating security vulnerabilities via poor coding efforts. Many times there is bad implementation of encrypted channels for data transmission or even improper password protection. Ineffective development can lead to security weaknesses whether in PCs or mobile phones.

(8) **Bluetooth Attacks :** As easy as Bluetooth is to use, it can be just as easy for attackers to gain access to one's phone and everything stored within. It's fairly simple for a hacker to run a program to locate available Bluetooth connections. It's important to remember to disable the Bluetooth functionality when not in use.

(9) **Malware on the Rise :** As is the case with computers, malware is rather damaging to mobile phones. This is one of the unknown risk which can cause heavy losses.

(10) **Serious Threats in New Features :** Newly added features and updates are serious risks too. The Neat Field Communication, or NFC, technology is a prime example. NFC is designed to allow people to use their mobile phones as a wallet to purchase products. Unfortunately, all one needs to do to take over the mobile device is brush a NFC chip embedded tag over the phone.

2.11.1 How to Ensure Your Mobile Security and Privacy

(1) **Always password-protect your phone :** Use passwords and if possible, fingerprint detection. This way if you forget your phone, lose it or it is stolen whoever finds it won't have easy access.

(2) **Only download safe apps :** Apps are the easiest point of entry for hackers and malware because we willingly download them to our phone. All they have to do is make one attractive enough for us to want to download it. This is why it is important to get apps from trusted sources like the Google Play App Store or the iTunes App Store and even then it is important to verify an app's trustworthiness by checking reviews from other users.

(3) **Always read the terms and privacy policy :** All apps collect and use our information to some extent. Always be sure to read the terms of use and privacy policy to see what information is collected, how it is used and where it may be shared.

(4) **Turn off the Bluetooth :** It is a good idea to turn off the Bluetooth on your mobile device when not using it. Aside from closing down a potential point of entry it will also cut down on your battery usage.

(5) **Encrypt your phone :** Most of today's phones have some form of automatic encryption or encryption feature you can enable. Be sure to do so.

(6) **Set up remote locate/wipe :** Most phones have features that can be used to remotely wipe your phones memory and/or geolocate it. This feature is especially useful if there is sensitive data on your phone or you do not expect to get it back. When used in conjunction with password protection, it can keep the loss of data to a minimum.

(7) **Back up your data :** Most mobile users back up their data about as often as they update their operating systems, which is to say not too often. You can upload your phone's settings, data, pictures, music and etc. to the cloud, which in itself poses a risk to your security, or directly to a laptop or PC.

2.14 ATTACKS ON MOBILE/CELL PHONES

GQ. Write a short note on Attacks on Mobile/Cell Phones.

A smartphone user is exposed to various threats when they use their phone. In just the last few years, the number of unique mobile threats grew much more. These threats can disrupt the operation of the smartphone, and transmit or modify user data. For these reasons, the applications deployed there must guarantee privacy and integrity of the information they handle.

There are three prime targets for attackers :

- **Data :** smartphones are devices for data management, therefore they may contain sensitive data like credit card numbers, authentication information, private information, activity logs (calendar, call logs);
- **Identity :** smartphones are highly customizable, so the device or its contents are associated with a specific person. For example, an attacker may want to steal the identity of the owner of a smartphone to commit other offenses;
- **Availability :** by attacking a smartphone one can limit access to it and deprive the owner of the service.

- Followings are some of the most common types of Wireless and Mobile Device Attacks :

  (i) **Mishing :** Mishing is a combination of mobile phone and phishing. Mishing is similar to phishing the only diffrenece is technology. The attack is chances increases when you purchase goods using the M-commerce, someone can cheat a m-commerce customer by making a call using some malicious number so by the end of the call your mobile is infected with the malwares.

  (ii) **Vishing :** Voice call phishing is known as vishing. For instance, the cybercriminal may employ war dialers to place a call and play a recorded message informing the victim that their credit card may be blocked and that in order to keep it active, they must supply the card data. The user may become a victim of a phishing attempt if he provides the card data. However the cybercriminal uses many other ways to perform phishing like voice mail.

(1) **SMiShing :** Smishing become common now as smartphones are widely used. SMiShing uses Short Message Service (SMS) to send fraud text messages or links. The criminals cheat the user by calling. Victims may provide sensitive information such as credit card information, account information, etc. Accessing a website might result in the user unknowingly downloading malware that infects the device.

(2) **War driving :** War driving is a way used by attackers to find access points wherever they can be. With the availability of free Wi-Fi connection, they can drive around and obtain a very huge amount of information over a very short period of time.

(3) **WEP attack :** Wired Equivalent Privacy (WEP) is a security protocol that attempted to provide a wireless local area network with the same level of security as a wired LAN. Since physical security steps help to protect a wired LAN, WEP attempts to provide similar protection for data transmitted over WLAN with encryption.

2.16 SECURITY IMPLICATIONS FOR ORGANIZATIONS

GQ. Explain in brief about Security Implications for Organizations.

- Data security is a big deal for any company. Indeed, there was millions of cyber-attacks happened in past few years and the numbers are increasing day by day. One breach could deeply harm any business organisation. This could suffer heavy losses to organisation in long term and harm for reputation also.
- Keeping Data safe should be a priority for any organisation or company. Following are the best Data Security measures,

(1) Firewall

- A firewall is one of these tools, and the security functionalities that it brings to the table are immense.
- For one, it filters your network traffic and avails you a way of selectively blocking IP addresses. And, since one or more of your processes are based on the cloud, it is ideal to use a firewall as an identity authorization tool. The same is true for your company's back-end database, which is integral to the running of your websites and apps.

(2) Secure Browsers

- Browsers remain the de facto gateway to the internet. Obviously, it is almost impossible to avoid them, even if hackers and third parties occasionally capitalize on their security weaknesses to track internet users.
- Organizations, therefore, should enforce the use of secure browsers, which do not save or log employees' online activities and restrict cookies and third-party sites or service providers from trying to track your business.
- If company is more comfortable with popular and more efficient browsers, however, one should ensure that employees use the safe mode feature.

(3) Install and Keep Antivirus Up-to-date

- Every computer authorized to access your server or database is a potential access point for nefarious infiltrations. As such, a device with outdated antivirus or security tools is a weak link that could be detrimental to the safety of your business. In light of this, comparing different service providers and choosing the right antivirus software is also highly important.
- In as much as you have adopted various cloaking and network protection tools, do not underestimate today's hacking ingenuity, which rightly has directors worried, by forgoing the need for a formidable and up-to-date antivirus.

(4) Virtual Private Network (VPN)

- A VPN offers control on organisations data as it comes with encryption features for all your internet data transfer. For companies that make their online resources remotely accessible to employees, a VPN could ensure that the security status of their connection does not risk the integrity of their network or cloud database.

(6) Educate Your Employees

- Even any organisation have all these tools available on the ground, they are useless if they are not used.
- Therefore, organisations must have well-defined security policies and frequently educate the employees on the importance of being security-conscious by providing guidelines on how to use security tools.

(8) Embrace Cloud Solutions

- Staying up-to-date with the many protective tools and technologies for in-house servers or databases can be a daunting task.
- The easiest way around this is to transfer these resources to secure cloud platforms. These providers have robust security systems and, as they are commercial platforms, they tend to invest in the latest sophisticated solutions.

(9) Secure Your IoT Infrastructure

- IoT is a trending technology, particularly in the business world.
- On the downside, employing this technology multiplies your security vulnerabilities.
- Nevertheless, organisation can change the narrative by ensuring that each IoT - enabled device is secure and that the IoT network comes with high-end encryptions.

✡Devices-Related Security Issues:

- Employees aren't just bringing their mobile devices to the workplace they're living on them. For many, checking their phones is the first and last thing they do every day.
- As smartphones and tablets become constant companions, hackers are seeking every avenue available to break into them.

- Many people expect that iPhone or Android devices are secure by default, when in reality it is up to the user to make security configuration changes.
- With the right equipment, hackers can gain access to a nearby mobile device in less than 30 seconds and either mirror the device and see everything on it, or install malware that will enable them to draw off data from it at their freedom.
- The nature and types of cyber attacks are evolving rapidly, and mobile devices have become a critical part of enterprise cybersecurity efforts with good reason.
- In order to secure the corporate data passing through or residing on mobile devices, it is imperative to fully understand the issues they present.
- The threat and attack vectors for mobile devices are largely composed of retargeted versions of attacks aimed at other endpoint devices. These risks can be categorized into five areas.

(1) Physical access

- Mobile devices are small, easily portable and extremely lightweight. While their diminutive size makes them ideal travel companions, it also makes them easy to steal or leave behind in airports, airplanes or taxicabs.
- As with more traditional devices, physical access to a mobile device equals "game over." The cleverest intrusion-detection system and best anti-virus software are useless against a malicious person with physical access. Circumventing a password or lock is a trivial task for a seasoned attacker, and even encrypted data can be accessed.

(2) Malicious Code

- Mobile malware threats are typically socially engineered and focus on tricking the user into accepting what the hacker is selling.

- Android devices are the biggest targets, as they are widely used and easy to develop software for. Mobile malware Trojans designed to steal data can operate over either the mobile phone network or any connected Wi-Fi network. They are often sent via SMS (text message); once the user clicks on a link in the message, the Trojan is delivered by way of an application, where it is then free to spread to other devices. When these applications transmit their information over mobile phone networks, they present a large information gap that is difficult to overcome in a corporate environment.

(3) Device Attacks

- Attacks targeted at the device itself are similar to the PC attacks of the past. Browser-based attacks, buffer overflow exploitations and other attacks are possible.
- The short message service (SMS) and multimedia message service (MMS) offered on mobile devices afford additional avenues to hackers.
- Device attacks are typically designed to either gain control of the device and access data, or to attempt a distributed denial of service (DDoS).

(4) Communication Interception

- Wi-Fi-enabled smartphones are susceptible to the same attacks that affect other Wi-Fi-capable devices.
- The technology to hack into wireless networks is readily available, and much of it is accessible online, making Wi-Fi hacking and man-in-the-middle (MITM) attacks easy to perform. Cellular data transmission can also be intercepted and decrypted.

(5) Insider Threats

- Mobile devices can also facilitate threats from employees and other insiders. Humans are the weakest link in any security strategy, and many employees have neither the knowledge, nor the time to track whether or not their devices have updated security software installed.
- The downloading of applications can also lead to unintentional threats. Most people download applications from app stores and use mobile applications that can access enterprise assets without any idea of who developed the application, how good it is, or whether there is a threat vector through the application right back to the corporate network.