2.3. How Do Criminals Plan Attacks?

Cybercriminals make use of many tools and techniques to locate the vulnerability of their target/victim. The target can be an individual, an organisation, a computer system or a group of computer systems. Attackers plan attacks in either passive or active mode. They try to gain information about the target in a passive attack. Whereas, through active attacks, they try to alter computer systems.

Attacks can also be categorised as inside attacks and outside attacks. Attacks performed within organisations are called inside attacks whereas attacker get information from outside is called outside attack. Inside attacks are always more dangerous than outside attacks because inside attackers have more resources than outsider attackers.

The following are three major phases involved in the planning of a cybercrime.

1. **Reconnaissance**

   It is the first step of attackers towards cybercrime. "Reconnaissance" means an act of reconnoitring. In this phase, an attacker tries to explore and gain every possible information about system resources, vulnerabilities, or services on the victim's/target's system. This is also referred as "foot printing". Foot printing provides information about the overall system structure, loopholes and exploration of those loopholes. The goal of the attacker in this phase is to understand the system, personal information about the target, networking ports and services running on those ports and any other related information. In reconnaissance, information is gathered in active and passive phases.

Passive Attacks

Passive attacks are used to gain information about individuals or organisations. They exploit confidential information. Such attacks involve gaining data about a target without the knowledge of the target. In today's Internet era, it has become much easier for an attacker to launch a passive attack to gather information about a target.

Some of the simple ways to gather information about the target are given as follows:

- **Use Google or other search engines:** Gather information about the target by searching on Google.
- **Social media:** Search on social media websites like Facebook, Twitter, and LinkedIn.
- Use properly privacy setting in social media to avoid
- **Organisation website:** An attacker may get detailed employee information using an organisational website.
- **Blog or press release:** These are new sources where an attacker can easily get company or individual information.
- **Job posting:** A job profile provides valuable information about a person. The job profile of a technical person can give data about the type of technology, that is, software, server, database or network devices, a company is using on its network.
- **Network sniffing:** This attack is used to gather information such as IP address, network range, hidden server and other valuable services on the network.

Table 1 shows some of the famous tools used for launching passive attacks.

Table 1: Tools Used for Launching Passive Attacks

CheckUserNames: It is an online tool used to find usernames across over 170 social networks. This is useful for the investigation to determine the usage of the same username on different social networks. It can also be used to check for brand company names, not just for individuals.
BuiltWith: BuiltWith detects technologies used at particular websites on the Internet. It includes full detailed information about CMS, JavaScript and CSS libraries, web server type, SSL provider as well as web hosting provider used.
WHOIS: It is a domain registration lookup tool. The WHOIS database of a domain is the publicly displayed information about a domain's ownership, billing, technical, administrative, and nameserver information. Running a WHOIS on your domain will look the domain up at the registrar for the domain information. All domains have WHOIS information. WHOIS database can be queried to obtain administrative contact details, including names, e-mail addresses, telephone numbers, mailing addresses for office locations relating to the target organisation and details of authoritative name servers for each given domain.
Nslookup: The Nslookup command is used to query Internet name servers interactively for information. It is a useful tool for finding out information about a named domain.
Traceroute: The traceroute command is used to discover the routes that packets actually take when travelling to their destination. It prints the complete route information that packets take to reach the network host.
eMailtrackerPro: eMailtrackerPro is an e-mail header analyser tool which gives detail e-mail tracing information and discloses the original sender's details.
HTTrack: HTTrack allows the download of a website to a local directory by building recursively all directories, and by getting HTML, images, and other files from the server to the user's computer. HTTrack can also update an existing mirrored site and resume interrupted downloads.

Active Attacks

Active attacks are mostly used to manipulate or alter a system. They may have an effect on the integrity, authenticity and availability of data. Information from the passive phase acts as input to the active phase. In this phase, the attacker verifies and gathers information (IP address, operating system, network range, hidden server, personal information). This is also referred as active reconnaissance. It gives a complete picture about the security measures enforced at the target system. Table 2 shows some common tools used for launching active attacks.

Table 2: Tools Used for Launching Active Attacks

Arphound: Arphound is a tool that listens to all traffic on a network interface and reports IP/MAC address pairs as well as events such as IP conflict, IP changes, IP addresses with no RDNS, various ARP spoofing and packets not using the expected gateway. Reporting is done to stdout, to a specified file or to syslog in a format that can be easily parsed by scripts.
Arping: Arping probes hosts on the attached network link by sending link Layer frames using the Address Resolution Protocol (ARP) request method addressed to a host identified by its MAC address of the network interface.
Bing: Bing determines bandwidth on a point-to-point link by sending ICMP ECHO_REQUEST packets and measuring their roundtrip times for different packet sizes on each end of the link. Host1 is supposed to be the nearest end of the link, while Host2 is the other end.
Dig: Dig stands for Domain Information Groper. It is a network administration command-line tool for querying Domain Name System (DNS) name servers. It is useful for verifying and troubleshooting DNS problems and also for performing DNS lookups. It displays the answers that are returned from the name servers that were queried.
DNStracer: DNStracer determines where a given Domain Name Server (DNS) gets its information from. It follows the chain of DNS servers back to the servers which know the data. It sends the specified name-server a non-recursive request for the name.
Fping: Fping is a small command line tool to send ICMP (Internet Control Message Protocol) echo request to network hosts, just as in ping. However, fping performs much better when pinging multiple hosts. Fping totally differs from ping in that you can define any number of hosts on the command line or specify a file with the list of IP addresses or hosts to ping.
Dsniff: Dsniff is a collection of tools for network auditing and penetration testing. It automatically detects and minimally parses each application protocol and uses Berkeley DB as its output file format, only logging unique authentication attempts.
Filesnarf: Filesnarf saves files sniffed from NFS traffic in the current working directory.
Fping: Fping is a program like ping which uses the Internet Control Message Protocol echo request to determine if a target host is responding. In fping, you can specify any number of targets on the command line, or specify a file containing the lists of targets to ping. Instead of sending to one target until it times out or replies, fping will send out a ping packet and move on to the next target in a round-robin fashion. Unlike ping, fping is meant to be used in scripts so its output is designed to be easy to parse.
Fragroute: Fragroute intercepts, modifies and rewrites egress traffic destined for the specified host. In simple words, fragroute fragments packets originating from our (attacker) system to the destination system. It is used by security personnel or hackers for evading firewalls, avoiding IDS/IPS detections and alerts, etc. Also, pen testers use it to gather information from a highly secured remote host.
Hmap: Hmap is a tool for fingerprinting web servers. Basically, it collects a number of characteristics and compares them with known profiles to find the closest match. The closest match is its best guess for the identity of the server.
Hping: Hping is a free packet assembler and analyser for the TCP/IP protocol. It is one of the de facto tools for security auditing and testing of firewalls and networks. It was used to exploit the idle scanning technique. It is now implemented in the Nmap Security Scanner. The new version of hping, hping3, is scriptable using the Tcl language. It implements an engine for string based, human-readable description of TCP/IP packets so that the programmer can write scripts related to low-level TCP/IP packet manipulation and analysis in a very short time.
Httping: It shows how long the given URL will take to connect, send a request and retrieve a reply (only the headers). It measures the latency of the web server plus the latency of the network.
Mailsnarf: Mailsnarf is one of the tools included in the dsniff package of network security auditing tools. It is capable of reading e-mails transferred to and from an Ethernet network device. The use of mailsnarf is limited to the LAN the computer running mailsnarf is on, unless it is used in conjunction with arpspoof.
Urlsnarf: Urlsnarf outputs all requested URLs sniffed from HTTP traffic in CLF (Common Log Format used by almost all web servers) suitable for offline post-processing with your favourite weblog analysis tool.
NBTscan: NBTscan is a program for scanning IP networks for NetBIOS name information. It sends a NetBIOS status query to each address in a supplied range and lists received information in human-readable form. For each responded host, it lists IP address, NetBIOS computer name, logged-in username and MAC address.

Netcat: Netcat is a computer networking utility for reading from and writing to network connections using TCP or UDP. This command is designed to be a dependable back end that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and investigation tool since it can produce almost any kind of connection its user could need and has a number of built-in capabilities. Its list of features include port scanning, file transferring, and port listening, and it can be used as a backdoor.

Nmap: Nmap is used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, it sends specially crafted packets to the target host and then analyses the responses. It is able to extend its discovery capabilities beyond simply figuring out whether a host is up or down and which ports are open and closed; it can determine the operating system of the target, names and versions of the listening services, estimated uptime, type of device and presence of a firewall.

Nikto: Nikto is a very popular and easy to use web server assessment tool to find potential problems and vulnerabilities very quickly.

ScanSSH: ScanSSH supports the scanning of a list of addresses and networks for open proxies, SSH protocol servers, Web, and SMTP servers. Wherever possible, ScanSSH displays the version number of the running services. ScanSSH protocol scanner supports the random selection of IP addresses from large network ranges. It is useful for gathering statistics on the deployment of SSH protocol servers in a company or the Internet as a whole.

SMTPscan: SMTPscan is a remote SMTP server version detector. It can be used to guess the mail software which is used on a remote server that may hide its SMTP banner.

TCPdump: TCPdump is the most powerful and widely used command-line packet sniffer or package analyser tool which is used to capture or filter TCP/IP packets that are received or transferred over a network on a specific interface. It is available under most of the Linux/Unix based operating systems. TCPdump also gives us the option to save captured packets in a file for future analysis.

TCPreplay: TCPreplay is a suite of free open-source utilities for editing and replaying previously captured network traffic. Originally designed to replay malicious traffic patterns to intrusion detection/prevention systems, it has seen many evolutions including capabilities to replay to web servers.

THCAmap: THCAmap is a tool for determining what application is listening on a given port.

XProbe2: XProbe2 is an active operating system fingerprinting tool with a different approach to operating system fingerprinting. It relies on fuzzy signature matching, probabilistic guesses, simultaneous multiple matches, and a signature database.

2. Scanning and Scrutinizing

In this phase, the attacker collects the validity of information as well as finds out the existing vulnerability. This phase is also referred as "enumeration". The objectives of this phase are to:

1. Validate user accounts and groups
2. Explore lists of network resources and shared network devices
3. Find different types of operating systems and applications running on the target system.

It is a key phase before the actual attack takes place.

Various scanning techniques used by attackers are stated as follows:

- **Port scanning:** Identify all ports, port status (open/closed), services running on those ports, etc.
- **Network scanning:** Understand and verify the IP address of the target and related network information before launching an attack.
- **Vulnerability scanning:** Check and understand loopholes in the target system.

3. Launching an Attack

Once step two is completed, the cyberattacker is ready to launch the attack to gain system information. The steps that will be followed by him/her are listed as follows:

- Crack the password
- Exploit the privilege
- Execute malicious commands / applications
- Hide files
- Final but most important step—cover the track - delete the access logs, so that there is no trail illicit activity.

2.4. Social Engineering

Unlike other threats in information security, social engineering targets the unwitting humans who are operating, maintaining, overseeing and even protecting the information systems. In social engineering, an attacker tries to gain the trust of the victim so as to get sensitive information required to gain access to the system. It does not require a very high level of technical expertise but needs social skills. A social engineer uses psychological tricks to obtain the policies and practices followed in organisations in order to gain access to computer systems.

Social engineering is the practice of deceiving someone, in person, over the phone or by using a computer, with the express intent of breaching some level of security, either personal or professional. Social engineers use social skills to gain the trust of legitimate people. Once the trust is established, they try technical and non-technical skills to obtain information about an organisation or its computer systems. Social engineering comprises activities like foot printing, trust establishment, psychological manipulation and clear exit.

- **Foot printing:** In this, a social engineer tries to accumulate information regarding the victim and its surrounding environment. It gives the list of individuals with whom the attacker can establish a relationship to improve the chances of attacks. The information gathered during this stage includes personal and professional details of the person, department information, organisation chart, location information, etc. of a particular organisation. Tools used by social engineers to gather such information are ***creepy***, ***SET*** and ***Maltgo***.
- **Trust establishment:** After getting the possible list of targets, the attacker tries to develop a relationship with the target, usually, an employee or some other personnel linked to the victim and develop a good rapport with them. Once the trust is established, it can be later used to gain confidential and sensitive information which can cause severe harm to an individual, an organisation, or a business.
- **Psychological manipulation:** Using social skills, a social engineer starts manipulating the trust he/she has gained to extract as much confidential/sensitive information related to target as possible so as to penetrate into the system with ease. On the collection of the required information, the social engineer can start manipulating other people whose information was obtained from the previous target or move towards exploiting the system.
- **Clear exit:** After extracting confidential/sensitive information, the attacker has to make a clear exit so that nobody suspects anything. The attacker has to make sure that no trace is left which will reveal his/her real identity or link him/her with any kind of unauthorised access into the target system.

2.4.1. Types of Social Engineering Attacks

1. **Pretexting**

   It is one of the common social engineering methods wherein the attacker tries to create convincing fictitious scenarios using e-mail or phone to extract personal information. The victim easily believes the pretext assuming that the attacker is a legitimate person and submits sensitive information as a favour to the attacker. Typical examples of pretext are asking to participate in a survey, research projects, or similar data collection activities initiated by the attacker impersonating as legitimate agencies. On such requests, the victim starts giving valuable information or performing the asked action on behalf of the attacker. In some cases, the attacker can claim to be working for a utility company by wearing a uniform and being present at the location to help the victims. By gaining their trust, the attacker later gets confidential information. Pretexting is one of the aspects of social engineering that is almost entirely psychological in nature.

2. **Baiting**

   It is a technique in which the attacker places a "bait" for the victim to take on his/her own initiative. One of the typical examples of baiting is leaving one or more USB flash drives containing a malicious executable at a place where the victim is likely to notice them. The victim would take it out of curiosity or greed and unintentionally help the attacker to cross the malicious payload over the security boundary that the attacker himself/herself cannot physically break with adequate access control.

3. **Role Playing**

   This is one of the important weapons used by social engineers. Generally, it involves requesting or gathering information through e-mails, phone, online chat sessions or other methods that legitimate companies use for online interaction with the public. Social engineers pretend to be a helpdesk employee or technician with helpless or important users to get confidential information.

4. **Dumpster Diving**

   It involves examining of trash for any kind of sensitive/confidential information leaks. Most of the organisations dump items like organisation phone diary, system manuals, organisation chart, policy manuals, old documents containing sensitive data or login names and passwords, etc. An attacker can find huge amounts of information about the organisation and its employees from these dumpsters. This method of searching through the dumpster to get personal, sensitive and confidential and potentially useful information is known as dumpster diving. Many organisations are adopting document disposal/shredding policies to get rid of such social engineering attacks.

5. **Shoulder Surfing**

   Shoulder surfing is an extremely simple social engineering method. It is carried out by simply looking over a victim's shoulder to observe and get sensitive/confidential information (e.g. password, PIN, etc.) that is being typed by the victim. This can be performed from a close range as well as from a long range using binoculars or other vision-enhancing devices.

6. **Phishing**

   In this technique, the attacker designs and uses websites and e-mails which look like those of well-known and legitimate businesses, government agencies, financial organisations, etc., to deceive users into disclosing their personal and confidential information. The attacker falsely claims to be an established legitimate enterprise to scam the user into submitting private information which will be further used for identity theft.

7. **Surfing Organisation Websites and Online Forums**

Social engineers generally use this approach to gather primary information about the victim/target. Lots of information about an organisation, e-mail ids, phone numbers, etc., are openly available on the organisation's website and other open forums. This gathered information can be further refined and used by the attacker to identify the victim and attack policy.

2.4.3. Defence Against Social Engineering

As social engineering involves the human factor, there is no effective way to protect against a social engineering attack. However, there are certain ways to reduce the likelihood of success of such attacks. It is also important for organisations to establish clear and strong security policies and processes to reduce the threat of social engineering. The following are some of the steps to ensure protection against social engineering attacks:

- Every employee must be given security awareness training to reduce the chances of leaking sensitive/confidential information. The employees must be instructed to report any suspicious behaviour to authorities.
- Background verification of employees is very important as there may be a chance that an attacker joins the organisation to gather insider information about the organisation. Verification should be applied to not only the regular employees but also to the vendors and contractual workers whenever they become part of the organisation and access the organisation's network.
- There should be appropriate physical access control to allow only authorised people to access restricted parts of an organisation.
- There should be a policy on what information is to be kept about the organisation on websites and other forums. It must be reviewed and if any irregularities are found, they must be taken care of.
- Mock social engineering activities should be performed by the security team so as to keep track of security in an organisation.
- There should be strict and layered access control policies for accessing an organisation's data.
- Installation and maintenance of firewalls, anti-viruses and e-mail filters should be done regularly.
- There should be a proper incident response strategy in the organisation.
- Usage of corporate IDs on public domain, blogs, discussion forums, etc., should be restricted.
- Confidential and critical online resources should not be accessed in public places, cafes, hotels, etc.
- E-mail solicitations requesting personal or financial information should not be responded to.
- Personal information or organisational details should never be shared to anyone unless the employee is certain of the person's authority to have that information.
- Documents containing sensitive data should always be shred.

2.5. Cyberstalking

Cyberstalking is an escalated form of online harassment directed at a specific person. It causes substantial emotional distress and serves no legitimate purpose. The action is to annoy, alarm, and emotionally abuse another person. Perpetrators utilise social media accounts, publicly accessible information and sometimes illegally accessed information to learn more about their targets. The perpetrators may also spread rumours and misinformation to discredit or intimidate them.

Cyberstalker may obtain personal information about their victims (e.g., home address, phone number) from the Internet and utilise this information to meet their victims in person.

2.5.1. How It Works?

Cyberstalking is a form of harassment that takes advantage of the anonymity and relative protection the Internet provides from law enforcement. Cyberstalkers use the following list of actions to abuse their victims. The following actions are repeated to intimidate or harm people:

- Leaving messages or comments on an individual's online post, publication, web blog, or website with the intent to threaten, harass, or cause emotional distress.
- Sending online correspondence that is inappropriate and unwanted.
- Impersonating another person and posting materials online using that person's name or likeness.
- Creating online materials (including websites, blogs, and social media pages) with the name and/or likeness of another person in order to disseminate false and defamatory information or pictures.
- Purposefully sending malware or computer viruses to a specific person as a means to harass him/her or compromise his/her computer's security.
- Employing spyware on an individual's computer or other electronic devices in order to track his/her movements, the information they access, and whom they interact with online.
- Hacking an individual's computer.
- Sending defamatory and/or harassing messages to an individual's friends, family, employer, co-workers, neighbours, students, teachers, or other community members either in their name or the victim's name.

2.5.2. Defence Against Cyberstalking

The following points can help to defend against cyberstalking:

- Understand and learn how to use privacy settings of social media platforms.
- Make use of the two-factor or double authentication security option as and when available and possible.
- Review and filter the personal information supplied on public accounts.
- Do not accept friend requests or follower requests from a person who is not personally known.
- Tell friends not to post your personal information (even pictures) without your permission.
- Do not publicly share pictures or other identifying information about your children or other close family members.
- Do not share your personal information on online surveys, quizzes and polls websites.
- Do not publicly RSVP to events.
- Always make use of strong and different passwords for each online account.

2.5.3. Cyberstalking Case Study

A 35-year-old man will serve three months in jail for sending obscene pictures and videos via e-mail to a woman he met on a social networking site.

Prabhu has been sentenced three months simple imprisonment and fined Rs. 10,000 for the offence under section 509 (word, gesture or act intended to insult the modesty of a woman) of the IPC and section 66 (E) (punishment for violation of privacy) of the Information Technology Act, 2008 and Rs. 5,000 for intending to insult the modesty of a woman. The woman initially chatted with him, but she said she started finding his behaviour suspicious and stopped responding to his messages. She even removed him from her friend's list. According to the police sources, their relationship could have turned sour after the woman turned down Prabhu's proposal to get married. As the woman is a year older than Prabhu, her parents were opposed to the marriage. The woman then stopped communicating with him. Prabhu, however, continued to keep an eye on her profile and her whereabouts.

The following month, the woman got mails from an unknown ID. The mails contained obscene images and videos. She initially ignored them. But when they did not stop, she wrote a complaint to the Cyber Crime Investigation Cell.

The Internet Protocol (IP) address of the computer was traced. The cyber cell filed a 200-page charge sheet in September 2009 after which the trial began. Eight witnesses, including the woman, Prabhu's colleagues, cyber experts and police officials were examined. When the court convicted Prabhu, it said the prosecution had proved the case beyond a reasonable doubt.

2.6. Cybercafe and Cybercrimes

In recent years, cybercafes have become the favourite place for youngsters for public Internet access point and online game playing zone. Even though it gives ease of use to access the Internet, this public access point is also the most loved place of cybercriminals. Cybercriminals can easily hack visitors' data because of a lack of awareness of cybercrime in cybercafe users. In addition, it is very easy to cover the crime they are committing as they are making use of public Internet services. Because of lack of awareness of cybersecurity, numerous cybercafe visitors commit errors such as use of decoded devices or conventions, not logging out after work is finished, straightforward secret word, same watchword for various locales, information left on the hard drive, not clearing browsing history, putting away of data on public hard circle, not checking for illicit software before utilising public machine which brings about misfortune to the visitors.

Most of the cybercafes hold two types of risks. Users are unaware of the programs installed on the computers placed in cybercafes. Some malicious programs like keyloggers, spywares, rootkits, etc. might be installed and running in the background collecting confidential information and activities performed by the user. Secondly, there are chances of shoulder surfing through which the user activities and confidential information can be monitored.

In a recent survey conducted in various cybercafes in India, the following facts were figured out:

1. In most of the cybercafes, pirated software are installed in all computer systems.
2. In many cybercafes, antiviruses are not installed. Also, it was found that antiviruses were not updated with the latest patch in most of the cybercafes.
3. Several cybercafes have installed "Deep Freeze" to protect computer systems. However, this also helps cybercriminals to cover the attack launched using those computer systems.
4. Annual Maintenance Contract (AMC) was not found for servicing of computers. This helps cybercriminals to install and use malicious programs to make the launch of an attack easier.
5. Pornographic websites and some websites with offensive contents were not blocked.
6. Most of the cybercafe owners do not have awareness about IT security and cyber laws.
7. No cyber audit was initiated by the cybercafe association or cyber cell of the police in cybercafes.

After reviewing these eye-opening facts, various recommendations were given. Now, the owners of cybercafes are required to maintain log registers of persons and record users' identity details. Also, minors are restricted from using cybercafes. Cybercafes are instructed to install licenced software with regular updates. A special training was given to the cyber

cell police to conduct regular security audits at cybercafes. Some of the tips outlined for cybercafe users are stated as follows:

1. Always Logout: While checking e-mail or logging in for chatting, always click logout/sign out.
2. Stay with the computer: While surfing, do not leave the system unattended for any period of time.
3. Clear history and temporary files: Before browsing, deselect the AutoComplete option. Browser -> Tools -> Internet options -> Content tab–Tools -> Internet Option -> General Tab -> Temporary Internet Files -> Delete files and then Delete Cookies.
4. Avoid online financial transactions: One should avoid online banking, shopping, etc. Do not provide sensitive information such as credit card number or bank account details.
5. Change passwords/use virtual keyboard: Change password after the completion of a transaction.
6. Be alert: One has to be alert about others snooping over their shoulder.

2.7. Botnets

Currently, cyberspace is facing a huge threat from various malware. One of them is botnet. A botnet is a collection of compromised computer systems called bots. The term bot, derived from Ro-Bot, is nothing but a script, a set of scripts, or a program designed to perform predefined functions repeatedly and automatically after being triggered intentionally or through a system infection. Unlike the existing malware, such as virus and worm, bots focus on attacking the infecting host. Bots may run automatically or execute a task once they are given a precise input. They are controlled by an agent called the Botmaster or Botherder. It is a group of persons who manage remote bots and botnet. Bots receive commands from the Botmaster and these are used in a distributed attack platform.

A botnet can also use the command and control channel (C&C) to control the botnet. Figure 1 shows the C&C botnet architecture. In C&C, all the bots present are connected to the servers, hence the Botmaster can communicate with all the bots at the same time. After communicating with the bots, the Botmaster issues commands. Command and control infrastructure is considered the most essential part of a botnet. C&C traffic is hidden behind normal web traffic to evade the mechanisms of detection.

escape/ avoid

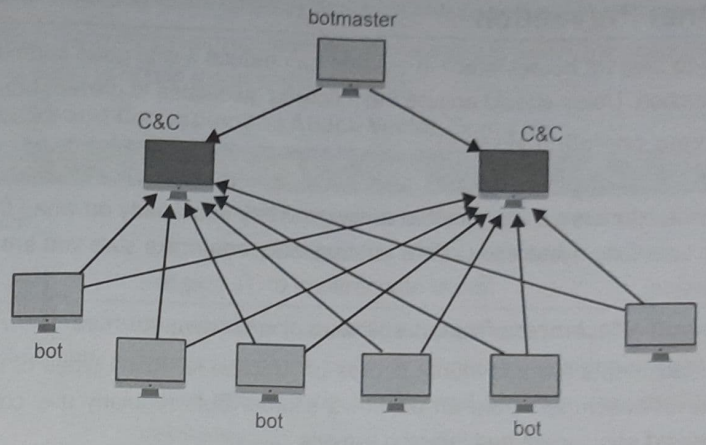

Figure 1: C&C Botnet Architecture

The Botmaster often deploys botnets onto computers through a Trojan horse. The strategy typically requires the users to infect their own systems by opening e-mail attachments, clicking on malicious pop-up ads, or downloading dangerous software from a website. After infecting devices, botnets are then free to access and modify personal information, attack other computers, and commit other crimes. Some of the botnets can even self-propagate, finding and infecting devices automatically. Such autonomous bots carry out seek-and-infect missions, constantly searching the web for vulnerable Internet-connected devices lacking operating system updates or antivirus software.

It is very difficult to detect botnets. They use only a small amount of computing power to avoid disrupting normal device functions and alerting the user. Advanced botnets are even designed to update their behaviour to prevent detection by cybersecurity software. Users are unaware that their connected device is being controlled by cybercriminals. Botnets grow in time. Many botnets can lay dormant within devices, waiting for the botmaster's trigger to launch an attack. Most of the well-known and large botnets used for launching cyberattacks are Conficker, TDL-4, MegaD, Kraken, and Srizbi.

A botnet can be used by the Botmaster to build advertisement fraud schemes by commanding thousands of infected devices to visit fraudulent websites and click on advertisements placed there. For every click, the hacker then gets a percentage of the advertising fees. Also, botnets can be sold or rented on the Internet. The buyers of botnets use them to carry out cyberattacks, spread ransomware, or steal personal information.

Case Study on Botnet

In 2016, a large DDoS attack hit the Internet infrastructure company Dyn. The attack used a botnet that comprised security cameras and DVRs. The DDoS disrupted the Internet service of large sections of the country, creating problems for many popular websites like Twitter and Amazon.

2.7.1. Botnet Prevention

It is not easy to prevent botnet infection but one can reduce it with good surfing habits and antivirus protection. Users should ensure the following guidelines to prevent botnet:

- **Update your operating system**

  One of the malware preventative measures is to keep the operating system updated. Software developers actively combat malware. They know early on when threats arise. Set your operating system to update automatically and make sure you are running the latest version.

- **Avoid e-mail attachments from suspicious or unknown sources**

  E-mail attachments are a favourite source of infection for many types of malware. Do not open an attachment from an unknown source. Bots regularly use contact lists to compose and send spam and infected e-mails.

- **Avoid downloads from P2P and file sharing networks**

  Botnets use P2P networks and file sharing services to infect computers. Scan all downloads before executing the files or find the safest alternatives for transferring files.

- **Do not click on suspicious links**

  Links to malicious websites are common infection points, so avoid clicking them without a thorough examination. Hover your cursor over the hypertext and check to see where the URL actually goes.

- **Get antivirus software**

  Getting antivirus software is the best way to avoid and eliminate botnets. Look for antivirus protection which is designed to cover all devices connected to your computer.

2.8. Attack Vector

A path or means by which an attacker can gain access to a computer or network server in order to deliver a payload or malicious outcome is called an attack vector. It enables hackers to exploit system vulnerabilities, including the human element. Table 3 shows some well-known attacks and their corresponding attack vectors.

Attackers always try to devise new attack vectors in the cyberspace. The methodology they follow includes:

- **Analysis and inspection of the potential target:** Attackers can perform inspection and analysis on selected targets with the help of sniffing, e-mails, malware or social engineering.
- **Encoding:** On primary inspection, attackers select the best tools to exploit the vulnerabilities found at the application, system and network levels.
- **Installation:** Security of the target system gets broken and malicious software is planted.
- **Exploiting:** Once the system is breached, attackers try to exploit the collected information (sensitive data) to obtain the intended benefits.

Table 3: Attacks and Corresponding Attack Vector Examples

Attack	Attack Vector
SQL Injection	The attacker uses leaks or flaws in the authentication or session management functions (e.g. exposed accounts, passwords, session ID) to impersonate users.
Cross Site Scripting	The attacker sends text-based attack scripts that exploit the interpreter in the browser. Almost any source of data can be an attack vector, including internal sources such as data from the database.
Cross Site Request Forgery	The attacker creates forged HTTP requests and tricks a victim into submitting them via image tags, XSS, or numerous other techniques. If the user is authenticated, the attack succeeds.
APPs with Known Vulnerability	The attacker identifies a weak component through canning or manual analysis. He/she customises the exploit as needed and executes the attack. It gets more difficult if the used component is deep in the application.

Various attack vectors can be used to expose us to potential vulnerabilities resulting in attacks. One needs to debug the network to explore various attack vectors. The following guidelines can shield the networks and remove any attack vectors.

- Keep your networks and servers free of redundant software.
- Update and apply all security patches to remove vulnerabilities discovered over time.
- Frame security policies and enforce them to be followed by each and every user of the system. Make campaigns and regular meetings about updating security policies.
- Use firewalls to monitor and control traffic between private and public networks.
- Make periodic backups of sensitive data so that recovery can always be possible in case of failure or system attacks.
- Keep an eye on the latest trends in digital security through specialised magazines or technology websites.
- Use constantly updated antivirus.

2.9. Cloud Computing

The use of cloud computing services has become an essential part of everyday life in private as well as in the business context. It is now possible to access your data anytime and anywhere, using any computing device. Nowadays, the cloud is a part of almost everything on your computer system. It is integrated with your operating system, applications and other services. You can save your files online using cloud applications and later on share them with other users or choose to work together simultaneously using one of the integrated cloud services.

2.9.1. Cloud Computing Services

Cloud computing services are provided on demand to users over the Internet. The cloud service providers use their own servers to provide this service unlike companies that use their on-premise servers. There are different types of cloud services which may or may not be necessary for end users but are of significant use to software developers. The most prominent cloud services are related to infrastructure, storage, software and platform.

Infrastructure as a Service (IAAS): This is the most commonly used cloud service. It includes virtual servers, storage disks and networks and provides a basic structure to an organisation which is manageable and flexible. Customers can access and use the storage space that is provided using their handheld devices, such as smartphones, to store data, including pictures, videos and music on the cloud.

Platform as a Service (PaaS): This is a cloud-based development platform designed for developers to build, run and manage applications over the Internet. The PaaS infrastructure is built and managed by the cloud service provider who provides the software and hardware tools required for application development as a service. The platform gives developers the flexibility to focus on the application they are running on the cloud services. The cloud provider deals with the complexities of maintaining and building the infrastructure to run such applications.

Software as a Service (SaaS): SaaS means that the users can access different software present on the cloud on a pay per use basis. This is a very useful service as software licences are exorbitantly priced and it is not possible to licence all software. This is where SaaS comes in. It provides access to a multitude of software which provide more or less the same functionality as their licenced counterparts.

Cloud providers are responsible for the efficient management and availability of these programs.

2.9.2. Threats Associated with Cloud Computing

A cloud network is accessible to users and multiple other networks. This makes it vulnerable to threats originating from computers that follow similar or different architecture. Therefore, it is important to be aware of the kinds of threat that are posed and take necessary precautions so that we are ready to face these threats. In this regard, it is very important to choose the right kind of cloud service provider.

Users store a lot of personal information and sensitive data on their computers and this information is now being stored on the cloud. The data stored on the cloud is valuable to individuals with crime on their mind. Therefore, it is important for the users to find out and evaluate the security measures that their cloud provider has in place. Additionally, users must adhere to the safety checklist and take precautions to secure their data.

The types of threat associated with cloud computing are described as follows:

- **Data breach:** Data breach can happen when data is stored locally or on the cloud. However, if the cloud data is compromised, it has far-reaching consequences. In order to prevent this, the cloud providers ensure that their network is highly secure and the security protocol that is implemented is regularly updated. This is done to remain ahead of the newer and more severe threats that are evolving. A cloud data breach places multiple enterprises and their user data at risk. Therefore, cybercriminals prefer to attack a cloud system rather than standalone systems.
- **Data ownership and control:** The chances of a data breach become significantly higher if the management of your organisation's data that is stored on the cloud is outsourced to a third-party provider. Many issues such as geographical location, backup processes and the steps taken to ensure data protection are now outside the control exercised by your organisation.
- **Data loss:** No matter where the data is stored, the impact of permanent data loss is huge. It has the potential to affect an organisation financially, legally and operationally.
- **Malicious attacks:** Cybercriminals can attack and abuse a cloud storage for conducting illegal activities or for monetary gains.
- **Insider threat:** The possibility of an attack originating from within an organisation is also possible. Assigning incorrect access levels to users or neglect in revoking access privileges to users can result in data getting exposed to people who are not authorised to access it.
- **Shared space:** Since the cloud is a shared space, multiple users share and store data on a single server. One user getting access to the data of another user using the same technology cannot be totally ruled out.

2.9.3. Safety Measures Against Threats to Cloud Computing

Data servers of cloud providers are scattered all over the world and are governed by different privacy and cyber laws in different countries. There is no single law that governs these data centres. Therefore, in the event of data loss, it would be impossible to decide which countries' laws are applicable if your data is stored across multiple locations. Some of the general precautionary measures to protect cloud data are listed as follows:

- Backing up data
- Understanding the cloud provider's service agreement
- Updating the backups created
- Password protection
- Two-step authentication
- Encryption and decryption
- Disciplined online behaviour
- Not storing sensitive information on cloud servers

2.10. Summary

In this chapter, we have discussed the systematic approach used by attackers to launch cyberattacks by gathering information about targets using some passive attacks like social engineering. Cyberstalking is one of the common approaches followed by attackers to threaten targets. A cybercafe is a boon for attackers; they are cleverly using it to gather information on a target as well as to launch attacks on a remote network or an individual target. The Internet has become an integral part of our life and we are making use of online shared resources for storage and computation, which can be easily exploited by an attacker to launch an attack. Botnets are sold or rented over the Internet, which is a major threat to connected resources in a network.

Questions

1. What are cyber offences? Discuss.
2. How do criminals plan attacks? Explain with examples.
3. Explain in detail active attacks and passive attacks with examples.
4. What is social engineering? Explain with the help of an example.
5. Explain the impact of cybercrimes in social engineering.
6. Write a short note on cyberstalking.
7. What are botnets? Explain the significance of botnets in cybercrime.
8. How are cybercriminals attacking cloud services? Explain with examples.
9. What are the different attacks launched with the attack vector? Explain in detail.
10. How are cybercafes used in cybercrimes? Explain with a suitable example.

3.1. Introduction

In recent years, a wide range of mobile devices including smartphones, tablets and notebook PCs are being used by people in their day-to-day activities. These mobile devices are typically network-connected for most of the time they are switched on. This can often pose well-known but not well-understood threats from cybercriminals. Along with these devices, various mobile objects like RFID tags embedded in devices, chip-based payment cards, electronic key fobs, etc., are also getting connected with mobile devices. This can lead to various types of attack as many heterogeneous devices are getting connected with wireless technology.

Cybercriminals may have many different motives for performing an attack on a mobile device, including hardware theft, information theft, or simply denial of service or sabotage. It is difficult to enumerate all the ways a criminal might seek to gain from an attack. It becomes hard to determine where, how and in what way criminals will compromise mobile and wireless devices. Therefore, it becomes essential to consider all possible security issues when trying to address cybercrime in mobile and wireless devices.

3.2. Proliferation of Mobile and Wireless Devices

With the rising advancement of high-speed, large bandwidth 3G, 4G and upcoming 5G mobile networks, customers can perform Internet activities on their smartphones as quickly and reliably as they can via a normal computer. The proliferation of mobile devices in our daily life and the significant advancement of wireless network technologies and infrastructures have become an increasing driving force for a variety of emerging mobile applications. A mobile application can be developed and run on mobile handheld devices and communicate with other devices via wireless communication. There are various mobile devices like smartphones, tablet PCs, personal digital assistants (PDAs), carputers, pen top computers, etc. These devices are connected using a wireless network for transferring information amongst them.

Nowadays, almost every organisation involves the use of information technology. Organisations are investing large amounts of capital on purchasing laptops and other handheld devices to be used by their employees at work as well as in travelling. The high usage of mobile devices requires a greater emphasis on securing both the stored and communicated information. Security should be made a priority as this information can contain valuable organisational data. It is necessary that users of mobile devices follow a mobile security policy, personal or corporate, to protect organisational data.

3.3. Trends in Mobility

Mobile computing is becoming increasingly important due to the rise in the number of portable computers and the desire to have continuous network connectivity to the Internet irrespective of the physical location of the node. Mobile computing has quickly become an important new paradigm in today's world of networked computing systems. From wireless laptops to cellular phones and WiFi/Bluetooth-enabled PDA's to wireless sensor networks, mobile computing has become ubiquitous in its impact on the daily lives of people. Along with the existing 3G and 4G technologies, 5G technology is well underway to provide speedier connections that stay online no matter where you are. It is worth noting the various trends in mobility before studying the use of mobile and wireless devices in cybersecurity.

1. **User mobility:** Users should be able to move from one physical location to another using the same service. The service could be in the home network or a remote network. One of the classical examples is when a user travels for business and uses corporate services and applications as if he/she were in the office.
2. **Device mobility**: Users should be able to move from one device to another using the same service. Sales representatives use their desktop computer in their home/office. During the day while travelling they can use their Palmtop to access the application.
3. **Session mobility:** A user session should be able to move from one user-agent environment to another. A typical example would be of a user using a service through a CDMA network. The user drives through a tunnel and gets disconnected from the network. He/she then returns to the office and uses the desktop computer, continuing the unfinished session from where he/she was at the time of disconnection.
4. **Service mobility:** A user should be able to move from one service to another. Suppose a user is writing an e-mail. To complete the e-mail, the user needs to refer to some other information. In a desktop PC, the user simply opens another service (browser) and moves between them using the taskbar. He/she should be able to switch amongst services in small footprint wireless devices like a desktop.
5. **Host mobility:** A user device can be either a client or a server. When it is a server or host, some of the complexities of the host get changed based on whether it is playing the role of a client or a server.

3.4. Credit Card Frauds in Mobile and Wireless Computing Era

In recent years, electronic gadgets have become an integral part of business, providing connectivity with the Internet outside the office. They provide ease of use but at the same time there are many challenges in securing these devices from being a victim of cybercrime. Credit card frauds are the new trends in cybercrime that are coming up with mobile commerce and mobile banking. Customers tend to do more online transactions than traditional banking transactions. This leads to a rise in digital card usage as it is very easy and convenient with the help of mobile commerce and point of sale (POS) terminals. However, it was observed that there is tremendous growth in credit card frauds in recent years with mobile and credit

card transactions. A credit card (or debit card) fraud is a form of identity theft that involves taking someone's credit card information in an unauthorised way for the purpose of charging purchases to that card or removing funds from it. Credit card frauds are committed in the following ways:

- An act of criminal deception (mislead with intent) by the use of an unauthorised account and/or personal information
- Illegal or unauthorised use of an account for personal gain
- Misrepresentation of account information to obtain goods and/or services

3.4.1. Types of Credit Card Fraud

- **Lost or stolen cards: This type of fraud offers the easiest way to a fraudster to get hold of other individual's credit cards without investment in technology. It is also perhaps the hardest form of traditional credit card fraud to tackle. It** should be reported immediately to minimise any damages.
- **Account takeover:** This type of fraud occurs when a fraudster illegally obtains a valid customer's personal information. The fraudster takes control of (takeover) a legitimate account by either providing the customer's account number or the card number. The fraudster then contacts the card issuer, masquerading as the genuine cardholder, to ask that mail be redirected to a new address. The fraudster reports the loss of the card and asks for a replacement to be sent.
- **Counterfeit cards**: The creation of counterfeit cards together with lost/stolen cards poses the highest threat in credit card frauds. Fraudsters are constantly finding new and more innovative ways to create counterfeit cards. Some of the techniques used for creating false and counterfeit cards are erasing the magnetic strip, creation of fake card, alteration of card details, skimming and cloning.
- **Never received: N**ew or replacement card is stolen from the mail, while in transmission and never reach its rightful owner.
- **Fraudulent application: A** fraudster uses another person's name and information for applying for and obtaining a credit card.
- **Collusive merchants:** This type of fraud occurs when merchant owners and/or their employees conspire to commit fraud using their customers' (cardholder) accounts and/or personal information.
- **Triangulation:** The fraudster in this type of fraud operates from a website. Goods are offered at heavily discounted rates and also shipped before payment. The fraudulent site appears to be a legitimate auction or traditional sales site. While placing orders online, customers provide information such as name, address and valid credit card details to the site. Once the fraudster receives these details, he/she orders goods from a legitimate site using the stolen credit card details. The fraudster then goes on to purchase other goods using the credit card numbers of the customers. This process is designed to cause a great deal of initial confusion, and the fraudulent Internet company, in this manner, can operate long enough to accumulate a vast amount of goods with the stolen credit card numbers.

3.4.2. Protection Against Credit Card Fraud

Incorporating a few practices into your daily routine can help keep your cards and account numbers safe. For example, keep a record of your account numbers, their expiration dates and the phone number of each company in a secure place. Do not lend your card to anyone. Do not leave your cards, receipts, or statements around your home or office; when you no longer need them, shred them before throwing them away. Other fraud protection practices include:

- Do not give your account number to anyone on the phone unless you have made the call to the company you know to be reputable. If you have never done business with it before, first do an online search for reviews or complaints.
- Carry your cards separately from your wallet. It can minimise your losses if someone steals your wallet or purse. Moreover, only carry the card you would need for a certain outing.
- During a transaction, keep your eyes 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've made.
- Report any questionable charges to the card issuer.
- Notify your card issuer if your address changes or if you will be travelling.
- Do not write your account number on the outside of an envelope.

Staying vigilant about protecting your personal information can greatly reduce the risk of theft or fraud. It is an important and necessary step in today's digital world.

3.5. Security Challenges Posed by Mobile Devices

Recently, advancement in wireless technology and improvement in mobile devices helped to increase the mobile market. Almost in all day-to-day activities, mobile devices are used by an individual or organisation. This has created challenges for individuals, society and businesses, particularly in mobile added value services like mobile banking, mobile check-in,

mobile ticket, etc., and government security services. Some of the major security challenges posed by mobile devices due to threats and vulnerabilities are described as follows:

1. **Poor authorisation and authentication:**

   In mobile devices, generally, authorisation and authentication schemes rely on device identifiers such as IMEI (International Mobile Equipment Identity), IMSI (International Mobile Subscriber Identity), UUID (Universally Unique Identifier) values. If security for them is not enforced, the devices tend to fail and can lead to poor authentication and privilege access issues.

2. **Insecure data storage:**

   Due to increased processing power and higher storage in mobile devices, users are storing lots of day-to-day data in mobile devices. Sensitive data is stored on the device or in the cloud and is often left unprotected. It generally happens that non-encryption of sensitive data, non-caching of information for long term storage, lack of global file permissions and not leveraging platform best practices result in the exposure of sensitive information, privacy violations and non-compliance.

3. **Security decisions via untrusted inputs:**

   Applications making security decisions via user input may become the victims of malware or client-side injection attacks, which further results in the consumption of paid resources, and data and privilege escalation.

4. **Sensitive information disclosure:**

   If sensitive information, such as login credentials, shared secret keys, access tokens, sensitive business logic, etc., is hardcoded into the application code, then there are chances that the attacker gets this information by applying reverse engineering. If such details are in the hands of attackers, it becomes easy for them to compromise an organisation's security. However, code obfuscation makes it difficult to understand the code.

5. **Broken cryptography:**

   Often, users make use of customised algorithms instead of standard cryptographic algorithms for performing encryption. They believe that encoding and obfuscation are equivalent to encryption and make the mistake of hardcoding cryptographic keys into the application code itself. It may lead to loss of confidentiality of data, privilege escalation, etc., due to the failure in cryptographic implementation.

6. **Insufficient transport layer protection:**

   The transport layer does not provide inbuilt security. Users need to enforce encryption before transmitting data. It has been observed that the data is transmitted as plaintext in most of the mobile applications. Even though strong encryption is applied to data in transmission, ignoring certificate validation errors or falling back to plaintext communication after failures can put security in danger and have severe impacts such as lack of confidentiality of data, data tampering, and facilitation of man-in-the-middle attacks.

7. **Server-side controls:**

   At the server side, proper updation of system and application software, secure configurations, default accounts credential updation or disabling of unnecessarily running services should make the server robust against malicious attacks. Failing to implement proper security controls can result in security compromise and confidentiality and data integrity risks.

8. **Client-side injection:**

   Along with the known html injection, SQL injection attacks applicable to mobile web and hybrid applications, new attacks like abusing phone dialer, SMS and in-application payments are also launched by attackers in mobile applications.

9. **Improper session handling:**

   A session with longer expiry time or the use of default device identifiers as session identification poses security risks such as privilege escalation, unauthorised access, etc.

10. **Side channel data leakage:**

    Side channel data leakages are caused due to programmatic flaws or because insecure operating system features in mobile applications are not disabled. They can lead to storage of sensitive data at places like web caches, global operating system logs, screenshots, temp directories and thus make the data easily accessible to attackers once the mobile device is compromised.

These challenges are mainly caused by various threats and vulnerabilities in mobile devices.

3.6. Authentication Service Security

Modern computer systems provide service to multiple users and require the ability to accurately identify the user making a request. Password-based authentication is not suitable for use on a computer network as it can be easily intercepted by the eavesdropper to impersonate the user.

There are two components of security in mobile computing:

1. **Security of devices:** A secure network access involves mutual authentication between the device and the base station or web servers. This ensures that the authenticated devices can be connected to the network to get the requested services. In this regard, Authentication Service Security is important due to typical attacks on mobile devices through WAN.
2. **Security in network**: Security measures in this regard come from Wireless Application Protocol (WAP), use of Virtual Private Networks (VPN) and MAC address filtering.

3.6.1. Cryptographic Security for Mobile Devices

Cryptographically Generated Addresses (CGA) are IPv6 addresses for which the interface identifier is generated by computing a cryptographic one-way hash function from a public key and auxiliary parameters. The binding between the public key and the address can be verified by re-computing the hash value and comparing the hash with the interface identifier. Messages sent from an IPv6 address can be protected by attaching the public key and auxiliary parameters and by signing the message with the corresponding private key. IPv6 consists of a 64-bit network prefix and a 64-bit interface identifier. The network prefix is used for routing in the network. A specific node in a link is identified with the interface identifier, which must be unique in the link. The protection works without a certification authority or any security infrastructure. CGA-based authentication is particularly useful in securing IP-layer signalling protocols, such as neighbour discovery and mobility protocols, where IPv6 addresses are the primary identifiers for the protocol participants. The biggest advantage of CGA-based authentication compared to public key infrastructure (PKI) or address based key (ABK) is that it does not require a trusted authority, pre-established trust relationships or other security infrastructure.

3.6.2. LDAP Security for Handheld Mobile Computing Devices

LDAP (Lightweight Directory Access Protocol) is a software protocol generally used to locate organisations, individuals, and other resources, such as files and devices, on the public Internet or on a corporate intranet. LDAP is a lightweight version of Directory Access Protocol (DAP) which is a part of X.500, a standard for directory services in a network. In a network, the domain name system (DNS) is the directory system used to relate the domain name to a specific network address. However, if the domain name is not known, LDAP allows searching for an individual without knowing his/her location. An LDAP directory is organised using the tree structure with the following levels:

1. The root directory
2. Countries
3. Organisations
4. Organisational units
5. Individuals

An LDAP directory is distributed among many servers with periodically synchronised replicas. An LDAP server is called a Directory System Agent (DSA). LDAP uses a relatively simple, string-based query to extract information from Active Directory. Users submit the request to an LDAP server which in turn passes it to other DSAs, if necessary, and generates a response for the user.

3.6.3. RAS Security on Mobile Devices

Remote access server (RAS) provides a collection of services to remotely connected users over a network or on the Internet. It acts as a remote gateway to connect remote users with an organisation's internal network. As RAS has specialised server software which provides remote connectivity. This software provides the functionalities like authentication, connectivity and resource access services to connecting users. An RAS is deployed within an organisation and directly connected with the organisation's internal network and systems. Once connected with an RAS, a user can access his or her data, desktop, application, print and/or other supported services. In an organisation, many mobile devices within the organisation and from outside the organisation are getting connected to RAS. Therefore, it becomes essential to enforce security on RAS.

For the secure operation of a RAS system, it is essential that the hardware and software components of the system are securely installed and configured. Secure configuration of the RAS system must, therefore, be performed before the RAS system goes live. In addition, all the organisational processes must be defined and implemented. It should also be noted that the desired level of system security can only be assured if the physical security of the hardware components, which make up the RAS system, is also assured. The security of a RAS system can be roughly broken down into three areas:

- Security of the RAS server
- Security of the RAS client
- Security of data transmission

Though the desired level of security of the RAS server can be controlled through the implementation of local security guidelines, the RAS client is typically not under the complete control of the IT personnel who are responsible for the LAN. The security of data transmission media is generally completely out of their control. For this reason, the communication between the client and the server must be secured by additional means.

3.7. Attacks on Mobile/Cell Phones

Smartphones or mobile phones with advanced capabilities, like those of personal computers (PCs), are appearing in pockets, purses, and briefcases of more and more people. Smartphones' popularity and relatively lax security have made them attractive targets for attackers. According to a report published earlier this year, smartphones outsold PCs for the first time. Attackers have been exploiting this expanding market by using old techniques along with the new ones. There are three prime targets for attackers:

- **Data:** Mobile phones are utilised for data management. They may contain sensitive information like credit card numbers, authentication information, private information, activity logs, calendar, call logs, etc.

- **Identity:** Mobile phones provide the ease of customisation to users. The contents of a phone reveal the identity of its owner.
- **Availability:** By attacking a mobile phone, one can limit access to it and deprive the owner of the service.

3.7.1. Mobile Phone Theft

In recent years, mobile devices gained popularity due to their capability to handle multiple application and data processing, like laptops. Also, due to advancements in technology and lesser price, it became easier for people to purchase high-end mobile phones. However, due to their growing popularity, mobile phones are becoming a favourite target of thieves. Mobile phone theft often occurs in bars, nightclubs, restaurants, or on public transport.

Most mobile phones have a range of security features that are intended to stop anyone else from accessing and using them should they be stolen. These security features include:

- Access control using unique code (a PIN, password or some form of pattern) or biometric authentication (such as fingerprint or facial recognition) is used on the user interface of your handset to unlock it.
- Tracing the location of your phone using a remote service.
- Wiping data from or locking your handset remotely (for example, by using another Internet-enabled device)
- Function to display a home/lock screen message to someone who may find your handset to help you recover it.
- Preventing the thief from resetting your handset to its factory setting in order to bypass any unique codes or other security features that you are using to protect your handset.

The aforementioned security features are available in only a few latest configuration mobile phones. Some generalised safety tips to secure all kinds of mobile phones against theft are listed as follows:

- Always keep your phone details, such as your bills and contacts, safe and secure.
- Keep your mobile phone out of sight when not in use.
- When in a public place, do not leave your phone unattended.
- When talking on your mobile phone, be alert and aware of your surroundings.
- Do not leave your phone unattended in a vehicle.
- Ensure that your mobile phone has a Personal Identification Number (PIN) activated.
- If your phone is stolen, contact your network provider to disable the SIM card. Quote your IMEI (International Mobile Equipment Identity) number.
- Report the theft to the police.

- Change account credentials. If you used your phone to access any remote resources, such as corporate networks or social networking sites, revoke all credentials that were stored on the lost device.
- Install find your phone application for tracking your mobile phone in case it gets lost or stolen. For example, an iPhone (and iPad) can be tracked by the owner by using the "Find my iPhone" app. Similar apps are available for download for Android- and Windows-based phones; however, many older mobiles do not have this capability.
- Install anti-theft software on your phone. It does not allow a criminal to insert a new SIM card. Even if the criminal tries to do so, it asks for a verification code. Also, it sends a message about the change of SIM to two contact numbers registered while installing anti-theft software. Some of the well-known anti-theft software are Cerberus, Crook Catcher, Prey, Lookout, etc.
- Wipe out the phone. Some mobile service providers offer remote wipe.

3.7.2. Mobile Virus

A mobile virus is very much like a computer virus that infects applications running on a mobile device. A mobile phone virus spreads via Internet downloads, MMS attachments and Bluetooth transfers. The most common type of cell phone infection, right now, occurs when a cell phone downloads an infected file from a PC or the Internet. However, phone-to-phone viruses are also on the rise.

A mobile virus spreads primarily in three ways:

- **Internet downloads:** The virus spreads in the same way as a traditional computer virus does. The user downloads an infected file to his/her phone through a PC or the phone's own Internet connection. This may include file-sharing downloads, applications available from add-on sites and false security patches posted on the Symbian Website.
- **Bluetooth wireless connection:** The virus spreads between phones through their Bluetooth connection. The user receives a virus via Bluetooth when the phone is in discoverable mode, i.e. it can be seen by other Bluetooth-enabled phones. In this case, the virus spreads like an airborne illness.
- **Multimedia messaging service (MMS):** The virus comes as an attachment with an MMS text message. As with computer viruses that arrive as e-mail attachments, the user must choose to open the attachment and then install it for the virus to infect the phone. Typically, a virus that spreads via MMS gets into the phone's contact list and sends itself to every phone number stored there.

The first mobile virus was introduced in a game called Mosquito by Ojam. Ever since then, malware has been introduced in various ways and affecting MCDs (Mobile Computing Devices) all over the world. Some of the well-known mobile viruses on different operating systems are given in Table 1:

Table 1: Mobile Viruses on Different Operating Systems

Virus Name	Mobile Operating System
Cabir	Symbian
Mosquito	Symbian
Skulls	Symbian
CardTrap	Symbian & Windows
CommWarrior	Symbian
Rick Astley/Ikee	iOS-iPhone
Duh	iOS-iPhone
GG Tracker	Android OS
Google ++	Android OS
Angry Birds Trojan	Android OS
Zeus Trojan	BlackBerry OS
LibertyCrack	Palm OS
Phage	Palm OS
Vapor	Palm OS

Protecting Mobile Phones from Viruses

Every mobile user needs to follow the following tips to safeguard his/her mobile phone from viruses:

- Maintain up-to-date system and application software.
- Install antivirus software and updates as and when they become available.
- Enable the personal identification number (PIN) or password to access the mobile device, if available.
- Read and understand permissions while installing applications as some of the applications access the data stored on our mobile device.
- Encrypt personal and sensitive data, when possible.
- Disable Bluetooth, infrared, or Wi-Fi when they are not in use.
- Always set Bluetooth-enabled devices in the non-discoverable mode so that they become invisible to unauthenticated devices.
- Use caution when opening e-mail and text message attachments and clicking links.
- Avoid opening attachments, links, or calling numbers contained in illegitimate e-mail or text messages.
- Never join unknown public Wi-Fi networks.
- Delete all information stored in a device prior to discarding it.

3.7.3. Vishing

Vishing is the criminal practice of using the telephone system to gain access to the personal and financial information of customers for the purpose of committing fraud. It exploits a person's trust in telephone services as the victim is often unaware that fraudsters can use methods such as caller ID spoofing and complex automated systems to commit this type of scam.

Fraudsters are making use of vulnerabilities in public branch exchange (PBX) to connect to Voice over Internet Protocol (VoIP) services and perform auto dialling to thousands of people in an hour. A typical process involves the following steps:

1. A war dialler is used to call numbers in a given region or a legitimate voice messaging system is compromised and calls are made with a list of phone numbers stolen from a financial institution.
2. When a customer answers the call, an automated recording alerts the customer regarding a fraudulent or suspicious activity that has been detected on his/her credit card or bank account. The message instructs the customer to place a call to the bank immediately and provides a false phone number. Often time, this is also the phone number that is displayed on the caller ID screen.
3. When the victim calls the number, automated instructions request that he/she enters a credit card or bank account number into the keypad. However, the call can also be used to harvest additional details such as personal identification numbers, expiration date, CVV number and date of birth.
4. As the customer enters the requested data, the fraudster gets the information necessary to make fraudulent use of the card to access the account.

Some sophisticated attacks combine vishing and traditional phishing in which a phishing e-mail, which appears to be from a legitimate company such as a bank, a credit card company, or an online retailer, is sent to an online user stating that there has been a problem with an online account. The e-mail then directs the user to call a number and enter certain information to verify his/her account.

How to avoid vishing scams?

A widely known vishing scam is ***Microsoft tech support scam***. In this scam, an attacker typically calls a victim posing as a member of the Microsoft technical department and informs the victim that his/her computer is infected with malware which is generating all sorts of errors. The attacker can then ask for remote access of the victim's computer or ask the victim to download some software or fake anti-malware programs to solve the problem. Some attacker may even convince a victim to reveal his/her bank account information to make a payment.

Unfortunately, we cannot fully avoid vishing scams. Frauds against businesses and institutions that reveal your private information are completely out of your control. A user's mobile number is often associated with many accounts and there are chances to lose the number to scammers in a data breach at some point.

There are a few technical and proactive steps you can take to avoid vishing scams. They are described as follows:

1. **Never answer a call from an unknown number**

   Answering the call from unknown number can lead you right into a scammer's waiting arms. Picking up the call will alert the vishing scammers that the number is active, leading to more calls down the road. Make use of the Voicemail so that if any legitimate person is calling, then he/she will leave a voicemail or call back later. Many vishing scams will also leave a pre-recorded voicemail message which will give you a chance to properly scrutinise whether the caller is a legitimate source.

   Many a time, scammers call back immediately. Users are more likely to pick up an unknown number that calls back as traditionally this indicates that the caller is not only someone that we know, but also that the call is important.

2. **Never share personal information over the phone**

   Banks and government institutions never ask for personal information over the phone. If you have any doubt, ask for the caller's name and let him/her know that you will call back after acquiring an official number. The suspicious caller may try to give you a number to call back on. If that occurs, cross-check this number with the information available online. If the numbers differ, call the number you have found through your online search at the business's or institution's website. Once you call back, inquire about the original caller to verify identity.

3. **Do not completely trust caller ID**

   Even with a more effective caller ID app installed, avoid numbers that are not in your phone book. You may still receive fraud calls from spoofed numbers that appear to be legitimate. Even with a caller ID app installed, let any calls that are not in your phone book go directly to voicemail.

4. **Avoid automated calls**

   Get your number registered on the National Do Not Call Registry to block automated calls. It may not stop vishing, but it will reduce the number of automated calls.

5. **Report the incident**

   If you notice that you have become a victim of vishing and your financial information is compromised, immediately call the bank and report the incident. Verify whether there has been any unauthorised transaction. Immediately change your IPIN, ATM PIN, password and other related credentials that may have been compromised. Also, report the incident to appropriate legal authority. It helps in catching the actual criminals.

3.7.4. Smishing

Smishing or SMS phishing is a technique where a text message is sent to an individual's mobile phone to get him/her divulge personal information. The two most common types of smishing attack are given as follows:

1. A person receives a text message that directs him/her to call a phone number to confirm personal or account information.
2. A person receives a text message that directs him/her to visit a website to confirm the information but is served with a malicious Trojan on his/her computer or mobile phone capable of stealing passwords.

Smishing has become a more attractive alternative to phishing. Success rates are higher with a smishing attack as compared to a standard phishing attack. This is because customers are not conditioned to receive spam on their mobile phone. Thus, they are more likely to believe that the communication is legitimate. Furthermore, most phishing e-mails are now stopped by spam filters and often never reach their intended targets. There is no mainstream mechanism for weeding out spam text messages.

Most of the smishing attacks target banks or financial institutions by sending a phone number that the victim calls after receiving the message, resulting in a vishing attack.

There are several common themes in smishing messages. The following examples include phone numbers for victims to call. The messages may originate from either a spoofed phone number or an e-mail address. Many of these systems use voicemail to steal user information, including bank account information.

Example 1:

Official Microsoft ANNOUNCEMENT: Congratulations! Your mobile phone has won US$ 10 million prize money. To claim your money, call this number XXXXXXXX tomorrow at 8 am. Thank you.

Example 2:

Dear Credit union customer, we regret to inform you that we had to lock your bank account access. Call (647) 827-2796 to restore your bank account.

Organisations should monitor their own SMS number services via sites like ***whocallsme.com*** to see if users are suspicious of their services. Such suspicions could indicate mistrust in the legitimate service or attackers who are spoofing the number of the affected organisation to improve their chances of gaining trust.

Anti-phishing software programs are designed to filter e-mails, but mobile phishing is more difficult to filter for both users and automatic products. SMS messages contain much less tracking information; therefore, recipients will not be able to determine from where they originate. Mobile phone browsers and SMS programs also lack integrated phishing defences built into today's e-mail clients and browsers. Smishers also often spoof the source address and use many different phone numbers to perform vishing. Mobile browsers also make it difficult to determine the legitimacy of a URL. The small-form factor and limited display are incapable of displaying full URLs, and it can take as many as ten clicks to access the security information of a site. Most mobile browsers lack support for protections normally available on desktop systems such as URL filtering, phishing toolbars, and extended validation (EV) SSL certificates. Based upon these concerns, it seems likely that users of mobile devices have an increased risk of falling victim to a phishing attack when they surf with mobile browsers or receive fraudulent SMS messages. To protect mobile devices from such phishing attacks, users from any organisation should follow the given guidelines:

1. Add mobile security to the existing employee security awareness programs.
2. Create and implement an IT policy that governs usage and ensures employees' understanding.
3. Perform threat modelling to identify the risks of moving applications to a mobile platform.
4. Train application developers in secure coding practices for mobile device platforms.
5. Limit the sensitive data transferred to mobile devices or consider view-only access.
6. Utilise Mobile Device Management software to create an encrypted password-protected sandbox for sensitive data and enforce device-side technical policies.
7. Perform technical security assessments on mobile devices and the supporting infrastructure and focus on device-side data storage.
8. Establish a program that continually evaluates new and emerging threats in mobile platforms.
9. Increase monitoring controls around mobile device connection points when feasible.
10. Assess classic threats against web-based applications and infrastructure.

3.7.5. Hacking Bluetooth

Bluetooth is one of those technologies that is so common that it has become a part of our daily lives. It has become a solution to problems like driving and talking on a cell phone and introduced new and interesting marketing opportunities for attacks. Bluetooth devices are connected through a process called pairing. The pairing process usually involves one device searching for other devices in the area and then selecting the device to partner with based on its BD_ADDR or a logical name. Once pairing is complete, the devices bond with one another. Depending on the action being taken, a PIN for the device being connected will be required to complete the process. The PIN acts as a password in an encryption scheme between the two devices and is used to generate a link key. This key is used to secure communication between the devices and to authenticate devices in the future.

With the widespread adoption and convenience of Bluetooth device comes the inevitable implementation problems that cause unexpected things to happen. Most Bluetooth-based attacks are based on a simple and common flaw. Users often are very poor at reading documentation, at understanding risks and threats, and generally, at changing defaults. Most attacks revolve around users not changing the default settings on their devices.

As with most attacks, the first thing to do is to find the device. This allows legitimate users to find the device they are seeking, but also allows a nearby attacker to find those same devices and silently interrogate them to find out if they are suitable to attack.

Some of the common attacks for hacking Bluetooth are Bluejacking, Bluesnarfing, Bluebugging and Car Whisperer.

1. **Bluejacking**

   Bluejacking is probably the most common form of Bluetooth hacking. This happens when a hacker searches for discoverable devices in the area and then sends spam in the form of text messages to the devices. This form of hacking is harmless.

   It was once used mainly to prank people in the past when mobile devices came with Bluetooth that was automatically set to discoverable. Bluejacking is used today for spam messaging and the hackers who use this do it just to frustrate others. The method does not give hackers access to your phone or the information on it.

   The best way to deal with Bluejacking is to ignore the messages if you receive them. If you keep your Bluetooth settings to invisible or non-discoverable, you are not likely to

receive these messages. Also, you can keep your smartphone or device set to invisible while you are in a busy or open Wi-Fi area.

2. **Bluesnarfing**

   This form of hack is more serious than Bluejacking and can leave open some of the private information stored on your smartphone. This is made possible through software. A hacker may purchase software that allows him/her to request information from your device. Even though this form of hacking can happen while your device is set to invisible or non-discoverable, it is unlikely to happen due to the time, effort, and money needed to complete it. The information stolen may seem important to you, but it might not be as precious as banking information. That data can be accessed by hacking your device through Bluebugging.

3. **Bluebugging**

   If a hacker blue bugs your phone, he/she gains total access and control of your device. This makes the hacker capable of accessing all information including photos, apps, contacts, etc. Bluebugging can happen when your device is left in the discoverable state. From here, hackers gain access to your phone at the same point they do when performing Bluejacks. This is a much harder form of hacking than Bluesnarfing and Bluejacking.

   This is only feasible on older phones with outdated firmware. Newer smartphones and their owners are less likely to have this happen to them because of the constant updates mobile operating systems perform.

4. **Car Whisperer**

   Car Whisperer is a hacking technique which can be used by attackers to hack hands-free Bluetooth in a car system and connect it to a system to inject audio to or record audio from a bypassing car. It can be easily used by attackers to invade privacy and listen to conversations inside a car and exploit that for illegitimate purposes.

   This attack takes advantage of the fact that most of the Bluetooth systems in cars need a simple four-digit security key and this security key is not enough . Many car manufacturers use the default security key, and this results in the vulnerability. Experts could not confirm till now whether Car Whisperer attack can be used to do even more serious activities like disabling airbags or breaks.

Consider the following simple tips to protect yourself from Bluetooth hacking:

1. Update all software to keep your mobile phone up to date. Also, change all default passwords and keep changing them regularly.
2. Turn the Bluetooth services off when they are not in use. Turning your Bluetooth setting to invisible makes it harder for hackers to discover your device, thus making it more difficult for them to steal your data.
3. Never use public Wi-Fi networks. These connections are unsecure. Always disable automatic connections to public networks to keep your device from connecting to an untrustworthy source without your knowledge.
4. Consider a virtual protected network (VPN). VPNs are available for download in app stores and offer a more secure way to connect while on the go.

3.8. Mobile Devices: Security Implications for Organisations

With the rapid growth of wireless technology, increased bandwidth, efficient and powerful mobile hardware and applications, devices like smartphones, laptops, tablet PCs, and PDAs are becoming increasingly ubiquitous in the workplace.

Mobile technology is currently used not only for calling but also in business for utility computing. Cell phones untethered employees from landline phones, and laptops revolutionised the ability of employees to work remotely. But these tools pale in comparison to today's mobile devices, whose portability and ability to access corporate servers, data, and information, regardless of where the employee is geographically, are revolutionising the way business gets done. Telecommunication companies and governing regulators around the world have recognised this coming and evolving technology for decades.

The shift towards mobile devices, replacing the desktops and laptops, is clear, yet many have not thought about the significance of that shift being leveraged in a purely business environment. The evolving mobile device technology can, if properly utilised, enable the enterprise to achieve several significant benefits:

- **Improved workforce productivity**: Along with onsite job functioning, employees can also remotely access company information and complete work off-site.
- **Improved customer service:** With real-time access to customer information, employees can significantly improve turnaround times for problem resolution.
- **Increased business process efficiency:** Making use of mobile devices significantly improves supply-chain management which leads to improvement in overall business processes by shortening the time between order, production, and shipment.
- **Employee security and safety:** Even if employees are travelling for work-related tasks and not available in the office, they can always be in touch and connected.
- **Employee retention:** It provides improved work-life balance as mobile devices facilitate tasks to be performed remotely.

In an organisation, if proper and strong security policies are not enforced, there is a huge risk of loss, theft, or misuse of confidential information available on mobile devices. Each and every business process is handled using mobile devices; so, lots of data is being kept

on employees' devices. Mobile devices, whether deployed by the company or simply those in possession of employees, are at risk if not handled properly.

All these mobile devices must be viewed like existing PCs and laptops as they are also susceptible to malicious attacks using viruses, worms, Trojan horses, etc. They can also become the victims of cyberattacks through the use of malicious applications, spam, and phishing schemes. As they are portable, they are more susceptible to loss, theft, and damage. Mobile device functioning is different when compared with existing PCs in terms of the operating system, applications, updates, etc. One of the unique threats to these devices is jailbreak software. It allows strangers to hijack a device and access its information. It may result in some other attacks by making these devices zombies and controlling them to connect automatically to an unknown Bluetooth device or other devices in an open unsecured Wi-Fi network. Furthermore, with the increasing expansion and availability of new applications developed on open platforms for specific use on mobile devices, there are now many ways to undermine the security protocols and policies of most organisations that were designed around servers, PCs, and laptops. Since the risks are more difficult to identify, managers must consciously take key steps to protect their business from risks that may be under the corporate security radar. Has your company created systems designed to take advantage of mobile security features that are unique to mobile devices that could pose a risk? These risks can be categorised 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, aeroplanes or taxicabs. As with more traditional devices, physical access to a mobile device equals "game over". The cleverest intrusion-detection system and the best antivirus software are useless against a malicious person with physical access. Circumventing a password or lock is a trivial task for a seasoned attacker; even encrypted data can be accessed. This may include not only the corporate data found in the device, but also passwords residing in places like the iPhone Keychain, which could grant access to corporate services such as e-mail and virtual private network (VPN). To make matters worse, full removal of data is not possible using a device's built-in factory reset or by re-flashing the operating system. Forensic data retrieval software — which is available to the general public — allows data to be recovered from phones and other mobile devices even after it has been manually deleted or undergone a reset.

2. **Malicious code**

   Mobile malware threats are typically socially engineered and focus on tricking the user into accepting what the hacker is selling. The most prolific include spam, weaponised links on social networking sites and rogue applications. While mobile users are not yet subject to the same drive-by downloads that PC users face, mobile ads are increasingly being used as part of many attacks — a concept known as "malvertising." Android devices are the biggest targets as they are widely used and it is easy to develop software for them. 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 the 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. Hackers can exploit weaknesses in these Wi-Fi and cellular data protocols to eavesdrop on data transmission, or to hijack users' sessions for online services, including web-based e-mail. For companies with workers who use free Wi-Fi hot spot services, the stakes are high. While losing a personal social networking login may be inconvenient, people logging on to enterprise systems may be giving hackers access to an entire corporate database.

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 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; nobody has any idea about who developed an application, how good it is, or whether there is a threat vector through the application right back to the corporate network. The misuse of personal cloud services through mobile applications is another issue; when used to convey enterprise data, these applications can lead to data leaks that the organisation remains entirely unaware of. Not all insider threats are inadvertent; malicious insiders can use a smartphone to misuse or misappropriate data

by downloading large amounts of corporate information to the device's secure digital (SD) flash memory card, or by using the device to transmit data via e-mail services to external accounts, circumventing even robust monitoring technologies such as data loss prevention (DLP).

Mobile security threats will continue to advance as corporate data is accessed by a seemingly endless pool of devices and hackers try to cash in on the trend. Making sure users fully understand the implications of faulty mobile security practices and getting them to adhere to best practices can be difficult. Many device users remain unaware of threats, and the devices themselves tend to lack basic tools that are readily available for other platforms, such as antivirus, anti-spam, and endpoint firewalls.

3.9. Organisational Measures for Handling Mobile Devices-Related Security Issues

Although mobile phones are taking on more capabilities formerly available only on PCs, technical security solutions for mobile phones are not as sophisticated or widespread as those for PCs. This means that the bulk of mobile phone security relies on the user making intelligent, cautious choices. Even the most careful users can still fall victim to attacks on their mobile phones. Four key questions need to be addressed when developing a mobile security strategy:

1. **How do we deny access to unauthorised users?**

   Instruct employees to set a strong password on their mobile device and to change it every three to six months. Mobile management systems can automate enforcement.

2. **What is our plan if a personal device gets lost or stolen?**

   Passwords are not enough. You must be able to lock and wipe the device remotely. This, first, lets you "freeze" a device, which is useful if there is a good chance that it will turn up again. If it is gone for good, remote wipe lets you permanently erase stored data.

3. **How do we remove corporate data from a personal device whose owner is leaving the company?**

   Management tools can be used to segregate enterprise and personal data. When an employee leaves, IT can wipe the enterprise data while leaving personal data unaffected. This capability protects the organisation without inconveniencing the user.

4. **How do we keep prying eyes away from confidential files?**

   Use mobility management software to encrypt enterprise data, both as it is transmitted and when it is "at rest" in the device's memory.

Some of the most common security features used to protect mobile assets are:

- **Enforced authentication**: Whenever any mobile device is connected to an organisation's network, users should enforce to enter authentication details.
- **Over-the-air data encryption**: An organisation should force the use of Secure Sockets Layer (SSL) when exchanging data wirelessly over mobile devices.
- **Over-the-air provisioning**: IT technicians should be able to configure and update mobile applications remotely from a central platform.
- **Remote wipe and data fading**: There should be a provision to clear all data remotely and change the settings on a lost or stolen PDA, smartphone, or tablet.
- **Full disk encryption**: An organisation should use full disk encryption to make it virtually impossible for anyone without authorisation to read private data on mobile devices.
- **Separation of personal and enterprise information**: There should be a facility to secure, control, and erase corporate data and applications without impacting a user's personal photos, music, or games.
- **User access rights and security policies**: An organisation should keep track and control exactly what data users can access with their mobile devices.
- **Network filters**: Network filtering should be applied to monitor who is attempting access to the corporate network and to block access unless a device management client is installed on the device.

3.10. Organisational Security Policies and Measures in Mobile Computing Era

Mobile devices are receiving more attention as technological advancements shift productivity tools from desktops to pockets amid increasing reliance on mobile applications. Systems and policies should be developed to evaluate and manage the security features of various devices that are already in the workplace or corporately deployed. This should be done to know what information they are able to access on company servers or stand-alone computers. Again, this parallels commonly known concerns with PCs and laptops, but with mobile devices, several other considerations must be considered. An organisation should adhere to the following rules for effective mobile device management:

1. **Identify all mobile devices on the network:** Regular audit should be done in the organisation to identify servers and other mobile systems to make sure that there are no unauthorised devices.
2. **Know which back-office systems employees need to access:** Identify which employees can suffice with just e-mail access / which need special purpose applications / which need executive-level access.
3. **Formalise user types and set policies:** Appropriate user groups should be created

and strict governance policies need to be set for each of the user group.

4. **Be ready to block access:** Filters should be used to control access to back-end systems to block access to devices that do not have a management client installed.
5. **Add password and encryption policies plus remote wipe:** The organisation should implement minimum mobile security measures such as password enforcement, on-device data encryption, remote wipe for lost devices, and inventory management to identify which devices are connected to the network.
6. **Consider separating personal data from business data:** Mobile devices should be able to store enterprise data in one area of the device and encrypt and password-protect only that area.
7. **Enable users to be self-sufficient:** Burden on the organisation should be minimised by using a client management application that keeps mobile devices in compliance. User training should be organised regularly.

Effective remote management and data-protection tools and policies are key to preventing mobile security breaches. Protecting sensitive information on mobile devices requires an understanding of the many ways in which security can be compromised. Providing a bullet-proof strategy requires mobile security policies and functions, security-aware employees, and a comprehensive set of mobile device management tools. Steps to secure an organisation's mobile devices are listed as follows:

1. Configure mobile devices securely by:
   a. Enabling auto-lock.
   b. Enabling password protection that requires complex passwords.
   c. Avoiding the use of auto-complete features that remember usernames or passwords.
   d. Ensuring that browser security settings are configured appropriately.
   e. Enabling remote wipe.
   f. Ensuring that SSL protection is enabled, if available.
2. Connect to secure Wi-Fi networks and disable Bluetooth, infrared, or Wi-Fi when not in use. Additionally, set Bluetooth-enabled devices to non-discoverable to render them invisible to unauthenticated devices. Avoid joining unknown Wi-Fi networks.
3. Update mobile devices frequently. Select the automatic update option. Maintain up-to-date software, including operating systems and applications.
4. Utilise antivirus programs, configure automatic updates and maintain up-to-date signatures.
5. Use an encryption solution to keep portable data secure in transit.
   a. Data protection is essential. If confidential data must be accessed or stored using a mobile device, make sure the users have installed an encryption solution (e.g. Guardian Edge Smartphone Protection, McAfee Endpoint Encryption, PGP Mobile, and Pointsec Mobile Encryption).
   b. Do an assessment or at least be aware of the encryption options available for mobile devices. Some devices may offer more mature security solutions than others.
   c. Consider using thin client models so that data is centrally and securely maintained. This is one option to help avoid storing confidential data on mobile devices. It also means not having to develop new solutions every time a new mobile technology is released.
   d. Educate users to avoid using or storing confidential data on a mobile device whenever possible.
6. Use digital certificates on mobile devices.
7. Take appropriate physical security measures to prevent theft or enable recovery of mobile devices.
   a. Make use of cable locks for laptops.
   b. Use tracking and tracing application software.
   c. Never leave your mobile device unattended.
   d. Report lost or stolen devices immediately.
   e. Remember to back up data on your mobile device on a regular basis.
8. Use appropriate sanitisation and disposal procedures for mobile devices. Delete all stored information prior to discarding, exchanging, or donating devices.
9. Develop appropriate policies, procedures, standards, and guidelines for mobile devices.
10. Educate employees about mobile device security.
    a. Employees should be cautious when opening e-mail and text message attachments or clicking on links.
    b. They should avoid opening attachments, clicking links, or calling numbers contained in illegitimate e-mails or text messages. They should be aware of what they are downloading.
    c. They should be aware of the current threats affecting mobile devices.

Every organisation needs to frame a comprehensive yet flexible mobile device policy and enforce it on all devices employees are using. It should be centrally managed by the IT staff. The security policy must be auditable so that assurance can be gained that the organisation is doing everything possible to protect its investment in mobile technology. Audit procedures for assessing the operating efficiency of mobile device policies and procedures are highlighted as follows:

1. **Policy:** Auditors should check whether a security policy is available for mobile devices or not. If it is available, check whether the policy has rules for physical and logical

handling of mobile devices. The organisation should have a policy specifying different types of information and information services that may be accessible through these devices.

2. **Antivirus updates:** The organisation should include rules and regulations for antivirus updates to keep the system secure and check whether those rules and regulations are being followed by the employees.
3. **Encryption:** Auditors should verify whether sensitive data in storage as well as in transit is properly secured or not.
4. **Secure transmission:** Auditors should check and verify that mobile device users are connecting to the enterprise network via a secure connection using one of the specified methods in the security policy of the organisation (for example, VPN, IP security (IPsec), or Secure Sockets Layer (SSL))
5. **Device management:** Auditors should carefully check asset management to verify lost and stolen devices as well as procedures for employees who have been terminated or have resigned from the enterprise.
6. **Access control:** Auditors should check access privileges and escalations if anything happens in the organisation and report it for further action.
7. **Awareness training:** Auditors need to verify whether the organisation has an awareness program in place that addresses the importance of securing mobile devices physically and logically. The training should also make clear the types of information that can and cannot be stored on such devices.
8. **Risk:** Auditors should check and confirm that policies and procedures exist and are functioning as management intended to ensure that the company's information assets are not subjected to high risk of data leakage and loss.

3.11. Laptops

Laptops have enabled us to work whenever and wherever we choose, greatly enhancing our productivity, but they also put huge volumes of confidential data at risk. In today's mobile business environment, the protection of confidential data on laptops has become a top priority both for corporations and government agencies. To reduce the risk and impact of data loss, organisations must proactively secure confidential data before the laptop is stolen or goes missing and be prepared to respond immediately when a theft does occur. Some of the basic security principles that need to be followed for laptops are given as follows:

1. **Choose a secure operating system and lock it down**

   To care about your data, you must pick an operating system that is secure. Windows 2000 Professional and Windows XP Professional both offer secure log-in, file level security, and the ability to encrypt data. Such type of security is not provided by Windows 95/98/ME, etc. If you are running any of them, anyone who picks up your laptop can access your data.

2. **Enable a strong BIOS password**

   Security begins right from the start by password protecting the BIOS. Some laptop manufacturers use stronger BIOS protection schemes than others. So, you should find out from your laptop manufacturer what the procedure is for resetting the BIOS password. If they absolutely demand that you send the laptop back into the factory and do not give you a "workaround", you have a better chance of recovering the machine and maybe even catching the thief (both IBM and Dell provide this feature). Also, find out if the BIOS password locks the hard drive so that it cannot simply be removed and reinstalled into a similar machine.

3. **Engrave the laptop:**

   Permanently marking the outer case of the laptop with your company name, address, and phone number may greatly increase your odds of getting it returned to you if you carelessly leave it in a hotel room or somewhere else. According to the FBI, 97% of unmarked computers are never recovered. Marking may also prevent it from simply being resold over the Internet via an online auction.

4. **Register the laptop with the manufacturer:**

   Most of us are in the habit of throwing away the registration cards of all of the electronic items we buy every day because we have learned that it just leads to more junk mail. Registering your laptop with the manufacturer will "flag" it if a thief ever sends it in for maintenance and increase your chances of getting it back. It also pays to write down your laptop's serial number and store it in a safe place. In the event your laptop is stolen, it will be impossible for the police to ever recover it if they cannot trace it back to you.

   Many laptops and mobile devices are lost each year. So, their physical security should be high on any priority list, especially because right protection can save time, money, data and embarrassment. There is a wide range of physical laptop security options available, they are as follows:

5. **Get a cable lock and use it:**

   Over 80% of the laptops in the market are equipped with a Universal Security Slot (USS) that allows them to be attached to a cable lock or laptop alarm. Although this may not stop determined thieves with bolt cutters, it can effectively keep the casual thieves away who generally take advantage of you while you're sleeping in an airport lobby, leaving it on a table to go the bathroom, etc. These devices are not very costly and can be found at office supply stores or online. Tubular locks are preferable to common tumbler lock design.

6. **Use a docking station:**

   Almost 40% of laptop thefts occur in the office. Poorly screened housekeeping staff, contractors, and disgruntled employees are the usual suspects. You can help prevent this by using a docking station that is permanently affixed to your desktop and has a feature which locks the laptop securely in place.

7. **Lock up your PCMCIA cards:**

   Apart from locking your PC to the desk with a cable lock to keep someone from walking away with your laptop, you can do something to keep someone from stealing the PCMCIA NIC card or modem that is sticking out of the side of your machine. When not in use, eject these cards from the laptop bay and lock them in a safe place. Even when they are not being used, PCMCIA cards still consume battery power and contribute to the heat levels within your laptop while they are left inserted into their slots.

8. **Use a personal firewall on your laptop:**

   It is a popular practice for the corporate networks to protect their servers and workstations by configuring a firewall to prevent intruders from hacking their system via the company's Internet connection. But once the users leave the corporate buildings and connect to the web from home or other places, their data is vulnerable to attack. Personal firewalls such as BlackIce and ZoneAlarm are an effective and inexpensive layer of security that takes only a few minutes to install. The use of a good third-party personal firewall to secure your Windows XP workstations is recommended.

9. **Use tracking software to have your laptop call home:**

   There are several vendors that offer stealthy software solutions that enable your laptop to check in to a tracking centre periodically using a traceable signal. In the event your laptop is lost or stolen, these agencies work with the police, phone company and Internet service providers to track and recover your laptop. CompuTrace, SecureIT, Stealth Signal, and ZTrace provide tracking services for corporations and individuals.

3.12. Summary

In today's era, traditional computing devices are being replaced by portable devices. These devices increase productivity and ease of work at any place. However, loss of confidential data is the potential threat for such portable systems. Even though organisations have peripheral security, it will not be applicable all the time to such portable devices. Also, these devices are susceptible to being lost or stolen. This chapter focuses on how handheld devices can be exploited to launch attacks to steal sensitive and confidential information about organisations. Security challenges posed by wireless devices are discussed and various authentication service security mechanisms are suggested to safeguard the devices. Various specialised attacks on mobile phones are discussed and different organisational measures and security policy design and implementation guidelines are suggested. Finally, physical security guidelines to safeguard laptops in organisations are discussed.

Questions

1. What is the proliferation of mobile and wireless devices? Explain.
2. What are the different trends in mobility?
3. Discuss cybercrime activities in mobile devices.
4. Write about cybercrime activities in wireless devices.
5. What are the different trends in wireless devices?
6. Explain credit card frauds in the era of mobile and wireless computing.
7. What are the different security challenges posed by mobile devices? Explain.
8. Discuss authentication service security.
9. Explain with examples attacks on mobile devices.
10. Discuss the security implications for organisations.
11. What different organisational measures are taken for handling mobile devices?
12. Explain organisational security policies for mobile devices.
13. What are the different security policies on measures in mobile devices?
14. What are the different security policies on laptops and wireless devices? Explain.
15. Explain different cybersecurity aspects related to mobile and wireless devices.
16. Write short notes on:
    a. Phishing
    b. Smishing
    c. Vishing
    d. Bluetooth hacking
17. Explain security measures in terms of physical and logical access control for the protection of the laptop.

References

1. Different Types of Mobile Security Threats, Available at: https://www.infostretch.com/blog/different-types-of-mobile-security-threats/
2. How to prevent Vishing ?, Available at: https://www.thesecuritybuddy.com/phishing/how-to-prevent-vishing/2/
3. Different Types of Mobile Security Threats, Available at: https://www.infostretch.com/blog/different-types-of-mobile-security-threats/
4. Cybersecurity for Electronic Devices, Available at: https://www.us-cert.gov/ncas/tips/ST05-017