Unit 2
Cybercrime: Mobile and Wireless devices

CYBER CRIME: Mobile and Wireless Devices-Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era.

Mobile and Wireless Devices: INTRODUCTION

Why should mobile devices be protected?

Every day, mobile devices are lost, stolen, and infected. Mobile devices can store important business and personal information, and are often be used to access University systems, email, banking.

✚ *Proliferation of mobile and wireless devices:*

- People hunched over their smartphones or tablets in cafes, airports, supermarkets and even at bus stops, seemingly oblivious to anything or anyone around them.
- They play games, download email, go shopping or check their bank balances on the go.
- They might even access corporate networks and pull up a document or two on their mobile gadgets.
- Today, incredible advances are being made for mobile devices. The trend is for smaller devices and more processing power. A few years ago, the choice was between a wireless phone and a simple PDA. Now the buyers have a choice between high-end PDAs with integrated wireless modems and small phones with wireless Web-browsing capabilities. A long list of options is available to the mobile users. A simple hand-held mobile device provides enough computing power to run small applications, play games and music, and make voice calls. A key driver for the growth of mobile technology is the rapid growth of business solutions into hand-held devices.
- As the term "mobile device" includes many products. We first provide a clear distinction among the key terms: mobile computing, wireless computing and hand-held devices.

✓ Figure below helps us understand how these terms are related.

✓ Let us understand the concept of mobile computing and the various types of devices.

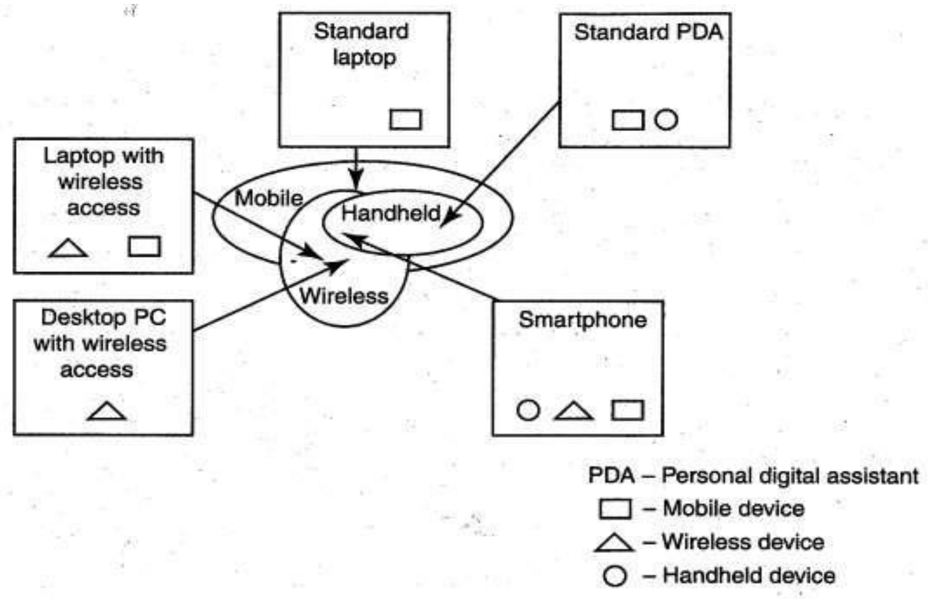

Figure : Mobile, Wireless and hand-held Devices

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

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

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

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

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

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

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

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

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

Trends in Mobility:

Mobile computing is moving into a new era, third generation (3G), which promises greater variety in applications and have highly improved usability as well as speedier networking. "iPhone" from Apple and Google-led "Android" phones are the best examples of this trend and there are plenty of other developments that point in this direction. This smart mobile technology is rapidly gaining popularity and the attackers (hackers and crackers) are among its biggest fans.

It is worth noting the trends in mobile computing; this will help readers to readers to realize the seriousness of cybersecurity issues in the mobile computing domain. Figure below shows the different types of mobility and their implications.

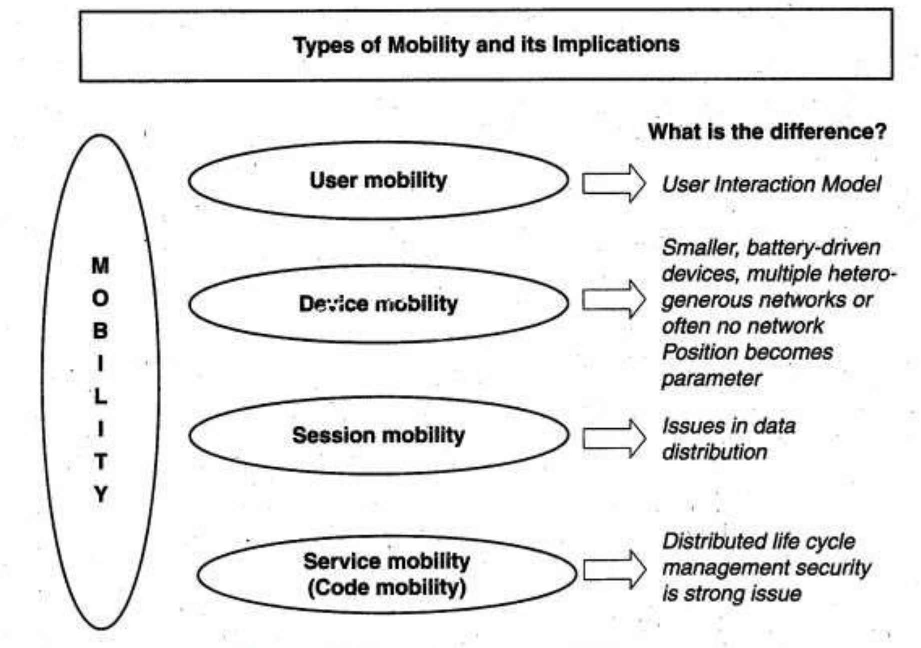
Types of Mobility and its Implications
What is the difference?
MOBILITY
User mobility
User Interaction Model
Device mobility
Smaller, battery-driven devices, multiple hetero-generous networks or often no network Position becomes parameter
Session mobility
Issues in data distribution
Service mobility (Code mobility)
Distributed life cycle management security is strong issue

Figure: Mobility types and implications

The technology 3G networks are not entirely built with IP data security. Moreover, IP data world when compared to voice-centric security threats is new to mobile operators. There are numerous attacks that can be committed against mobile networks and they can originate from two primary vectors. One is from outside the mobile network - that is, public Internet, private networks and other operator's networks - and the other is within the mobile networks- that is, devices such as data-capable handsets and Smartphones, notebook computers or even desktop computers connected to the 3G network.

Popular types of attacks against mobile networks are as follows:

1. ***Malwares, viruses and worms**:* Although many users are still in the transient process of switching from 3G to 4G it is a growing need to educate the community people and provide awareness of such threats that exist while using mobile devices. Here are few examples of malware(s) specific to mobile devices:

- G *Skull Trojan*: It targets Series 60 phones equipped with the Symbian mobile OS.
- G *Cabir Worm:* It is the first dedicated mobile-phone worm infects phones running on Symbian OS and scans other mobile devices to send a copy of itself to the first vulnerable phone it finds through Bluetooth Wireless technology. The worst thing about this worm is that the source code for the Cabir-H and Cabir-I viruses is available online.
- G *Mosquito Trojan:* It affects the Series 60 Smartphones and is a cracked version of "Mosquitos" mobile phone game.
- G *Brador Trojan:* It affects the Windows CE OS by creating a svchost. exe file in the Windows start-up folder which allows full control of the device. This executable file is conductive to traditional worm propagation vector such as E-Mail file attachments.
- G *Lasco Worm:* It was released first in 2005 to target PDAs and mobile phones running the Symbian OS. Lasco is based on Cabir's source code and replicates over Bluetooth connection.

2. ***Denial-of-service (DoS):*** The main objective behind this attack is to make the system unavailable to the intended users. Virus attacks can be used to damage the system to make the system unavailable. Presently, one of the most common cyber security threats to wired Internet service providers (ISPs) is a distributed denial-of-service (DDos) attack. DDoS attacks are used to flood the target system with the data so that the response from the target system is either slowed or stopped.

3. ***Overbilling attack:*** Overbilling involves an attacker hijacking a subscriber's IP address and then using it (i.e., the connection) to initiate downloads that are not "Free downloads" or simply use it for his/her own purposes. In either case, the legitimate user is charged for the activity which the user did not conduct or authorize to conduct.

4. ***Spoofed policy development process (PDP):*** These of attacks exploit the vulnerabilities in the GTP [General Packet Radio Service (GPRS) Tunneling Protocol].

5. ***Signaling-level attacks:*** The Session Initiation Protocol (SIP) is a signaling protocol used in IP multimedia subsystem (IMS) networks to provide Voice Over Internet Protocol (VoIP) services. There are several vulnerabilities with SIP-based VoIP systems.

Credit Card Frauds in Mobile and Wireless Computing Era:

These are new trends in cybercrime that are coming up with mobile computing - mobile commerce (M-Commerce) and mobile banking (M-Banking).

Credit card frauds are now becoming commonplace given the ever-increasing power and the ever-reducing prices of the mobile hand-held devices, factors that result in easy availability of these gadgets to almost anyone.

Today belongs to "mobile computing," that is, anywhere anytime computing. The developments in wireless technology have fueled this new mode of working for white collar workers. This is true for credit card processing too; wireless credit card processing is a relatively new service that will allow a person to process credit cards electronically, virtually anywhere.

Wireless credit card processing is a very desirable system, because it allows businesses to process transactions from mobile locations quickly, efficiently and professionally. It is most often used by businesses that operate mainly in a mobile environment

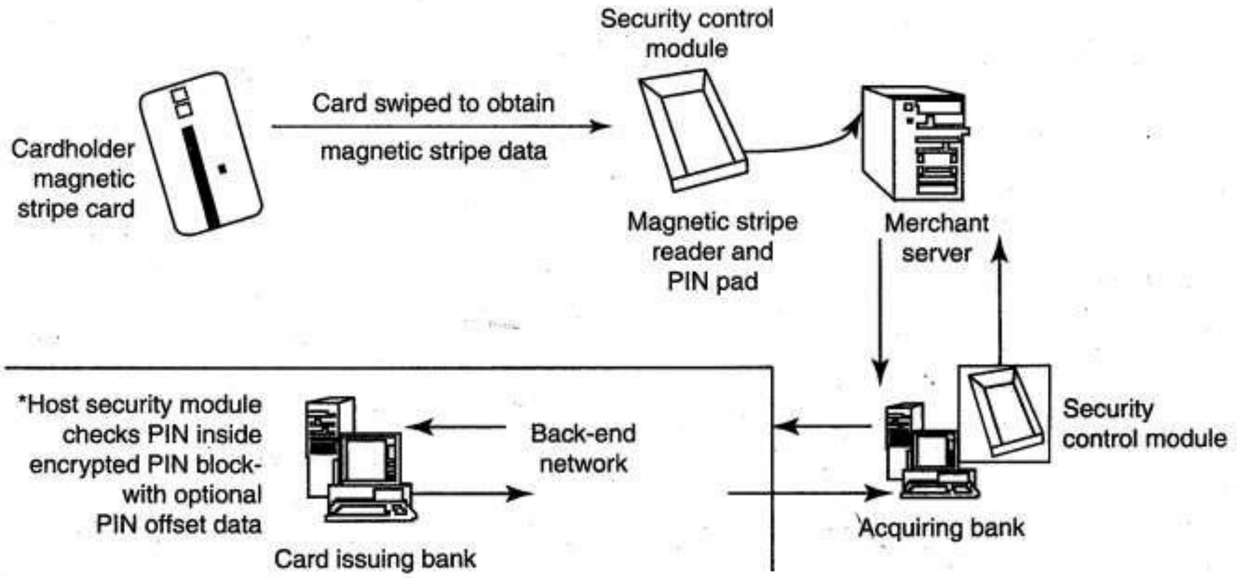
Security control module
Cardholder magnetic stripe card
Card swiped to obtain magnetic stripe data
Magnetic stripe reader and PIN pad
Merchant server
*Host security module checks PIN inside encrypted PIN block- with optional PIN offset data
Back-end network
Card issuing bank
Security control module
Acquiring bank

Figure : Online environment for credit card transactions

There is a system available from an Australian company "Alacrity" called closed-loop environment for wireless (CLEW). Figure above shows the flow of events with CLEW which is a registered trademark of Alacrity used here only to demonstrate the flow in this environment.

As shown in Figure, the basic flow is as follows:

1. Merchant sends a transaction to bank
2. The bank transmits the request to the authorized cardholder
3. The cardholder approves or rejects (password protected)

4. The bank/merchant is notified
5. The credit card transaction is completed.

Elements of Credit Card Fraud

Debit/credit card fraud is thus committed when a person
1) fraudulently obtains, takes, signs, uses, sells, buys, or forges someone else's credit or debit card or card information;
2) uses his or her own card with the knowledge that it is revoked or expired or that the account lacks enough money to pay for the items charged; and
3) sells goods or services to someone else with knowledge that the credit or debit card being used was illegally obtained or is being used without authorization.

Theft, the most obvious form of credit card fraud, can happen in a variety of ways, from low tech dumpster diving to high tech hacking. A thief might go through the trash to find discarded billing statements and then use your account information to buy things. A retail or bank website might get hacked, and your card number could be stolen and shared. Perhaps a dishonest clerk or waiter takes a photo of your credit card and uses your account to buy items or create another account. Or maybe you get a call offering a free trip or discounted travel package. But to be eligible, you have to join a club and give your account number, say, to guarantee your place. The next thing you know, charges you didn't make are on your bill, and the trip promoters who called you are nowhere to be found.

Types of Credit Card Fraud:

- The first category, **lost or stolen cards,** is a relatively common one, and should be reported immediately to minimize any damages.
- The second is called **"account takeover"** — when a cardholder unwittingly gives personal information (such as home address, mother's maiden name, etc.) to a fraudster, who then contacts the cardholder's bank, reports a lost card and change of address, and obtains a new card in the soon-to-be victim's name.
- The third is **counterfeit cards** — when a card is "cloned" from another and then used to make purchases. In Asia Pacific, 10% to 15% of fraud results from malpractices such as card skimming but this number has significantly dropped from what it was a couple of years prior, largely due to the many safety features put in place for payment cards, such as EMV chip.
- The fourth is called **"never received"** — when a new or replacement card is stolen from the mail, never reaching its rightful owner.
- The fifth is **fraudulent application**— when a fraudster uses another person's name and information to apply for and obtain a credit card.
- The sixth is called **"multiple imprint"**— when a single transaction is recorded multiple times on old-fashioned credit card imprint machines known as "knuckle busters".
- The seventh is **collusive merchants** — when merchant employees work with fraudsters to defraud banks.

- The eighth is **mail order/telephone order (MO/TO) fraud,** which now includes e-commerce, and is the largest category of total payment card fraud in Asia-Pacific, amounting to nearly three-quarters of all fraud cases. The payments industry is working tirelessly to improve card verification and security programs to prevent fraud in so-called "card-not-present" transactions online or via mail order and telephone transactions.

What Can You Do?

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 to report fraud for each company in a secure place. Don't lend your card to anyone — even your kids or roommates — and don't 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:

√ Don't give your account number to anyone on the phone unless you've made the call to a company you know to be reputable. If you've never done business with them before, do an online search first for reviews or complaints.

√ Carry your cards separately from your wallet. It can minimize your losses if someone steals your wallet or purse. And carry only the card you need for that outing.

√ During a transaction, keep your eye on your card. Make sure you get it back before you walk away.

√ Never sign a blank receipt. Draw a line through any blank spaces above the total.

√ Save your receipts to compare with your statement.

√ Open your bills promptly — or check them online often — and reconcile them with the purchases you've made.

√ Report any questionable charges to the card issuer.

√ Notify your card issuer if your address changes or if you will be traveling.

√ Don't write your account number on the outside of an envelope.

Staying vigilant about protecting your personal information can greatly reduce risk of theft or fraud — an important and necessary step in today's digital world. While credit and debit cards have built in protections, the first line of defense really starts with the cardholder.

Security Challenges Posed by Mobile Devices:

Mobility brings two main challenges to cybersecurity:

~ first, on the hand-held devices, information is being taken outside the physically controlled environment and

~ second remote access back to the protected environment is being granted.

Perceptions of the organizations to these cybersecurity challenges are important in devising appropriate security operating procedure. When people are asked about important in managing a diverse range of mobile devices, they seem to be thinking of the ones shown in below figure.

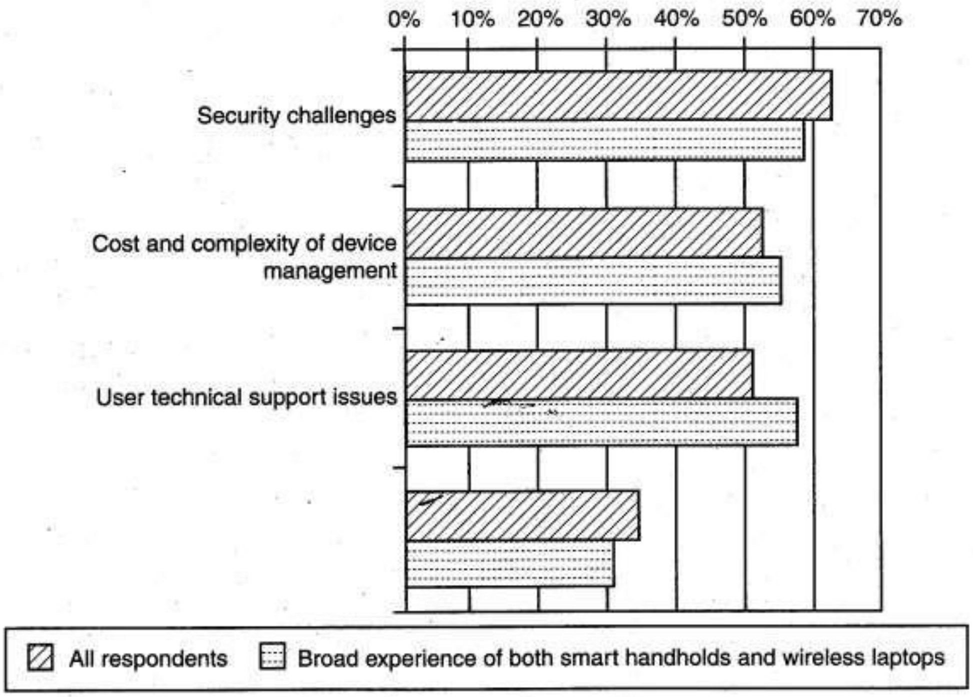

Figure: Important issues for managing mobile devices

As the number of mobile device users increases, two challenges are presented: one at the device level called "***micro challenges***" and another at the organizational level called "***macro challenges***."

Some well-known technical challenges in mobile security are:

- managing the registry settings and configurations,
- authentication service security,
- cryptography security,
- Lightweight Directory Access Protocol (LDAP) security,
- remote access server (RAS) security,
- media player control security,
- networking application program interface (API), security etc.

Mobile phone security threats generally include application based, web-based, network-based and physical threats.

1. Application based threat:

The most of application are downloadable and purposed the most common risk for mobile users; most devices don’t do much on their own, and it is the applications that make them so awesome and we all download apps. If it comes to apps the risks run from bugs and basic security risks on the low end of the scale all the way through malicious apps with no other purpose to commit cyber crime.

- ~ Malware
- ~ Spyware
- ~ Privacy
- ~ Zero Day Vulnerabilities

2. Web based threat:

According to the nature of mobile use, the fact that we have our devices with us everywhere we go and are connecting to the Internet while doing so, they face the number of unique web-based threats as well as the run-of-the-mill threats of general Internet use.

- ~ Phishing Scams
- ~ Social Engineering
- ~ Drive By Downloads
- ~ Operating System Flaws

3. Network-based threat:

Any mobile devices which typically support a minimum of three network capabilities making them three-times vulnerable to network-based attack. And a network often found on a mobile include cellular, WiFi and Bluetooth. Network exploits

- ~ WiFi sniffing
- ~ Cross-Platform Attacks

4. Physical Threats:

It is happened any time, unlikely a desktop sitting at your workstation, or even a laptop in your bag, a mobile device is subject to a number of everyday physical threats.

Loss/Theft:

Loss or theft is the most unwanted physical threat to the security of your mobile device. Any devices itself has value and can be sold on the secondary market after all your information is stolen and sold.

Top Mobile Security Threats:

Mobile devices can be attacked at different levels. This includes the potential for malicious apps, network-level attacks, and exploitation of vulnerabilities within the devices and the mobile OS. As mobile devices become increasingly important, they have received additional attention from cybercriminals. As a result, cyber threats against these devices have become more diverse.

1. Malicious Apps and Websites

Like desktop computers, mobile devices have software and Internet access. Mobile malware (i.e. malicious applications) and malicious websites can accomplish the same objectives (stealing data, encrypting data, etc.) on mobile phones as on traditional computers.

Malicious apps come in a variety of different forms. The most common types of malicious mobile apps are trojans that also perform ad and click scams.

2. Mobile Ransomware

Mobile ransomware is a particular type of mobile malware, but the increased usage of mobile devices for business has made it a more common and damaging malware variant. Mobile ransomware encrypts files on a mobile device and then requires a ransom payment for the decryption key to restore access to the encrypted data.

3. Phishing

Phishing is one of the most common attack vectors in existence. Most cyberattacks begin with a phishing email that carries a malicious link or an attachment containing malware. On mobile devices, phishing attacks have a variety of media for delivering their links and malware, including email, SMS messaging, social media platforms, and other applications.

In fact, while emails are what people most commonly think of when they hear phishing, they are not even close to the most commonly phishing vector on mobile devices. In fact, emails only account for 15% of mobile phishing attacks, placing them behind messaging, social media and “other” apps (not social, messaging, gaming, or productivity).

4. Man-in-the-Middle (MitM) Attacks

Man-in-the-Middle (MitM) attacks involve an attacker intercepting network communications to either eavesdrop on or modify the data being transmitted. While this type of attack may be possible on different systems, mobile devices are especially susceptible to MitM attacks. Unlike web traffic, which commonly uses encrypted HTTPS for communication, SMS messages can be easily intercepted, and mobile applications may use unencrypted HTTP for transfer of potentially sensitive information.

MitM attacks typically require an employee to be connected to an untrusted or compromised network, such as public Wi-Fi or cellular networks. However, the majority of organizations lack policies prohibiting the use of these networks, making this sort of attack entirely feasible if solutions like a virtual private network (VPN) are not used.

5. Advanced Jailbreaking and Rooting Techniques

Jailbreaking and rooting are terms for gaining administrator access to iOS and Android mobile devices. These types of attacks take advantage of vulnerabilities in the mobile OSs to achieve root access on these devices. These increased permissions enable an attacker to gain access to more data and cause more damage than with the limited permissions available by default. Many mobile users will jailbreak/root their own devices to enable them to delete unwanted default apps or install apps from untrusted app stores, making this attack even easier to perform.

6. Device and OS exploits

Often, the focus of cybersecurity is on top-layer software, but lower levels of the software stack can contain vulnerabilities and be attacked as well. With mobile devices – like computers – vulnerabilities in the mobile OS or the device itself can be exploited by an attacker. Often, these exploits are more damaging than higher-level ones because they exist below and outside the visibility of the device's security solutions.

Registry Settings for Mobile Devices:

Let us understand the issue of registry settings on mobile devices through an example:
Microsoft Active sync is meant for synchronization with Windows-powered personal computers (PCs) and Microsoft Outlook. ActiveSync acts as the "gateway between Windows powered PC and Windows mobile-powered device, enabling the transfer of applications such as Outlook information, Microsoft Office documents, pictures, music, videos and applications from a user's desktop to his/her device.
In addition to synchronizing with a PC, ActiveSync can synchronize directly with the Microsoft exchange server so that the users can keep their E-Mails, calendar, notes and contacts updated wirelessly when they are away from their PCs. In this context, registry setting becomes an important issue given the ease with which various applications allow a free flow of information.

Authentication Service Security:

There are two components of security in mobile computing: *security of devices and security in networks.*

Security of devices:- A secure network access involves mutual authentication between the device and the base station or web servers. So that authenticated devices can be connected to the network to get requested services. In this regard Authentication Service Security is important due to typical attacks on mobile devices through WAN:

DoS attacks: –
Traffic analysis:-
Eavesdropping:-
Man-in-the-middle attacks: –

Security in network: – Security measures in this regard come from

Wireless Application Protocol (WAP)

use of Virtual Private Networks (VPN)
MAC address filtering

A secure network access involves authentication between the device and the base stations or Web servers. This is to ensure that only authenticated devices can be connected to the network for obtaining the requested services. No Malicious Code can impersonate the service provider to trick the device into doing something it does not mean to. Thus, the networks also play a crucial role in security of mobile devices.

Some eminent kinds of attacks to which mobile devices are subjected to are: push attacks, pull attacks and crash attacks.

Pull Attacks: In pull Attack, the attacker controls the device as a source of data by an attacker which obtained data by device itself.

Push Attacks: It's creation a malicious code at mobile device by attacker and he may spread it to affect on other elements of the network.

Authentication services security is important given the typical attacks on mobile devices through wireless networks: Dos attacks, traffic analysis, eavesdropping, man-in-the-middle attacks and session hijacking. Security measures in this scenario come from Wireless Application Protocols (WAPs), use of VPNs, media access control (MAC) address filtering and development in 802.xx standards.

Attacks on Mobile-Cell Phones:

• Mobile Phone Theft:

Mobile phones have become an integral part of everbody's life and the mobile phone has transformed from being a luxury to a bare necessity. Increase in the purchasing power and availability of numerous low-cost handsets have also led to an increase in mobile phone users. Theft of mobile phones has risen dramatically over the past few years. Since huge section of working population in India use public transport, major locations where theft occurs are bus stops, railway stations and traffic signals.

The following factors contribute for outbreaks on mobile devices:

1. *Enough target terminals:* The first Palm OS virus was seen after the number of Palm OS devices reached 15 million. The first instance of a mobile virus was observed during June 2004 when it was discovered that an organization "Ojam" had engineered an antipiracy Trojan virus in older versions of their mobile phone game known as Mosquito.

This virus sent SMS text messages to the organization without the users' knowledge.

2. *Enough functionality:* Mobile devices are increasingly being equipped with office functionality and already carry critical data and applications, which are often protected insufficiently or not at all. The expanded functionality also increases the probability of malware.

3. *Enough connectivity:* Smartphones offer multiple communication options, such as SMS, MMS, synchronization, Bluetooth, infrared (IR) and WLAN connections. Therefore, unfortunately, the increased amount of freedom also offers more choices for virus writers.

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

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

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

WEP attack: Wired Equivalent Privacy (WEP) is a security protocol that attempted to provide a wireless local area network with the same level of security as a wired LAN. Since physical security steps help to protect a wired LAN, WEP attempts to provide similar protection for data transmitted over WLAN with encryption. WEP uses a key for encryption. There is no provision for key management with Wired Equivalent Privacy, so the number of people sharing the key will continually grow. Since everyone is using the same key, the criminal has access to a large amount of traffic for analytic attacks.

WPA attack: Wi-Fi Protected Access (WPA) and then WPA2 came out as improved protocols to replace WEP. WPA2 does not have the same encryption problems because an attacker cannot recover the key by noticing traffic. WPA2 is susceptible to attack because cyber criminals can analyze the packets going between the access point and an authorized user.

Bluejacking: Bluejacking is used for sending unauthorized messages to another Bluetooth device. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers and other devices.

Replay attacks: In a Replay attack an attacker spies on information being sent between a sender and a receiver. Once the attacker has spied on the information, he or she can intercept it and retransmit it again thus leading to some delay in data transmission. It is also known as playback attack.

Bluesnarfing: It occurs when the attacker copies the victim's information from his device. An attacker can access information such as the user's calendar, contact list, e-mail and text messages without leaving any evidence of the attack.

RF Jamming: Wireless signals are susceptible to electromagnetic interference and radio-frequency interference. Radio frequency (RF) jamming distorts the transmission of a satellite station so that the signal does not reach the receiving station.

There are several types of attacks that target these devices, each with its own advantages and disadvantages:

Wi-Fi Spoofing: Wi-Fi spoofing involves setting up a fake wireless access point to trick users into connecting to it instead of the legitimate network. This attack can be used to steal sensitive information such as usernames, passwords, and credit card numbers. One advantage of this attack is that it is relatively easy to carry out, and the attacker does not need sophisticated tools or skills. However, it can be easily detected if users are aware of the legitimate network's name and other details.

Packet Sniffing: Packet sniffing involves intercepting and analyzing the data packets that are transmitted over a wireless network. This attack can be used to capture sensitive information such as email messages, instant messages, and web traffic. One advantage of this attack is that it can be carried out without the user's knowledge. However, the attacker needs to be in close proximity to the victim and must have the technical skills and tools to intercept and analyze the data.

Bluejacking: Bluejacking involves sending unsolicited messages to Bluetooth-enabled devices. This attack can be used to send spam, phishing messages, or malware to the victim's device. One advantage of this attack is that it does not require a network connection, and the attacker can be located anywhere within range of the victim's Bluetooth signal. However, it requires the attacker to have the victim's Bluetooth device's address and is limited to devices that have Bluetooth capabilities.

SMS Spoofing: SMS spoofing involves sending text messages that appear to come from a trusted source, such as a bank or a government agency. This attack can be used to trick users into revealing sensitive information or downloading malware. One advantage of this attack is that it can be carried out without the user's knowledge. However, it requires the attacker to have the victim's phone number, and it can be easily detected if users are aware of the legitimate source of the message.

Malware: Malware is software designed to infect a device and steal or damage data. Malware can be distributed through email attachments, software downloads, or malicious websites. One advantage of this attack is that it can be carried out remotely, without the attacker needing to be physically close to the victim. However, it requires the attacker to have a way to deliver the malware to the victim's device, such as through a phishing email or a fake website.

Organizational Policies for the Use of Mobile Hand-Held Devices

There are many ways to handle the matter of creating policy for mobile devices. One way is creating distinct mobile computing policy. Another way is including such devices existing policy. There are also approaches in between where mobile devices fall under both existing policies and a new one. In the hybrid approach, a new policy is created to address the specific needs of the mobile devices but more general usage issues fall under general IT policies. As a part of this approach, the "acceptable use" policy for other technologies is extended to the mobile devices. Companies new to mobile devices may adopt an umbrella mobile policy but they find over time the they will need to modify their policies to match the challenges posed by different kinds of mobile hand-held devices.

For example, wireless devices pose different challenges than non-wireless Also, employees who use mobile devices more than 20%% of the time will have different requirements than less-frequent users. It may happen that over time, companies may need to create separate policies for the mobile devices on the basis of whether they connect wirelessly and with distinctions for devices that connect to WANs and LANs.

Concept of Laptops:

As the price of computing technology is steadily decreasing, usage of devices such as the laptops is becoming more common. Although laptops, like other mobile devices, enhance the business functions owing to their mobile access to information anytime and anywhere, they also pose a large threat as they are portable Wireless capability in these devices has also raised cyber security concerns owing to the information being transmitted over other, which makes it hard to detect. The thefts of laptops have always been a major issue, according to the cybersecurity industry and insurance company statistics.

Cybercriminals are targeting laptops that are expensive, to enable them to fetch a quick profit in the black market. Very few laptop thieves are actually interested in the information that is contained in the laptop. Most laptops contain personal and corporate information that could be sensitive.

Physical Security Countermeasures

Organizations are heavily dependent upon a mobile workforce with access to information, no matter where they travel. However, this mobility is putting organizations at risk of having a data breach if a laptop containing sensitive information is lost or stolen. Hence, physical security countermeasures are becoming very vital to protect the information on the employees laptops and to reduce the likelihood that employees will lose laptops.

1. *Cables and hardwired locks:* The most cost-efficient and ideal solution to safeguard any mobile device is securing with cables and locks, specially designed for laptops. Kensington cables are one of the most popular brands in laptop security cable. These cables are made of aircraft-grade steel and Kevlar brand fiber, thus making these cables 40%% stronger than any other conventional security cables. One end of the security cable is fit into the universal security slot of the laptop and the other end is locked around any fixed furniture or item, thus making a loop. These cables come with a variety of options such as number locks, key locks and alarms.

2. *Laptop safes:* Safes made of polycarbonate - the same material that is used in bulletproof windows, police riot shields and bank security screens-can be used to carry and safeguard the

laptops. The advantage of safes over security cables is that they protect the whole laptop and its devices such as CD-ROM bays, PCMCIA cards and HDD bays which can be easily removed in the case of laptops protected by security cables.

3. *Motion sensors and alarms*: Even though alarms and motion sensors are annoying owing to their false alarms and loud sound level, these devices are very efficient in securing laptops. Once these devices are activated, they can be used to track missing laptops in crowded places.

Also owing to their loud nature, they help in deterring thieves. Modern systems for laptops are designed wherein the alarm device attached to the laptop transmits radio signals to a certain range around the laptop.

4. *Warning labels and stamps:* Warning labels containing tracking information and identification details can be fixed onto the laptop to deter aspiring thieves. These labels cannot be removed easily and are a low-cost solution to a laptop theft. These labels have an identification number that is stored in a universal database for verification, which, in turn makes the resale of stolen laptops a difficult process. Such labels are highly recommended for the laptops issued to top executives and/or key employees of the organizations.

5. *Other measures for protecting laptops are as follows:*

□ Engraving the laptop with personal details

□ Keeping the laptop close to oneself wherever possible

□ Carrying the laptop in a different and unobvious bag making it unobvious to potential thieves

□ Creating the awareness among the employees to understand the responsibility of carrying a laptop and also about the sensitivity of the information contained in the laptop

□ Making a copy of the purchase receipt, laptop serial number and the description of the laptop

□ Installing encryption software to protect information stored on the laptop

□ Using personal firewall software to block unwanted access and intrusion

□ Updating the antivirus software regularly

□ Tight office security using security guards and securing the laptop by locking it down in lockers when not in use

□ Never leaving the laptop unattended in public places such as the car, parking lot, conventions, conferences and the airport until it is fitted with an anti theft device;

□ Disabling IR ports and wireless cards and removing PCMCIA cards when not in use. Information systems security also contains logical access controls. This is because, information, be it corporate or private, needs high security as it is the most important asset of an organization or an individual.

A few logical or access controls are as follows:

√ Protecting from malicious programs/attackers/social engineering.

√ Avoiding weak passwords/ access.

- √ Monitoring application security and scanning for vulnerabilities.
- √ Ensuring that unencrypted data/unprotected file systems do not pose threats.
- √ Proper handing of removable drives/storage mediums /unnecessary ports.
- √ Password protection through appropriate passwords rules and use of strong passwords.
- √ Locking down unwanted ports/devices.
- √ Regularly installing security patches and updates.
- √ Installing antivirus software/firewalls / intrusion detection system (IDSs).
- √ Encrypting critical file systems

Organizational security Policies and Measures in Mobile Computing Era:

Proliferation of hand-held devices used makes the cybersecurity issue graver than what we would tend to think. People have grown so used to their hand-helds they are treating them like wallets! For example, people are storing more types of confidential information on mobile computing devices than their employers or they themselves know; they listen to music using their-hand-held devices. One should think about not to keep credit card and bank account numbers, passwords, confidential E-Mails and strategic information about organization, merger or takeover plans and also other valuable information that could impact stock values in the mobile devices.

Imagine the business impact if an employee's USB, pluggable drive or laptop was lost or stolen, revealing sensitive customer data such as credit reports, social security numbers (SSNs) and contact information.

Operating Guidelines for Implementing Mobile Device Security Policies

In situations such as those described above, the ideal solution would be to prohibit all confidential data from being stored on mobile devices, but this may not always be practical.

Organizations can, however, reduce the risk that confidential information will be accessed from lost or stolen mobile devices through the following steps:

1. Determine whether the employees in the organization need to use mobile computing devices at all, based on their risks and benefits within the organization, industry and regulatory environment.

2. Implement additional security technologies, as appropriate to fit both the organization and the types of devices used. Most (and perhaps all) mobile computing devices will need to have their native security augmented with such tools as strong encryption, device passwords and physical locks. Biometrics techniques can be used for authentication and encryption and have great potential to eliminate the challenges associated with passwords.

3. Standardize the mobile computing devices and the associated security tools being used with them. As a matter of fundamental principle, security deteriorates quickly as the tools and devices used become increasingly disparate.

4. Develop a specific framework for using mobile computing devices, including guidelines for data syncing, the use of firewalls and anti-malware software and the types of information that can be stored on them.
5. Centralize management of your mobile computing devices. Maintain an inventory so that you know who is using what kinds of devices.
6. Establish patching procedures for software on mobile devices. This can often be simplified by integrating patching with syncing or patch management with the centralized
7. Provide education and awareness training to personnel using mobile devices. People cannot be expected to appropriately secure their information if they have not been told how.