Unit III

CYBERCRIME: MOBILE AND WIRELESS DEVICES

Introduction

Definition of Mobile and Wireless

The definition of mobile and wireless varies from person to person and organization to organization. In many cases, the terms mobile and wireless are used interchangeably, even though they are two different things. Let's start with the term mobile. Mobile is the ability to be on the move. A mobile device is anything that can be used on the move, ranging from laptops to mobile phones. As long as location is not fixed, it is considered mobile. Areas that are not included in our definition of mobile include remote offices, home offices, or home appliances. While these are definitely remote, they are not considered mobile.

Wireless refers to the transmission of voice and data over radio waves. It allows workers to communicate with enterprise data without requiring a physical connection to the network. Wireless devices include anything that uses a wireless network to either send or receive data. The wireless network itself can be accessed from mobile workers, as well as in fixed locations. Figure 1.1 depicts the relationship between mobile and wireless. As you can see, in most cases, wireless is a subset of mobile; but in many cases, an application can be mobile without being wireless.

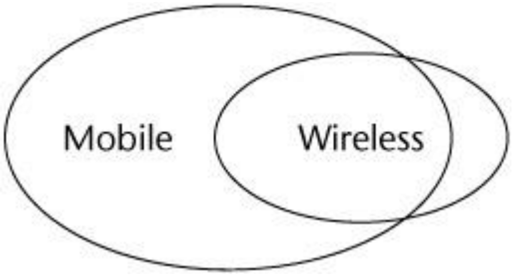

Figure 1.1: Relationship between mobile and wireless.

For an application to be considered mobile or wireless, it must be tailored to the characteristics of the device that it runs on. Limited resources, low network bandwidth, and intermittent connectivity all factor into the proper design of these applications.

Wireless applications that are not mobile use fixed wireless networks. These are wireless networks that provide network access in a fixed environment. An example is a wireless local area network (WLAN) that is used to give desktops network access. Many businesses as well as home users are installing WLAN technology to avoid having to install network cables throughout their buildings. Another example is network access via satellites in remote locations where there are no other connectivity options.

On the other side, we have mobile applications that are not wireless. There are many examples where this is the case. Any application that can be used on the move and that does not have wireless connectivity fits into this category. This includes many laptop and personal digital assistant (PDA) applications. Until only a few years ago, it was actually rare to have wireless data access for mobile devices. For these mobile applications, data is often synchronized using a fixed connection and stored on the device for use at a later time. It is worthwhile to note that even though these applications do not require wireless connectivity, they can often benefit from it when it is available. A sizeable portion of this book is dedicated to looking at these types of applications, which are referred to as smart client applications.

Now that we have defined mobile and wireless, it is time to look at some of the areas in which mobile applications are being deployed. Similar to the terms mobile and wireless, there is often confusion around the terms m-commerce and m-business.

Proliferation of Mobile and Wireless Devices

Mobile Technologies – Definition, Types, Uses, Advantages

-

Mobile technology is a type of technology in which a user utilizes a mobile phone to perform communications-related tasks, such as communicating with friends, relatives, and others. It is used to send data from one system to another. Portable two-way communications systems, computing devices, and accompanying networking equipment make up mobile technology.
Mobile technology is largely employed in cellular communication systems and other related areas. It employs a network architecture that allows multiple transmitters to deliver data on a single channel at the same time. Because it reduces the potential of frequency interference from two or more sources, this platform allows multiple users to use single frequencies. The channel has evolved over time.

This is fast expanding; its applications are getting increasingly broad over time, and it is gradually replacing other similar sources of communication on the market, such as post offices and landlines. Mobile technology has progressed from a simple phone and texting device to a multi-tasking system that can be used for GPS navigation, internet browsing, gaming, and instant messaging, among other things. With the rise, experts claim that the future of computer technology is dependent on wireless networking and mobile computing.

Through tablets and small PCs, mobile technology is becoming increasingly popular. This smartphone system has since been improved to a big multitasking computer that can be used for GPS navigation, gaming, internet browsing, and instant messaging. Tablets and portable laptops have increased the adoption of mobile technology. The mobile networks that connect these devices are referred to as wireless systems. They allow speech, data, and (mobile) apps to be shared between mobile devices.

Mobile technology is becoming increasingly prevalent. Smartphone users have surpassed 3 billion, and the global mobile workforce is expected to reach 1.87 billion by 2022. Any gadget with internet capabilities that can be accessed from anywhere is referred to as mobile technology. Smartphones, tablets, some iPods, and laptops already fall within this category, but this list will undoubtedly grow in the future years.

Types of Mobile Technologies

Followings are the few famous mobile technologies:

- SMS
- MMS
- 4G
- 3G
- GSM
- CDMA
- Wi-Fi

Let discuss them one by one in detail:

1. SMS: "SMS" stands for "Short Message Service." It is now the most widely used and oldest text messaging service. SMS are also sent over cellular networks, therefore you'll need a wireless plan and a wireless carrier. SMS is fast gaining popularity in the world as a low-cost messaging medium. Every text message delivered to a cell phone has become known as SMS. Messages can usually be up to 140 characters long. SMS was originally developed for GSM phones, although it is now supported by all major cellular phone networks.

Although SMS is most commonly used for text messaging between friends or coworkers, it also has a variety of additional uses. For example, SMS subscription services can send weather, news, sports updates, and financial quotes to consumers' phones. Employees may also be notified of sales requests, service stops, and other business-related information via SMS.

Fortunately, text messages sent via SMS do not require the receiver's phone to be turned on in order for the message to be delivered. The message will be kept in the SMS service until the receiver switches on his or her phone, at which point it will be transmitted to the recipient's phone. Most cell phone providers enable you to send a specific amount of text messages per month for free.

2. MMS: MMS (Multimedia Messaging Service) messaging is a standard method of delivering multimedia material, including messages. MMS, as opposed to SMS, can send up to forty seconds of video, one picture, a multi-image slideshow, or audio. MMS texting will be supported by the majority of contemporary devices. MMS capability is typically embedded within the text message interface and is turned on automatically when needed. If you enter in a text-only message, for example, it will be transmitted by SMS. If you include a graphic or video, the multimedia part will be sent via MMS. Similarly, if someone sends you a multimedia message, your phone will automatically receive the file via MMS.

An MMS message can convey rich media content to mobile devices at any time and from any location. It is a powerful and effective tool that assists businesses in reinforcing and deepening client loyalty by providing crucial information about their products and services. Because MMS texts are packed with photographs and videos, they are a significant marketing communication tool. As well as other audios. MMS is a cutting-edge method of communicating with others via mobile devices. Text messages are more successful because they deliver valuable information and services to the recipient. The more a corporation approaches its customers, the more probable it is to form a long-term brand partnership.

3. 3G: The third letter in the designation 3G stands for third-generation access technology, which allows mobile phones to connect to the internet. Every new technology introduces new frequency bands and data transmission rates.
The first generation emerged in the 1980s. First-generation uses large phones that had to be mounted on top of cars because they were too heavy to hold. Text messaging was made possible by the second-generation network, which became available in the 1990s. This huge and game-changing advancement also provided a more secure network and laid the path for today's ubiquitous 3G and 4G technology.

The development of 3G connection-based networks in 2001 marked the start of mainstream Internet use on mobile phones. Soon after, smartphones were introduced, bringing all of the capabilities of a device into the palm of your hand. The signals are transmitted by a network of telephone towers, ensuring robust and relatively rapid long-distance communication. The user's mobile phone is receiving data from the tower nearest to it. Although it may not appear complicated, 3G technology was revolutionary at the time it was introduced.

Upload speeds of up to 3 Mbps are possible on 3G networks. For example, about 15 seconds for uploading a 3-minute MP3 song. The fastest 2G phones, on the other hand, may get up to 144Kbps For example, about 8 minutes to download a 3-minute song. 3G systems are intended for digital phones with a full-screen display and better connectivity.

4. 4G: The fourth generation of mobile networking technology is known as 4G, which comes after the 2G and 3G networks. Although it's commonly referred to as 4G LTE, this isn't exactly right because LTE is just one sort of 4G. Most mobile network service providers use it now since it is the most developed technology.
However, as you may have heard, 5G is becoming operational alongside current 3G and 4G mobile networks. When it initially came out, 4G revolutionized how we use the mobile internet. Despite the fact that 3G networks were relatively limited, 4G network connectivity allowed consumers to browse the internet and watch HD films on their mobile devices, thereby turning smartphones into laptops.

Most tasks that you can do on a laptop or desktop computer can now be done on mobile devices such as smartphones or tablets. No matter how much data you require, 4 G networks allow you to keep consistent speeds practically anywhere. 4G was launched in the United Kingdom in 2012. Currently, the number of mobile subscribers using 3G outnumbers those using 4G. Expect this to alter in the coming years as 4G contracts become more affordable and 4G network coverage increases across the UK.

Premium 4G offers download speeds of around 14 Mbps, which is over five times quicker than the 3G network's predecessor. 4G networks can currently attain speeds of up to 150 Mbps, allowing users to download gigabytes of data in minutes, if not seconds, rather than hours as with 3G networks. Uploading data is also significantly faster with 4G – normal upload speeds are over 8 Mbps, with theoretical rates of up to 50 Mbps, whereas 3G upload speeds are under 0.5 Mbps.

5. Global System for Mobile technology: The (GSM) is an acronym for Global System for Mobile Communication. GSM is a cellular technology that is open and digital and is used for mobile communication. It operates on the 850 MHz, 900 MHz, 1800 MHz, and 1900 MHz frequency ranges. It employs a hybrid of FDMA and TDMA.
6. Code Division Multiple Access: (CDMA) is an acronym for code division multiple access. It is a channel access mechanism that also serves as an example of multiple access. Multiple access

simply means that data from multiple transmitters can be delivered onto a single communication channel at the same time.

7. Wi-Fi (Wireless Fidelity): Wi-Fi is a wireless networking technology that allows us to connect to a network or to other computers or mobile devices across a wireless channel. Data is delivered in a circular region over radio frequencies in Wi-Fi. Wi-Fi (Wireless Fidelity) is a generic acronym for a communication standard for a wireless network that functions as a Local Area Network without the use of cables or other types of cabling.

Use of Mobile technology

- The incorporation of mobile technology into business has aided telecollaboration. Now, people could connect from anywhere using mobile technology, and access the papers and documents they need to complete collaborative work.
- Work is being redefined by mobile technologies. Employees are no longer confined to their desks; they can work from anywhere in the world.
- Mobile technology can help your company save time and money. Employees who work from home save thousands on a regular basis. Mobile phones eliminate the need for costly technology like landline carrier services. Cloud-based services are less expensive than traditional systems. Technology can also help your company become more flexible and productive.
- Mobile technology has the potential to boost productivity significantly. Mobile application integration saves an average of 7.5 hours per week per employee. Workers can also become more productive with the use of smartphones and mobile gadgets.
- The popularity of cloud-based services has skyrocketed in recent years. Cloud-based mobile technology applications have been seen to be more useful than any smartphone, particularly in terms of available storage space.

Advantages of Mobile technology

- Through a variety of applications, we can now stay in touch with our friends and family members anytime we choose. We may now communicate or video visit with anybody we want by just using our cell phone or cell phone. Aside from that, the portable keeps us informed about the rest of the globe.
- Today’s mobile phones have made our day-to-day activities much more natural. Today, one may check the current traffic situation on their phone and make appropriate decisions to arrive on time. The weather is also a factor.
- With the advancement of mobile technology, the entire gaming world is now under one roof. When we are tired of monotonous work or during breaks, we can listen to music, view movies, watch our favorite shows, or simply watch a video of our favorite song.
- Mobile phones are being used for a variety of legitimate tasks, including meeting schedules, sending and receiving documents, providing introductions, warnings, and job applications, among others. Cell phones have become an indispensable tool for all working people.
- These days, mobile phones are also used as a wallet to make payments. Utilities might be used to send money to friends, relatives, and others right now.

Disadvantages of Mobile technology

- The modern family has become reliant on mobile phones. In any case, when we don’t have to travel, we surf the internet, play around, and create a genuine junkie.
- Because of the widespread use of mobile technology, people nowadays don’t meet in person but rather tweet or comment on social media sites.
- Because of the widespread use of mobile devices, there is a major risk of losing one’s protection. By efficiently reading through your web-based social networking account, anyone may now easily obtain data such as where you reside, your loved ones, what you do for a living, where you live, and so on.
- Mobile phone prices have risen in tandem with their worth. People nowadays spend a significant amount of money on cell phones, which could be better spent on more useful things like education or other beneficial items throughout our lives.

Trends in Mobility

Mobile device and connection trends: By 2023, there will be 13.1 billion global mobile devices and connections (up from 8.8 billion in 2018). Mobile devices are evolving from lower-generation network connectivity (2G) to higher-generation network connectivity (3G, 3.5G, 4G or LTE, and now 5G).

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 realize the seriousness of cybersecurity issues in the mobile computing domain.
□ Figure 3.3 shows the different types of mobility and their implications.

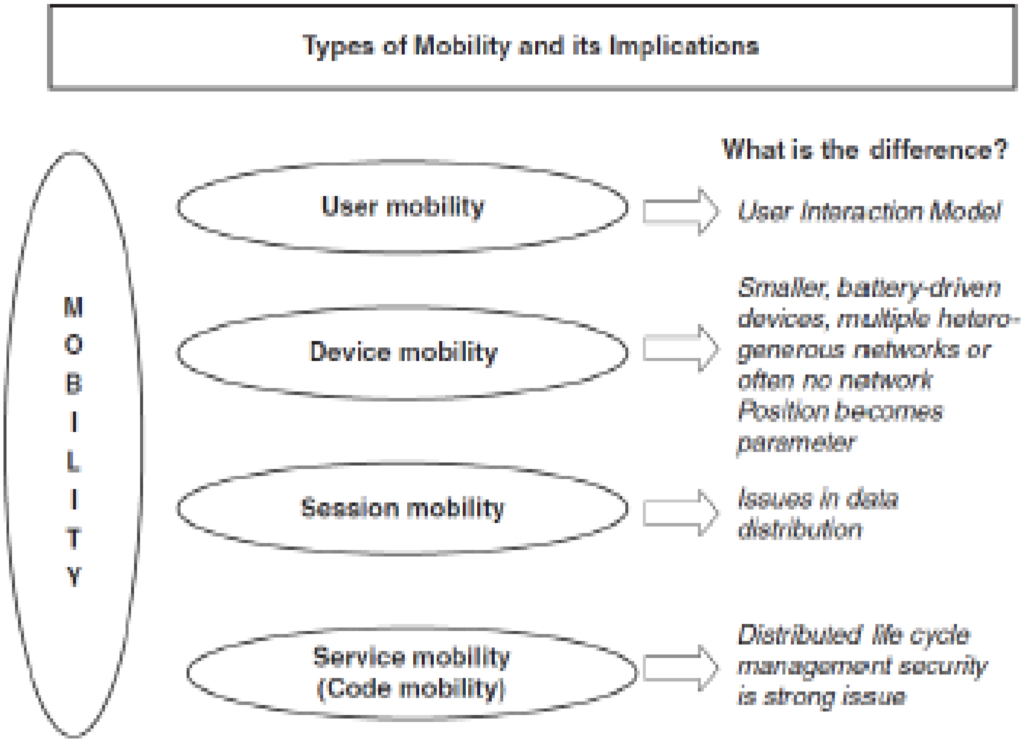
Types of Mobility and its Implications
What is the difference?
MOBILITY
User mobility
User Interaction Model
Device mobility
Smaller, battery-driven devices, multiple hetero-generous networks or often no network Position becomes parameter
Session mobility
Issues in data distribution
Service mobility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

Figure 3.3 | Mobility types and implications.

Credit card Frauds in Mobile and Wireless Computing Era

This era belongs to technology where technology becomes a basic part of our lives whether in business or home which requires connectivity with the internet and it is a big challenge to secure these units from being a sufferer of cyber-crime. Wireless credit card processing is a tremendously new service that will enable an individual to process credit cards electronically, virtually anywhere. It permits corporations to process transactions from mobile locations quickly, efficiently, and professionally and it is most regularly used via organizations that function in general in a cellular environment.

Nowadays there are some restaurants that are using wifi processing tools for the safety of their credit card paying customers. Credit card fraud can take place when cards are misplaced or stolen, mails are diverted by means of criminals, employees of a commercial enterprise steal some consumer information.

Techniques of Credit Card Frauds :

1. Traditional Techniques :

- **Paper-based Fraud –**
  Paper-based fraud is whereby a criminal makes use of stolen or faux files such as utility payments and financial institution statements that can construct up beneficial Personally Identifiable Information (PII) to open an account in anybody else's name.
- **Application Fraud –**
  1. ID Theft **:**
     Where a person pretends to be anybody else.
  2. **Financial Fraud :**
     Where a person offers false data about his or her monetary reputation to gather credit.

2. Modern Techniques :

Skimming to Commit Fraud is a kind of crime in which dishonest employees make unlawful copies of credit or debit cards with the help of a 'skimmer'. A skimmer is a gadget that captures credit card numbers and other account information which should be personal. The data and records held on either the magnetic stripe on the lower back of the deposit card or the records saved on the smart chip are copied from one card to another.

ML | Credit Card Fraud Detection

The challenge is to recognize fraudulent credit card transactions so that the customers of credit card companies are not charged for items that they did not purchase.

Main challenges involved in credit card fraud detection are:

1. Enormous Data is processed every day and the model build must be fast enough to respond to the scam in time.
2. Imbalanced Data i.e most of the transactions *(99.8%)* are not fraudulent which makes it really hard for detecting the fraudulent ones
3. Data availability as the data is mostly private.

4. Misclassified Data can be another major issue, as not every fraudulent transaction is caught and reported.
5. Adaptive techniques used against the model by the scammers.

How to tackle these challenges?

1. The model used must be simple and fast enough to detect the anomaly and classify it as a fraudulent transaction as quickly as possible.
2. Imbalance can be dealt with by properly using some methods which we will talk about in the next paragraph
3. For protecting the privacy of the user the dimensionality of the data can be reduced.
4. A more trustworthy source must be taken which double-check the data, at least for training the model.
5. We can make the model simple and interpretable so that when the scammer adapts to it with just some tweaks we can have a new model up and running to deploy.

In this modern era, the rising importance of electronic gadgets – which became an integral part of business, providing connectivity with the internet outside the office – brings many challenges to secure these devices from being a victim of cyber crime. These Credit card frauds and all are the new trends in cybercrime that are coming up with mobile computing – mobile commerce (M-COMMERCE) and mobile banking (M-Banking).

Today belongs to " Mobile computing" that is anywhere any time computing. The developments in wireless technology have fuelled this new mode of working for white collar workers. This is true for credit card processing too. Credit card (or debit card) fraud is a form of identity theft that involves an unauthorized taking of another's credit card information for the purpose of charging purchases to the account or removing funds from it.

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

Believe it or not there are security risks when using a mobile device. We know, it is surprising right, that your phone or tablet could be a possible threat to your safety. When you consider all the potential threats that exist on the Internet and the fact that most of today's mobile devices are connecting to and through the Internet with every function, I think it becomes easier to understand just how vulnerable they are. While more of the threats are the same as those faced by the average laptop or desktop user there are some unique to the mobile world. 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
- BOYD

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.

Protecting Against Mobile Threats

With the large and diverse mobile threat landscape, businesses require enterprise mobile security solutions. This is especially true as the shift to remote work makes these mobile devices a more common and critical component of an organization's IT infrastructure.

An effective mobile threat defense solution needs to be able to detect and respond to a variety of different attacks while providing a positive user experience. Accomplishing this requires implementing these guiding principles:

- A 360° view of security across device, apps, and the network
- Full flexibility and scalability
- Full visibility into the risk level of the mobile workforce
- Privacy protection by design
- An optimal user experience

Check Point's Harmony Mobile provides a comprehensive mobile security to keep corporate data safe by securing employees' mobile devices across all attack vectors: apps, network and OS solution. Check To check outsee Harmony Mobile's capabilities for yourself, request a personalized demo with a mobile security expert. You’re also welcome to try it out for yourself with a free trial. And for further information about the guiding principles and other important aspects of a mobile security solution, check out this mobile protection buyer’s guide.

A cyber-crime is a criminal act in which someone targets a computer or a network of devices in order to gain illegal rights, steal data from them, frauds etc. This type of crime is carried out using technology which primarily takes place online.

Some cyber-crime includes the following −

- Harassment
- Cyber-stalking
- Bullying

Types of Cyber-crimes

The types of cyber crimes are as follows −

Hacking

It is a type of cyber crime in which a person tries to identify and exploit weakness in a computer system or a computer network for his own benefits.

Some types of hacking are given below −

- Social Engineering & Phishing
- Malware-Injecting Devices
- Cracking Passwords
- Distributed Denial-of-Service

Virus dissemination

Virus dissemination is a process in which a Malicious software attaches itself to other software (which can be a trojan horse, time bond, virus , worm etc) which has the ability to destroy the victim computer/system.

Cyber Terrorism

Cyber terrorism is a type of attack in which a person uses the Internet to establish violent acts which may result in loss of a life, harm to a person or threaten to life. The main object of this is to gain political advantages by the use of threat.

Computer Vandalism

Computer Vandalism is a type of process in which a program has the ability to perform malicious tasks such as getting someone’s passwords or important data. This can even include the removal of user data or deleting one's hard drive.

Security Threats

Now, let us see the Security threats related to mobile devices, which are as follows −

- Data Leakage
- Unsecured Wi-Fi
- Network Spoofing
- Phishing Attacks
- Spyware
- Broken Cryptography
- Improper Session Handling

Let us discuss each threat in detail.

Unsecured Wi-Fi

Free wi-fi is easily attractive to people, if anyone connects to the free wifi, then the hackers might steal your data. Never use the free wifi when accessing confidential services like banking and transactions, there might be a chance of stealing your money.

Phishing Attacks

Phishing attacks are mostly seen in emails and messages. When the user clicks on a suspicious link, there might be a chance of virus files download which can corrupt and hack your devices which results in data loss. In some cases, they will send a form to fill in the confidential information.

Malicious Apps and websites

When you download any app manually from the websites, there might be a chance that the app can accomplish some objectives like stealing data, encrypting the data, etc.

Weak Passwords

If the passwords of the mobile devices are weak there might be a change of others accessing the data. This might result in data leakage and privacy issues. So make sure that the passwords for mobile devices or apps must be strong.

Iot Mobile security threats

As we all know most of the things are correcting to the internet and works easily, fast with the internet from wearable tech like smartphones, watches, etc. If these devices are hacked then misuse of these devices might result in huge costs.

Types of Wireless and Mobile Device Attacks

Wireless and mobile devices have become ubiquitous in today's society, and with this increased usage comes the potential for security threats. Wireless and mobile device attacks are a growing concern for individuals, businesses, and governments.

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.

Conclusion: *Wireless and mobile device attacks can have severe consequences, including the theft of sensitive data, identity theft, financial loss, and reputational damage. To protect against these attacks, users should always use strong passwords, keep their devices and software up-to-date, avoid connecting to unsecured networks, and use reputable app stores. Businesses should also implement security measures such as firewalls, intrusion detection systems, and employee training to protect against wireless and mobile device attacks.*

Registry Settings for Mobile Devices

Let us understand the issue of registry settings on mobile devices through an example: Microsoft Activesync 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. 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. 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.

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 computer network – as it can be easily intercepted by the eavesdropper to impersonate the user.

There are 2 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. 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:
   a. DoS attacks: –
   b. Traffic analysis:-
   c. Eavesdropping:-
   d. Man-in-the-middle attacks: –

2. Security in network: – Security measures in this regard come from
    a. Wireless Application Protocol (WAP)
    b. use of Virtual Private Networks (VPN)
    c. MAC address filtering

Device hardening is a collection of tools and techniques to reduce vulnerability and helps in securing the network. Some of these methods involve Mutual Authentication, WEP and WPA/WPA2.

- **Mutual Authentication:** One of the remarkable vulnerabilities of wireless networks is the utilization of rogue access points. An access point is a device that enables wireless devices to connect to a network. Any device that has a wireless transmitter and hardwired interface to a network can go about as a rogue access point. The rogue access point can impersonate an authorized access point. The outcome is that wireless devices establish communication with the rogue access point rather than the authorized access point. The hoaxer can receive connection requests, copy the data in the request and forward the data to the authorized network access point. To prevent rogue access points, mutual authentication is used. In Mutual authentication, both entities in a communications link authenticate to each other. The client validates to the access point and the access point authenticates the client. It is also known as two-way authentication.
- **Wired Equivalent Privacy (WEP):** Wired Equivalent Privacy (WEP) is one of the first and widely used Wi-Fi security guidelines. WEP became a security standard in September 1999. It provides authentication and encryption protections. The WEP standards are out of date however numerous devices still support WEP. Regardless of corrections to the standard and expanded key size, WEP experienced various security shortcomings. Cyber criminals can crack WEP passwords easily and quickly.
- **Wi-Fi Protected Access (WPA/WPA2)** The most widely recognized WPA configuration is WPA-PSK (Pre-Shared Key). The keys used by WPA are 256-bit. WPA provides message integrity checks which could detect if an attacker had captured and changed information gone between the wireless access point and client. Another key security improvement is Temporal Key Integrity Protocol (TKIP). The TKIP standard provides the ability to secure and change encryption keys. One of the most noteworthy security improvements from WPA to WPA2 was the obligatory utilization of Advanced Encryption Standard algorithms.

Interesting Facts:

- WPA2 is the fastest of the encryption protocols.
- WPA2 passwords can be up to 63 characters in length.

Attacks on Mobile/Cell Phones

Cybercrime or Cyber-attack is a much-talked topic recently, and cybercriminals use different techniques to disable one or multiple computers & networks. Cyberattacks can disable computers and steal data. Cybercriminals use varied technologies to steal data from computers. Cyber-attacks include Phishing, malware, etc.

Types of cyber Attacks

Undoubtedly, cyber-attacks have substantial negative impacts. A cyber-attack can cause data breaches or data manipulation. Once an organization faces a cyber-attack, it can suffer huge losses. Today, all need to have a bit of knowledge of different types of cyber-attacks.

- **Malware** − Malware is a malicious virus, including spyware, Trojans, adware, etc. Trojan viruses conceal its feature as legitimate software, whereas Ransomware does not allow a computer to access prime components of the network.
- **Phishing** − Among the most common cyberattacks, Phishing creates a significant impact on computers and networks. You can get affected via Phishing if you open an unknown mail or click on the links of the mail.
- **Attack through password** − This is a typical attack where hackers identify and hack your password.

Apart from those above, people worldwide suffer from other cyberattacks like SQL injunction attacks, Denial of service attacks, Insider threats, etc.

Cyber Security - History

Cyber threats or cyberattacks have increased significantly in the last few years, and cyber security has been launched to protect computers from different types of cyber threats. Cyber security, or IT security, has emerged as one of the most efficient ways of protecting computers. These security measures have made it possible to keep the software, electronic data, and hardware safe & secured.

The journey of Cyber Security began in the year 1970. Bob Thomas, the famous researcher & Programmer, generated a computer program called Creeper. It can move across the network ARPANET.

Commercial antivirus launched first time in the market in the 1980s. The founder of G Data Software, Andreas Luning and Kai Figge, launched 1985 the first antivirus known as the Atari ST Platform. In 1987, another antivirus was launched known as Ultimate Virus Killer.

The antivirus companies started growing in 1988, and Tjark Auerbach released Avira and the first version of AntiVir. 2014 to present era is known as the Next Gen, and loads of antivirus have been released within this time frame.

Brief on mobile security threats

Smartphones have emerged as one of the most significant devices in recent times, and many organizations also consider this device to improve operations and yield. With the increase in the usage of mobile devices, it has become easy to access computer systems from remote locations. This can lead to data breaches, and here, organizations must take necessary precautions against any data breach.

Normally, organizations can face different types of mobile security threats, like mobile application security, web-based security, mobile network security, and mobile device security.

Types of mobile threats

Every organization must pay attention to varied mobile threats and take necessary actions. Mobile devices also have software and internet access, which can easily get affected by malicious viruses. Here all can check the probable mobile threats that every device can suffer.

- **Suffering from malicious apps** − Like computers, mobiles also get infected through a malicious virus. Several malicious websites can steal mobile data and adversely impact users' lives. Trojans are the most common malicious apps for mobile devices.
- **Ransomware** − Ransomware is another damaging malware. While your mobile devices face this challenge, you cannot access the data. Sometimes this malware can block your access to get data permanently.
- **Phishing** − At present, Phishing is one of the most prevalent online threats that users can often experience via mobile or computer. Mobile phishing is a sub-type of Phishing that shares personal information with hackers. The use of smartphones has increased the risk of Phishing. SMS and voice phishing are some common methods used to fool mobile users.
- **Using public WIFI** − Public WIFI is less secure than private WIFI. At present, WIFI connections have become easy to access among the mass. People can use free WIFI in shopping complexes, hotels, etc. However, using open WIFI is always a threat to mobile devices.
- **MitM threats** − MitM is also known as the Man-in-the-Middle attacks. Here the attacker incepts between the communications of the two parties without the knowledge of the communicating parties. Here the attacker controls the entire communication between the parties. This cybercrime has emerged as one of the most prominent cyber threats, as it can manipulate an individual's confidential information. Here the attacker installs a sniffer to incept an insecure network connection—Internet protocol spoofing, domain name system spoofing, HTTP spoofing, hijacking of emails, etc.
- **The exploitation of operating systems** − This is another recent threat every mobile user has faced. This cybercrime takes advantage of limitations in the mobile device's operating system. As per this technology, hackers also manipulate software codes.

Preventive measures against cyber attacks

With the advancement in technology, the cases of cyber-attacks have been considerably enhanced. Organizations from different parts of the world often claim to suffer from advanced cyberattacks. With the increasing rate of cyber threats, experts have also invented fruitful solutions to stay protected from cyber threats. Let's check some effective solutions against cybercrimes.

- Organizations need to train their staffs who take care of emails and messages on behalf of the companies. They should only open a link with proper checking.
- Experts also suggest keeping software used in mobiles or laptops constantly updated. Cybercriminals can only detect the weakness of software if you update them on time.
- Experts suggest ensuring endpoint protection for corporate networks connecting mobiles, laptops, etc. The paths of these connections should be protected using proper endpoint protection.
- Installation of a Firewall is another effective way to stay from any type of cyber threat.
- Experts also suggest keeping a backup of your data to recover the data despite cyber attacks.

Besides, controlling access systems and maintaining WIFI security is also necessary to eliminate cyber threats.

Organizational security Policies and Measures in Mobile Computing Era

Laptops