UNIT-V

MOBILE COMPUTING

Mobile computing as a generic term describing ability to use the technology to wirelessly connect to and use centrally located information and/or application software through the application of small, portable, and wireless computing and communication devices.

In mobile computing, a set of distributed computing systems or service provider servers participate, connect, and synchronies through mobile communication protocols. Provides decentralized (distributed) computations on diversified devices, systems, and networks, which are mobile, synchronized, and interconnected via communication standards and protocols. Mobile device does not restrict itself to just one application, such as, voice communication Provides decentralized (distributed) computations on diversified devices, systems, and networks, which are mobile, synchronized, and interconnected via mobile communication standards and protocols.

Mobile device does not restrict itself to just one application, such as, voice communication. Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link.

ADVANTAGES:

1- **Increase in Productivity**- Mobile devices can be used out in the field of various companies, therefore reducing the time and cost for clients and themselves.

2- **Entertainment**- Mobile devices can be used for entertainment purposes, for personal and even for presentations to people and clients.

3- **Portability**- this would be one of the main advantages of mobile computing, you are not restricted to one location in order for you to get jobs done or even access email on the go

4- **Cloud Computing**- This service is available for saving documents on a online server and being able to access them anytime and anywhere when you have a connection to the internet and can access these files on several mobile devices or even pcs at home.

DISADVANTAGES:

1- **Quality of connectivity**- as one of the disadvantages, mobile devices will need either wifi connectivity or mobile network connectivity such as GPRS, 3G and in some countries even 4G connectivity that is why this is a disadvantage because if you are not near any of these connections your access to the internet is very limited.

2- **Security concerns**- Mobile phones are unsafe to connect to, and also syncing devices might also lead to security concerns. Accessing a wifi network can also be risky because WPA and WEP security can be bypassed easily.

3- **Power Consumption**- due to the use of batteries in these devices, these do not tend to last long, if in a situation where there is no source of power for charging then that will certainly be a letdown.

MAJOR ISSUES IN MOBILE COMPUTING

Resource constraints: Battery
Interference: the quality of service (qos)
Bandwidth: connection latency
Dynamic changes in communication environment: variations in signal power within a region, thus link delays and connection losses
Network Issues: discovery of the connection-service to destination and connection stability
Interoperability issues: the varying protocol standards
Security constraints: Protocols conserving privacy of communication

MOBILE COMPUTING FUNTIONS

A computing environment is defined as mobile if it supports one or more of these characteristics:

- User mobility: User should be able to move from one physical location to another location and use same service
- Network mobility: User should be able to move from one network to another network and use same service
- Device mobility: User should be able to move from one device to another and use same service
- Session mobility: A user session should be able to move from one user-agent environment to another.
- Service mobility: User should be able to move from one service to another
- Host mobility: The user can be either a client or server.

Mobile computing functions can be logically divided into the major segments:

1- User with device: fixed, portable

2- Network: different networks: GSM, CDMA, Ethernet, Wireless LAN etc.

3- Gateway: Interfacing different transport bearers

4- Middleware: handling the presentation and rendering of the content on a particular device.

5- Content: it is the domain where the origin server and content is.

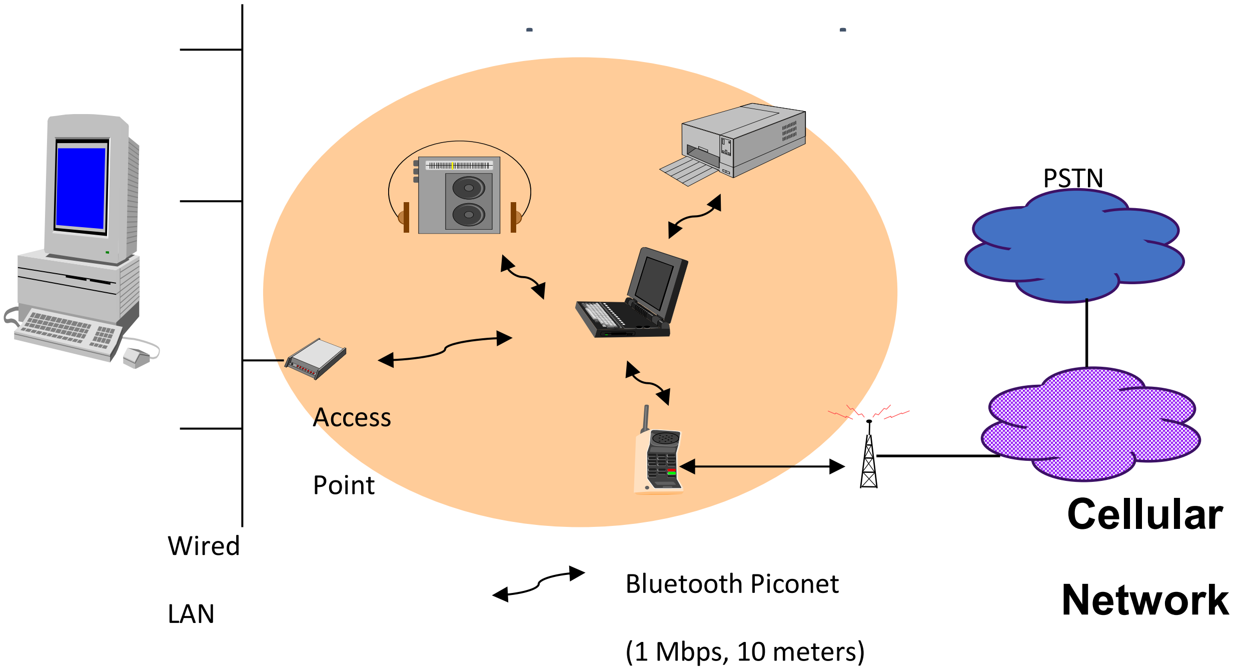
EMERGING TECHNOLOGIES – BLUE TOOTH

Bluetooth is a wireless cable replacement standard that provides a 1 Mbps data rate over 10 meters or less. It typically consists of a group of linked devices, such as a computer wirelessly connecting to a set of peripherals, known as a "piconet." Multiple piconets can be formed to provide wider coverage. Due to its relatively low data rates and very short distances, Bluetooth is being used in home appliances, "Bluetooth-enabled" cars, and other such applications.

- Founders: Ericsson, IBM, Intel, Nokia, Toshiba; May 98
- Currently: Over 850 companies, V1.0 spec issued 7/99
- Small form factor, low-cost, short range radio link between mobile pcs, phones and other portable devices

- Relatively fast, short packets
- Software for service and device discovery
- Typical application: cellular phone to PDA or earphone

The next Figure shows a simple Bluetooth was designed to allow low-bandwidth wireless connections to become so simple to use that they seamlessly mesh into your daily life. A simple example of a Bluetooth application is updating your cellular phone directory. The main idea is that this could happen automatically as soon as the phone is within the range (10 meters) of your desktop computer where your directory resides.



RADIO-FREQUENCY IDENTIFICATION

Radio Frequency Identification is a technology that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency (RF) portion of the electromagnetic spectrum to uniquely identify an object, animal, or person. RFID is coming into increasing use in industry as an alternative to the bar code. The advantage of RFID is that it does not require direct contact or line-of-sight scanning.

RFID stands for **Radio-Frequency identification**. The acronym refers to small electronic devices that consist of a small chip and an antenna. The chip typically is capable of carrying 2,000 bytes of data or less.

The RFID device serves the same purpose as a bar code or a magnetic strip on the back of a credit card or ATM card; it provides a unique identifier for that object. And, just as a bar code or magnetic strip must be scanned to get the information, the RFID device must be scanned to retrieve the identifying information.

An RFID system consists of three components: an antenna, transceiver (often combined into one reader) and a transponder (the tag).

The antenna uses radio frequency waves to transmit a signal that activates the transponder. When activated, the tag transmits data back to the antenna. The data is used to notify a programmable logic controller that an action should occur. The action could be as simple as raising an access gate or as complicated as interfacing with a database to carry out a monetary transaction.

Low-frequency RFID systems (30 khz to 500 khz) have short transmission ranges (generally less than six feet). High-frequency RFID systems (850 mhz to 950 mhz and 2.4 ghz to 2.5 ghz) offer longer transmission ranges (more than 90 feet). In general, the higher the frequency, the more expensive the system.

RFID stands for **Radio-Frequency identification**. The acronym refers to small electronic devices that consist of a small chip and an antenna. The chip typically is capable of carrying 2,000 bytes of data or less. The RFID device serves the same purpose as a bar code or a magnetic strip on the back of a credit card or ATM card; it provides a unique identifier for that object. And, just as a bar code or magnetic strip must be scanned to get the information, the RFID device must be scanned to retrieve the identifying information.

RFID Works Better Than Barcodes

A significant advantage of RFID devices over the others mentioned above is that the RFID device does not need to be positioned precisely relative to the scanner. We're all familiar with the difficulty that store checkout clerks sometimes have in making sure that a barcode can be read. And obviously, credit cards and ATM cards must be swiped through a special reader.

In contrast, RFID devices will work within a few feet (up to 20 feet for high-frequency devices) of the scanner. For example, you could just put all of your groceries or purchases in a bag, and set the bag on the scanner. It would be able to query all of the RFID devices and total your purchase immediately

RFID technology has been available for more than fifty years. It has only been recently that the ability to manufacture the RFID devices has fallen to the point where they can be used as a "throwaway" inventory or control device. Alien Technologies recently sold 500 million RFID tags to Gillette at a cost of about ten cents per tag. One reason that it has taken so long for RFID to come into common use is the lack of standards in the industry. Most companies invested in RFID technology only use the tags to track items within their control; many of the benefits of RFID come when items are tracked from company to company or from country to country.

Common Problems with RFID

Some common problems with RFID are reader collision and tag collision. Reader collision occurs when the signals from two or more readers overlap. The tag is unable to respond to simultaneous queries. Systems must be carefully set up to avoid this problem. Tag collision occurs when many tags are present in a small area; but since the read time is very fast, it is easier for vendors to develop systems that ensure that tags respond one at a time. See Problems with RFID for more details.

Radio frequency identification (RFID) is a form of wireless communication that uses radio waves to identify and track objects.

RFID takes the bar coding concept and digitizes it for the modern world providing the ability to:

- Uniquely identify an individual item beyond just its product type
- Identify items without direct line-of-sight
- Identify many items (up to 1,000s) simultaneously
- Identify items within a vicinity of between a few centimeters to several meters

An RFID system has *readers* and *tags* that communicate with each other by radio. RFID tags are so small and require so little power that they don’t even need a battery to store information and exchange data with readers. This makes it easy and cheap to apply tags to all kinds of things that people would like to identify or track.

RFID technology has the capability to both greatly enhance and protect the lives of consumers, and also revolutionize the way companies do business. As the most flexible auto-identification technology, RFID can be used to track and monitor the physical world automatically and with accuracy.

RFID can tell you what an object is, where it is, and even its condition, which is why it is integral to the development of the Internet of Things—a globally interconnected web of objects allowing the physical world itself to become an information system, automatically sensing what is happening, sharing related data, and responding.

RFID use is increasing rapidly with the capability to “tag” any item with an inexpensive communications chip and then read that tag with a reader. Endless applications range from supply chain management to asset tracking to authentication of frequently counterfeited pharmaceuticals. Applications are limited, in fact, only by the imagination of the user.

RFID can help:

- Automate inventory and asset-tracking in healthcare, manufacturing, retail, and business sectors
- Identify the source of products, enabling intelligent recall of defective or dangerous items, such as tainted foods, defective toys, and expired or compromised medication
- Prevent use of counterfeit products in the supply chain

- Improve shopping experience for consumers, with fewer out-of-stock items and easier returns
- Provide visibility into the supply chain, yielding a more efficient distribution channel and reduced business costs
- Decrease business revenue lost to theft or inaccurate accounting of goods
- Improve civilian security through better cargo monitoring at ports
- Wirelessly lock, unlock and configure electronic devices
- Enable access control of certain areas or devices

Whatever the application, RFID has the potential to increase efficiency of operations, improve asset visibility and traceability, decrease reliance on manual processes, reduce operations costs, and provide useful data for business analytics.

WIRELESS BROADBAND

Originally the word "broadband" had a technical meaning, but became a marketing term for any kind of relatively high-speed computer network or Internet access technology. According to the 802.16-2004 standard, broadband means "having instantaneous bandwidths greater than 1 mhz and supporting data rates greater than about 1.5 Mbit/s." The Federal Communications Commission (FCC) recently re-defined the definition to mean download speeds of at least 25 Mbit/s and upload speeds of at least 3 Mbit/s.

Wimax is an IP based, wireless broadband access technology that provides performance similar to 802.11/Wi-Fi networks with the coverage and QOS (quality of service) of cellular networks. Wimax is also an acronym meaning "Worldwide Interoperability for Microwave Access (wimax). Wimax is a wireless digital communications system, also known as IEEE 802.16, that is intended for wireless "metropolitan area networks". Wimax can provide broadband wireless access (BWA) up to 30 miles (50 km) for fixed stations, and 3 - 10 miles (5 - 15 km) for mobile stations. In contrast, the wifi/802.11 wireless local area network standard is limited in most cases to only 100 – 300 feet (30 - 100m). Wimax operates on both licensed and non-licensed frequencies, providing a regulated environment and viable economic model for wireless carriers. The average cell ranges for most wimax networks will likely boast 4-5 mile range (in NLOS capable frequencies) even through tree cover and building walls. Service ranges up to 10miles (16 Kilometers) are very likely in line of sight (LOS) applications (once again depending upon frequency). Mobile wimax capabilities on a per customer basis are much better than competing 3G technologies. Wimax is often cited to possess a spectral efficiency of 5 bps/Hz, which is very good in comparison to other broadband wireless technologies, especially 3G.

WIMAX SYSTEM

A wimax system consists of two parts:

• A **wimax tower - s**imilar in concept to a cell-phone Tower- A single wimax tower can provide coverage to a Very large area as big as 3,000 square miles (~8,000 squareKm).

• A **wimax receiver** – The receiver and antenna could be A small box or PCMCIA card, or they could be built into a Laptop the way wifi access is today. A wimax tower station can connect directly to the Internet using a high bandwidth, wired connection (for
Example, a T3 line). It can also connect to another wimax Tower using a line-of-sight, microwave link. This Connection to a second tower (often referred to as a **Backhaul**), along with the ability of a single tower to cover Up to 3,000 square miles, is what allows wimax to Provide coverage to remote rural areas. Compared to the complicated wired network, a wimax

System only consists of two parts:

The wimax base station (BS) and wimax subscriber Station (SS), also referred to as customer premise Equipments (CPE). Therefore, it can be built quickly at a Low cost. Ultimately, wimax is also considered as the Next step in the mobile technology evolution path. The Potential combination of wimax and CDMA standards is Referred to as 4G.

System Model

IEEE 802.16 supports two modes of operation: PTP and PMP.

Point-to-point (PTP)

The PTP link refers to a dedicated link that connects only two nodes: BS and subscriber terminal. It utilizes resources In an inefficient way and substantially causes high Operation costs. It is usually only used to serve high-value Customers who need extremely high bandwidth, such as Business high-rises, video postproduction houses, or scientific research organizations. In these cases, a single Connection contains all the available bandwidth to generate High throughput. A highly directional and high-gain Antenna is also necessary to minimize interference and Maximize security.

Point-to-multipoint (PMP)

The PMP topology, where a group of subscriber terminals Are connected to a BS separately (shown in Figure), is abettor choice for users who do not need to use the entire Bandwidth. Under PMP topology, sector al antennas with Highly directional parabolic dishes (each dish refers to a Sector) are used for frequency reuse. The available Bandwidth now is shared between a group of users, and the Cost for each subscriber is reduced.

Mesh Topology

In addition to PTP and PMP, 802.16a introduces the mesh Topology, which is a more flexible, effective, reliable, and Portable network architecture based on the multihop Concept. Mesh networks are wireless data networks that Give the sss more intelligence than traditional wireless Transmitters and receivers. In a PMP network, all the Connections must go through the BS, while with mesh Topology, every SS can act as an access point and is able to Route packets to its neighbors by itself to enlarge the Geographical coverage of a network. The architecture of a Mesh system is shown in Figure. The routing across the Network can be either proactive (using predetermined Routing tables) or reactive (generating routes on demand).

Benefits of WiMAX

Component Suppliers

- Assured wide market acceptance of developed and components
- Lower production costs due to economies of scale
- Reduced risk due to interoperability Equipment Manufacturers
- Stable supply of low cost components and chips
- Freedom to focus on development of network elements consistent with core competencies, while knowing that equipment will interoperate with third party products
- Engineering development efficiencies
- Lower production costs due to economies of scale Operators and Service Providers
- Lower CAPEX – with lower cost base station, customer premises equipment (CPE), and network deployment costs
- Lower investment risk due to freedom of choice among multiple vendors and solutions
- Ability to tailor network to specific applications by mixing and matching equipment from different vendors
- Improved operator business case with lower OPEX End Users
- Lower subscriber fees
- Wider choice of terminals enabling cost performance analysis
- Portability of terminals when moving locations/networks from WiMAX operator “A” to operator “B”
- Lower service rates over time due to cost efficiencies in the delivery chain.

Limitations of Wimax

Wireless Technologies

Wireless technologies can be classified in different ways depending on their range. Each wireless technology is designed to serve a specific usage segment. The requirements for each usage segment are based on a variety of variables, including Bandwidth needs, Distance needs, and Power.

Wireless Wide Area Network (WWAN)

This network enables you to access the Internet via a wireless wide area network (WWAN) access card and a PDA or laptop.

These networks provide a very fast data speed compared with the data rates of mobile telecommunications technology, and their range is also extensive. Cellular and mobile networks based on CDMA and GSM are good examples of WWAN.

Wireless Personal Area Network (WPAN)

These networks are very similar to WWAN except their range is very limited.

Wireless Local Area Network (WLAN)

This network enables you to access the Internet in localized hotspots via a wireless local area network (WLAN) access card and a PDA or laptop. It is a type of local area network that uses high-frequency radio waves rather than wires to communicate between nodes. These networks provide a very fast data speed compared with the data rates of mobile telecommunications technology, and their range is very limited. Wi-Fi is the most widespread and popular example of WLAN technology.

Wireless Metropolitan Area Network (WMAN)

This network enables you to access the Internet and multimedia streaming services via a wireless region area network (WRAN). These networks provide a very fast data speed compared with the data rates of mobile telecommunication technology as well as other wireless network, and their range is also extensive.

WIMAX BUILDING BLOCKS:

A WiMAX system consists of two major parts:

1. A WiMAX base station
2. A WiMAX receiver

WiMAX Base Station

A WiMAX base station consists of indoor electronics and a WiMAX tower similar in concept to a cell-phone tower. A WiMAX base station can provide coverage to a very large area up to a radius of 6 miles. Any wireless device within the coverage area would be able to access the Internet. The WiMAX base stations would use the MAC layer defined in the standard, a common interface that makes the networks interoperable and would allocate uplink and downlink bandwidth to subscribers according to their needs, on an essentially real-time basis.

Each base station provides wireless coverage over an area called a cell. Theoretically, the maximum radius of a cell is 50 km or 30 miles however, practical considerations limit it to about 10 km or 6 miles.

WiMAX Receiver

A WiMAX receiver may have a separate antenna or could be a stand-alone box or a PCMCIA card sitting in your laptop or computer or any other device. This is also referred as customer premise equipment (CPE). WiMAX base station is similar to accessing a wireless access point in a WiFi network, but the coverage is greater.

Backhaul

A WiMAX tower station can connect directly to the Internet using a high-bandwidth, wired connection (for example, a T3 line). It can also connect to another WiMAX tower using a line-of-sight microwave link. Backhaul refers both to the connection from the access point back to the base station and to the connection from the base station to the core network. It is possible to connect several base stations to one another using high-speed backhaul microwave links. This would also allow for roaming by a WiMAX subscriber from one base station coverage area to another, similar to the roaming enabled by cell phones.

SECURITY ISSUES IN MOBILE COMPUTING

Mobile Computing Security Issues

Mobile computing is a broad area that describes a computing environment where the devices are not restricted to a single place. It is the ability of computing and communicating while on the move. Wireless networks help in transfer of information between a computing device and a data source without a physical connection between them. These networks include wireless LAN, wireless access point, and cellular networks [3]. So some of the new security issues introduced in mobile computing are originated from the security issues of wireless networks and distributed computing systems. In addition, poorly managed mobile devices introduce new security issues involving information exposure and compromise especially when these devices like laptops, PDAs, iPhones, Blackberrys, and others are loaded with sensitive information and are stolen or fallen into the hands of an unauthorized person. Hence **t**he new types of threats and security challenges introduced by mobile computing can be classified into two main classes: Security issues related to wireless networks and the transmission of information 'over the air' between mobile units and mobile support stations and networks.Security issues related to the mobility of the devices and the information residing on them.

Wireless Networks Security Issues

Wireless networks have their own security issues and challenges. This is mainly due to the fact that they use radio signals that travel through the air where they can be intercepted by location-less hacker that are difficult to track down. In addition, most wireless networks are dependent on other private networks, owned and managed by others, and on a public-shared infrastructure where you have much less control of, and knowledge about, the implemented security measures. Although encryption aid to some extend in securing information moving across wireless networks, the moment the data leaves a mobile device and heads onto a communication network, it's the network operator's job to ensure that the information is securely transported to its final destination.

In what follows, I will list and discuss the main mobile computing security issues introduced by the use of wireless networks. Most of these issues can fall under one of the following categories: Availability where the availability of information and services could be disrupted, confidentiality where the privacy of information when it passes through the wireless medium can be compromised, and integrity of data where data interchanged can be modified and retransmitted

Denial of Service. This attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. DOS attacks are common in all kinds of networks, but they are p articularly threatening in the wireless context. This is because, the attacker does not require any physical infrastructure and he gets the necessary anonymity in the wireless environment. The attacker floods the communication server or access point with a large number of connection requests so that the server keeps responding to the attacker alone hindering legitimate users from connecting and receiving the normal service.

Traffic Analysis. The attacker can monitor the transmission of data, measure the load on the wireless communication channel, capture packets, and reads the source and destination fields. In order to do this, the attacker only needs to have a device with a wireless card and listen to the traffic flowing through the channel. By doing such things, the attacker can locate and trace communicating users and gain access to private information that can be subject to malicious use.

Eavesdropping. This is a well known security issue in wireless networks. If the network is not secure enough and the transmitted information is not encrypted then an attacker can log on to the network and get access to sensitive data, as long as he or she is within range of the access point.

Session Interception and Messages Modification. The attacker can intercept a session and alter the transmitted messages of the session. Another possible scenario by an attacked is to intercept the session by inserting a malicious host between the access point and the end host to form what is called man-in-the-middle. In this case all communications and data transmissions will go via the attacker's host.

Spoofing. The attacker may hijack a session and impersonate as an authorized legitimate user to gain access to unauthorized information and services.

Captured and Retransmitted Messages. The attacker can capture a full message that has the full credential of a legitimate user and replay it with some minor but crucial modification to the same destination or to another one to gain unauthorized access and privileged to the certain computing facilities and network services.

Information Leakage. This potential security issue lies in the possibility of information leakage, through the inference made by an attacker masquerading as a mobile support station. The attacker may issue a number of queries to the database at the user's home node or to database at other nodes, with the aim of deducing parts of the user's profile containing the patterns and history of the user's movements.

Device Security Issues

Mobile Devices are essential and key components of a mobile computing environment. A mobile device is any portable device that belongs to a specific user and has computing and storage capabilities. Mobile devices like laptops, cell phones, iPhones, Blackberrys, PDAs, USBs and other small devices can store vital and sensitive data outside office environment for convenient use by mobile users. But this convenience of mobility and portability is accompanied by several new security threats related to possible unintended data disclosure. Mobile devices are easily stolen, and theft of such devices is on the rise. In most theft cases the aim was the data stored on the device rather than the device itself. One such well known case that happened in Beirut-Lebanon on Oct, 27, 2010 was the attack on the investigation team of the UN created International Tribunal for Lebanon, set up in 2007 to bring to justice those involved in the assassination of then Prime Minister Rafiq Hariri. The result of the attack was the confiscating of the laptop computers, cell phones, notebooks and other materials that were in the possession of the investigation team. One of the main goals of the attack was the sensitive and crucial data stored on these mobile and portable devices. There is compelling evidence that mobile devices pose one of the fast growing areas of security concern. Since January 2008, Privacy Rights International's published Chronology of Data Breaches documents that 20 percent of the data breaches reported resulted from mobile device losses: Lost laptops, notebook computers, PDAs, portable drives, USBs, CDs, flash cards, SD cards, and disks . As a result of these incidents, all of the major mobile devices makers have taken steps during the past few years to improve device security, such as by providing longer device unlock codes like the case of Apple iOS devices, and extending encryption support to SD cards and other mobile data storage devices. However, many defense technology experts feel that protection measures remain insufficient for defense needs and therefore must be strengthen with additional safety measures. Mobile devices have extra stringent security needs and are vulnerable to new types of security threats and attacks. They need to operate in foreign networks, such as coffee shops, airport kiosks, or other hotspots, and therefore, can't rely on the organization's firewall for protection. The organization needs a means of managing security configuration, patch deployment and antivirus updates on their devices in the field. The main new mobile computing security issues introduced by the use of mobile devices include the following:

Pull Attacks: The attacker controls the device as a source of propriety data and control information. Data can be obtained from the device itself through the data export interfaces, a synchronized desktop, mobile applications running on the device, or the intranet servers.

Push Attacks: The attacker use the mobile device to plant a malicious code and spread it to infect other elements of the network. Once the mobile device inside a secure network is compromised, it could be used for attacks against other devices in the network

Forced De-authentication. The attacker transmits packets intended to convince a mobile end-point to drop its network connection and reacquire a new signal, and then inserts a crook device between a mobile device and the genuine network.

Multi-protocol Communication. This security issue is the result of the ability of many mobile devices to operate using multiple protocols, e.g. one of the 802.11 family protocols, a cellular provider's network protocol, and other protocols which may have well-known security loop-holes. Although these types of protocols aren't in active usage, many mobile devices have these interfaces set "active" by default. Attackers can take advantage of this vulnerability and connect to the device, allowing them access to extract information from it or use its services.

Mobility and Roaming. The mobility of users and data that they carry introduces security issues related to the presence and location of a user, the secrecy and authenticity of the data exchanged, and the privacy of user profile. To allow roaming, certain parameters and user profiles should be replicated at different locations so that when a user roams across different zones, she or he should not experience any degradation in the access and latency times. However, by replicating sensitive data across several sites, the number of points of attack is increased and hence the security risks are also increased.

Disconnections. The frequent disconnections caused by hand-offs that occur when mobile devices cross different introduce new security and integrity issues. The transition from one level of disconnection to another may present an opportunity for an attacker to masquerade either the mobile unit or the mobile support station.

Delegation. The attacker can hijack mobile session during the delegation process. A delegation is a powerful mechanism to provide flexible and dynamic access control decisions. It is a temporary permit issued by the delegator and given to the delegate who becomes limited authorized to act on the delegator's behalf. Mobile devices have to switch connections between different types of networks as they move and some kind of delegation has to be issues to different network access points. Delegations may be issued and revoked frequently as mobile devices detach and reattach to different parts of the network system.

Mobile Security Requirements

The rise of mobile computing brings with it a rise in concerns about security issues in general and about data security in particular. In addition, the rise in the number of lost and stolen mobile computing devices raise the need to implement some protection for the data contained on the mobile devices. Organizations involved in mobile computing cannot rely on the traditional security controls of the mobile devices and network infrastructure, they must ensure that these devices, networks, and communication systems have sufficient integral security controls to protect exchanged and stored data. This is because the mobile devices, computers, and networks used for mobile computing may not be owned by these organizations and may be shared by anyone. Therefore, security controls implemented on the systems within the organizations are not enough and must be complemented by other security mechanisms on top of a mandatory good practice by their mobile users. Different security measures and requirements are implemented and suggested for both the mobile devices and the networks. Some of these measures include the following:

Encryptions: If critical information is held on a mobile device, data encryption should be done to protect the data and prevent access by unauthorized persons.

Compliance. Remote and wireless network access from mobile devices must be subject to the same organization's internal network security policies compliance and measures applied to inner users. Access and connection through public hotspots

Standards. Mobile users must ensure that the mobile devices they use and the information they contains are well protected at all times and adhere to a set of requirements such as strong password protection, full disk strong encryption, locking, regular backups, current antivirus software, firewalls with similar configuration to the organization network's configuration.

Routing anonymity. To prevent communication endpoints from being linked, anonymous routing may be used at the network layer. It is extremely useful as a building block for higher level applications as a security echanism for general networked systems.

VPN and Wireless Encryption Protocol. A strong wireless encryption protocol should be used whenever possible, and all external connections to the internal organizational network must be over an encrypted virtual private network (VPN).

Network Access Control (NAC). Network Access Control system should be in place to check and analyze mobile devices trying to connect to the organization network. This will protect the internal network from any system compromises or malicious code or infections the mobile device may have picked up while it was away. It could also ensure that the mobile device is patched, has the appropriate security software installed, running and up to date, and that it otherwise meets the organization’s security policy requirements before allowing it to connect to internal network resources. Most NAC solutions offer an option between simply rejecting connections from noncompliant clients, or redirecting them to a site or server with information and resources to enable the device to become compliant.

Wireless Zero Configurations (WZC). WZC should be used so that mobile devices and network configuration setting will be done automatically without any intervention from the user. WZC, also know as WLAN AutoConfig, is a wireless connection management utility included with Microsoft Windows XP and later operating systems as a service that dynamically selects a wireless network to connect to based on a user's preferences and various default settings.

Use Mobile IPV6 (MIPv6). Mobile IPv6 is a protocol developed as a subset of Internet Protocol version 6 (IPv6) to support mobile connections. Using MIPv6, the quality of services and the management of mobility issues in mobile computing environment will be taken care of in a very efficient and standard way that will aid in securing the data transmission.

Integration of IPSec/AAA and Hierarchical Mobile IPV6. Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session, and the Authentication Authorization Accounting (AAA) protocol helps in managing and controlling network accesses. This requirement can be considered as a fully integrated solution for securing data transmission and network access, and it could encompasses several previous mentioned security requirements.

Threats to Mobile Computing

Mobile computing brings with it threats to the user and to the corporate environment. From personal information to corporate data, mobile devices are used for a wide variety of tasks by individuals and companies. Mobile devices have added a new threat to the corporate landscape as they have introduced the concept of bring your own device . While this is not necessarily an entirely new concept, the wide acceptance of bring your own device with mobile devices has created a paradigm shift, where the security and safety of the device is not necessarily to protect the corporate data, but to keep the personal data out of the hands of corporate management.

Data Loss from lost, stolen, or decommissioned devices: By their nature, mobile devices are with us everywhere we go. The information accessed through the device means that theft or loss of a mobile device has immediate consequences. Additionally, weak password access, no passwords, and little or no encryption can lead to data leakage on the devices. Users may also sell or discard devices without understanding the risk to their data. The threat level from data loss is high, as it occurs frequently and is a top concern across executives and IT admins.

Information stealing mobile malware: Android devices, in particular, offer many options for application downloads and installations. Unlike iOS devices, which need to be jailbroken, Android users can easily opt to download and install apps from third-party marketplaces other than Google’s official Play Store marketplace. To date, the majority of malicious code distributed for Android has been disseminated through third-party app stores. Most of the malware distributed through third-party stores has been designed to steal data from the host device. This threat level is high, as Android malware in particular is becoming a more popular attack surface for criminals who traditionally have used PCs as their platforms.

Data Loss and data leakage through poorly written third-party applications: Applications for smartphones and tablets have grown exponentially on iOS and Android. Although the main marketplaces have security checks, certain data collection processes are of questionable necessity; all too often, applications either ask for too much access to data or simply gather more data than they need or otherwise advertise. This is a mid-level threat. Although data loss and leaking through poorly written applications happens across mobile operating systems.

Vulnerabilities within devices, OS, design, and third-party applications: Mobile hardware, OS, applications and third-party apps contain defects (vulnerabilities) and are susceptible to exfiltration and/or injection of data and/or malicious code (exploits). The unique ecosystem inherent in mobile devices provides a specialized array of security concerns to hardware, OS, and application developers, as mobile devices increasingly contain all of the functionalities attributed to desktop computing, with the addition of cellular communication abilities. This is a mid-level threat; although the possibility is high, the number of exploits is not.

Unsecured WiFi, network access, and rogue access points: This has increased the attack surface for users who connect to these networks. In the last year, there has been a proliferation of attacks on hotel networks, a skyrocketing number of open rogue access points installed, and the reporting of eavesdropping cases. This threat level is high. Increased access to public WiFi, along with increased use of mobile devices, creates a heightened opportunity for abuse of this connection.

Unsecured or rogue marketplaces: Android users can easily opt to download and install apps from third-party marketplaces other than Google's official Play Store marketplace. To date, the majority of malicious code distributed for Android has been distributed through third-party app stores. This threat level is high: Android malware in particular is being distributed through these marketplaces more and more frequently.

Insufficient management tools, capabilities, and access to APIs (includes personas): Granting users and developers access to a device's low-level functions is a double-edged sword, as attackers, in theory, could also gain access to those functions. However, a lack of access to system-level functions to trusted developers could lead to insufficient security. Additionally, with most smartphone and tablet operating systems today, there is little, if any, guest access or user status. Thus, all usage is in the context of the admin, thereby providing excessive access in many instances. This is a mid-level threat.

NFC and proximity-based hacking: Near-field communication (NFC) allows mobile devices to communicate with other devices through short-range wireless technology. NFC technology has been used in payment transactions, social media, coupon delivery, and contact information sharing.

Due to the information value being transmitted, this is likely to be a target of attackers in the future. The threat level is low, as the threat is still in the proof-of-concept phase.