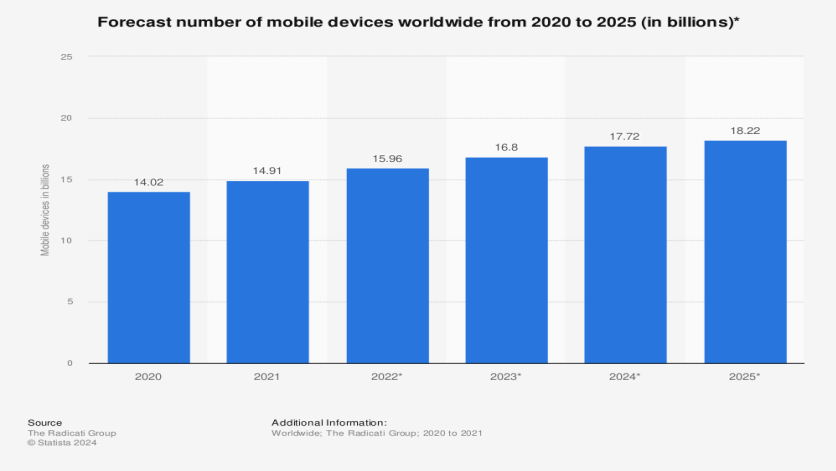
Lecture Delivery Plan

UNIT 2: CYBER CRIME

Lecture -9

2.9.1 Mobile and Wireless Devices

An Introduction:
In this modern era, the rising importance of electronic gadgets (i.e., mobile hand-held devices) – 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 cybercrime. In the recent years, the use of laptops, personal digital assistants (PDAs) and mobile phones has grown from limited user communities to widespread desktop replacement and broad deployment.



In 2021, the number of mobile devices operating worldwide stood at almost 15 billion, up from just over 14 billion in the previous year. The number of mobile devices is expected to reach 18.22 billion by 2025, an increase of 4.2 billion devices compared to 2020 levels.

The complexity of managing these devices outside the walls of the office is something that the information technology (IT) departments in the organizations need to address. Remote connection has extended from fixed location dial-in to wireless-on-the-move, and smart handheld devices such as PDAs have become networked, converging with mobile phones. Furthermore, the maturation of the PDA and advancements in cellular phone technology have converged into a new category of mobile phone device: the Smartphone. Smart phones combine the best aspects of mobile and wireless technologies and blend them into a useful business tool. Although IT departments of organizations as yet are not swapping employees' company-provided PDAs (as the case may be) for the Smart phones, many users may bring these devices from home and use them in the office. Thus, the larger and more diverse community of mobile users and their devices increase the demands on the IT function to secure the device, data and connection to the network, keeping control of the corporate assets, while at the same time supporting mobile 2 user productivity. Clearly, these technological developments present a new set of security challenges to the global organizations.

2.9.2 Proliferation of Mobile and Wireless Devices:

Today, incredible advances are being made for mobile devices. The trend is for smaller devices and more processing power. A few years ago, the choice was between a wireless phone and a simple PDA. Now the buyers have a choice between high-end PDAs with integrated wireless modems and small phones with wireless Web-browsing capabilities.

A simple hand-held mobile device provides enough computing power to run small applications, play games and music, and make voice calls. As the term "mobile device" includes many products. We first provide a clear distinction among the key terms: mobile computing, wireless computing and hand-held devices. Below figure helps to understand how these terms are related.

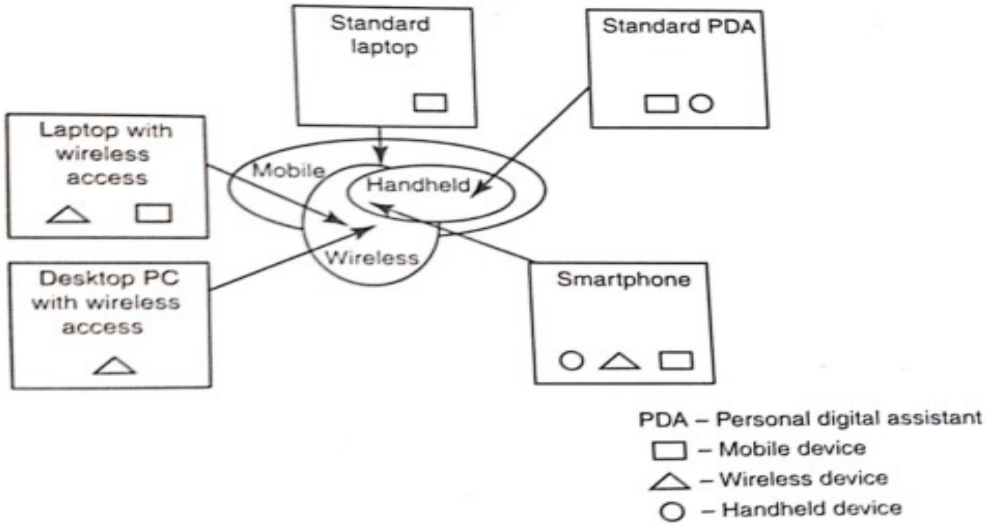


Figure: Mobile, Wireless & Hand-held devices

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

1. Portable Computer: It is a general-purpose computer that can be easily moved from one place to another, but cannot be used while in transit, usually because it requires some "setting-up" and an AC power source.
2. Tablet PC: It lacks a keyboard, is shaped like a slate or a paper notebook and has features of a touch screen with a stylus and handwriting recognition software. Tablets may not be best suited for 3 applications requiring a physical keyboard for typing, but are otherwise capable of carrying out most tasks that an ordinary laptop would be able to perform.
3. Internet Tablet: It is the Internet appliance in tablet form. Unlike a Tablet PC, the Internet tablet does not have much computing power and its applications suite is limited. Also it cannot replace a general purpose computer. The Internet tablets typically feature an MP3 and video player, a Web browser, a chat application and a picture viewer.
4. Personal Digital Assistant (PDA): It is a small, usually pocket-sized, computer with limited functionality. It is intended to supplement and synchronize with a desktop computer, giving access to contacts, address book, notes, E-Mail and other features.
5. Ultramobile PC: It is a full-featured, PDA-sized computer running a general-purpose operating system (OS).
6. Smartphone: It is a PDA with integrated cell phone functionality. Current Smartphones have a wide range of features and installable applications.

7. Carputer: It is a computing device installed in an automobile. It operates as a wireless computer, sound system, global positioning system (GPS) and DVD player. It also contains word processing software and is Bluetooth compatible.
8. Fly Fusion Pentop Computer: It is a computing device with the size and shape of a pen. It functions as a writing utensil, MP3 player, language translator, digital storage device and calculator.

Wireless refers to the method of transferring information between a computing device (such as a PDA) and a data source (such as an agency database server) without a physical connection. Not all wireless communication technologies are mobile. For example, lasers are used in wireless data transfer between buildings, but cannot be used in mobile communications at this time. Mobile simply describes a computing device that is not restricted to a desktop that is not tethered. As more personal devices find their way into the enterprise, corporations are realizing cyber security threats that come along with the benefits achieved with mobile solutions.

Mobile computing does not necessarily require wireless communication. In fact, it may not require communication among devices at all. Thus, while "wireless" is a subset of "mobile," in most cases, an application can be mobile without being wireless. Smart hand-helds are defined as hand-held or pocket-sized devices that connect to a wireless or cellular network, and can have software installed on them; this includes networked PDAs and Smart phones.

Lecture -10

2.10.1 Trends in Mobility:

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

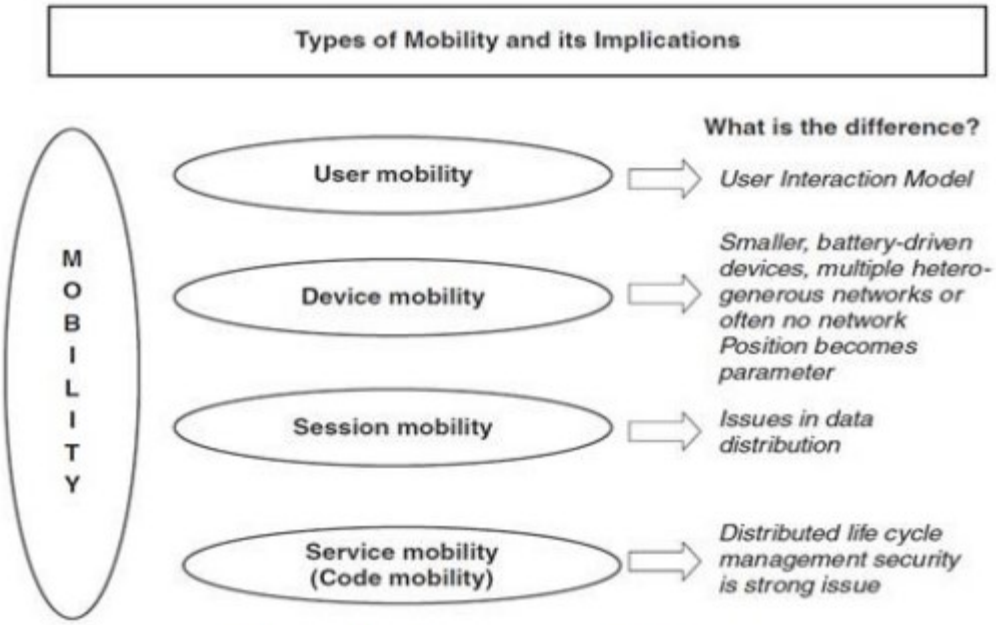


Figure: Mobility types & implications

Popular types of attacks against 3G mobile networks are as follows:

1. Malwares, Viruses and Worms: Although many users are still in the transient process of switching from 2G, 2.5G to 3G, it is a growing need to educate the community people and provide awareness of such threats that exist while using mobile devices. Here are few examples of malware(s) specific to mobile devices:

a. Skull Trojan: It targets Series 60 phones equipped with the Symbian mobile OS.

b. Cabir Worm: It is the first dedicated mobile-phone worm; infects phones running on Symbian OS and scans other mobile devices to send a copy of itself to the first vulnerable phone it finds through Bluetooth Wireless technology. The worst thing about this worm is that the source code for the Cabir-H and Cabir-I viruses is available online.

c. Mosquito Trojan: It affects the Series 60 Smart phones and is a cracked version of "Mosquitos" mobile phone game. 5

d. Brador Trojan: It affects the Windows CE OS by creating a svchost.exe file in the Windows start-up folder which allows full control of the device. This executable file is conductive to traditional worm propagation vector such as E-Mail file attachments (refer to Appendix C).

e. Lasco Worm: It was released first in 2005 to target PDAs and mobile phones running the Symbian

OS. Lasco is based on Cabir's source code and replicates over Bluetooth connection.

2. Denial-of-Service (DoS): The main objective behind this attack is to make the system unavailable to the intended users. Virus attacks can be used to damage the system to make the system unavailable.

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

4. Spoofed Policy Development Process (PDP): These types of attacks exploit the vulnerabilities in the GTP [General Packet Radio Service (GPRS) Tunneling Protocol].

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

2.10.2 Credit Card Frauds in Mobile and Wireless Computing Era:

These are new trends in cybercrime that are coming up with mobile computing – Mobile Commerce (M-Commerce) and mobile banking (M-Banking). Credit card frauds are now becoming commonplace given the ever- increasing power and the ever-reducing prices of the mobile hand-held devices, factors that result in easy availability of these gadgets to almost anyone. Mobile credit card transactions are now very common; new technologies combine low-cost mobile phone technologies with the capabilities of a point-of-sale (POS) terminal. Today belongs to "mobile computing," that is, anywhere anytime computing.

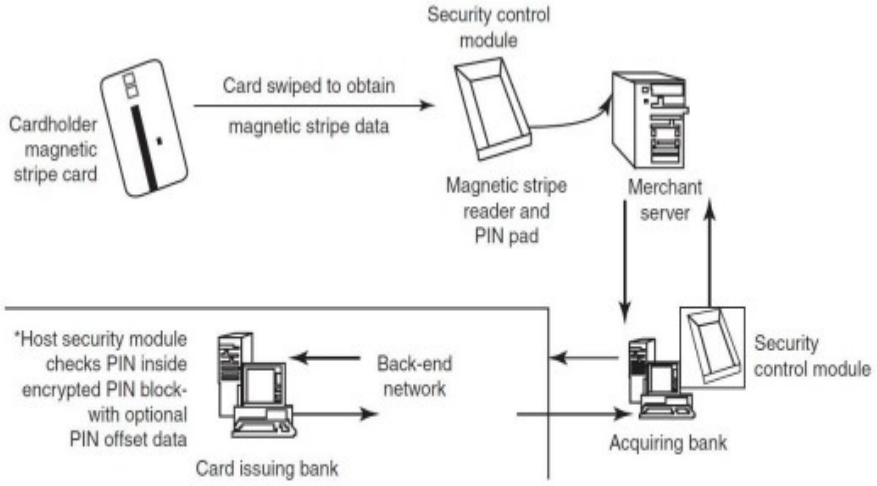


Figure: Online Environment for Credit Card Transactions

Credit card companies, normally, do a good job of helping consumers resolve identity (ID) theft problems once they occur. But they could reduce ID fraud even more if they give consumers better tools to monitor their accounts and limit high-risk transactions.

Tips to Prevent Credit Card Frauds:

Do's:

1. Put your signature on the card immediately upon its receipt.
2. Make the photocopy of both the sides of your card and preserve it at a safe place to remember the card number, expiration date in case of loss of card.

3. Change the default Personal Identification Number (PIN) received from the bank before doing any transaction.
4. Always carry the details about contact numbers of your bank in case of loss of your card.
5. Carry your cards in a separate pouch/card holder than your wallet.
6. Keep an eye on your card during the transaction, and ensure to get it back immediately.
7. Preserve all the receipts to compare with credit card invoice.
8. Reconcile your monthly invoice/statement with your receipts.
9. Report immediately any discrepancy observed in the monthly invoice/statement.
10. Destroy all the receipts after reconciling it with the monthly invoice/statement.
11. Inform your bank in advance, about any change in your contact details such as home address, cell phone number and E-Mail address.
12. Ensure the legitimacy of the website before providing any of your card details.
13. Report the loss of the card immediately in your bank and at the police station, if necessary.

Don'ts:

1. Store your card number and PINs in your cell.
2. Lend your cards to anyone.
3. Leave cards or transaction receipts lying around.
4. Sign a blank receipt (if the transaction details are not legible, ask for another receipt to ensure the amount instead of trusting the seller).
5. Write your card number/PIN on a postcard or the outside of an envelope.
6. Give out immediately your account number over the phone (unless you are calling to a company/ to your bank).
7. Destroy credit card receipts by simply dropping into garbage box/dustbin.
7 There is a system available from an Australian company "Alacrity" called Closed-Loop Environment for Wireless (CLEW). Below figure shows the flow of events

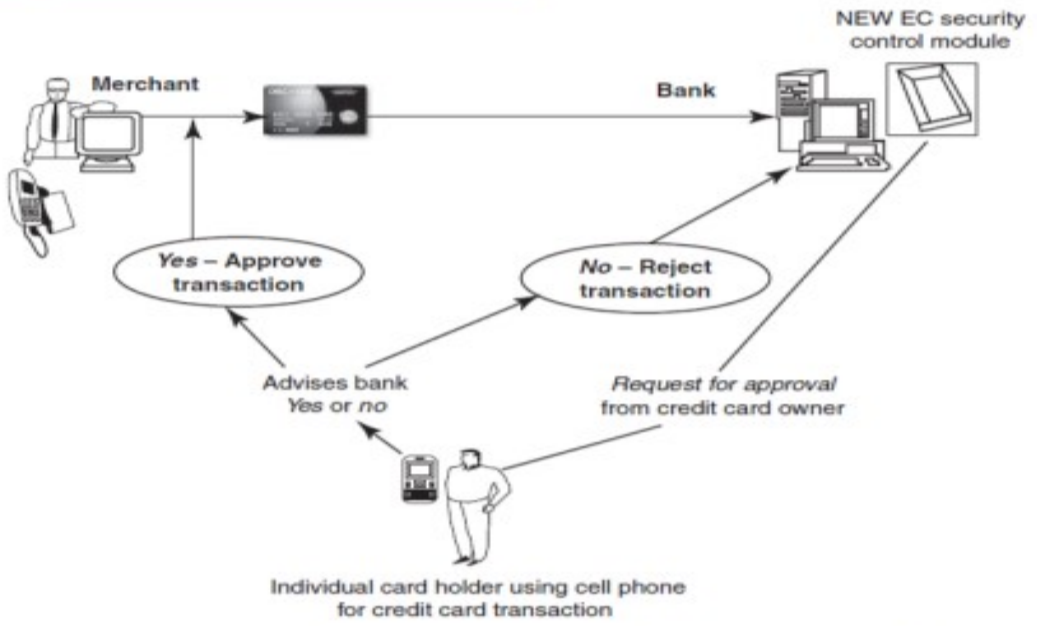


Figure: Closed-Loop Environment for Wireless (CLEW)

1. Merchant sends a transaction to bank;
2. The bank transmits the request to the authorized cardholder [not short message service (SMS)];
3. The cardholder approves or rejects (password protected);
4. The bank/merchant is notified;

5. The credit card transaction is completed.

Types and Techniques of Credit Card Frauds:

1. Traditional Techniques

a. ID theft: Where an individual pretends to be someone else

b. Financial fraud: Where an individual gives false information about his or her financial status to acquire credit.

2. Modern Techniques

a. Triangulation:

• The criminal offers the goods with heavy discounted rates through a website designed and hosted by him, which appears to be legitimate merchandise website.

• The goods are shipped to the customer and the transaction gets completed.

• The criminal keeps on purchasing other goods using fraudulent credit card details of different

b. Credit card generators: It is another modern technique – computer emulation software – that creates valid credit card numbers and expiry dates. The criminals highly rely on these generators to create valid credit cards. These are available for free download on the Internet.

Lecture -11

2.11.1 Security Challenges Posed By Mobile Devices

Mobility brings two main challenges to cyber security:
1. On the hand-held devices, information is being taken outside the physically controlled environment and
2. Remote access back to the protected environment is being granted Perceptions of the organizations to these cyber security challenges are important in devising appropriate security operating procedure.

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

Some well-known technical challenges in mobile security are:

- Managing the registry settings and configurations, authentication service security
- Cryptography security
- Lightweight Directory Access Protocol (LDAP) security
- Remote Access Server (RAS) security
- Media player control security
- Networking application program interface (API) security, etc.

2.11.2 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 mutual 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 (imitate) 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.

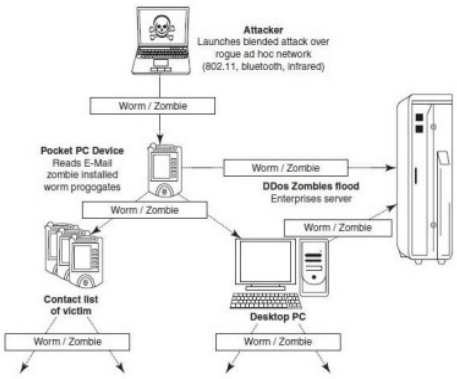


Figure: Push attack on mobile devices. DDoS implies distributed denial-of-service attack

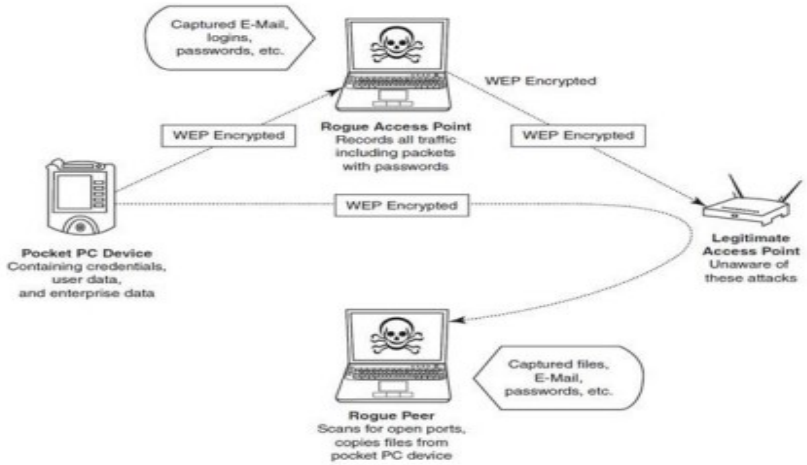


Figure: Pull attack on mobile devices

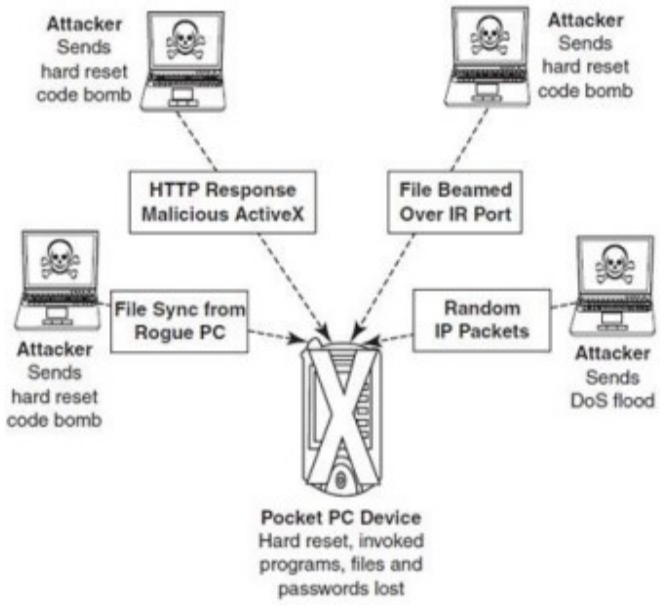


Figure: Crash attack on mobile devices. DoS- Denial-of-service attack

Lecture -12

Authentication Services Security:

2.12.1 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.

1. Cryptographic Security for Mobile Devices:

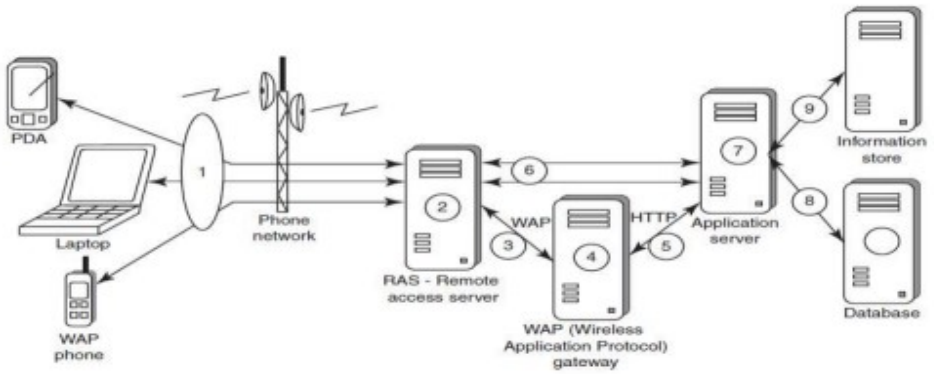
1. Cryptographic Security for Mobile Devices:
• Cryptographically Generated Addresses (CGA) is Internet Protocol version 6 (IPv6) that addresses up to 64 address bits that are generated by hashing owner's public-key address.
• The address the owner uses is the corresponding private key to assert address ownership and to sign messages sent from the address without a public-key infrastructure (PKI) or other security infrastructure.
• Deployment of PKI provides many benefits for users to secure their financial transactions initiated from mobile devices.
• CGA-based authentication can be used to protect IP-layer signaling protocols including neighbor discovery (as in context-aware mobile computing applications) and mobility protocols.
• It can also be used for key exchange in opportunistic Internet Protocol Security (IPSec). Palms (devices that can be held in one's palm) are one of the most common hand-held devices used in mobile computing.
• Cryptographic security controls are deployed on these devices.
• For example, the Cryptographic Provider Manager (CPM) in Palm OS5 is a system-wide suite of cryptographic services for securing data and resources on a palm-powered device.
• The CPM extends encryption services to any application written to take advantage of these capabilities, allowing the encryption of only selected data or of all data and resources on the device.

2.12.2. LDAP Security for Hand-held Mobile Computing Devices:

• LDAP is a software protocol for enabling anyone to locate individuals, organizations and other resources such as files and devices on the network (i.e., on the public Internet or on the organizations's Intranet).
• In a network, a directory tells you where an entity is located in the network.
• LDAP is a light weight (smaller Attacker Launches blended attack over rogue ad hoc network (802.11, bluetooth, infrared) amount of code) version of Directory Access Protocol (DAP) because it does not include security features in its initial version.

2.12.3. RAS Security for Mobile Devices:

RAS (Remote Access Server) is an important consideration for protecting the business-sensitive data that may reside on the employees' mobile devices. In terms of cybersecurity, mobile devices are sensitive. Below Figure: organization's sensitive data can happen through mobile hand-held devices carried by employees. In addition to being vulnerable to unauthorized access on their own, mobile devices also provide a route into the systems with which they connect. By using a mobile device to appear as a registered user (impersonating or masquerading) to these systems, a would-be cracker is then able to steal data or compromise corporate systems in other ways.



2.12.4 Another threat comes from the practice of port scanning:

• First, attackers use a domain name system (DNS) server to locate the IP address of a connected computer. A domain is a collection of sites that are related in some sense.
• Second, they scan the ports on this known IP address, working their way through its Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) stack to see what communication ports are unprotected by firewalls.
• For instance, File Transfer Protocol (FTP) transmissions are typically assigned to port 21. If this port is left unprotected, it can be misused by the attackers.
• Protecting against port scanning requires software that can trap unauthorized incoming data packets and prevent a mobile device from revealing its existence and ID.
• A personal firewall on a pocket PC or Smartphone device can be an effective protective screen against this form of attack for the users connecting through a direct Internet or RAS connection.

2.12. 5 Media Player Control Security:

Various leading software development organizations have been warning the users about the potential security attacks on their mobile devices through the "music gateways." There are many examples to show how a media player can turn out to be a source of threat to information held on mobile devices. For example, in the year 2002, Microsoft Corporation warned about this.
• According to this news item, Microsoft had warned people that a series of flaws in its Windows Media Player could allow a malicious hacker to hijack people's computer systems and perform a variety of actions.
• According to this warning from Microsoft, in the most severe exploit of a flaw, a hacker could take over a computer system and perform any task the computer's owner is allowed to do, such as opening files or accessing certain parts of a network.

2.12.6 . Networking API Security for Mobile Computing Applications:

• With the advent of electronic commerce (E-Commerce) and its further off -shoot into M-Commerce, online payments are becoming a common phenomenon with the payment gateways accessed remotely and possibly wirelessly.
• Furthermore, with the advent of Web services and their use in mobile computing applications, the API becomes an important consideration.
• Already, there are organizations announcing the development of various APIs to enable software and hardware developers to write single applications

• Most of these developments are targeted specifically at securing a range of embedded and consumer products, including those running OSs such as Linux, Symbian, Microsoft Windows CE and Microsoft Windows Mobile (the last three are the most commonly used OSs for mobile devices).
• Technological developments such as these provide the ability to significantly improve cyber security of a wide range of consumer as well as mobile devices. Providing a common software framework, APIs will become an important enabler of new and higher value services.

Lecture -13

2.13.1 Attacks On Mobile/Cell Phones:

1. Mobile Phone Theft:

Mobile phones have become an integral part of everybody's life and the mobile phone has transformed from being a luxury to a bare necessity. Theft of mobile phones has risen dramatically over the past few years. Since huge section of working population in India use public transport, major locations where theft occurs are bus stops, railway stations and traffic signals. Many Insurance Companies have stopped offering Mobile Theft Insurance due to a large number of false claims. When anyone looses his/her mobile phone, more than anything "Contact List" and "Personally Identifiable Information (PII)", that really matter, are lost. One might have just thought that his/her cell phone is much safer than a PC that is very often attacked by viruses; however, criminals made this thought as false statement. After PC, the criminals' (i.e., attackers') new playground has been cell phones, reason being the increasing usage of cell phones and availability of Internet using cell phones. Another reason is increasing demand for Wi-Fi zones in the metropolitans and extensive usage of cell phones in the youths with lack of awareness/knowledge about the vulnerabilities of the technology.

The following factors contribute for outbreaks on mobile devices:

1. Enough target terminals: The first Palm OD virus was seen after the number of Palm OS devices reached 15million. The 1st instance of a mobile virus was observed during June 2004 when it was discovered that an organization "Ojam" had engineered an antipiracy Trojan virus in older versions of their mobile phone game known as Mosquito. This virus sent SMS text messages to the organization without the user's knowledge.

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

3. Enough connectivity: Smartphones offer multiple communication options, such as SMS, MMS, synchronization, Bluetooth, infrared (IR) and WLAN connections.

2.13.2. Mobile Viruses:

• A mobile virus is similar to a computer virus that targets mobile phone data or applications/software installed in it.
• Virus attacks on mobile devices are no longer an exception or proof-of-concept nowadays.
• In total, 40 mobile virus families and more than 300(+) mobile viruses have been identified.
• First mobile virus was identified in 2004 and it was the beginning to understand that mobile devices can act as vectors to enter the computer network.
• Mobile viruses get spread through two dominant communication protocols – Bluetooth and MMS.
• Bluetooth virus can easily spread within a distance of 10–30 m, through Bluetooth-activated phones
• MMS virus can send a copy of itself to all mobile users whose numbers are available in the infected mobile phone's address book.

Following are some tips to protect mobile from mobile malware attacks: 1. Download or accept programs and content (including ring tones, games, video clips and photos) only from a trusted source.
2. If a mobile is equipped with Bluetooth, turn it OFF or set it to non-discoverable mode when it is not in use and/or not required to use.
3. If a mobile is equipped with beam (i.e., IR), allow it to receive incoming beams, only from the trusted source.
4. Download and install antivirus software for mobile devices.

2.13.3. Mishing:

Mishing is a combination of mobile and Phishing. Mishing attacks are attempted using mobile phone technology.

• M-Commerce is fast becoming a part of everyday life. If you use your mobile phone for purchasing goods/services and for banking, you could be more vulnerable to a Mishing scam.

• A typical Mishing attacker uses call termed as Vishing or message (SMS) known as Smishing.

• Attacker will pretend to be an employee from your bank or another organization and will claim a need for your personal details.

• Attackers are very creative and they would try to convince you with different reasons why they need this information from you.

2.13.4. Vishing:

Vishing is the criminal practice of using social engineering over the telephone system, most often using features facilitated by VoIP, to gain access to personal and financial information from the public for the purpose of financial reward. The term is a combination of V – Voice and Phishing. Vishing is usually used to steal credit card numbers or other related data used in ID theft schemes from individuals.

The most profitable uses of the information gained through a Vishing attack include:

• ID theft

• Purchasing luxury goods and services

• Transferring money/funds

• Monitoring the victims' bank accounts

• Making applications for loans and credit cards

How Vishing Works:

The criminal can initiate a Vishing attack using a variety of methods, each of which depends upon information gathered by a criminal and criminal's will to reach a particular audience.

1. Internet E-Mail: It is also called Phishing mail.

2. Mobile Text Messaging: Text is being messaged in Mobile.

3. Voicemail: Here, Victim is forced to call on the provided phone number, once he/she listens to voice mail.

4. Direct phone Call: Following are the steps detailing on how direct phone call works.

How to Protect from Vishing Attacks:

1. Be suspicious about all unknown callers.

2. Do not trust caller ID. It does not guarantee whether the call is really coming from that number, that is, from the individual and/or company – caller ID Spoofing is easy.

3. Be aware and ask questions, in case someone is asking for your personal or financial information.

4. Call them back. If someone is asking you for your personal or financial information, tell them that you will call them back immediately to verify if the company is legitimate or not. In case someone is calling from a bank and/or credit card company, call them back using a number displayed on invoice and/or displayed on website.

5. Report incidents: Report Vishing calls to the nearest cyber police cell with the number and name that appeared on the caller ID as well as the time of day and the information talked about or heard in a recorded message.

Lecture -14

2.14.1. Smishing:

Smishing is a criminal offense conducted by using social engineering techniques similar to Phishing. The name is derived from "SMs phISHING". SMS – Short Message Service – is the text messages communication component dominantly used into mobile phones. SMS can be abused by using different methods and techniques other than information gathering under cybercrime.

Smishing uses cell phone text messages to deliver a lure message to get the victim to reveal his/her PI. The popular technique to "hook" the victim is either provide a phone number to force the victim to call or provide a website URL to force the victim to access the URL, wherein, the victim gets connected with bogus website (i.e., duplicate but fake site created by the criminal) and submits his/her PI. Smishing works in the similar pattern as Vishing.

How to Protect from Smishing Attacks:

1. Do not answer a text message that you have received asking for your PI. Even if the message seems to be received from your best friend, do not respond, because he/she may not be the one who has actually sent it.
2. Avoid calling any phone numbers, as mentioned in the received message, to cancel a membership and/or confirming a transaction which you have not initiated but mentioned in the message. Always call on the numbers displayed on the invoice and/or appearing in the bank statements/passbook.
3. Never click on a hot link received through message on your Smartphone or PDA. Hot links are links that you can click, which will take you directly to the Internet sites. Smishing messages may have hot links, wherein you click on the link and download Spyware to your phone without knowing. Once this software has been downloaded, criminals can easily steal any information that is available on your cell phone and have access to everything that you do on your cell phone.

2.14.2. Hacking Bluetooth:

Bluetooth is an open wireless technology standard used for communication (i.e., exchanging data) over short distances (i.e., using short length radio waves) between fixed and/or mobile device. Bluetooth is a short-range wireless communication service/technology that uses the 2.4-GHz frequency range for its transmission/communication. The older standard – Bluetooth 1.0 has a maximum transfer speed of 1 Mbps (megabit per second) compared with 3 Mbps by Bluetooth 2.0. When Bluetooth is enabled on a device, it essentially broadcasts "I'm here, and I'm able to connect" to any other Bluetooth-based device within range.

This makes Bluetooth use simple and straightforward, and it also makes easier to identify the target for attackers. The attacker installs special software [Bluetooth hacking tools] on a laptop and then installs Bluetooth antenna. Whenever an attacker moves around public places, the software installed on laptop constantly scans the nearby surroundings of the hacker for active Bluetooth connections. Once the software tool used by the attacker finds and connects to a vulnerable Bluetooth-enabled cell phone, it can do things like download address book information, photos, calendars, SIM card details, make long-distance phone calls using the hacked device, bug phone calls and much more.

S.No	Name of the Tool	Description
1.	BlueScanner	This tool enables to search for Bluetooth enable device and will try to extract as much information as possible for each newly discovered device after connecting it with the target.
2.	BlueSniff	This is a GUI-based utility for finding discoverable and hidden Bluetooth enabled devices.
3.	BlueBugger	The buggers exploit the vulnerability of the device and access the images, phonebook, messages and other personal information
4.	Bluesnarfer	If a Bluetooth of a device is switched ON, then Bluesnarfing makes it possible to connect to the phone without alerting the owner and to gain access to restricted portions of the stored data.
5.	BlueDiving	Bluediving is testing Bluetooth penetration. It implements

2.14.3 Mobile Devices: Security Implications for Organizations

1. Managing Diversity and Proliferation of Hand-Held Devices:

Cybersecurity is always a primary concern to most organizations. Most organizations fail to see the long-term significance of keeping track of who owns what kind of mobile devices.

Mobile devices of employees should be registered in corporate asset register irrespective of whether or not the devices have been provided by the organization. In addition, close monitoring of these devices is required in terms of their usage. When an employee leaves, it is important to remove logical and physical access to organization networks. Thus, mobile devices that belong to the company should be returned to the IT department and, at the very least, should be deactivated and cleansed.

2. Unconventional/Stealth Storage Devices:

Compact disks (CDs) and Universal Serial Bus (USB) drives (also called zip drive, memory sticks) used by employees are the key factors for cyber attacks. As the technology is advancing, the devices continue to decrease in size and emerge in new shapes and sizes – storage devices available nowadays are difficult to detect and have become a prime challenge for organizational security. It is advisable to prohibit the employees in using these devices.

• Not only can viruses, worms and Trojans get into the organization network, but can also destroy valuable data in the organization network.

• Organization has to have a policy in place to block these ports while issuing the asset to the employee.

• Employees can connect a USB/small digital camera/MP3 player to the USB port of any unattended computer and will be able to download confidential data or upload harmful viruses.

• As the malicious attack is launched from within the organization, firewalls and antivirus software are not alerted.

• Using “Device Lock” software solution, one can have control over unauthorized access to plug and play devices. The features of the software allows system administrator to:

• Monitor which users or groups can access USB Ports, Wi-Fi and Bluetooth adapters, CD read-only memories (CD-ROMs) and other removable devices.

• Control the access to devices depending on the time of the day and day of the week.

• Create the white list of USB devices which allows you to authorize only specific devices that will not

be locked regardless of any other settings.
• Set devices in read-only mode.
• Protect disks from accidental or intentional formatting.

3. Threats through Lost & Stolen Devices:

This is a new emerging issue for cybersecurity. Often mobile hand-held devices are lost while people are on the move. Lost mobile devices are becoming even a larger security risk to corporations. The cybersecurity threat under this scenario is scary; owing to a general lack of security in mobile devices, it is often not the value of the hand-held device that is important but rather the content that, if lost or stolen, can put a company at a serious risk of sabotage, exploitation or damage to its professional integrity, as most of the times the mobile hand-held devices are provided by the organization. Most of these lost devices have wireless access to a corporate network and have potentially very little security, making them a weak link and a major headache for security administrators.

4. Protecting Data on Lost Devices:

At an individual level, employees need to worry about the importance of data protection especially when it resided on a mobile hand-held device. There are two reasons why cybersecurity needs to address this issue

• Data that is persistently stored on the device

• Always running applications For protecting data that are stored on the device, there are two precautions that individual can take to prevent disclosure of the data stored on a mobile device:

• Encrypting sensitive data

• Encrypting the entire file system A key point here is that the organizations should have a clear policy on how to respond to the loss or theft of a device, whether it is data storage, a PDA or a laptop. There should be a method for the device owner to quickly report the loss & device owners should be aware of this method.

5. Educating the Laptop Users:

Often it so happens that corporate laptop users could be putting their company's networks at risk by downloading non-work-related software capable of spreading viruses and spyware. This is because the software assets on laptops become more complex as more applications are used on an increasingly sophisticated OS with diverse connectivity options. The perception plays much role in terms of most people perceiving laptops as greater culprits compared with other innocuous-looking mobile hand-held devices.

Lecture -15

2.15.1 Organizational Measures For Handling Mobile Devices:

Encrypting Organizational Databases:

Critical and sensitive data reside on databases and with the advances in technology, access to these data is not impossible through hand-held devices. It is clear that to protect the organization's data loss, such databases need encryption.

Two Algorithms that are typically used to implement strong encryption of database files:

• Rijndael (pronounced Rain-dahl or Rhine-doll), a block encryption algorithm, chosen as the new Advanced Encryption Standard (AES) for block ciphers by the National Institute of Standards and Technology (NIST).

• The other algorithm used to implement strong encryption of database files is the Multi-Dimensional Space Rotation (MDSR) algorithm developed by Casio. Strong encryption means that it is much harder to break, but it also has a significant impact on performance. Database file encryption technology, using either the AES (or) MDSR algorithms, makes the database inoperable without the key (password). When using strong encryption, it is important not to store the key on the mobile devices, which is equivalent to leaving a key in a locked door. However if you lose the key, data is completely inaccessible. The key is case sensitive and must be entered correctly to access the database. For greater security there is an option available that instructs the database server to display a dialog box where the user can enter the encryption key. This option is necessary because the encryption key should not be entered on the machine in clear text. To protect the scenario of information attack/stealing through the mobile devices connecting to the corporate databases, additional security measures are possible through enforcing a self-destruct policy that is 23 controlled from the server. When a device that is identified or stolen connects to the organization server, IT department can have the server send a package to destroy privileged data on the device.

2.15.2 Including Mobile Devices in Security Strategy:

Organizational IT departments will have to take the accountability for cyber security threats that come through inappropriate access to organizational data from mobile-device–user employees. Encryption of corporate databases is not the end of everything. However, enterprises that do not want to include mobile devices in their environments often use security as an excuse, saying they fear the loss of sensitive data that could result from a PDA being stolen or an unsecured wireless connection being used. There are technologies available to properly secure mobile devices, which are enough for most organizations. Although mobile devices do pose unique challenges from a cybersecurity perceptive, there are some genera steps that the users can take to address them such as integrating security programs for mobile and wireless systems into the overall security blue print. A few things that organization can use are:

• Implement strong asset management, virus checking, loss prevention and other controls for mobile systems that will prohibit unauthorized access and the entry of corrupted data.

• Investigate alternatives that allow a secure access to the company information through a firewall, such as mobile VPNs.

• Develop a system of more frequent and thorough security audits for mobile devices.

• Incorporate security awareness into your mobile training and support programs so that everyone understands just how important an issue security is within a company's overall IT strategy.

• Notify the appropriate law-enforcement agency and change passwords. User accounts are closely monitored for any unusual activity for a period of time.

Lecture -16

2.16.1 Organizational Security Policies And Measures In Mobile Computing Era:

• Growth of mobile devices used makes the cyber security issue harder than what we would tend to think.
• People (especially, the youth) have grown so used to their mobiles that they are treating them like wallets!
• For example, people are storing more types of confidential information on mobile computing devices than their employers or they themselves know; they listen to music using their hand-held devices
• One should think about not to keep credit card and bank account numbers, passwords, confidential E-Mails and strategic information about organization & also other valuable information that could impact stock values in the mobile devices.
• Imagine the business impact if an employee's USB, pluggable drive or laptop was lost or stolen, revealing the sensitive customer data such as credit reports, Social Security Numbers (SSNs) & contact information.
• This not only the Public Relations (PR) disaster, but it could also violate laws & regulations.
• When controls cannot be implemented to protect data in the event they are stolen, the simplest solution is to prevent users from storing proprietary information on platforms deemed to be insufficiently secure.

Operating Guidelines for Implementing Mobile Device Security Policies:
• By using the following steps we can reduce the risk when mobile device lost or stolen
• Determine whether the employees in the organization need to use mobile computing devices or not.
• Implement additional security technologies like strong encryption, device passwords and physical locks.
• Standardize the mobile computing devices and the associated security tools being used with them.
• Develop a specific framework for using mobile computing devices.
• Maintain an inventory so that you know who is using what kinds of devices.
• Establish patching procedures for software on mobile devices.
• Label the devices and register them with a suitable service.
• Establish procedures to disable remote access for any mobile.
• Remove data from computing devices that are not in use • Provide education and awareness training to personnel using mobile devices. Organizational Policies for the Use of Mobile Hand-Held Devices: There are many ways to handle the matter of creating policy for mobile devices.
• One way is creating a distinct mobile computing policy.
• Another way is including such devices under existing policy. There are also approaches in between, where mobile devices fall under both existing general policies and a new one. There may not be a need for separate policies for wireless, LAN, WAN etc because a properly written network policy can cover all connections to the company data, including mobiles & wireless.

2.16.2 Laptops:

Laptops, like other mobile devices, enhance the business functions. Their mobile access to information anytime and anywhere, they also pose a large threat as they are portable. Wireless capability in these devices has also raised cyber security concerns owing to the information being transmitted over other, which makes it hard to detect. The thefts of laptops have always been a major issue, according to the cyber security industry and insurance company statistics. Cybercriminals are targeting laptops that are expensive, to enable them to fetch a quick profit in the black market. Most laptops contain personal and corporate information that could be sensitive. Such information can be misused if found by a malicious user. Physical Security Countermeasures:

1. Cables and hardwired locks: The most cost-efficient and ideal solution to safeguard any mobile device is securing with cables and locks, specially designed for laptops.
2. Laptop safes: Safes made of polycarbonate – the same material that is used in bulletproof windows, police riot shields and bank security screens – can be used to carry and safeguard the laptops
3. Motion sensors and alarms: Alarms and motion sensors are very efficient in securing laptops. Once these devices are activated, they can be used to track missing laptops in crowded places. Modern alarm systems for laptops are designed wherein the alarm device attached to the laptop transmits radio signals to a certain range around the laptop. The owner of the laptop has a key ring device that communicates with the laptop alarm device. The alarm is triggered when the distance between the laptop alarm device & the key ring device crosses the specified range.
4. Warning labels and stamps: Warning labels containing tracking information and identification details can be fixed onto the laptop to deter aspiring thieves. These labels cannot be removed easily and are a low-cost solution to a laptop theft. These labels have an identification number that is stored in universal database for verification, which in turn makes the resale of stolen laptops a difficult process.
5. Other measures for protecting laptops are as follows:
• Engraving the laptop with personal details
• Keeping the laptop close to oneself wherever possible
• Carrying the laptop in a different and unobvious bag
• Creating the awareness among the employees about the sensitive information contained in the laptop.
• Making a copy of the purchase receipt of laptop, serial number & description of laptop
• Installing encryption software to protect information stored on the laptop
• Using personal firewall software to block unwanted access and intrusion
• Updating the antivirus software regularly
• Tight office security using security guards and securing the laptop by locking it down in lockers when not in use • Never leaving the laptop unattended in public places
• Disabling IR ports and wireless cards when not in use
• Choosing a secure OS
• Registering the laptop with the laptop manufacturer to track down the laptop in case of theft
• Disabling unnecessary user accounts and renaming the administrator account
• Backing up data on a regular basis A few logical access controls are as follows:
• Protecting from malicious programs/attackers/social engineering
• Avoiding weak passwords/open access
• Monitoring application security and scanning for vulnerabilities
• Ensuring that unencrypted data/unprotected file systems do not pose threats
• Proper handling of removable drives/storage mediums/unnecessary ports
• Password protection through appropriate passwords rules and use of strong passwords
• Locking down unwanted ports/devices
• Regularly installing security patches and updates
• Installing antivirus software/firewalls/intrusion detection system (IDSs)
• Encrypting critical file systems

Other Counter measures:
▪ Choosing a secure OS that has been tested & has high security incorporated into it
▪ Registering the laptop with the laptop manufacturer to track down the laptop in case of theft
▪ Disabling unnecessary user accounts & renaming the administrator account
▪ Disabling display of the last logged in username in the login dialog box
▪ Backing up data on a regular basis