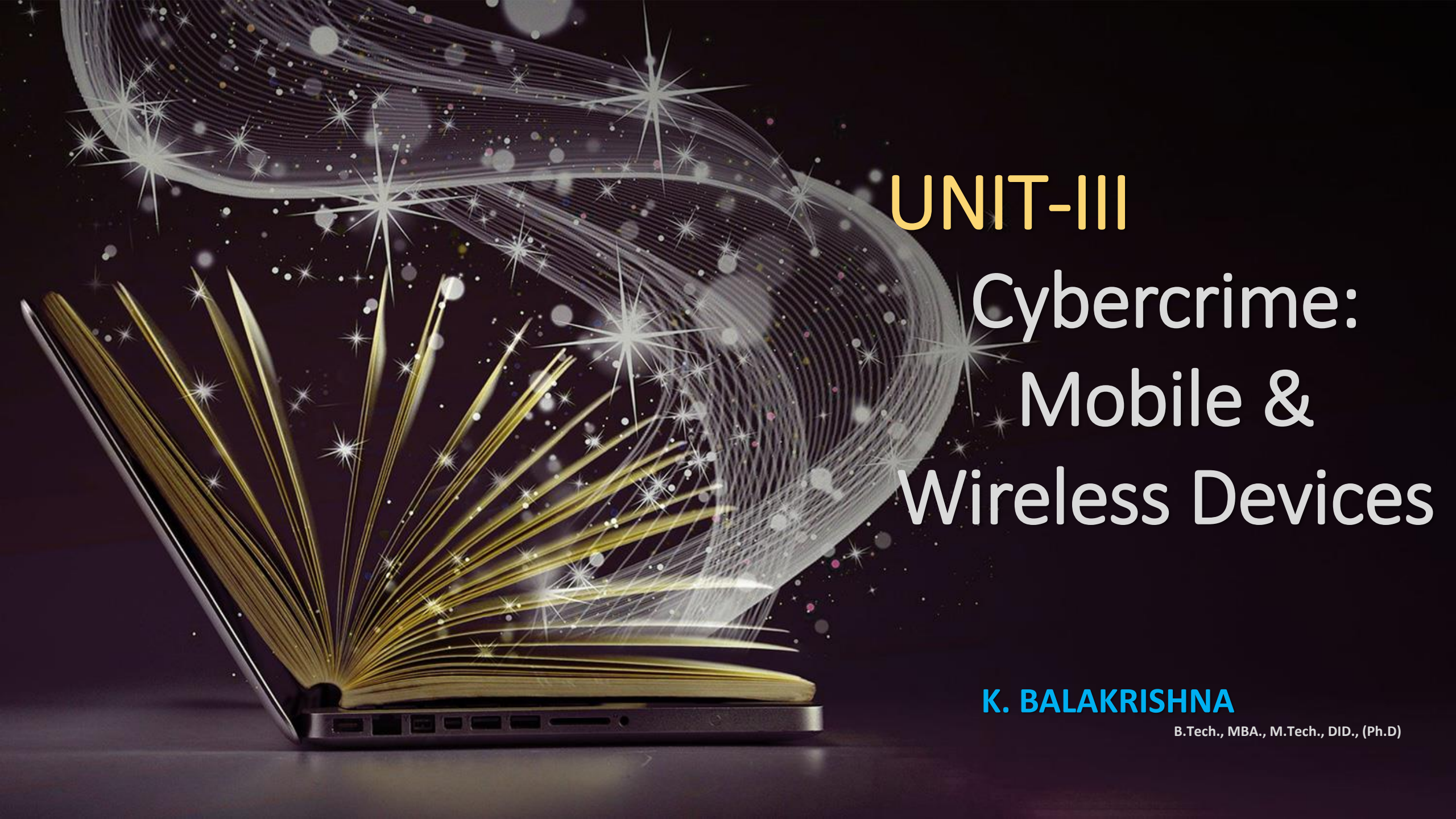

UNIT-III

Cybercrime: Mobile & Wireless Devices

K. BALAKRISHNA

B.Tech., MBA., M.Tech., DID., (Ph.D)

1. Introduction

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

A long list of options is available to the mobile users. A simple hand-held mobile device provides enough computing power to run small applications, play games and music, and make voice calls. A key driver for the growth of mobile technology is the rapid growth of business solutions into hand-held devices.

As the term "mobile device" includes many products. We first provide a clear distinction among the key terms: mobile computing, wireless computing and hand-held devices.

2. Proliferation of Mobile and Wireless Devices

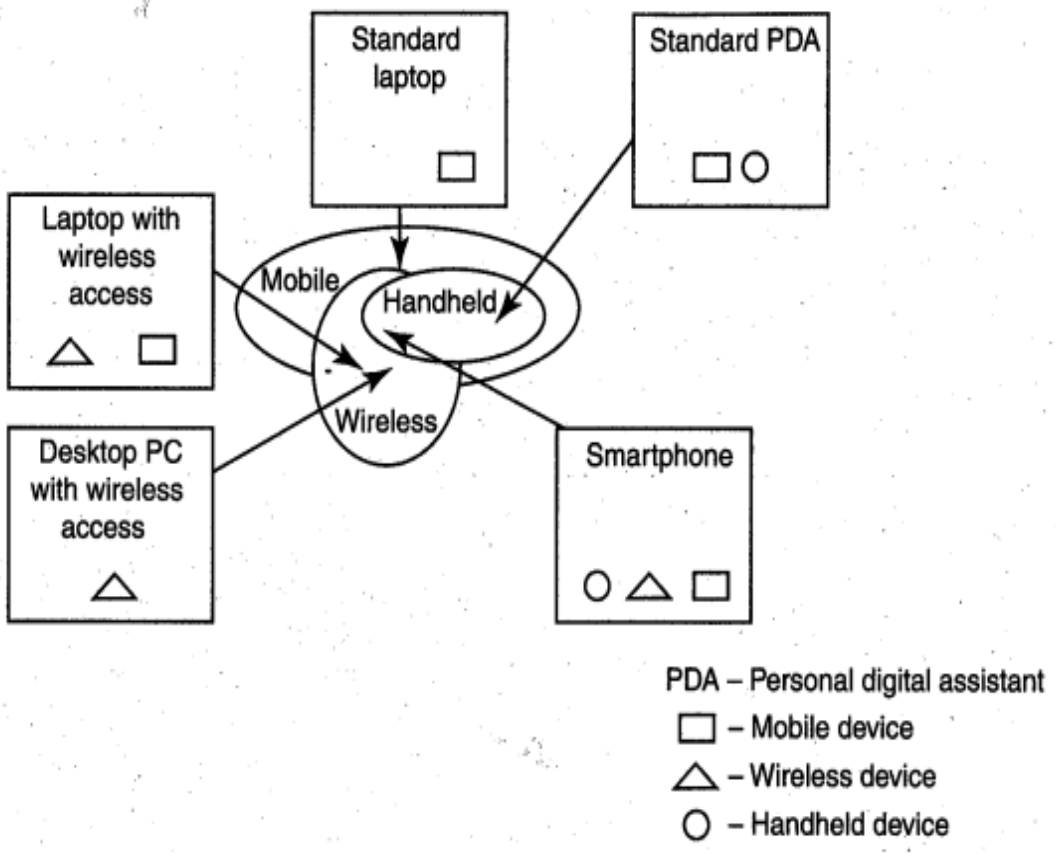

Figure : Mobile, Wireless and hand-held Devices

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

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

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

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

2. Proliferation of Mobile and Wireless Devices

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

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

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

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

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

3. Trends in Mobility

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

- It is worth noting the trends in mobile computing; this will help readers to readers to realize the seriousness of cybersecurity issues in the mobile computing domain.

- The new technology 3G networks are not entirely built with IP data security. Moreover, IP data world when compared to voice-centric security threats is new to mobile operators.

- There are numerous attacks that can be committed against mobile networks and they can originate from two primary vectors. **One** is from outside the mobile network - that is, public Internet, private networks and other operator's networks - and
  the other is within the mobile networks- that is, devices such as data-capable handsets and Smartphones, notebook computers or even desktop computers connected to the 3G network.

3. Trends in Mobility

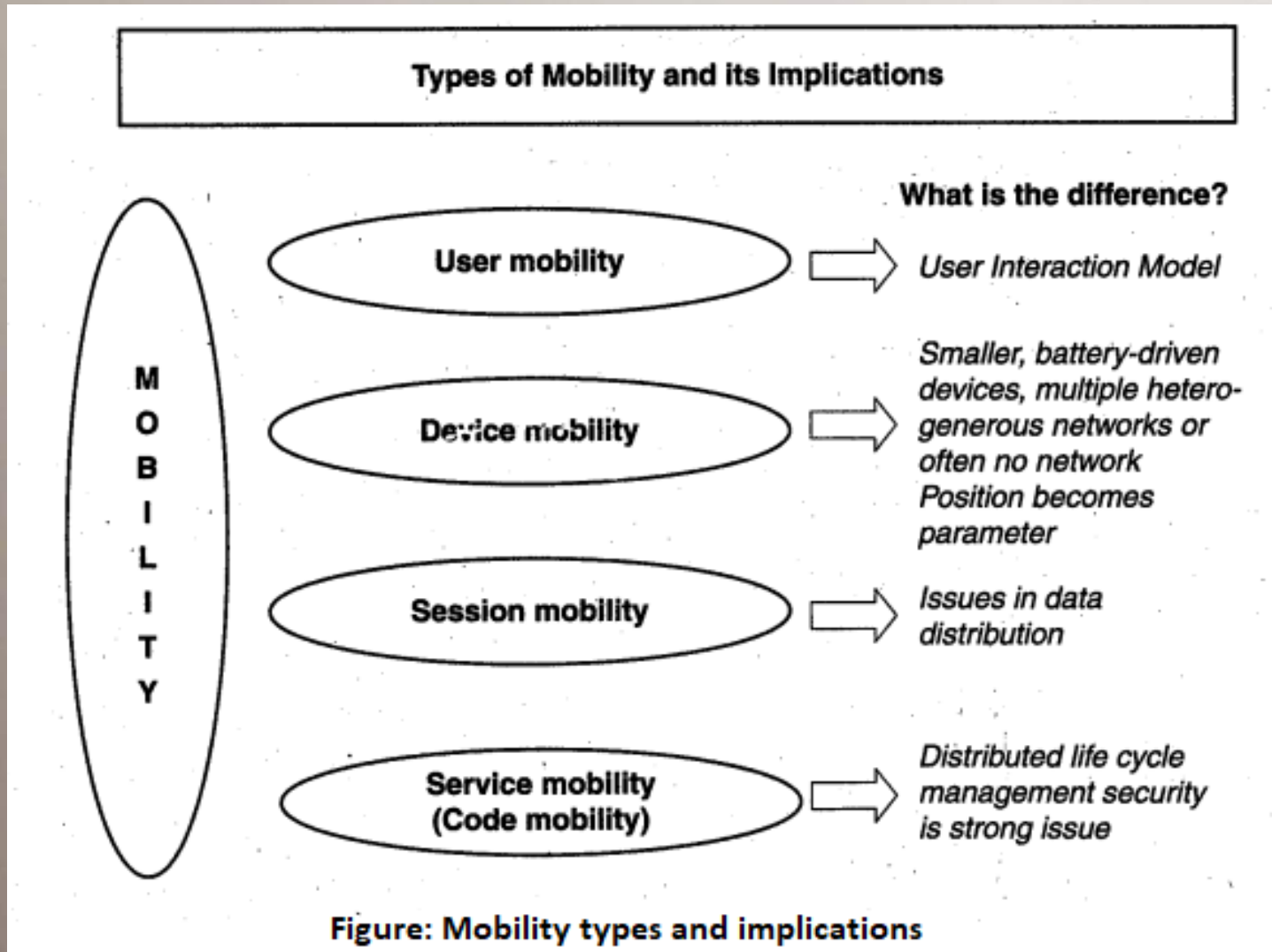

Figure: Mobility types and implications

3. Trends in Mobility

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:

- **Skull Trojan:** It targets Series 60 phones equipped with the Symbian mobile OS.
- **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.
- **Mosquito Trojan:** It affects the Series 60 Smartphones and is a cracked version of "Mosquitos" mobile phone game.
- **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.
- **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.

3. Trends in Mobility

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

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

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

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

4. Credit Card Frauds in Mobile and Wireless Computing Era

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

Wireless credit card processing is a very desirable system, because it allows businesses to process transactions from mobile locations quickly, efficiently and professionally. It is most often used by businesses that operate mainly in a mobile environment. These businesses include mobile utility repair service businesses, locksmiths, mobile windshield repair and others. Some upscale restaurants are using wireless processing equipment for the security of their credit card paying customers.

4. Credit Card Frauds in Mobile and Wireless Computing Era

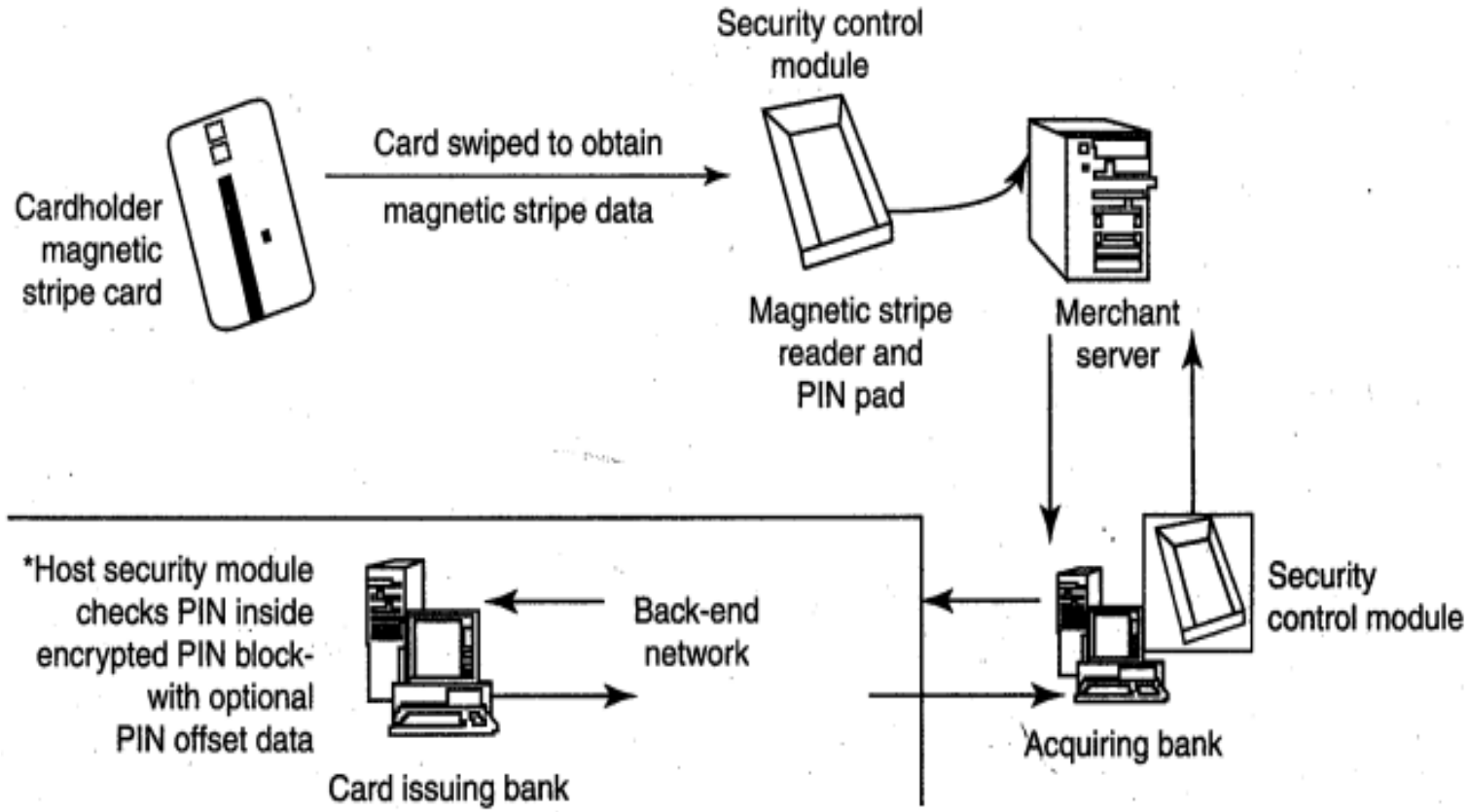

Figure : Online environment for credit card transactions

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

i. Merchant sends a transaction to bank
ii. The bank transmits the request to the authorized cardholder
iii. The cardholder approves or rejects (password protected)
iv. The bank/merchant is notified
v. The credit card transaction is completed.

4.1. Types and Techniques of Credit Card Frauds

a. Traditional Techniques:

The traditional and the first type of credit card fraud is paper-based-application fraud, wherein a criminal uses stolen or fake documents such as utility bills and bank statements that can build up useful personally Identifiable Information (PII) to open an account in someone else's name.

Application fraud can be divided into:

- **ID theft:** Where an individual pretends to be someone else.
- **Financial fraud:** Where an individual gives false information about his or her financial status to acquire credit. Illegal use of lost and stolen cards is another form of traditional technique. Stealing a credit card is either by pickpocket or from postal service before it reaches its final destination.

4.1. Types and Techniques of Credit Card Frauds

b. Modern Techniques:

1. Triangulation: It is another method of credit card fraud and works in the fashion as explained further.

- The criminal offers the goods with heavy discounted rates through a website designed and hosted
- The customer registers on this website with his/her name, address, shipping address and valid credit card details.
- The criminal orders the goods from a legitimate website with the help of stolen credit card details and supply shipping address that have been provided by the customer while registering on the criminal's 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 customers till the criminal closes existing website and starts a new one.

2. 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.

5. Security Challenges Posed by Mobile Devices

Mobility brings two main challenges to cybersecurity:

- **first**, on the hand-held devices, information is being taken outside the physically controlled environment and
- **second** remote access back to the protected environment is being granted.

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

Some well-known technical challenges in mobile security are: Managing the registry settings and configurations,

- Authentication service security,
- Cryptography security,
- Lightweight directory access protocol (LDAP) security,
- Remote access server (RAS) security,
- Media player control security,
- Networking application program interface (API) security etc.

6. 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.

7. Authentication Service Security

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

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

- Authentication services security is important given the typical attacks on mobile devices through wireless networks:
  - •Dos attacks,
  - •traffic analysis,
  - •eavesdropping,
  - •man-in-the-middle attacks and session hijacking.

- Security measures in this scenario come from Wireless Application Protocols (WAPs), use of VPNs, media access control (MAC) address filtering and development in 802.xx standards.

7.1 Cryptographic Security for Mobile Devices

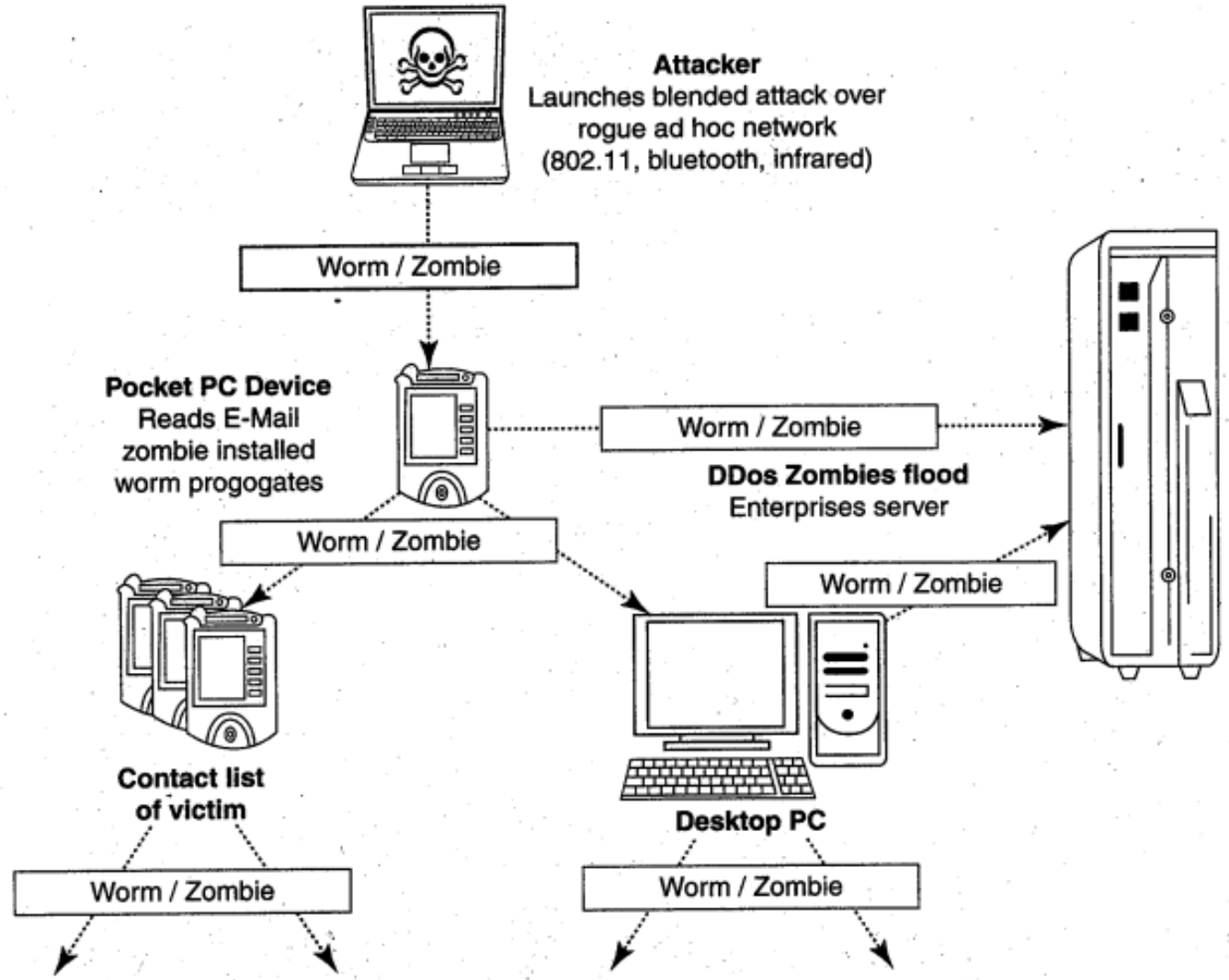

Figure : Push attack on mobile devices. DDoS implies distributed denial-of-service attack

- Cryptographically Generated Addresses (CGA) is Internet Protocol version 6 (IPv 6) 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 and mobility protocols. It can also be used for key exchange in opportunistic Internet Protocol Security (IPSec).

7.1 Cryptographic Security for Mobile Devices

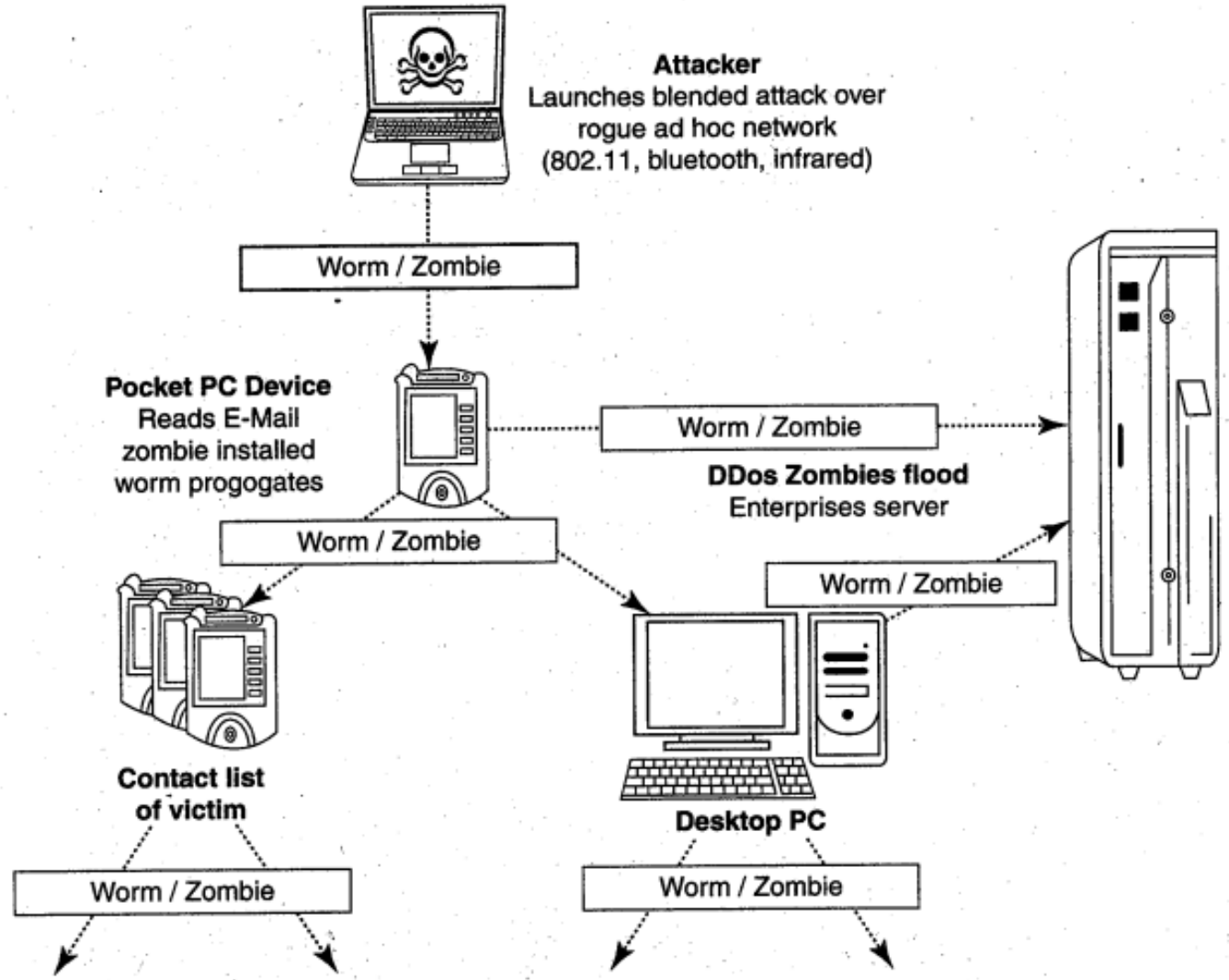

Figure : Push attack on mobile devices. DDoS implies distributed denial-of-service attack

- Palms 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.

7.2 LDAP Security for Hand-Held Mobile Computing Devices

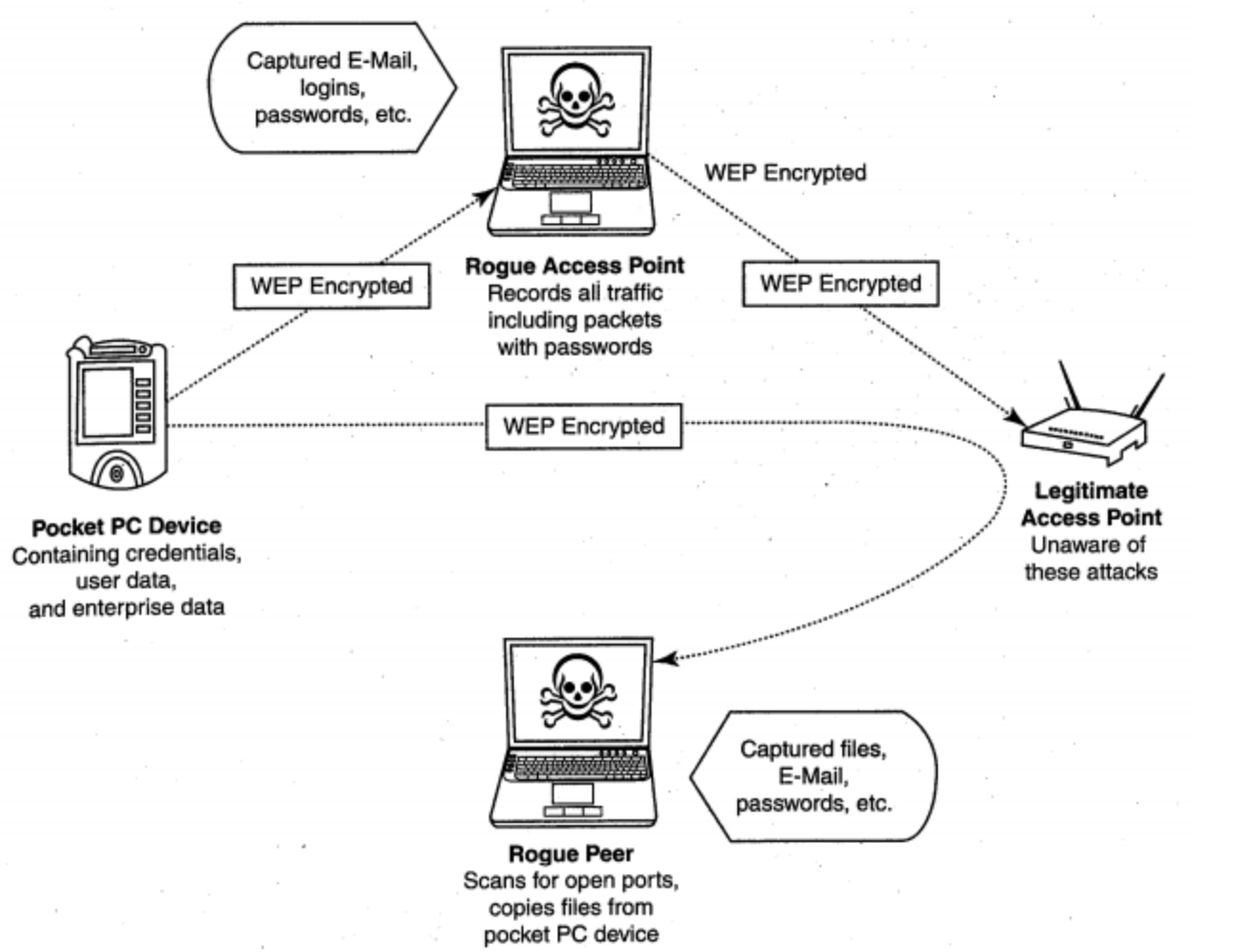

Figure : Pull attack on mobile devices

- LDAP(Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate individuals, organizations and other resources such as files and devices on the network/ In a network, a directory tells you where an entity is located in the network.
- LDAP is a light weight (smaller amount of code) version of Directory Access Protocol (DAP) because it does not include security features in its initial version.
- Centralized directories such as LDAP make revoking permissions quick and easy.

7.3 RAS Security for Mobile Devices

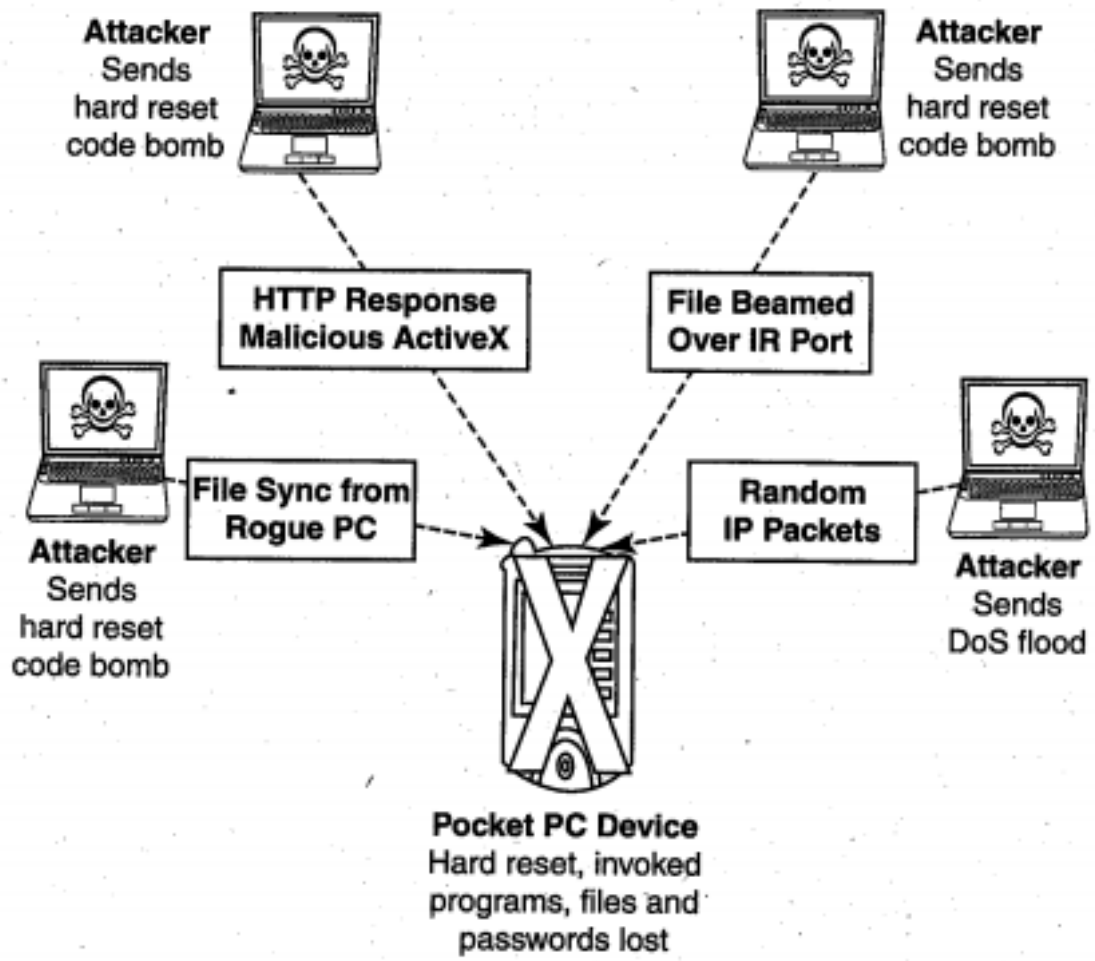

Figure 1: Crash attack on mobile devices. DoS - Denial-of-service attack

- RAS(Remote Access Services) 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.
- Figure 2. illustrates how access to an 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 to these systems, a would-be cracker is then able to steal data or compromise corporate systems in other ways.
- 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 connection of sites that are related in some sense.

7.3 RAS Security for Mobile Devices

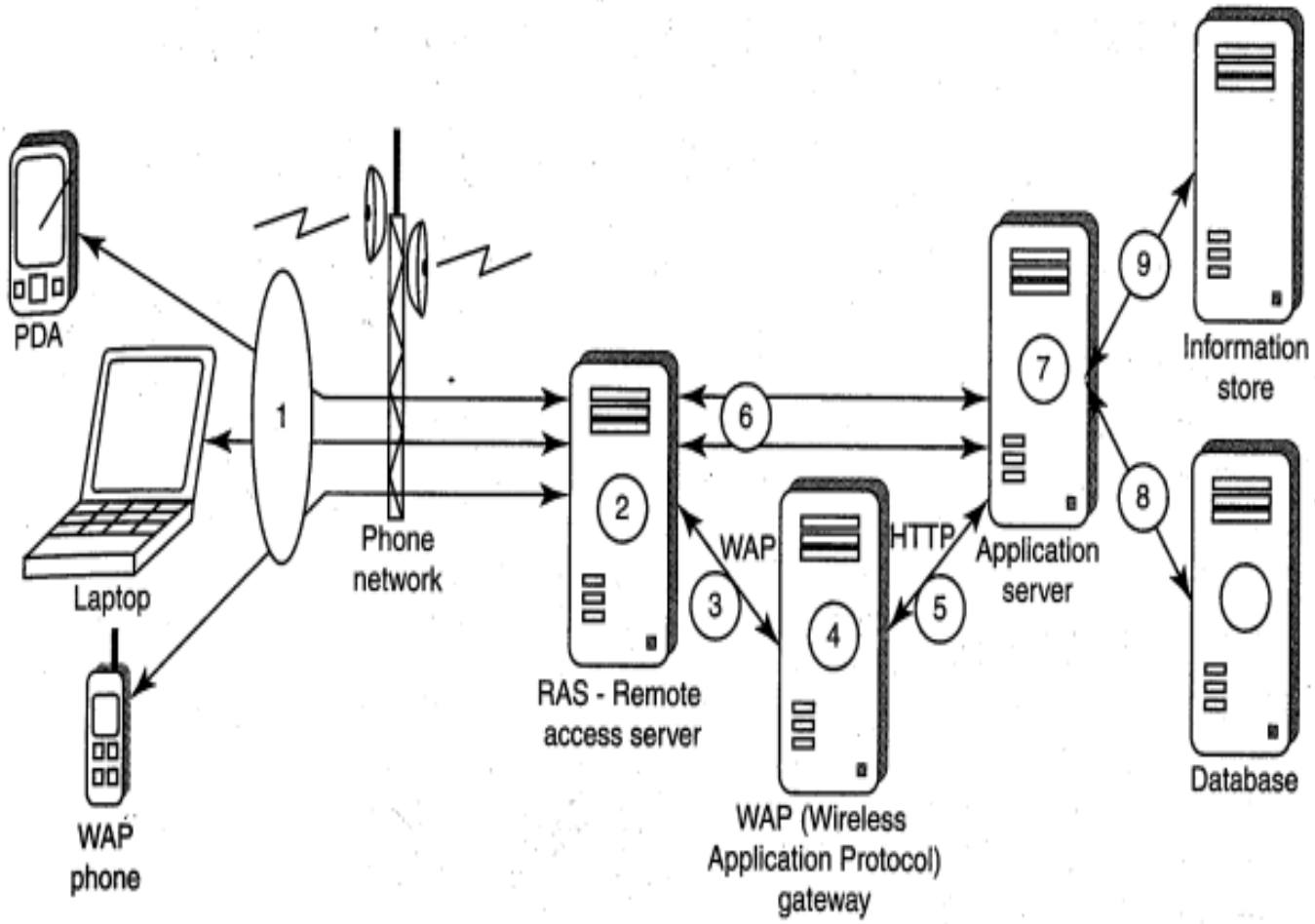

Figure 2: Communication from mobile client to organization information store

- 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. For situations where all connections to the corporate network pass through a gateway, placing the personal firewall on the gateway itself could be the simplest solution, because it avoids the need to place a personal firewall on each mobile device. In either case, deploying secure access methods that implement strong authentication keys will provide an additional protection.

7.4 Media Player Control Security

- Given the lifestyle of today's young generation, it is quite common to expect them embracing the mobile hand-held devices as a means for information access, remote working and entertainment. Music and video are the two important aspects in day-to-day aspects for the young generation. Given this, it is easy to appreciate how this can be a source for cybersecurity breaches.

- 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 or 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.

7.4 Media Player Control Security

- As another example, consider the following news item of the year 2004 : corrupt files posing as normal music and video files could allow an attacker to gain control of the downloader's computer.

- With this happening, there are three vulnerabilities:
  (a) files could be created that will open a website on the user's browser (e.g, the user could be accessing from his/her hand held device) from where remote JavaScript can be operated;
  (b) files could be created which allow the attacker to download and use the code on a user's machine or
  (c) media files could be created that will create buffer overrun errors.

7.5 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 that can be used to target multiple security platforms present in a range of devices such as mobile phones, portable media players, set-top boxes and home gateways.
- 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. Technological developments such as these provide the ability to significantly improve cybersecurity 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.

8. Attack on Mobile/ Cell Phones

8.1 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. Increase in the purchasing power and availability of numerous low cost handsets have also lead to an increase in mobile phone users.
- Theft of mobile phones has risen dramatically over the past few years. Since huge section of working population in India use public transport, major locations where theft occurs are bus stops, railway stations and traffic signals.
- 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.

8. Attack on Mobile/ Cell Phones

The following factors contribute for outbreaks on mobile devices:

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

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

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

8.2 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 10−30m, through Bluetooth-activated phones whereas MMS virus can send a copy of itself to all mobile users whose numbers are available in the infected mobile phone's address book.

- It is interesting to note that, like Computer Virus Hoax, variants of Mobile Phone Virus Hoax" have been circulating since ,1999. These hoax messages either will be sent through E-Mail or through SMS to the mobile users, The example of such hoax is given.

8.2 Mobile - Viruses

- If you receive a phone call and your mobile phone displays (XALAN) on the screen don't answer the call. END THE CALL IMMEDIATELY, if you answer the call, your phone will be infected by a virus. This virus WILL ERASE all IMEI and IMSI information from both your phone and your SIM card, which will make your phone unable to connect with the telephone network. You will have to buy a new phone. This information has been confirmed by both Motorola and Nokia. There are over 3 Million mobile phones being infected by this virus in all around the world now.

Following are some tips to protect mobile from mobile malware attacks:

- Download or accept programs and content (including ring tones, games, video clips and photos) only from a trusted source.
- 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.
- If a mobile is equipped with beam (i.e., IR), allow it to receive incoming beams, only from the trusted source.
- Download and install antivirus software for mobile devices.

9. Managing Diversity and Proliferation of Hand-Held Devices

Younger workers are pushing many enterprises to embrace mobility solutions. These younger workers prefer instant/text messaging instead of E-Mail, and frequently use social networking services such as Facebook, Myspace and Twitter. They often prefer to use personal, consumer-oriented devices (both laptops and mobile devices) in the work environment, and adapt quickly to new technology.

In contrast, **older workers** are found to be slow to accept mobility solutions and rely almost entirely on voice communications and E-Mail. These old workers often do not see the benefit of instant messaging and social networking. Interestingly, at the same time these older workers are often found to be on the seat that provides authority and control for staffing and budget, and they can therefore greatly influence mobility policy.

These different points of view between younger and older workers have created a mobility generational gap. Older workers sometimes see younger workers as being "spoiled" whereas younger workers sometimes see older workers as a barrier to progress.

9. Managing Diversity and Proliferation of Hand-Held Devices

Cybersecurity is always a primary concern; even then, at times, there is still some short sightedness. 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 his/her logical as well as physical access to corporate resources because employees (for malicious or other reasons) could be using their mobile devices to connect into the corporate 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.

In addition, employees should be encouraged to register with the IT department any devices they use for themselves, so that access can be provisioned in a controlled manner and de-provisioned appropriately when the employee leaves.

9.1 Unconventional/Stealth Storage Devices

We would like to emphasize upon widening the spectrum of mobile devices and focus on secondary storage devices, such as compact disks (CDs) and Universal Serial Bus (USB) drives (also called zip drive, memory sticks) used by employees. As the technology is advancing, the devices continue to decrease in size and emerge in new shapes and sizes - unconventional/stealth 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.

Firewalls and antivirus software are no defense against the threat of open USB ports. 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. However, sometimes the standard access controls with Windows OS do not allow the assignment of permissions for USB ports and restricting these devices becomes next to impossible. Disgruntled 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.

9.1 Unconventional/Stealth Storage Devices

Using "DeviceLock" software solution, one can have control over unauthorized access to plug and play 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.

10. Threats through Lost and Stolen Devices and Protecting Data on Lost Devices

Threats through Lost and Stolen Device:

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.

10. Threats through Lost and Stolen Devices and Protecting Data on Lost Devices

Protecting Data on Lost Devices:

For protecting data that are stored persistently on a device, there are two precautions that individuals can take to prevent disclosure of the data stored on a mobile device: (a) encrypting sensitive data and (b) encrypting the entire file.system. Data that are stored on hard disks in persistent memory or on removable memory sticks should be protected. There are many third party solutions/tools available to protect data on the lost devices, including encrypting the servers where a database file is residing. There are solutions using which individuals can enforce a self-destruct policy to destroy privileged data on a lost device or create a database action to delete the data on a user's device using a suitable tool.

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, and device owners should be aware of this method. Writing the emergency contact information on the device itself is unlikely to be very helpful.

11. Educating the Laptop users

According to year 2004 finding, through one survey, it was found that some 86% of employees with laptops admitted to installing software onto their machines when outside of the office, with many using their laptops to access peer-to-peer websites and downloading illegal music files and movies.

The result from a survey quoted in the figure, further supports this point on cybersecurity threats from corporate laptop users. However, despite the growth in corporate security risks, resulting from mobile working, the tone of most of the security-awareness surveys shows that only half of the companies have tools in place to manage the Internet access on laptops, with one quarter of businesses physically enforcing these policies. An important point to be noted is that the policies and procedures put in place for support of laptop have evolved over the years to be able to cope successfully with managing laptops, connected by wireless means or otherwise. This shows how much role-perception" plays in terms of most people perceiving laptops as greater culprits compared with other innocuous-looking mobile hand-held devices.

11. Educating the Laptop users

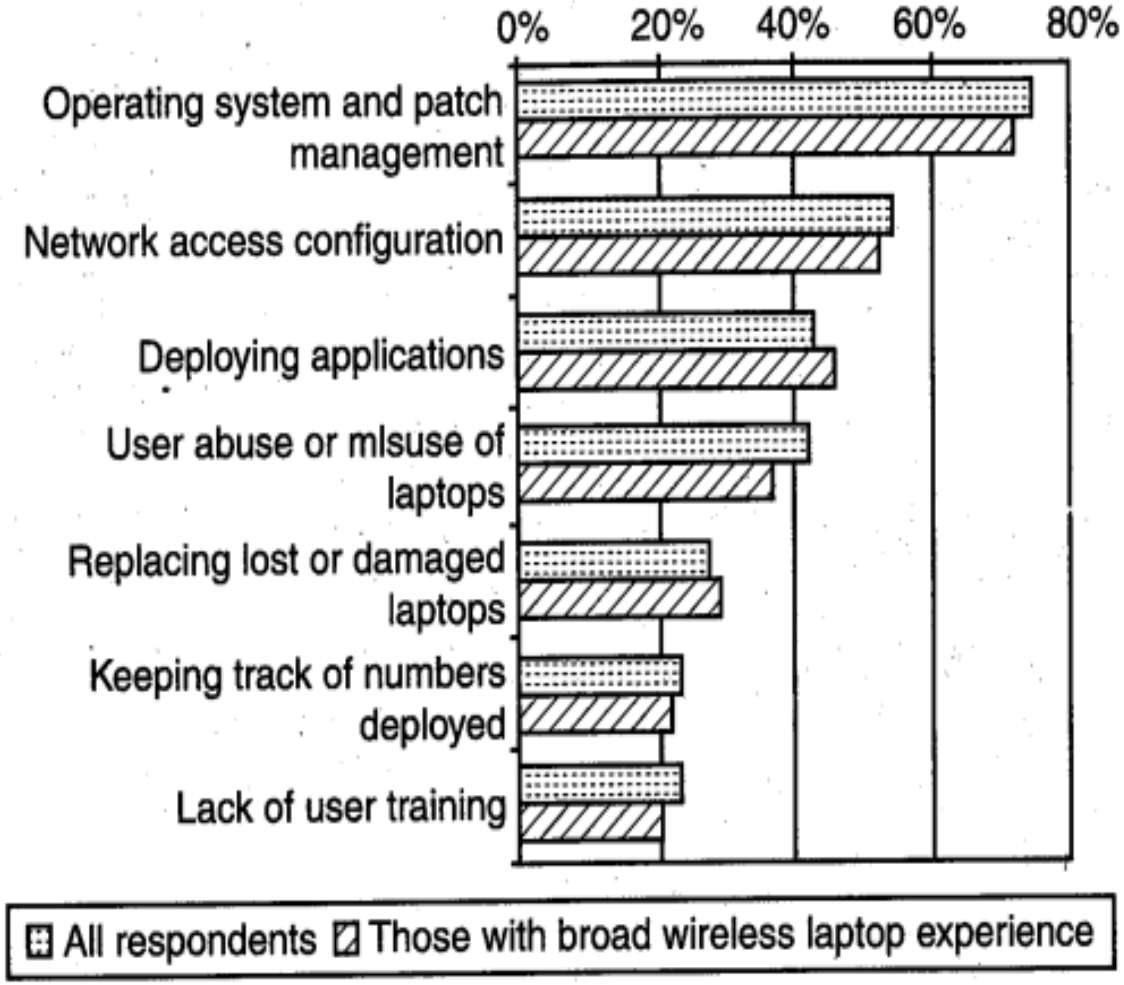

Figure : Most important management or support issues for laptops

12. Organizational Measures for Handling Mobile, Devices-Related Security Issues

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' data loss. such databases need encryption. We mention here two algorithms that are typically used to implement strong encryption of database files: Rijndael 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.

The term "strong encryption" is used here to describe these technologies in contrast to the simple encryption. 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 the MDSR algorithms, makes the database file inoperable without the key (password). Encrypting the database scrambles the information contained in the main database file (i.e, all temporary files and all transaction log files) so that it cannot be deciphered by looking at the files using a disk utility. There is a performance impact for using strong encryption. A weaker form of encryption is also available that has negligible performance impact.

12. Organizational Measures for Handling Mobile, Devices-Related Security Issues

When using strong encryption, it is important not to store the key on the mobile device: this is equivalent to leaving a key in a locked door. However, if you lose the key, your data are completely inaccessible. The key is case-sensitive and must be entered correctly to access your database. The key is required whenever you want to start the database or you want to use a utility on your database. When a device that is identified as lost or stolen connects to the organization server, IT department can have the server send a package to destroy privileged data on the device.

Including Mobile Devices in Security Strategy:

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. Their concerns are no longer viable. There are technologies available to properly secure mobile devices. These should be good enough for most organizations. Corporate IT departments just need to do their homework. For example, there are ways to make devices lock or destroy the lost data by sending the machine a special message. Also, some mobile devices have high-powered processors that will support 128− bit encryption.

12. Organizational Measures for Handling Mobile, Devices-Related Security Issues

Although mobile devices do pose unique challenges from a cybersecurity perspective, there are some general steps that the users can take to address them, such as integrating security programs for mobile and wireless systems into the overall security blueprint.

A few things that enterprises con 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.

13. Organizational Security Policies and Measures in Mobile Computing Era

Importance of Security Policies relating to Mobile Computing Devices:

Proliferation of hand-held devices used makes the cybersecurity issue graver than what we would tend to think. People have grown so used to their hand-helds they are treating them like wallets! For example, people are storing more types of confidential information on mobile computing devices than their employers or they themselves know; they listen to music using their-hand-held devices.One should think about not to keep credit card and bank account numbers, passwords, confidential E-Mails and strategic information about organization, merger or takeover plans and also other valuable information that could impact stock values in the mobile devices. Imagine the business impact if an employee's USB, pluggable drive or laptop was lost or stolen, revealing sensitive customer data such as credit reports, social security numbers (SSNs) and contact information. Not only would this be a public relations (PR) disaster, but it could also violate laws and regulations. One should give a deep thought about the potential legal troubles for a public company whose sales reports, employee records or expansion plans may fall into wrong hands.

13. Organizational Security Policies and Measures in Mobile Computing Era

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. This sort of policy can be difficult to enforce, however, by increasing awareness of 'the user, it can be reasonably effective. Information classification and handling policy should clearly define what sorts of data may be stored on mobile devices. In the absence of other controls, simply not storing confidential data on at-risk platforms will mitigate the risk of theft or loss.

Operating Guidelines for Implementing Mobile Device Security Policies:

In situations such as those described above, the ideal solution would be to prohibit all confidential data from being stored on mobile devices, but this may not always be practical. Organizations can, however, reduce the risk that confidential information will be accessed from lost or stolen mobile devices through the following steps:

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

13. Organizational Security Policies and Measures in Mobile Computing Era

- Implement additional security technologies, as appropriate to fit both the organization and the types of devices used. Most (and perhaps all) mobile computing devices will need to have their native security augmented with such tools as strong encryption, device passwords and physical locks. Biometrics techniques can be used for authentication and encryption and have great potential to eliminate the challenges associated with passwords.
- Standardize the mobile computing devices and the associated security tools being used with them. As a matter of fundamental principle, security deteriorates quickly as the tools and devices used become increasingly disparate.
- Develop a specific framework for using mobile computing devices, including guidelines for data syncing, the use of firewalls and anti-malware software and the types of information that can be stored on them.
- Centralize management of your 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. This can often be simplified by integrating patching with syncing or patch management with the centralized inventory database.
- Label the devices and register them with a suitable service that helps recovered devices to the owners.

13. Organizational Security Policies and Measures in Mobile Computing Era

- Establish procedures to disable remote access for any mobile devices reported as lost or stolen. Many devices allow the users to store usernames and passwords for website portals, which could allow a thief to access even more information than on the device itself.
- Remove data from computing devices that are not in use or before re-assigning those devices to new owners. This is to preclude incidents through which people obtain "old" computing devices that still had confidential company data.
- Provide education and awareness training to personnel using mobile devices. People cannot be expected to appropriately secure their information if they have not been told how.

13. Organizational Security Policies and Measures in Mobile Computing Era

Organizational Policies for the Use of Mobile Hand-Held Devices:

There are many ways to handle the matter of creating policy for mobile devices:

- One way is creating distinct mobile computing policy.
- Another way is including such devices existing policy. There are also approaches in between where mobile devices fall under both existing policies and a new one.
- In the hybrid approach, a new policy is created to address the specific needs of the mobile devices but more general usage issues fall under general IT policies. As a part of this approach, the "acceptable use" policy for other technologies is extended to the mobile devices. There may not be a need for separate policies for wireless, LAN, wide area network (WAN), etc. because a properly written network policy can cover all connections to the company data, including mobile and wireless.

13. Organizational Security Policies and Measures in Mobile Computing Era

Companies new to mobile devices may adopt an umbrella mobile policy but they find over time they will need to modify their policies to match the challenges posed by different kinds of mobile hand-held devices. For example, wireless devices pose different challenges than non-wireless Also, employees who use mobile devices more than 20% of the time will have different requirements than less-frequent users. It may happen that over time, companies may need to create separate policies for the mobile devices on the basis of whether they connect wirelessly and with distinctions for devices that connect to WANs and LANs .

It is never too early to start, planning for mobile devices, even when a company, at a given point of time, cannot afford creating any special security policies to mitigate the threats posed by mobile computing devices to cyber security. It is, after all, an issue of new technology adoption for many organizations. By contemplating its uses companies may think of ways they can use it and, perhaps just as important, how their competitors will use it.

14. Laptops: Physical Security Countermeasures

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

The thefts of laptops have always been a major issue, according to the cybersecurity industry and insurance company statistics. Cybercriminals are targeting laptops that are expensive, to enable them to fetch a quick profit in the black market. Very few laptop. thieves. are actually interested in the information that is contained in the laptop. Most laptops contain personal and corporate information that could be sensitive.

Such information can be misused if found by a malicious user, Senior executives commonly believe that the information stored on their laptops is only useful for them and would not be of any interest to others. Owing to this belief, most senior executives in an organization feel that it is unnecessary to protect the information stored on these laptops. However, this is not true.

14. Laptops: Physical Security Countermeasures

Physical Security Countermeasures:

Organizations are heavily dependent upon a mobile workforce with access to information, no matter where they travel. However, this mobility is putting organizations at risk of having a data breach if a laptop containing sensitive information is lost or stolen. Hence, physical security countermeasures are becoming very vital to protect the information on the employees laptops and to reduce the likelihood that employees will lose laptops. Management also has to take care of creating awareness among the employees about physical security countermeasures by continuous training and stringent monitoring of organizational policies and procedures about these 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. Kensington cables are one of the most popular brands in laptop security cable. These cables are made of aircraft-grade steel and Kevlar brand fiber, thus making these cables 40% stronger than any other conventional security cables. One end of the security cable is fit into the universal security slot of the laptop and the other end is locked around any fixed furniture or item, thus making a loop. These cables come with a variety of options such as number locks, key locks and alarms.

14. Laptops: Physical Security Countermeasures

2. Laptop safes: Safes made of polycarbonate - the same material that is used in bulletproof windows, police riot shields and bank security screens-can be used to carry and safeguard the laptops. The advantage of safes over security cables is that they protect the whole laptop and its devices such as CD-ROM bays, PCMCIA cards and HDD bays which can be easily removed in the case of laptops protected by security cables.

3. Motion sensors and alarms: Even though alarms and motion sensors are annoying owing to their false alarms and loud sound level, these devices are very efficient in securing laptops. Once these devices are activated, they can be used to track missing laptops in crowded places. Also owing to their loud nature, they help in deterring thieves. Modern systems for laptops are designed wherein the alarm device attached to the laptop transmits radio signals to a certain range around the laptop.

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

14. Laptops: Physical Security Countermeasures

Other measures for protecting laptops are as follows:

- Engraving the laptop with personal details
- Keeping the laptop close to oneself wherever possible
- Carrying the laptop in a different and unobvious bag making it unobvious to potential thieves
- Creating the awareness among the employees to understand the responsibility of carrying a laptop and also about the sensitivity of the information contained in the laptop
- Making a copy of the purchase receipt, laptop serial number and the description of the laptop
- Installing encryption software to protect information stored on the laptop
- Using personal firewall software to block unwanted access and intrusion
- Updating the antivirus software regularly
- Tight office security using security guards and securing the laptop by locking it down in lockers when not in use
- Never leaving the laptop unattended in public places such as the car, parking lot, conventions, conferences and the airport until it is fitted with an anti theft device;
- Disabling IR ports and wireless cards and removing PCMCIA cards when not in use.

14. Laptops: Physical Security Countermeasures

Information systems security also contains logical access controls. This is because, information, be it corporate or private, needs high security as it is the most important asset of an organization or an individual.

A few logical or access controls are as follows:

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