UNIT -III: Cybercrime Mobile and Wireless Devices:

1. Introduction,
2. Proliferation (Growth) of Mobile and Wireless Devices,
3. Trends in Mobility,
4. Credit Card Frauds in Mobile and Wireless Computing Era,
5. Security Challenges Posed by Mobile Devices,
6. Registry Settings for Mobile Devices,
7. Authentication Service Security,
8. Attacks on Mobile/Cell Phones,
9. Mobile Devices: Security Implications for Organizations,
10. Organizational Measures for Handling Mobile,
11. Organizational Security Policies and Measures in Mobile Computing Era,
12. Laptops.

RGANCET

3.1 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.
- By the end of 2008 around 1.5 billion individuals around the world had the Internet access.
- In November 2007, mobile phone users were numbered 3.3 billion, with a growing proportion of those mobile devices enabled for the Internet access.
- 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 hand-held 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*.
- **Smartphones** 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 Smartphones, 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 user productivity.
- Clearly, these technological developments present a new set of security challenges to the global organizations.

3.2 Proliferation (Growth) 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.
- Let us understand the concept **of mobile computing** and the various types of devices.

Mobile computing

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 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 computing

- 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 cybersecurity 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 Smartphones.

3.3 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.

R16 JNTUCSE

- "iPhone" from Apple and Google-led "Android" phones are the best examples of this trend and there are plenty of other developments that point in this direction.
- This smart mobile technology is rapidly gaining popularity and the attackers (hackers and crackers) are among its biggest fans.
- It is worth noting the trends in mobile computing; this will help readers to realize the seriousness of cybersecurity issues in the mobile computing domain.
- Figure 3.3 shows the different types of mobility and their implications.

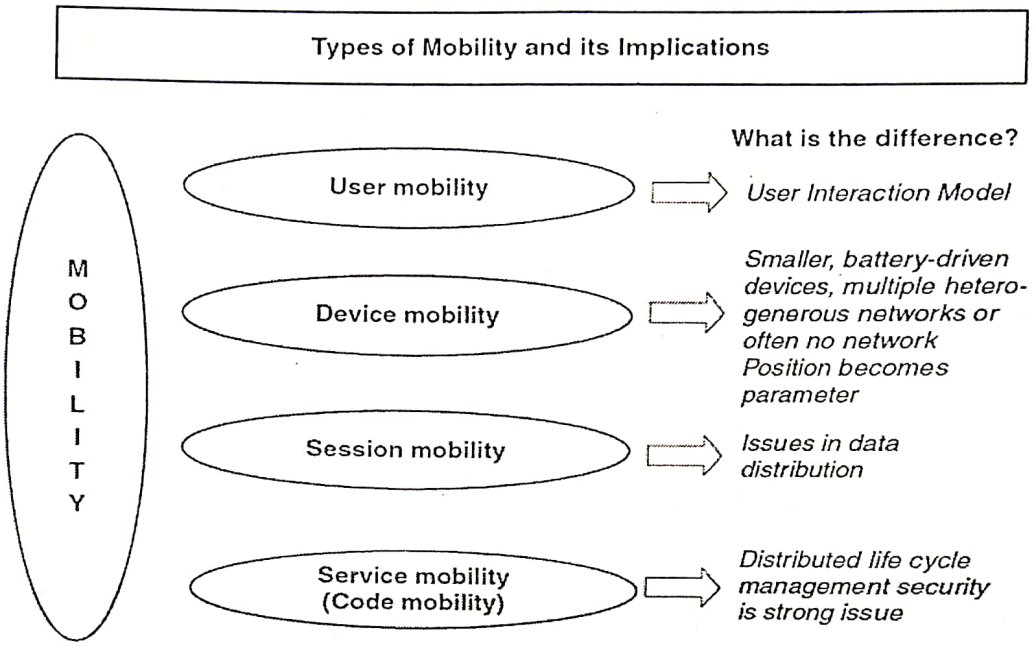


Figure 3.3 | Mobility types and implications.

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:

- ***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 Smart phones 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 (refer to Appendix C).
- ***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.

3.4 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.*
- The developments in wireless technology have fuelled this new mode of working for white collar workers.
- 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.
- Figure 3.4 shows the basic flow of transactions involved in purchases done using credit cards.

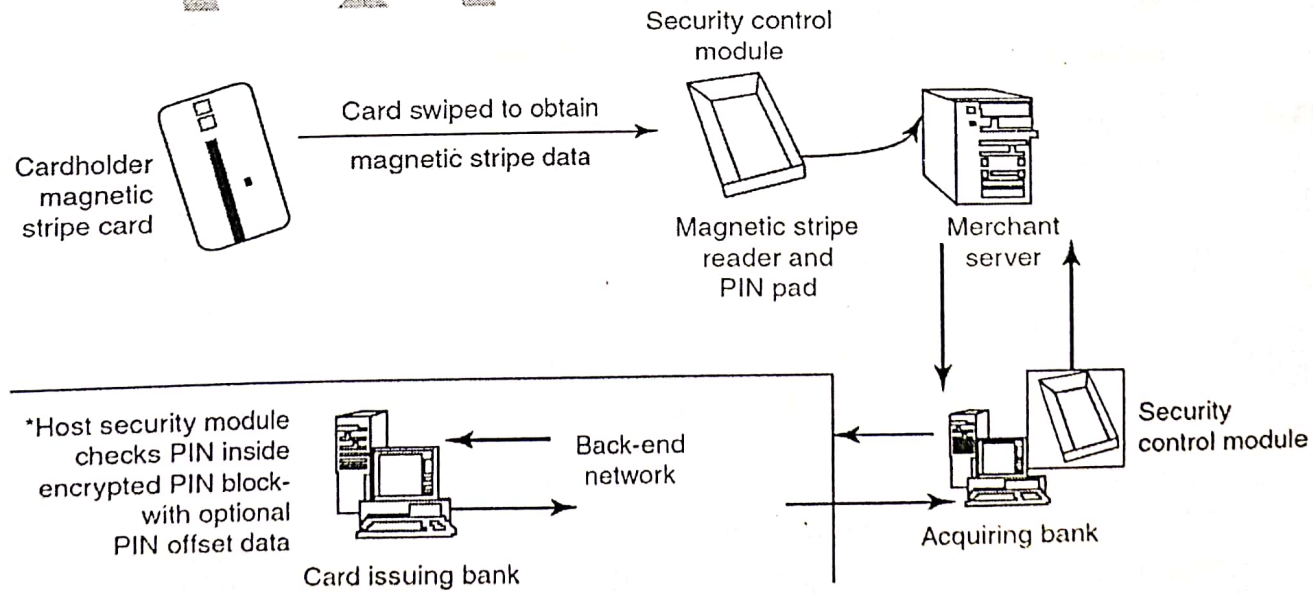


Figure 3.4 | Online environment for credit card transactions.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

- 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
- Figure 3.5, the basic flow is as follows:
  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.

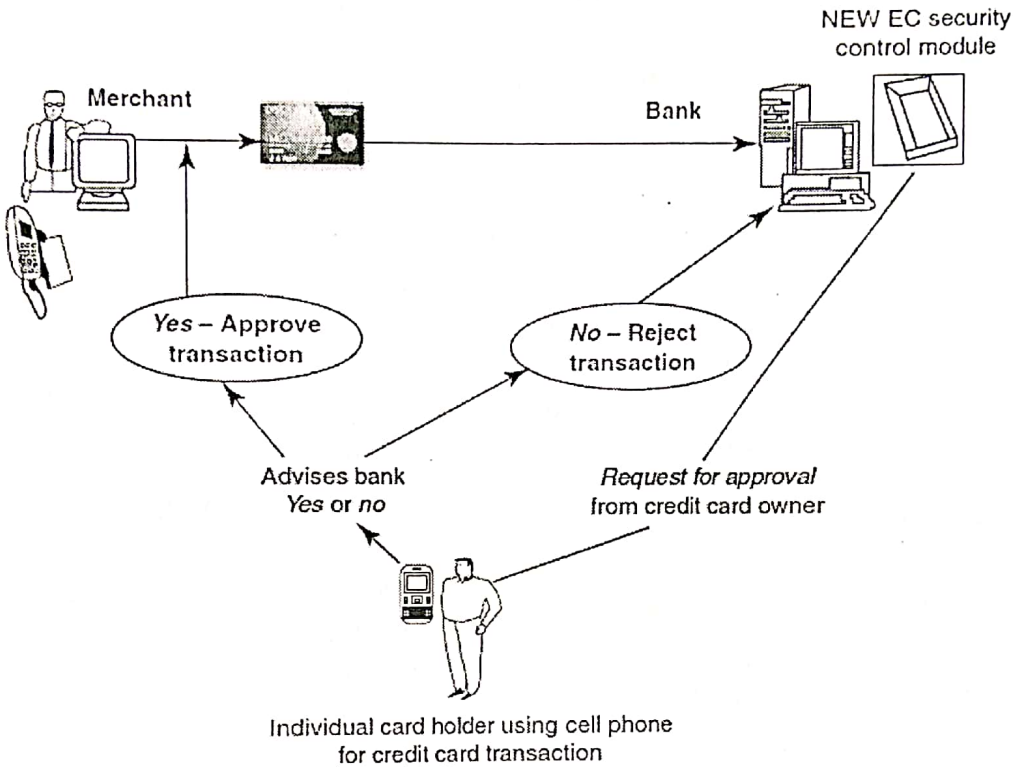


Figure 3.5 | Closed-loop environment for wireless (CLEW).
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*. Wiley India.

(Box 3.2). Tips to Prevent Credit Card Frauds
• The current topic is about credit card frauds in mobile and wireless computing era, however, we would like to include these tips to prevent credit card frauds[8] caused due to individual ignorance about a few known facts.
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.
Dont's
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.

3.4.1 Types and Techniques of Credit Card Frauds

Traditional Techniques

- The traditional and the first type of credit card fraud is paper-based fraud – *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

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

  2. 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.

Modern Techniques

- Skimming is where the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip are copied from one card to another.
- Site cloning and false merchant sites on the Internet are becoming a popular method of fraud and to direct the users to such bogus/fake sites is called Phishing.
- Such sites are designed to get people to hand over their credit card details without realizing that they have been directed to a fake weblink /website (i.e., they have been scammed).

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 by him, which appears to be legitimate merchandise website.

• 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.

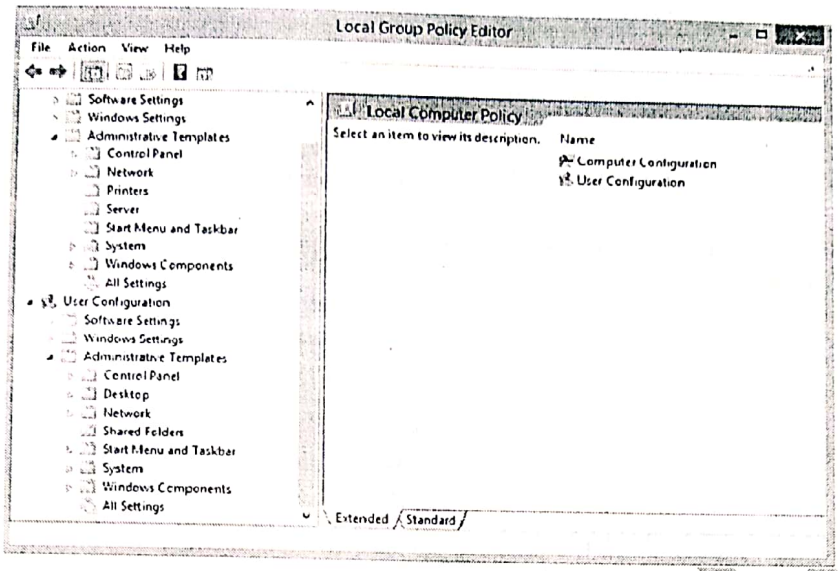
2. Credit card generators: It is another modern technique – computer emulation software – that creates valid credit card numbers and expiry dates. The criminals highly rely on these generators to create valid credit cards. These are available for free download on the Internet.

3.5 Security Challenges Posed by Mobile Devices

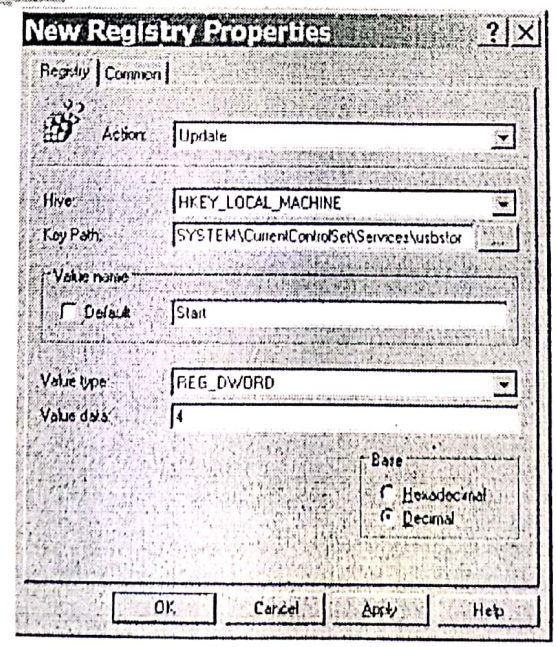
- Mobility brings two main challenges to cybersecurity:
  - **first**, on the hand-held devices, information is being taken outside the physically controlled environment and
  - **second** remote access back to the protected environment is being granted.
- Perceptions of the organizations to these cybersecurity 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 "microchallenges" and
  2. at the organizational level called "macrochallenges."
- 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.*

3.6 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.**
- Thus, establishing trusted groups through appropriate registry settings becomes crucial. One of the most prevalent areas where this attention to security is applicable is within "group policy." Group policy is one of the core operations that are performed by Windows Active Directory. (Run command box, type GPEDIT.MSC command to initiate the Local **Group Policy** Editor)



- There is one more dimension to mobile device security: new mobile applications are constantly being provided to help protect against *Spyware, viruses, worms, malware* and other Malicious Codes that run through the networks and the Internet.
- The mobile security issues on a Windows platform is that the baseline security is not configured properly.
- When you get a computer installed or use a mobile device for the first time, it may not be 100% secure. Even if users go through every *Control Panel setting* and *group policy* option, they may not get the computer to the desired baseline security.
- For example, the only way to get a Windows computer to a security level that will be near bulletproof is to make additional *registry* changes that are not exposed through any interface.
- There are many ways to complete these registry changes on every computer, but some are certainly more efficient than others.
- Naïve (Innocent) users may think that for solving the problem of mobile device security there are not many registry settings to tackle.
- However, the reality is far different! The reality of the overall problem becomes prevalent when you start researching and investigating the abundance of "registry hacks" that are discussed in Microsoft Knowledge Base articles.
- Figure 3.7 displays an illustration of how some tools allow users to browse to the desired registry value on their mobile devices.



3.7 Authentication Service Security

- There are two components of security in mobile computing: *security of devices* and *security in networks.*
- A secure network access involves 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* (see Figs. 3.8–3.10).
- 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*.

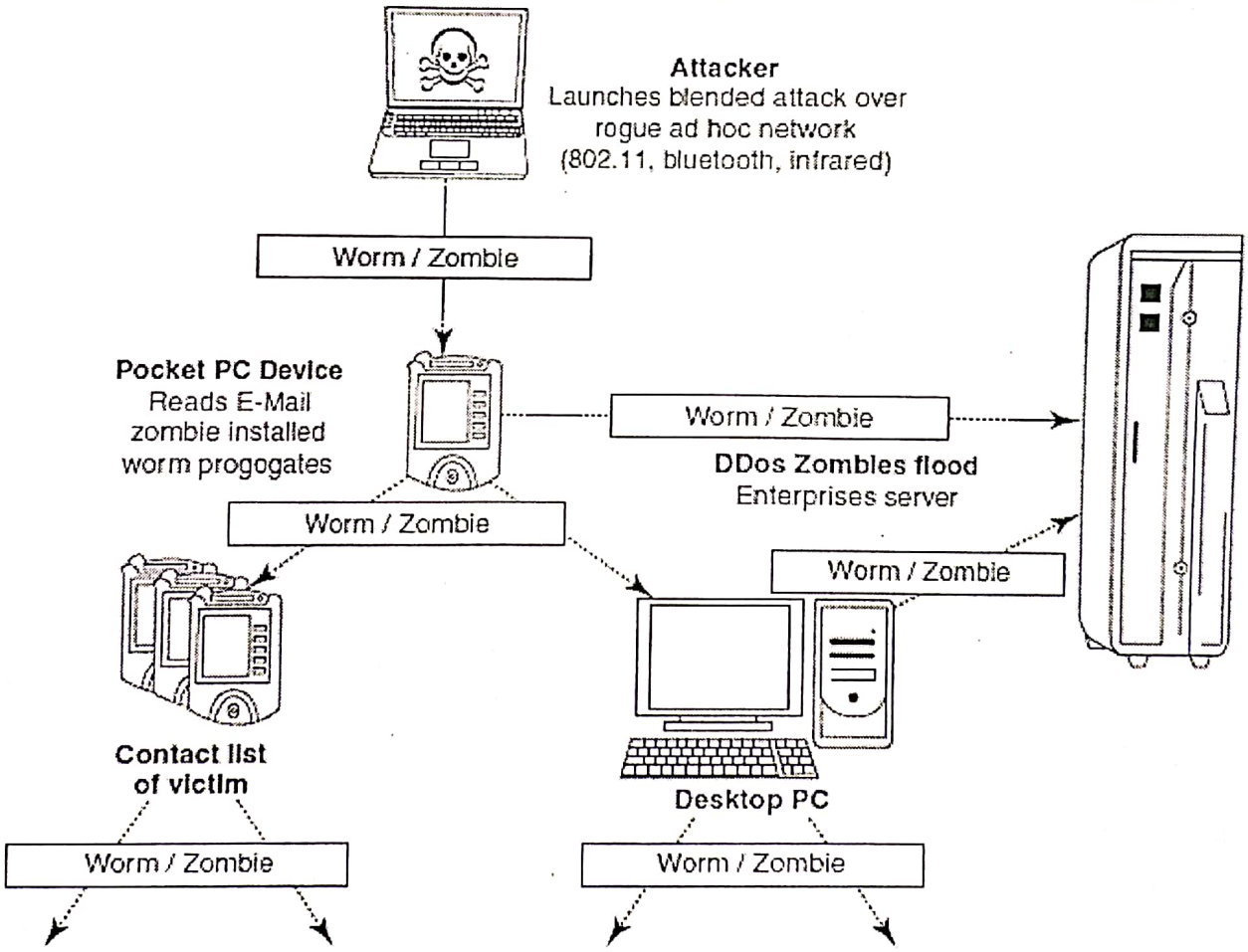


Figure 3.8 | Push attack on mobile devices. DDoS implies distributed denial-of-service attack. *Source:* Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

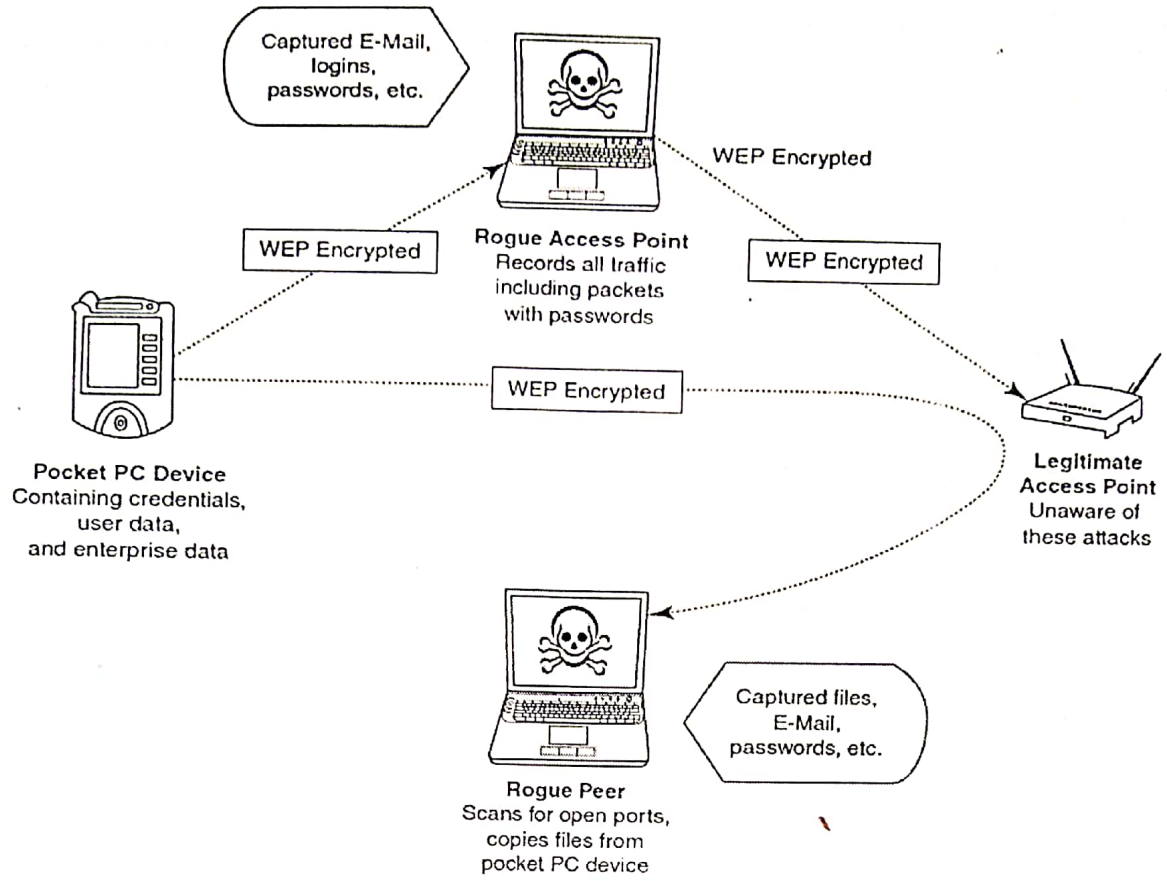


Figure 3.9 | Pull attack on mobile devices.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

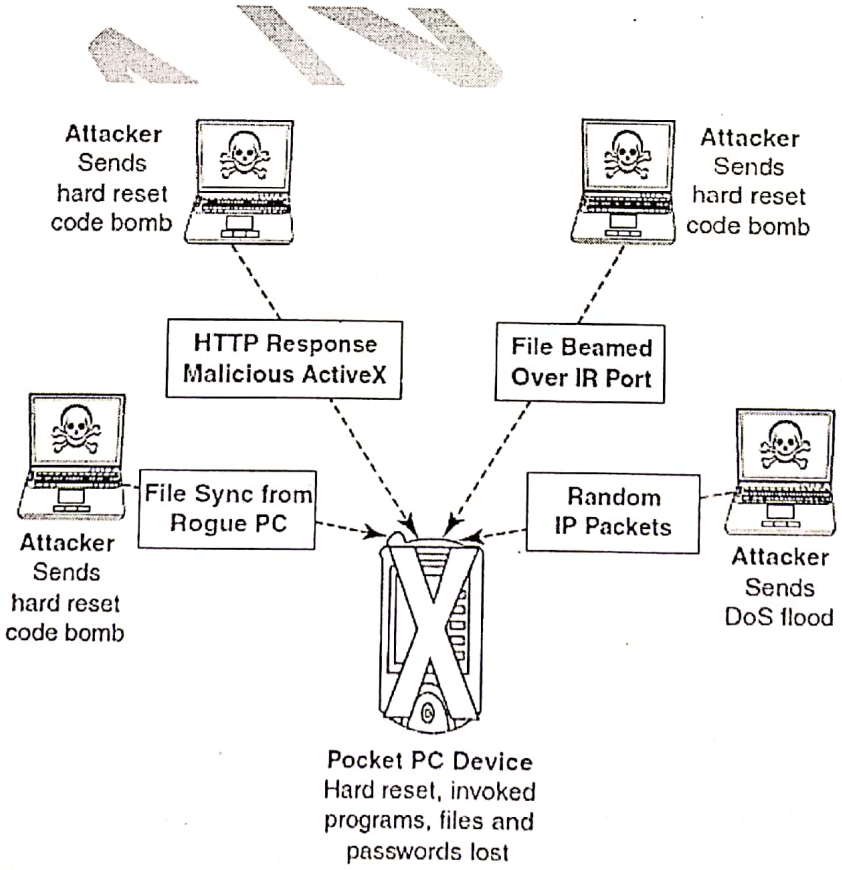


Figure 3.10 | Crash attack on mobile devices. DoS – Denial-of-service attack.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

3.7.1 Cryptographic Security for Mobile Devices

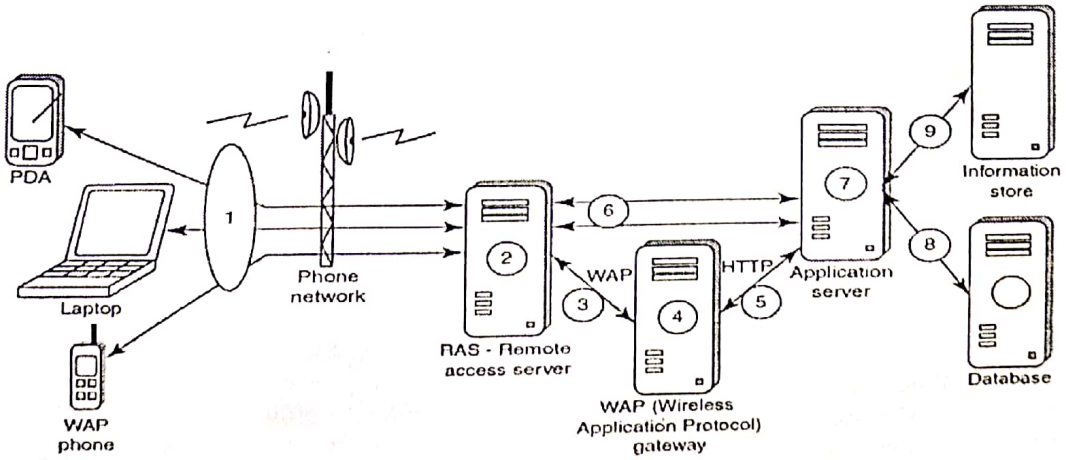
- ***Cryptographically Generated Addresses (CGA)*** is Internet Protocol version 6 (IPv6) that addresses up to 64 address bits that are generated by hashing owner's public-key address.
- The address the owner uses is the corresponding private key to assert address ownership and to sign messages sent 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.

3.7.2 LDAP (Lightweight Directory Access Protocol) 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.

3.7.3 RAS (Remote Access Server) 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. Figure 3.11 : 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.
- 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 (see Box 3.5).
- 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.

3.7.4 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.

3.7.5 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
- 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 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.

3.8 Attacks on Mobile/Cell Phones

3.8.1 Mobile Phone Theft

- Mobile phones have become an integral part of everbody's life and the mobile phone has transformed from being a luxury to a bare necessity.
- 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:** Enough terminals or more devices to attack.
2. **Enough functionality:** The expanded functionality ie. *office functionality and applications* 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.

Box 3.6 | Tips to Secure your Cell/Mobile Phone from being Stolen/Lost

Ensure to note the following details about your cell phone and preserve it in a safe place:
1. Your phone number; **2.** the make and model; **3.** color and appearance details;
4. PIN and/or security lock code; **5.** IMEI number.

The International Mobile Equipment Identity (IMEI)

- It is a number unique to every GSM, WCDMA and iDEN cell phone. It is a 15-digit number and can be obtained by entering *#06# from the keypad.
- The IMEI number is used by the GSM network to identify valid devices and therefore can be used to stop a stolen phone from accessing the network in that country.
- For example, if a mobile phone is stolen, the owner can call his or her service provider and instruct them to "lock" the phone using its IMEI number.
- This will help to stop the usage of phone in that country, even if a SIM is changed.
- Visit the weblink http://www.numberingplans.com/?page=analysis&sub=imeinr to check all information about your cell phone such as manufacturer, model type and country of approval of a handset.

- Following are few antitheft software(s) available in the market:

1. **GadgetTrak:** http://www.gadgettrak.com/products/mobile/
2. **Back2u:** http://www.bak2u.com/phonebakmobilephone.php
3. **Wavesecure:** https://www.wavesecure.com/
4. **F-Secure:** http://www.f-secure.com/

3.8.2 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 10–30 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.
- *How to Protect from Mobile Malwares Attacks*

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.

3.8.3 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 diferent reasons why they need this information from you.

3.8.4 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:

1. ID theft; **2.** purchasing luxury goods and services; **3.** transferring money/funds; **4.** monitoring the victims' bank accounts; **5.** making applications for loans and credit cards.

www.Jntufastupdates.com

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: **2. Mobile text messaging:**
3. Voicemail: **4. Direct phone call:**

Following are the steps detailing on how direct phone call works:

• The criminal gathers cell/mobile phone numbers located and steals mobile phone numbers after accessing cellular company.

• The criminal often uses a dialer to call phone numbers of people from a specific region, and that to from the gathered list of phone numbers.

• When the victim answers the call, an automated recorded message is played to alert the victim that his/her credit card has had fraudulent activity and/or his/her bank account has had unusual activity.

The message instructs the victim to call one phone number immediately.

The same phone number is often displayed in the spoofed caller ID, under the name of the financial company the criminal is pretending to represent.

• When the victim calls on the provided number, he/she is given automated instructions to enter his/her credit card number or bank account details with the help of phone keypad.

• Once the victim enters these details, the criminal (i.e., visher) has the necessary information to make fraudulent use of the card or to access the account.

• Such calls are often used to gain additional details such as date of birth, credit card expiration date, etc.

Some of the **examples of vished** calls, when victim calls on the provided number after receiving phished E-Mail and/or after listening voicemail, are as follows:
1. Automated message: Thank you for calling (name of local bank). Your business is important to us. To help you reach the correct representative and answer your query fully, please press the appropriate number on your handset after listening to options. • Press 1 if you need to check your banking details and live balance. • Press 2 if you wish to transfer funds. • Press 3 to unlock your online profile. • Press 0 for any other query.
2. Regardless of what the victim enters (i.e., presses the key), the automated system prompts him to authenticate himself: "The security of each customer is important to us. To proceed further, we require that you authenticate your ID before proceeding. Please type your bank account number, followed by the pound key."
3. The victim enters his/her bank account number and hears the next prompt: "Thank you. Now please type your date of birth, followed by the pound key. For example 01 January 1950 press 01011950."
4. The caller enters his/her date of birth and again receives a prompt from the automated system: "Thank you. Now please type your PIN, followed by the pound key."
5. The caller enters his PIN and hears one last prompt from the system: "Thank you.
We will now transfer you to the appropriate representative." At this stage, the phone call gets disconnected, and the victim thinks there was something wrong with the telephone line; or visher may redirect the victim to the real customer service line, and the victim will not be able to know at all that his authentication was appropriated by the visher.

How to Protect from Vishing Attacks

Following are some tips to protect oneself 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 cyberpolice 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.

3.8.5 Smishing

- Smishing is a criminal offense conducted by using social engineering techniques similar to Phishing.
- The name is derived from "SMS PhISHING."
- 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" (method used to actually "capture" your information) 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

Following are some tips to protect oneself 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.

R-CSE

3.8.6 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 a 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.

Table 3.1 | Bluetooth hacking tools
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 fi nding 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 attacks like Bluebug and BlueSnarf.

Bluejacking, *Bluesnarfing, Bluebugging* and *Car Whisperer* are common attacks that have emerged as Bluetooth-specific security issues.

1. Bluejacking: It means *Bluetooth + Jacking* where Jacking is short name for *hijack* – act of taking over something. Bluejacking is sending unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or computers (within 10-m radius), Bluejacking is harmless, as bluejacked users generally do not understand what has happened and hence they may think that their phone is malfunctioning.

2. Bluesnarfing: It is the unauthorized access from a wireless device through a Bluetooth connection between cell phones, PDAs and computers. This enables the attacker to access a calendar, contact list, SMS and E-Mails as well as enable attackers to copy pictures and private videos.

3. Bluebugging: It allows attackers to remotely access a user's phone and use its features without user's attention.
4. Car Whisperer: It is a piece of software that allows attackers to send audio to and receive audio from a Bluetooth-enabled car stereo.

Among the four above-mentioned attacks, Bluesnarfing is claimed to be much more serious than Bluejacking.
These vulnerabilities are an inevitable result of technological innovation, and device manufacturers' continuously research and release firmware upgrades to address new challenges/problems as they arise.

"Bluetooth and Bluetooth Security" is a separate subject in itself. Readers may visit the following
websites to explore more on this topic:
- https://www.bluetooth.org/apps/content/
- http://www.bluetooth.com/English/Pages/default.aspx
- http://www.bluetoothhack.info/

3.9 Mobile Devices: Security Implications for Organizations

3.9.1 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 to the organization.
- 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.

3.9.2 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 "DeviceLock" software solution, one can have control over unauthorized access to plug and play devices (for more details, visit http://www.devicelock.com/).

- The features of the software allows system administrator to:
  1. Monitor which users or groups can access USB Ports, Wi-Fi and Bluetooth adapters, CD read-only memories (CD-ROMs) and other removable devices.
  2. Control the access to devices depending on the time of the day and day of the week.
  3. 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.
  4. Set devices in read-only mode.
  5. Protect disks from accidental or intentional formatting.

3.9.3 Threats through Lost and 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.
- A report based on a survey of London's 24,000 licensed cab drivers quotes that 2,900 laptops, 1,300 PDAs and over 62,000 mobile phones were left in London in cabs in the year 2001 over the last 6-month period.
- Today this figure (lost mobile devices) could be far larger given the greatly increased sales and usage of mobile devices.
- 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.

3.9.4 Protecting Data on Lost Devices

- There are two reasons why cybersecurity needs to protect the data when device is lost :
  1. data that are persistently stored on the device and
  2. always running applications.
- For protecting data, there are two precautions to prevent disclosure of the data stored on a mobile device:
  1. encrypting sensitive data and
  2. encrypting the entire file system.

3.10 Organizational Measures for Handling Mobile

3.10.1 Encrypting Organizational Databases

- Critical and sensitive data reside on databases and with the advances in technology, access to these data is possible through mobiles.
- Through encryption we can protect organization data.
- 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.

- 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.

3.10.2 Including Mobile Devices in Security Strategy

- Organizational IT departments will have to take the accountability for cybersecurity threats that come through inappropriate access to organizational data from mobile-device–user employees.
- Encryption of corporate databases is not the end of everything.
- There are technologies available to properly secure mobile devices.
- 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.
- A few things that organization can use are:

1. 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.
2. Investigate alternatives that allow a secure access to the company information through a firewall, such as mobile VPNs.
3. Develop a system of more frequent and thorough security audits for mobile devices.
4. 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.
5. Notify the appropriate law-enforcement agency and change passwords. User accounts are closely monitored for any unusual activity for a period of time.

3.11 Organizational Security Policies and Measures in Mobile Computing Era

3.11.1 Importance of Security Policies relating to Mobile Computing Devices

- Growth of mobile devices used makes the cybersecurity 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.
- Imagine the business impact if mobile or laptop was lost or stolen, revealing sensitive customer data such as credit reports, social security numbers (SSNs) and contact information.

3.11.2 Operating Guidelines for Implementing Mobile Device Security Policies

- Through the following steps we can reduce the risk when mobile device lost or stolen

1. Determine whether the employees in the organization need to use mobile computing devices or not.
2. Implement additional security technologies like strong encryption, device passwords and physical locks.

3. Standardize the mobile computing devices and the associated security tools being used with them.
4. Develop a specific framework for using mobile computing devices.
5. Maintain an inventory so that you know who is using what kinds of devices.
6. Establish patching procedures for software on mobile devices.
7. Label the devices and register them with a suitable service.
8. Establish procedures to disable remote access for any mobile.
9. Remove data from computing devices that are not in use
10. Provide education and awareness training to personnel using mobile devices.

3.11.3 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.
-

3.12 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 cybersecurity concerns when 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.
- Most laptops contain personal and corporate information that could be sensitive.
- Such information can be misused if found by a malicious user.
- The following section provides some countermeasures against the theft of laptops, thereby avoiding cybersecurity exposures.

3.12.1 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 (Violation)** if a laptop containing sensitive information is lost or stolen.
- Hence, physical security is very important to protect the information on the employees' laptops.
- Physical security countermeasures are as follows.

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.
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.

5. Other measures for Protecting laptops are as follows:

- 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
- 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:

1. Protecting from malicious programs/attackers/social engineering.
2. Avoiding weak passwords/open access.
3. Monitoring application security and scanning for vulnerabilities.
4. Ensuring that unencrypted data/unprotected fi le systems do not pose threats.
5. Proper handling of removable drives/storage mediums/unnecessary ports.
6. Password protection through appropriate passwords rules and use of strong passwords.
7. Locking down unwanted ports/devices.
8. Regularly installing security patches and updates.
9. Installing antivirus software/firewalls/intrusion detection system (IDSs).
10. Encrypting critical file systems.
11. Other countermeasures:

Box 3.13 | Spy Phone Software!!!
Spy Phone software is installed on the mobile/cell phone of employees, if the employers wants to monitor phone usage. The Spy Phone software is completely hidden from the user, once it is installed and collects all the available data such as SMS messages, ingoing/outgoing call history, location tracking, GPRS usage and uploads the collected data to a remote server.
The employer can simply access the designated website hosted by Spy Phone vendor, and after entering his/her account details, he/she can have full access to all the data collected 24 hours a day, 7 days a week. The employer can access this website through the Internet; hence, he/she can keep an eye on their employees, regardless where he/she is in the world. The employer can read all SMS messages (both incoming and outgoing), know who they (employees) are calling or who is calling them and where they were when the call was received.
Following are few Spy Phone Software(s) available in the market:
1. SpyPhonePlus: http://www.spyphoneplus.com/
2. FlexiSpy: http://www.flexispy.com/
3. TheSpyPhone: http://www.thespyphone.com/spyphone.html
4. Mobile Spy: http://www.mobile-spy.com/