CYBER SECURITY

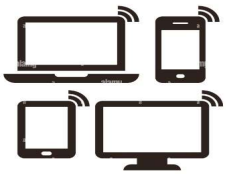
AKTU

Unit:-2

BCC-301 (3rd Sem)
BCC-401 (4th Sem)

CYBER CRIME

Mobile and Wireless Devices :-



SmartPhones combine the best aspects of mobile and wireless technologies and blend them into a useful business tool.

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.

What is a Mobile Device/Wireless?

- Mobile Device: a device that is easy to use, enables remote access to business networks and the internet, and enables quick transfer of data.
- Wireless Communication: the transfer of *information* over a distance without the use of electrical conductors or wires

- Wireless networks use electromagnetic radiation as their means of transmitting data through space.

Mobile and Wireless Devices

Pager
- receive only
- tiny displays
- simple text messages

Mobile phones
- voice, data
- simple graphical displays

PDA
- graphical displays
- character recognition
- simplified WWW

Smart phone
- tiny keyboard
- simple versions of standard applications

Laptop/Notebook
- fully functional
- standard applications

Proliferation of mobile and wireless devices

- You see them everywhere: people hunched over their smartphones or tablets in cafes, airports, supermarkets and even at bus stops, seemingly oblivious to anything or anyone around them.
- They play games, download email, go shopping or check their bank balances on the go.
- They might even access corporate networks and pull up a document or two on their mobile gadgets.

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. Figure

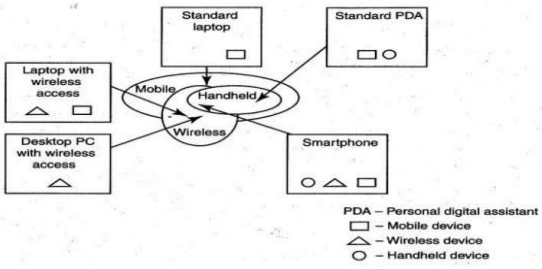


Figure : Mobile, Wireless and hand-held Devices

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.

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.

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. Figure below shows the different types of mobility and their implications.

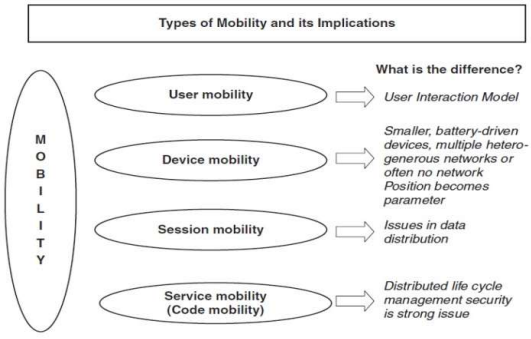
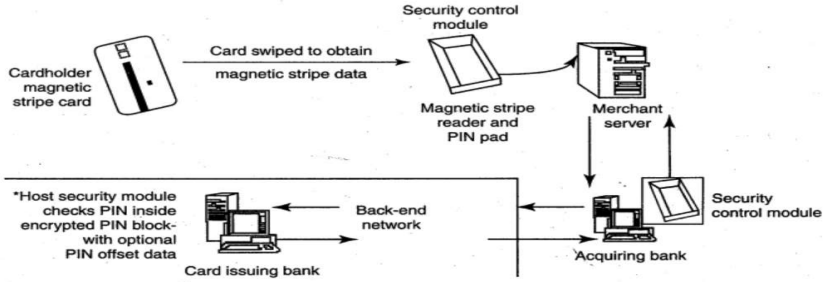


Figure 3.3 | Mobility types and implications.

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. Today belongs to "mobile compüting," that is, anywhere anytime computing. The developments in wireless technology have fuelled this new mode of working for white collar workers. This is true for credit card processing too; 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



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

1. Merchant sends a transaction to bank
2. The bank transmits the request to the authorized cardholder
3. The cardholder approves or rejects (password protected)
4. The bank/merchant is notified
5. The credit card transaction is completed.

Figure : Online environment for credit card transactions

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. When people are asked about important in managing a diverse range of mobile devices, they seem to be thinking of the ones shown in below figure.

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."

Security challenges posed by mobile devices:

- One at the device level: **microchallenges**
- Another at the organization level: **macrochallenges**

Well know challenges in mobile security:

- Managing the registry setting and configuration
- Authentication Service Security
- Cryptography Security
- Lightweight Directory Access protocol(LADP) Security
- Remote Access Server(RAS) security
- Media Player Control Security
- Network Application Program Interface (API) security

1.Registry settings for mobile devices: example

- Microsoft Active Sync : synchronize PCs and MS Outlook
- Gateway between Windows-Powered PC and Windows mobile-Powered device
- Enables transfer of Outlook information, MS Office documents, pictures, music, videos and applications
- Active sync can synchronize directly with MS Exchange Sever so that the user can keep their E-Mails, calendar, notes and contacts updated wirelessly.

Managing the registry setting and configuration:

- If you use an Active Directory® environment to administer the computers in your network, Group Policy provides a comprehensive set of policy settings to manage Windows® Internet Explorer® 8 after you have deployed it to your users' computers.
- You can use the Administrative Template policy settings to establish and lock registry-based policies for hundreds of Internet Explorer 8 options, including security options.
- 1700 settings in a standard group policy
- Even if the user go through every control panel setting and group policy option- no desired baseline security
- So make additional registry changes that are not exposed to any interface: avoid "registry hacks"

Example

- When using Pick-IT ASP in Internet Explorer, the SIP (software input panel, or virtual keyboard) will pop up when a textbox is activated. We cannot control this panel through Pick-IT.

  The method disables this SIP, depending on your mobile device model and operating system.

2. Authentication Service Security

Two components of security in mobile computing:

1. Security of devices
2. Security in Networks
   - Involves mutual authentication between the device and the base station/ servers.
   - Ensures that only authenticated devices can be connected to the network
   - Hence, no malicious code can impersonate the service provider to trick the device.

Eminent kinds of attacks on mobile devices:

- Push attacks
- Pull attacks
- Crash attack

Attacks on Mobile/ cell phones

- Mobile Phone Theft
- Mobile Viruses
- Mishing
- Vishing
- Smishing
- Hacking bluetooth

Mobile phone theft

With mobiles or cell phones becoming fancier, more popular, and more expensive, they are increasingly liable to theft.

The following factors contribute for outbreaks on mobile devices:

1. **Enough target terminals:** first mobile virus in 2004 :- Mosquito – this virus sent SMS text messages to the organization(Ojam)
2. **Enough functionality:** office functionality, critical data and applications protected insufficiently or not at all.
   expanded functionality increases the probability of malware
3. **Enough connectivity:** SMS, MMS, Synchronization, bluetooth, infrared(IR) and WLAN connections

How to Protect a Mobile Phone from Being Stolen

- **Keep details.** Make a record of all your phone information and keep this in a safe place. Include the following elements in the information: Your phone number
- The make and model
- Color and appearance details
- The pin or security lock code
- The IMEI number (on GSM phones)
  - International Mobile Equipment Identity

2. Mobile Viruses

- 40 virus families
- 300+ mobile viruses identified
- First mobile virus : june 2004
- Spread through dominant communication protocols
  - Bluetooth, MMS

How to protect from mobile malware attacks

- Download or accept progrms and content only from a trusted source
- Turn off bluetooth or set it to non-discoverable when not in use
- Receive IR beams only from trusted source
- Install antivirus software

3. Mishing

- 'Mishing' is a combination of the words mobile phone and phishing.
- Mishing is very similar to phishing—the only difference is the technology.
- Phishing involves the use of emails to trick you into providing your personal details, whereas mishing involves mobile phones.
- If you use your mobile phone for purchasing goods and services and convenient banking, you could be more vulnerable to a mishing scam.

Variants of Mishing

- Vishing : Mishing attacker makes call for phishing
- Smishing: Mishing attacker sends SMS for phishing

Vishing

- The term "vishing" is a socially engineered technique for stealing information or money from consumers using the telephone network.
- The term comes from combining "voice" with "phishing," which are online scams that get people to give up personal information.
- Vishing is very similar to phishing—the only difference is the technology.
- Vishing involves voice or telephone services. If you use a Voice over Internet Protocol (VoIP) phone service, you are particularly vulnerable to a vishing scam.
- Vishing is usually used to steal credit card numbers or other related data used in ID theft schemes from individuals.

Profitable uses of the information gained through a Vishing attack include:

- ID theft
- Purchasing luxury goods and services
- Transferring money/ funds
- Monitoring the victims bank accounts
- Making applications for loans and credit cards

Smishing

- Short for SMS Phishing, smishing is a variant of phishing email scams that instead utilizes Short Message Service (SMS) systems to send bogus text messages.
- Also written as SMiShing, SMS phishing made recent headlines when a vulnerability in the iPhone's SMS text messaging system was discovered that made smishing on the mobile device possible.

How smishing works?

- Smishing scams frequently seek to direct the text message recipient to visit a website or call a phone number, at which point the person being scammed is enticed to provide sensitive information such as credit card details or passwords.
- Smishing websites are also known to attempt to infect the person's computer with malware.

Example

Text message originating from either notice@jpecu or message@cccu :

- ABC CU – has –deactivated – your Debit_card. To reactivate contact:210957XXXX

This is an automated message from ABC Bank.

- Your ATM card has been suspended. To reactivate call urgent at 1 866 215 XXXX

Text message originating from sms.alert@visa.com :

- sms.alert@visa.com/VISA. (Card Blocked) Alert. For more information please call 1-877-269-XXXX

How to protect from Smishing attacks?

- Do not answer a text message
- Avoid calling any phone numbers
- Never click on a hot link received through messages

Hacking bluetooth

- Bluetooth hacking is a technique used to get information from another Bluetooth enabled device without any permissions from the host.
- This event takes place due to security flaws in the Bluetooth technology.
- It is also known as Bluesnarfing.
- Bluetooth hacking is not limited to cell phones, but is also used to hack PDAs, Laptops and desktop computers.
- Bluetooth hacking is illegal and can lead to serious consequences.

- The hacker can steal, delete contacts
- Hacker can extract personal files/pictures etc
- Your cell phone can be used for making calls and using internet at your expense
- The hacker may call or text your contacts to annoy them
- You mobile phone can be reset to default factory settings hence deleting your personal settings
- Hacker can even access your calendar, clock, International Mobile Equipment Identity (IMEI) number. IMEI number can be used to clone your cell phone so that your messages are also routed to another number. Cloning is also considered illegal.

Mobile Devices: Security Implications for Organizations

1. Managing diversity and proliferation of Hand-Held devices
2. Unconventional/ stealth storage devices
3. Threat through lost and stolen devices
4. Protecting data on lost devices
5. Educating the laptop users

1. Managing diversity and proliferation of Hand-Held devices

- Employees aren't just bringing their mobile devices to the workplace—they're *living* on them
- As smartphones and tablets become constant companions, cyber attackers are using every avenue available to break into them.
- With the right equipment, hackers can gain access to a nearby mobile device in less than 30 seconds and then;
  - either mirror the device and see everything on it, or
  - install malware that will enable them to siphon data from it at their leisure.
- Analysts predict that, 25 percent of corporate data will completely bypass perimeter security and flow directly from mobile devices to the cloud.
- Chief information security officers (CISOs) and other security executives are finding that the proliferation of mobile devices and cloud services are their biggest barriers to effective breach response.
- Given the threats to information systems through usage of mobile devices, the organizations need to establish security practices at a level appropriate to their security objectives, subject to legal and other external constraints.

2. Unconventional/ stealth storage devices

- We would like to emphasize upon widening the spectrum of mobile devices and focus on secondary storage devices, such as CDs, USB drives 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.
- Firewall n antivirus are no defense against the threats by open USB ports.

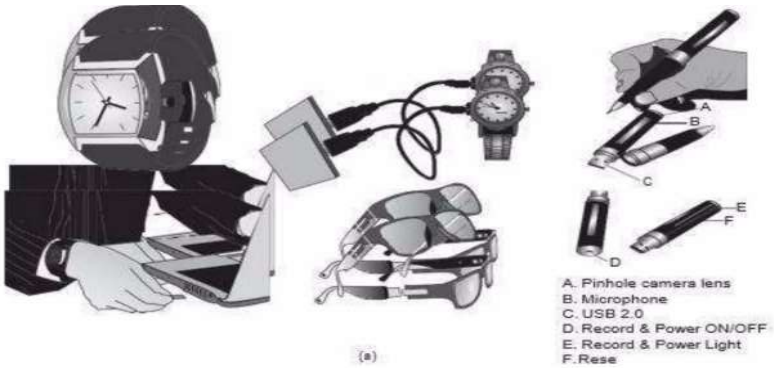


Fig: Unconventional/stealth storage devices.

3. Threats through lost and stolen devices

- This is a new emerging issue for cyber security.
- 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.

4. Protecting data on lost devices

- At an individual level, employees need to worry about this.
- 2 reasons cybersecurity need to address this issue;
    - Data persistently stored on devices and,
    - Always running applications.
- To protect stored data on device 2 precautions can be taken by individuals;
    - Encrypting sensitive data and,
    - Encrypting entire file system.
- A key point is that organization should have clear policy on how to respond to the loss or theft of a device.
- There should be method for device owner to quickly report the loss and device owner should be aware of this method.

5. Educating the laptop users

- Often it so happens that corporate laptop users could be putting their company's networks at risk by down- loading non-work-related software capable of spreading viruses and Spyware.
- No free downloads
- Illegal music files and movies
- But survey say that 86% employees do this.

Organizational Measures for Handling Mobile Devices-Related Security Issues

In this we discuss what organizations can do toward safeguarding their information systems in the mobile computing paradigm.

- Encrypting Organizational Databases
- Including Mobile Devices in Security Strategy

Encrypting Organizational Databases

- Critical and sensitive data reside on databases [say, applications such as CRM that utilize patterns discovered through data warehousing and data mining (DM) techniques] and with the advances in technology, access to these data is not impossible through hand-held devices.
- It is clear that to protect the organizations' data loss, such databases need encryption.
- Two algorithms that are typically used to implement strong encryption of database files;
    - Rijindael
    - AES (block encryption algorithm)
- The other algorithm is Multi-Dimensional Space Rotation(MDSR) algorithm developed by Casio.

Including Mobile Devices in Security Strategy

- The discussion so far makes a strong business case – in recognition of the fact that our mobile workforce is on the rise, organizational IT departments will have to take the accountability for cyber security threats that come through inappropriate access to organizational data from mobile-device–user employees.

- Encryption of corporate databases is not the end of everything.

A few things that enterprises 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.

Organizational Security Policies and Measures in Mobile Computing Era

1. Importance of Security Policies relating to Mobile Computing Devices

2. Operating Guidelines for Implementing Mobile Device Security Policies

3. Organizational Policies for the Use of Mobile Hand-Held Devices

Organizational security Policies and Measures in Mobile Computing Era:

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.

Laptops

Physical security counter measures

1. Cables and hardwires locks
2. Laptop safes
3. Motion sensors and alarms
4. Warning labels and stamps
5. Other measures for protecting laptops such as;
    1. Engraving the laptop with personal details
    2. Keeping the laptop close to oneself wherever possible
    3. Carrying laptops in a different and unobvious bags