# Cybercrime: Mobile and Wireless Devices

By: Dr. Ritika Ladha

Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era, Laptops

# Introduction

- In the modern era, the rising importance of electronic gadgets(i.e mobile hand held devices) brings many challenges to secure devices from being the victim of cybercrime.
- ***Mobile computing:*** is taking a computer and all necessary files and software out into the field.
- ***Wireless:*** method of transferring information between a computing device(such as PDA) and data source(database server) without physical connection.
- ***Smart hand-held devices:*** hand held or pocket sized devices that connect to a wireless or a cellular network and can have a software installed on them.

- Mobile computing does not necessarily require wireless communication .In fact,it may not require communication among devices at all.
- Wireless is a subset of mobile
- An application can be mobile without being wireless.

# Types of mobile computers

- **Portable Computer:** general purpose computer that can be easily moved from one place to another, but cannot be used during transit because it may need some setting up or AC power supply.

- **Tablet PC:** It is shaped like a slate or paper notebook, lacks keyboard and has features of touch screen with stylus and handwriting recognition software.

- **Internet tablet:** Internet appliance in tablet form. No much computing power and applications suite is limited. Eg: MP3 and video player, web browser, chat application, picture viewer.

- **Personal Digital Assistant(PDA):**Small, pocket sized computer with limited functionality. It is intended to supplement and synchronise with desktop computer giving access to contacts, address book, notes, email and other features

- **Ultramobile PC**: Full featured PDA sized computer running a general purpose OS.

- **Smartphone:** PDA with an integral cell phone functionality, wide range of features and installable applications.

- **Carputer :**Computing device installed in an automobile. It operates as a wireless computer, sound system, global positioning system, DVD player. Also has word processing software and is Bluetooth compatible.

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

# Trends in mobility

- User Mobility: User interaction Model
- Device Mobility: Smaller, battery driven devices, multiple heterogeneous networks or often no network position becomes parameter
- Session Mobility :Issues in data distribution
- Service Mobility(Code Mobility): Distributed life cycle management ,security is strong issue.

# Key findings of Mobile computing security scenario

- With usage experience, awareness of mobile users gets enhanced
- People continue to remain the weakest link for laptop security
- Wireless connectivity does little to increase burden of managing laptops.
- Laptop experience changes the view of staring a smart hand-held pilot.
- There is naivety and/or neglect in smart hand held security
- Rules rather than technology keep smart hand held's usage in check.

# Popular types of attacks on 3G mobile networks

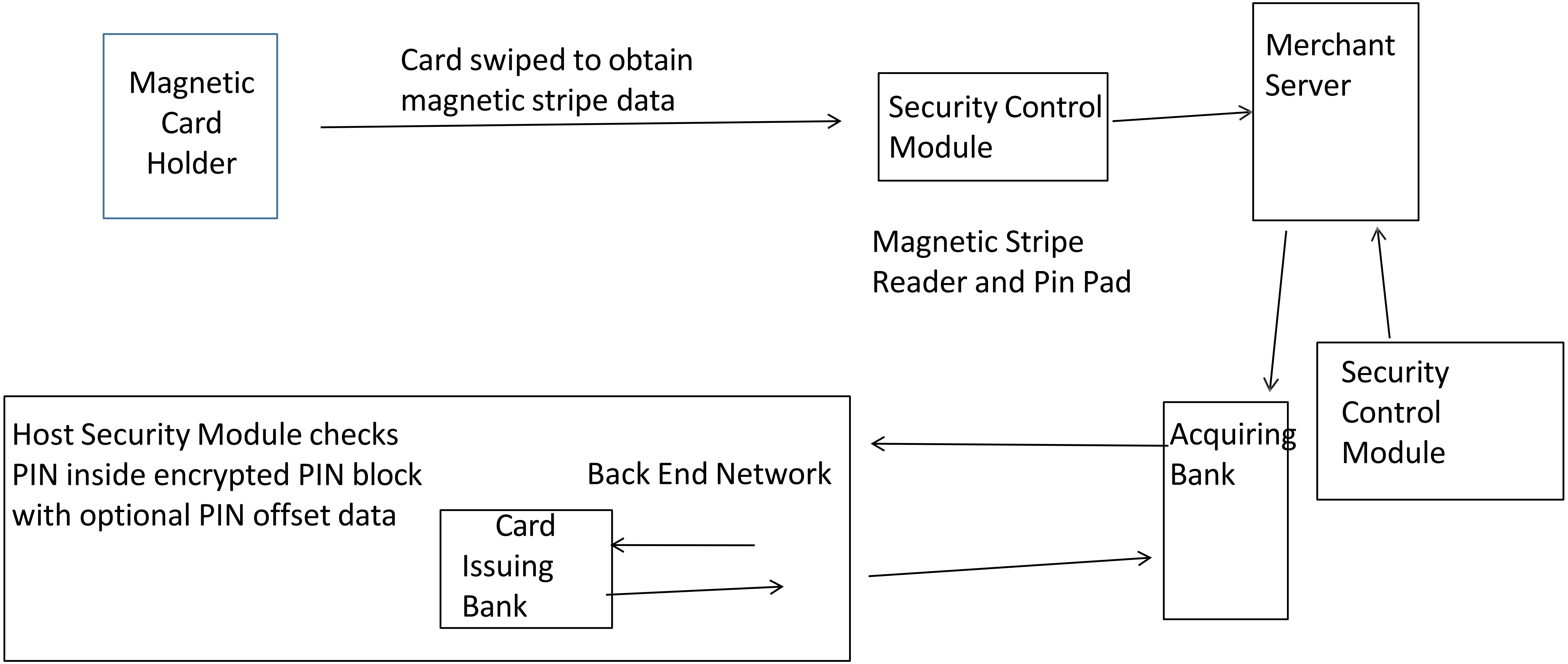
- **Malwares, viruses and worms:**
  - ***Skull Trojan***: It targets series 60 phones with Symbian mobile OS
  - ***Cabir Worm***: First dedicated mobile phone worm, infects phones running on Symbian OS and scans other mobile devices to send a copy of itself to the first vulnerable phone it finds through Bluetooth wireless technology. Source code for cabir-h and cabir –I available online
  - ***Mosquito Trojan: Affects*** 60's series Smartphone and cracked version of "Moquitos" mobile phone game.
  - ***Brador Trojan***: Affects windows CE OS by creating 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 such as Email file attachments.
  - ***Lasco Worm: Released*** in 2005 to attack PDA's and mobiles running Symbian OS.Based on Cabir's source code and replicates over Bluetooth connection.

- **Denial of Service(Dos)**: Make the target system unavailable for intended users. Flood the target system with requests so that it slows down or remains unavailable to process genuine requests.
- **Overbilling attack**: An attacker hijacking a subscriber's IP address and then using it to initiate downloads that are nit free or simply use it for his/her own purposes. In either case ,legitimate user is the charged for the activity which the user did not conduct or authorize to conduct.
- **Spoofed policy development process(PDP)**: exploit vulnerabilities in the General Packet Radio Service(GPRS) Tunnelling Protocol(GTP)
- **Signaling level attacks**: Session Initiation Protocol(SIP) is a signalling protocol used in IP multimedia subsystem(IMS) networks to provide Voice over Internet Protocol(VoIP) services.

# Credit Card Frauds in Mobile and Wireless Computing Era

- There are new trends in cyber crime 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.

# Online environment for credit card transactions



Magnetic Card Holder
Card swiped to obtain magnetic stripe data
Security Control Module
Merchant Server
Magnetic Stripe Reader and Pin Pad
Security Control Module
Acquiring Bank
Back End Network
Host Security Module checks PIN inside encrypted PIN block with optional PIN offset data
Card Issuing Bank

# Tips to prevent credit card frauds

## Do’s

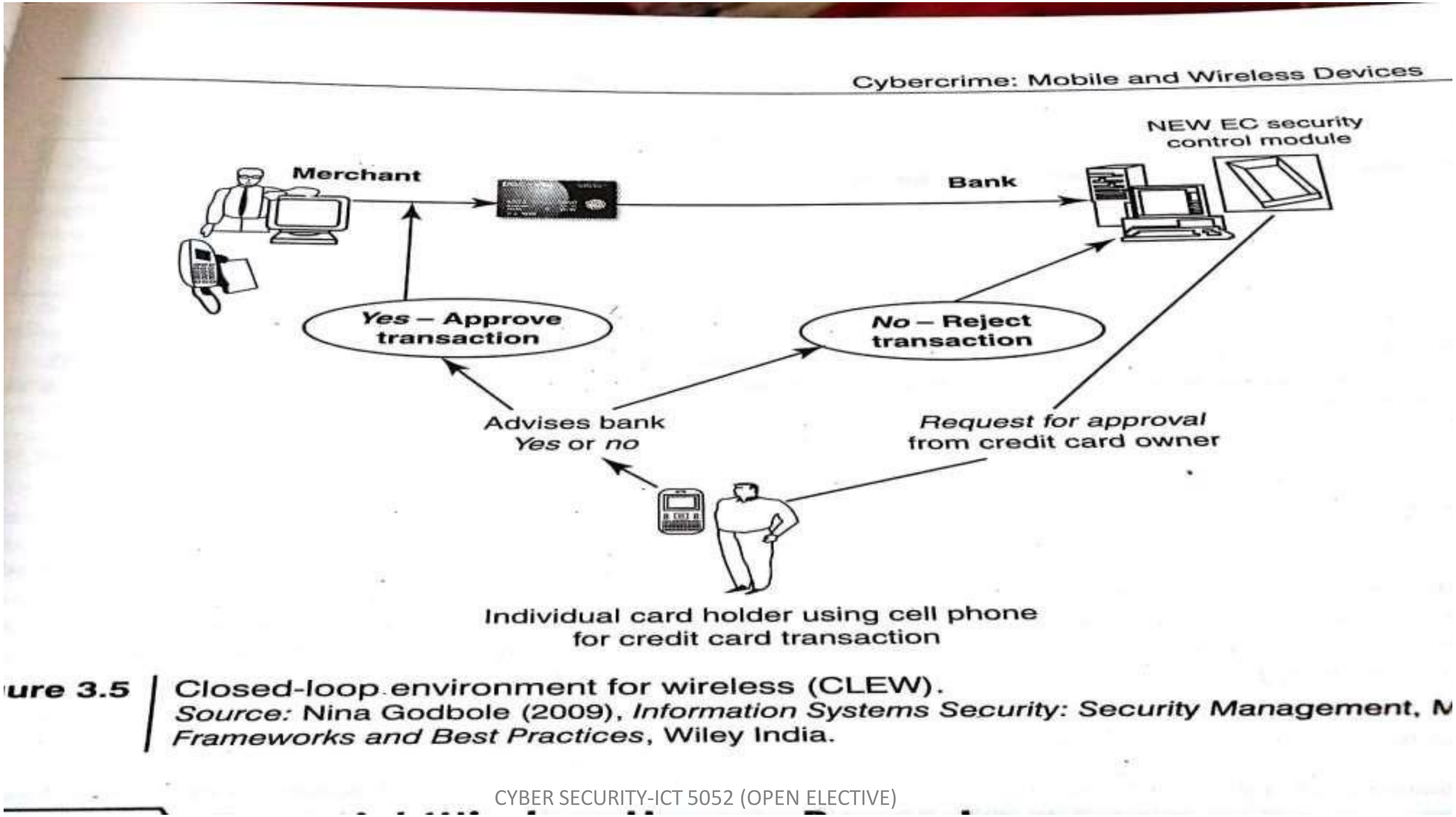
- Put your signature on the card immediately upon its receipt.
- Make photocopy of both he sides of your card and preserve it at a safe place to remember the card number, expiration date in case of loss of card.
- Change the default pin received from bank before doing any transaction
- Always carry the details about contact numbers of your bank in case of loss of your card.
- Carry your cards in a separate pouch or card holder than your wallet.
- Keep an eye on your card during the transaction and ensure to get it back immediately
- Preserve all the receipts to compare with the credit card invoice.

- Reconcile your monthly invoice/statement with your receipts
- Report immediately if any discrepancy observed in monthly invoice/statement
- Discard all the receipts after reconciling it with the monthly invoice statements
- Inform your bank in advance, about any changes in your contact details such as home address, cell phone number, email.
- Ensure Legitimacy of the website before providing any of your card details.
- Report the loss of card immediately in your bank and at the police station ,if necessary.

## Dont’s

- Store your card number and pin in your cell
- Lend your cards to anyone
- Leave cards or transaction receipt lying around
- Sign a blank receipt
- Write your card number/PIN on a postcard or outside of any envelope
- Give out immediately your account number over the phone
- Destroy credit card receipts by simply dropping into garbage/dustbin

# Closed Loop Environment for Wireless(CLEW)



Cybercrime: Mobile and Wireless Devices

NEW EC security control module
Merchant
Bank
Yes – Approve transaction
No – Reject transaction
Advises bank Yes or no
Request for approval from credit card owner
Individual card holder using cell phone for credit card transaction

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

# CLEW

- Merchant sends a transaction to the bank
- Bank transmits the request to the authorised cardholder
- Cardholder approves or rejects (password protected)
- Bank/merchant notified
- Credit card transaction is completed.

# Elements of Credit Card Fraud

Debit/credit card fraud is thus committed when a person
1) fraudulently obtains, takes, signs, uses, sells, buys, or forges someone else’s credit or debit card or card information;
2) uses his or her own card with the knowledge that it is revoked or expired or that the account lacks enough money to pay for the items charged; and
3) sells goods or services to someone else with knowledge that the credit or debit card being used was illegally obtained or is being used without authorization.

# Types of Credit Card Fraud

The first category, **lost or stolen cards,** is a relatively common one, and should be reported immediately to minimize any damages.

The second is called **“account takeover”** — when a cardholder unwittingly gives personal information (such as home address, mother’s maiden name, etc.) to a fraudster, who then contacts the cardholder’s bank, reports a lost card and change of address, and obtains a new card in the soon-to-be victim’s name.

The third is **counterfeit cards** — when a card is “cloned” from another and then used to make purchases.

The fourth is called **“never received”** — when a new or replacement card is stolen from the mail, never reaching its rightful owner.

The fifth is **fraudulent application**— when a fraudster uses another person’s name and information to apply for and obtain a credit card.

The sixth is called **“multiple imprint”**— when a single transaction is recorded multiple times on old-fashioned credit card imprint machines known as “knuckle busters”.

The seventh is **collusive merchants** — when merchant employees work with fraudsters to defraud banks.

# 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 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

Sophisticated techniques enable criminals to produce fake and doctored cards. Then there are also those who use skimming to commit fraud. 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.

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.

   The entire investigation process for tracking and reaching these criminals is time-consuming, and the criminals may close such fake website in between the process that may cause further difficulty to trace the criminal. The criminals aim to create a great deal of confusion for the authorities so that they can operate long enough to accumulate a vast amount of goods purchased through such fraudulent transactions.

- **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.

# Attacks on Mobile /Cell phones

1. Mobile Phone Theft
2. Mobile viruses
3. Mishing
4. Vishing
5. Smishing
6. Hacking Bluetooth

# Mobile Phone Theft

- Theft of mobile phones have risen dramtically over the years
- Theft occurs mainly at bus stops,buses, railway stations, trains,traffic signals etc
- Many Insurance companies have stopped offering Mobile Theft insurance due to false claims.

# 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.
- Add a security mark on your cell phone.
- Set a password and ensure the password is strong enough so that a finder of your cell phone cannot easily guess it.
- In case of loss of your cell phone, register a complaint with cell phone service provider immediately, using your IMEI number, to enable your service provider to block your cell phone and your account details.
- In case of loss of your cell phone, register a complaint at the police station and obtain FIR.

- Keep an eye on your mobile phone while travelling. During security check at airport security, ensure to retrieve your cell phone immediately after it enters the x-ray machine.
- Keep wifi and Bluetooth off when not in use.
- Periodic backup is important especially when travelling.
- Update cell phones regularly
- Update antivirus software regularly

## Antitheft software on your cell phone

- GadgetTrak
- Back2u
- Wavesecure
- F-Secure

## 1. GadgetTrak

**Location Tracking:** Uses GPS, Wi-Fi, and cell tower triangulation to locate the stolen device.
**Remote Control:** Owner can lock or wipe the device remotely.
**Theft Detection:** Can secretly capture photos of the thief using the front camera.
**Report Generation:** Provides detailed reports with location and device information to help recover it.

**2. Back2u**

**Tracking & Alerts:** Sends an SMS with the phone’s current location when the SIM card is changed.
**Anti-SIM Swap Protection:** Notifies the real owner if someone tries to replace the SIM.
**Remote Lock:** Allows the owner to lock the device to prevent misuse.
**Theft Alerts:** Sends alerts to pre-defined contacts to help trace the device.

## Wavesecure (later acquired by McAfee)

**Backup & Restore:** Regularly backs up contacts, SMS, photos, and call logs to the cloud.
**Remote Lock & Wipe:** Enables locking or erasing data remotely to prevent unauthorized access.
**SIM Change Alerts:** Notifies the owner if someone inserts a new SIM.
**Location Tracking:** Tracks the phone’s location in real time.
**Data Restore:** After recovery or on a new device, data can be restored easily.

## F-Secure (Anti-Theft)

**Remote Lock:** Lock your phone instantly via SMS if stolen.
**Remote Wipe:** Erase all sensitive data remotely to protect privacy.
**Locate:** Pinpoints the phone’s location using GPS.
**SIM Watch:** Detects unauthorized SIM changes and alerts the owner.
**Alarm Feature:** Allows triggering a loud alarm to help locate the device nearby.

## Common Benefits Across All

Protects **personal and financial data**.
Helps in **recovering stolen devices**.
Reduces chances of **SIM misuse**.
Provides peace of mind with **remote monitoring and control**.

| Feature / Software | GadgetTrak | Back2u | Wavesecure | F-Secure |
|---|---|---|---|---|
| **Location Tracking (GPS/Wi-Fi/Cell ID)** | ✅ Yes | ✅ Yes (via SMS alerts) | ✅ Yes | ✅ Yes |
| **Remote Lock** | ✅ Yes | ✅ Yes | ✅ Yes | ✅ Yes |
| **Remote Wipe (Erase Data)** | ✅ Yes | ❌ No | ✅ Yes | ✅ Yes |
| **SIM Change Alert** | ✅ Yes | ✅ Yes | ✅ Yes | ✅ Yes |
| **Theft Detection (e.g., photo capture of thief)** | ✅ Yes (stealth camera) | ❌ No | ❌ No | ❌ No |
| **Data Backup & Restore** | ❌ No | ❌ No | ✅ Yes (contacts, SMS, photos) | ❌ No |
| **Alarm / Siren** | ❌ No | ❌ No | ❌ No | ✅ Yes |
| **Report Generation** | ✅ Detailed reports (location, device info) | ❌ No | ❌ No | ❌ No |
| **Special Focus** | Device recovery with forensic evidence | SIM protection & alerts | Data protection + restore | Strong lock/wipe + alarm |

# Factors that 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 and WLAN connections. Therefore, unfortunately, the increased amount of freedom also offers more choices for virus writers.

# Mobile Viruses

- Similar to computer virus that targets mobile phone data or applications installed in it.
- In total,40 mobile virus families and more than 300(+) mobile viriuses have been identified.
- Mobile virus spreads through Bluetooth and MMS.
- Bluetooth virus can easily spread within a distance of 10-30m.
- MMS virus can send a copy of itself to the contact list of victim’s phone.
- Mobile phone virus hoax have been circulating since 1999.

# Cell-phone Viruses

Cabir.A

- First reported: June 2004
- Attacks: Symbian Series 60 phones
- Spreads via: Bluetooth
- Harm: none

Skulls.A

First reported: November 2004

Attacks: various Symbian phones

Spreads via: Internet download

Harm: disables all phone functions except sending/receiving calls

- Commwarrior.A
- First reported: January 2005
- Attacks: Symbian Series 60 phones
- Spreads via: Bluetooth and MMS
- Harm: sends out expensive MMS messages to everyone in phonebook (in course of MMS replication)

- Locknut.B
- First reported: March 2005
- Attacks: Symbian Series 60 phones
- Spreads via: Internet download (disguised as patch for Symbian Series 60 phones)
- Harm: crashes system ROM; disables all phone functions; inserts other (inactive) malware into phone

# How to protect 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.

# Mishing

- Is a combination of mobile phone and phishing.
- 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 known as smishing.
- Attacker will pretend to be an employee from your bank or another organization and will claim a need for your personal details.
- Attackers are very creative and they would try to convince you with different reasons why they need this information from you.

# 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.

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 victim’s bank accounts;
5. Making applications for loans and credit cards.

# How Vishing works

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

1. Internet E-Mail: It is also called Phishing mail.
2. Mobile text messaging
3. Voicemail: Here, victim is forced to call on the provided phone number, once he/she listens to voicemail.
4. Direct phone call: Following are the steps detailing on how direct phone call works:

- The criminal gathers cell/mobile phone numbers located in a particular region and/or steals cell/mobile phone numbers after accessing legitimate voice messaging company.
- The criminal often uses a war 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 harvest additional details such as date of birth, credit card expiration date, etc.

# 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.

# Smishing

- Is a criminal offense conducted by using social engineering techniques similar to Phishing. The name is derived from “SMS PhISHING”.
- Smishing uses cell phone text messages to deliver a lure message to get the victim to reveal his/her PI. Smishing uses cell phone text messages to deliver a lure message to get the victim to reveal his/her PI. The popular technique to hook the victim is either provide a phone number to force the victim to call or provide a website URL to force the victim to access the URL, wherein, the victim gets connected with bogus website and submits his/her PI.
- Smishing works in the similar pattern as Vishing. A few examples of Smishing are provided herewith to demonstrate how the victim is forced to disclose PI.

1. “We are happy to send our confirmation toward your enrolment for our club membership. You will be charged Rs.50 per day, unless you reconfirm your acceptance of your membership on our membership contact number.
2. “Name of popular online bank is confirming that you have purchased LCD TV set, worth Rs.90000 only from name of popular computer company. Visit www.abcdef.com if you did not make this online purchase.

# 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.

# Hacking Bluetooth

- Bluetooth is a wireless technology standard used for communication over short distances between fixed and/or mobile devices.
- When Bluetooth is enabled on a device, it essentially broadcasts that its available to any other Buetooth-based device within a range.
- This makes easier for attackers to identify the target.
- The attacker installs special software 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, calenders, SIM card details, make long distance phone calls using the hacked device.

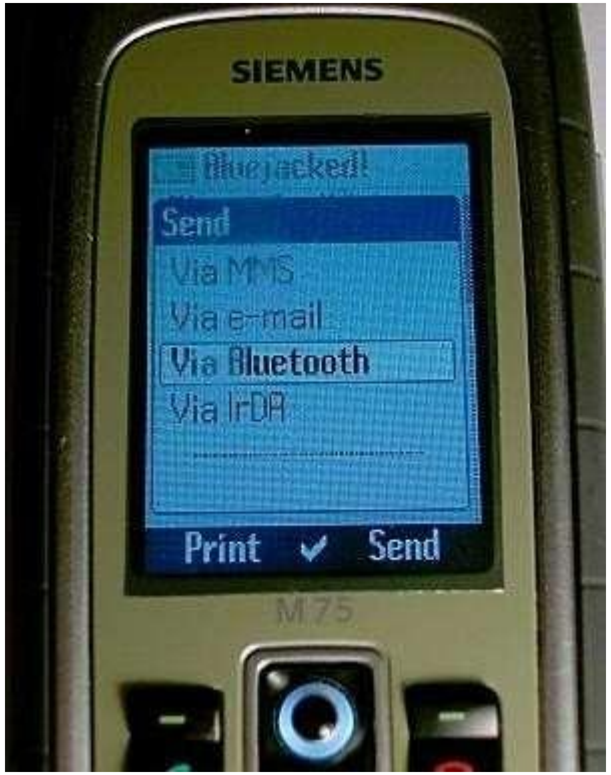
# Bluetooth hacking tools

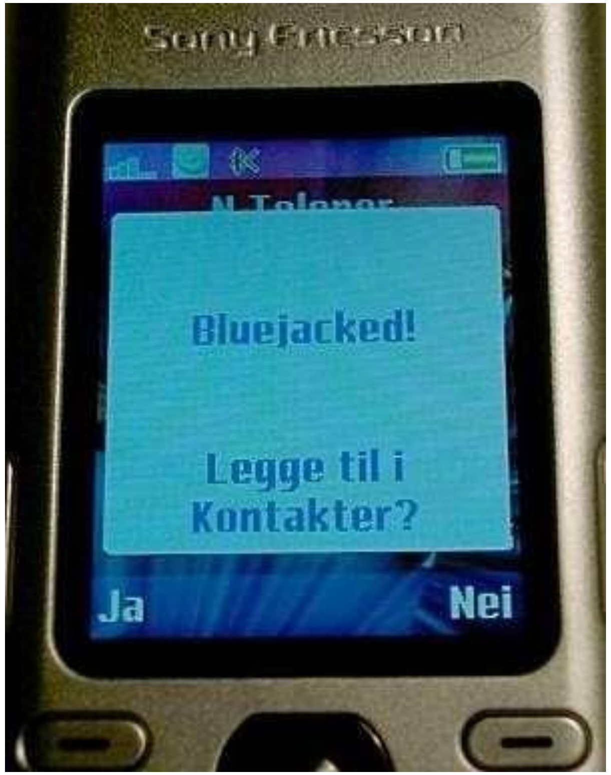
1. **BlueScanner**-This tool enables to search for Bluetooth enable device and will try to extract as much information as possible for each newly discovered device after connecting with the target.
2. **BlueSniff**- This is a GUI-based utility for finding discoverable and hidden Bluetooth enabled devices.
3. **BlueBugger**-The buggers exploit the vulnerability of the device and access the images, phonebook, messages and other personal information.
4. **Bluesnarfer**- If a Bluetooth of a device is switched ON, then Bluesnarfing makes it possible to connect to the phone without alerting the owner and to gain access to restricted portions of the stored data.
5. **BlueDiving**- BlueDiving is testing Bluetooth penetration. It implements attacks like Bluebug and BlueSnarf.

# Common attacks that have emerged as Bluetooth-specific security issues:

- **Bluejacking**-Bluetooth+Jacking where jacking is a short name for hijack-act of taking over something. If the user does not recognize/realize what the message is, he/she might allow the contact to be added to her/his address book, and the contact can send him messages that might be automatically opened because they are coming from a known contact. Bluejacking is harmless, as bluejacked users generally do not understand what has happened and hence they may think that their phone is malfunctioning.

# Bluejacking example





- **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.

- **Bluebugging**-It allows attackers to remotely access a user’s phone and use its features without user’s attention. During initial days, the attacker could simply listen to any conversation his/her victim is having; however, further developments in Bluebugging tools have enabled the attacker with the ability to take control of the victim’s phone and to conduct many more activities such as initiate phone calls; send and read SMS; read and write phonebook contacts; eavesdrop on phone conversations and connect to the Internet.

- **Car Whisperer-** It is a piece of software that allows attackers to send audio to and receive audio from a Bluetooth-enabled car stereo. Further research is underway to know whether Bluetooth attackers could do anything more serious such as disabling airbags or brakes through this kind of attack. The researchers are also investigating about possibility of an attacker accessing a telephone address book once the connection gets established with the Bluetooth system through this kind of attack.

Among the four above-mentioned attacks, **Bluesnarfing** is claimed to be much more serious than Bluejacking.

# Mobile Security Implications for organizations

- Managing Diversity and Proliferation of hand held devices
- Unconventional/Stealth Storage Devices
- Threats through lost and stolen devices
- Protecting data on lost devices
- Educating laptop users

- **Managing diversity and proliferation of hand held devices**:
  - Mobile devices of employees must be registered in the corporate asset regiter whether or not the mobile phone is given by the given by the company.
  - Mobile devices that belong to the company must be returned to IT department and should be deactivated and cleansed.
  - Employees should be encouraged to register with IT department any device they use themselves so that the access can be provisoned accordingly and deprovisioned when the employee leaves.

- **Unconventional stealth and storage devices**
  - It advisable for prohibit employees to use devices like compact disks, USBs, Concealer pens, concealer goggles etc and stealth storage devices.

Stealth storage devices

- **Threats from lost or stolen devices**
  - If employees mobiles (mostly provided by companies) are lost or stolen it can put company at a serious risk of sabotage, exploitation or damage to its professional integrity.
  - These mobiles have wireless and remote access to a corporate network and have weak security making the weak link and headache for security administrators.

- **Protecting data on lost devices**
  - Encrypt sensitive data
  - Encrypt entire file system
  - Encrypting servers where database file resides
  - Enforce self destruct policy to destroy privileged data
  - Create database action to delete the data on a user’s device using suitable tool

- **Educating the laptop users**
  - Employees must be discouraged to :
    - download non-work related software capable of spreading virus and spyware and putting company's networks at risk.
    - Installing  unwanted soft wares to the company laptops or official laptops.
    - Downlaoding music ,movies etc

# Organizational measures for handling mobile-device-related security issues.

- Encrypting organizational databases.
- Including mobile devices in security strategy

# Mobile device security strategy in companies:

- Implement strong asset management, virus checking, loss prevention and other controls for mobile systems that will prohibit unauthorised access and the entry of corrupted data.
- Investigate alternatives that allow a secure access to the company information through a firewall such as mobile VPN.
- 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 an issue security is within a company's overall IT strategy
- Notify then appropriate law-enforcement agency and change passwords. User accounts are closely monitored for any unusual activity for a period of time.

# Operating guidelines for organizations for Implementing Mobile Device Security Policies

1. 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.
2. Implement additional security technologies, as appropriate to fit both the organization and the types of devices used. Most mobile computing devices will need to have their native security augmented with such tools as strong encryption, device passwords and physical locks.
3. 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.
4. 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.
5. Centralize management of your mobile computing devices. Maintain an inventory so that you know who is using what kinds of devices.

6. 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.

7. Label the devices and register them with a suitable service that helps return recovered devices to the owners.

8. 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.

9. Remove data from computing devices that are not in use or before re-assigning those devices to new owners(in case of company-provided mobile devices to employees).

10. 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.

# Laptops

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:** Kensington cables are one of the most popular brands in laptop security cables. These cables are made of aircraft-grade steel and Kevlar brand fiber, thus making these cables 40% stronger than any other conventional security cables. These cables come with a variety of options such as number locks, key locks and alarms. However, the downside of the security cables lies in the fact that one can easily remove detachable bays such as CD-ROM bay, Personal Computer Memory Card Industry Association cards, HDD bay and other removable devices from the laptop as the cable only secures the laptop from being stolen. The other disadvantage of security cables is when the laptop is locked to an object that is not fixed or is weak enough for anyone to break it.

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:** 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. Modern alarm systems for laptops are designed wherein the alarm device attached to the laptop transmits radio signals to a certain range around the laptop. The owner of the laptop has a key ring device that communicates with the laptop alarm device. The alarm is triggered when the distance between the laptop alarm device and the key ring device crosses the specified range. Also available are security PCMCIA cards that act as a motion detector, an alarm system, and also have the capability to lockdown the laptop if the laptop is moved out of the designated range. They also secure the passwords and encryption keys and prevent access to the OS. These cards have batteries that keep them powered on even when the system is shutdown.

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.

5. **Other measures for protecting laptops are as follows:**

- Engraving the laptop with personal details;
- Keeping the laptop close to oneself wherever possible;
- Carrying the laptop in 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 antitheft device;
- Disabling IR ports and wireless cards and removing PCMCIA cards when not in use.

Kensington

VAULT

GPS TRACKING ALARM
This vehicle protected by a GPS tracking alarm. In the event of theft, alarm will be activated and real time satellite GPS tracking data will be provided to law enforcement.
GPS TRACKING ALARM
This vehicle protected by a GPS tracking alarm. In the event of theft, alarm will be activated and real time satellite GPS tracking data will be provided to law enforcement.

PROPERTY OF
LifeWatch Technologies
LifeWatch
000165
Helpdesk 877-774-9846 x4357

Help Number

INSIGHT INT
01273 475500
Chemical Etching

# Most important management or support issues for laptops

- Operating system and patch management
- Network access configuration
- Deploying applications
- User abuse or misuse of laptops
- Replacing lost or damaged laptops
- Keeping track of numbers deployed
- Lack of user training

# 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 file 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 systems.
10. Encrypting critical file systems.
11. Other countermeasures:
    - Choosing a secure OS that has been tested for quite sometime and whih has high security incorporated into it.
    - Registering the laptop with laptop manufacturer to track down the laptop in case of theft
    - Disabling unnecessary user accounts and renaming the administrator account.
    - Disabling display of the last logged in username in the login dialogbox.
    - Backing up data on regular basis.