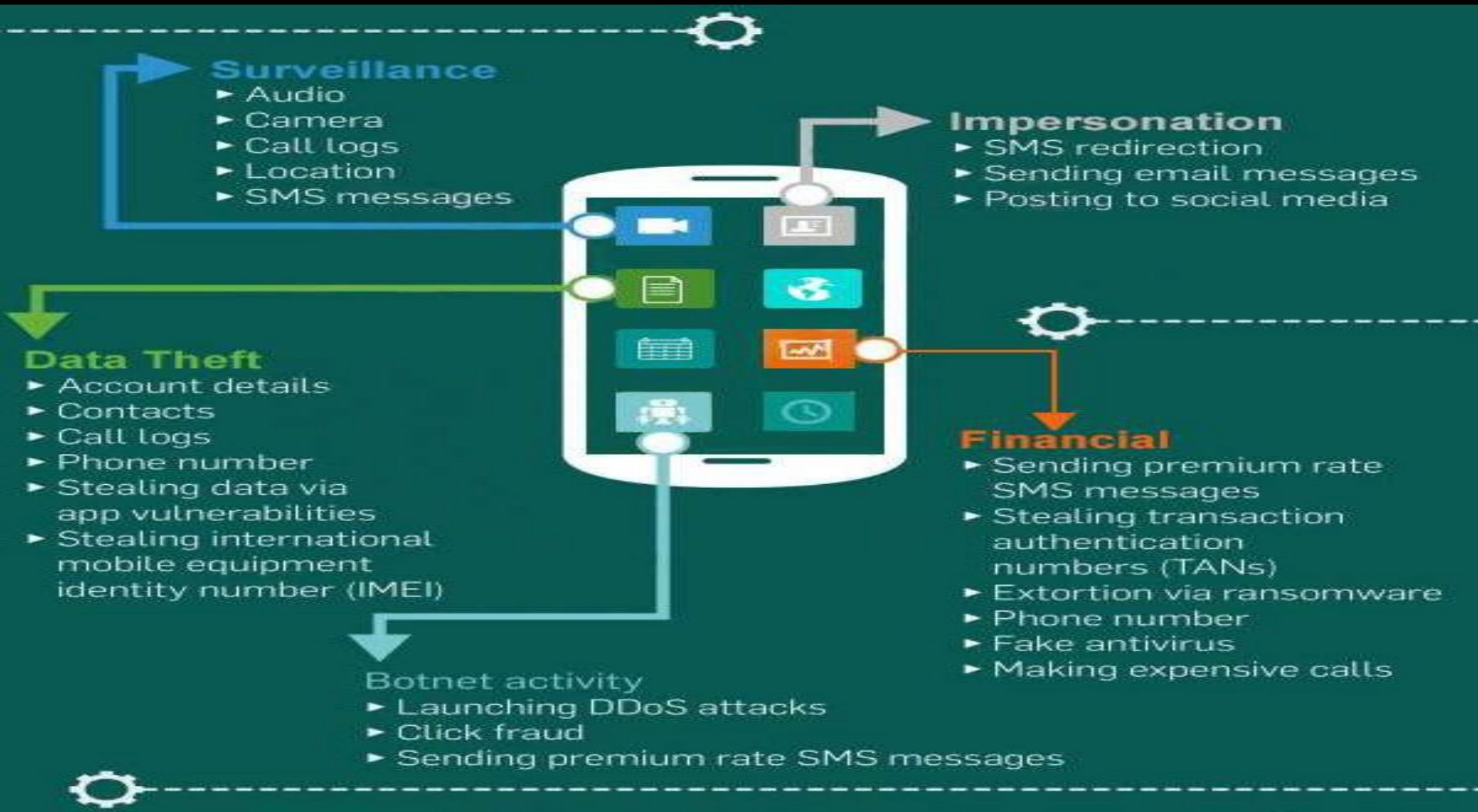
Security Vulnerabilities in Mobile Devices



Learning Objectives

- Understand the security challenges presented by mobile devices and information systems access in the cybercrime world.
- Understand challenges faced by the mobile workforce and implication under the cybercrime era.
- Mitigation strategy – credit card users.
- Security issues due to use of media players.
- Organizational security implications with electronic gadgets.
- Organizational measures for protecting information systems from threats in mobile computing area.
- Smishing, vishing attacks in mobile world.
- Security issues arising due to use of removable media- pen drives

Proliferation of mobile and wireless devices

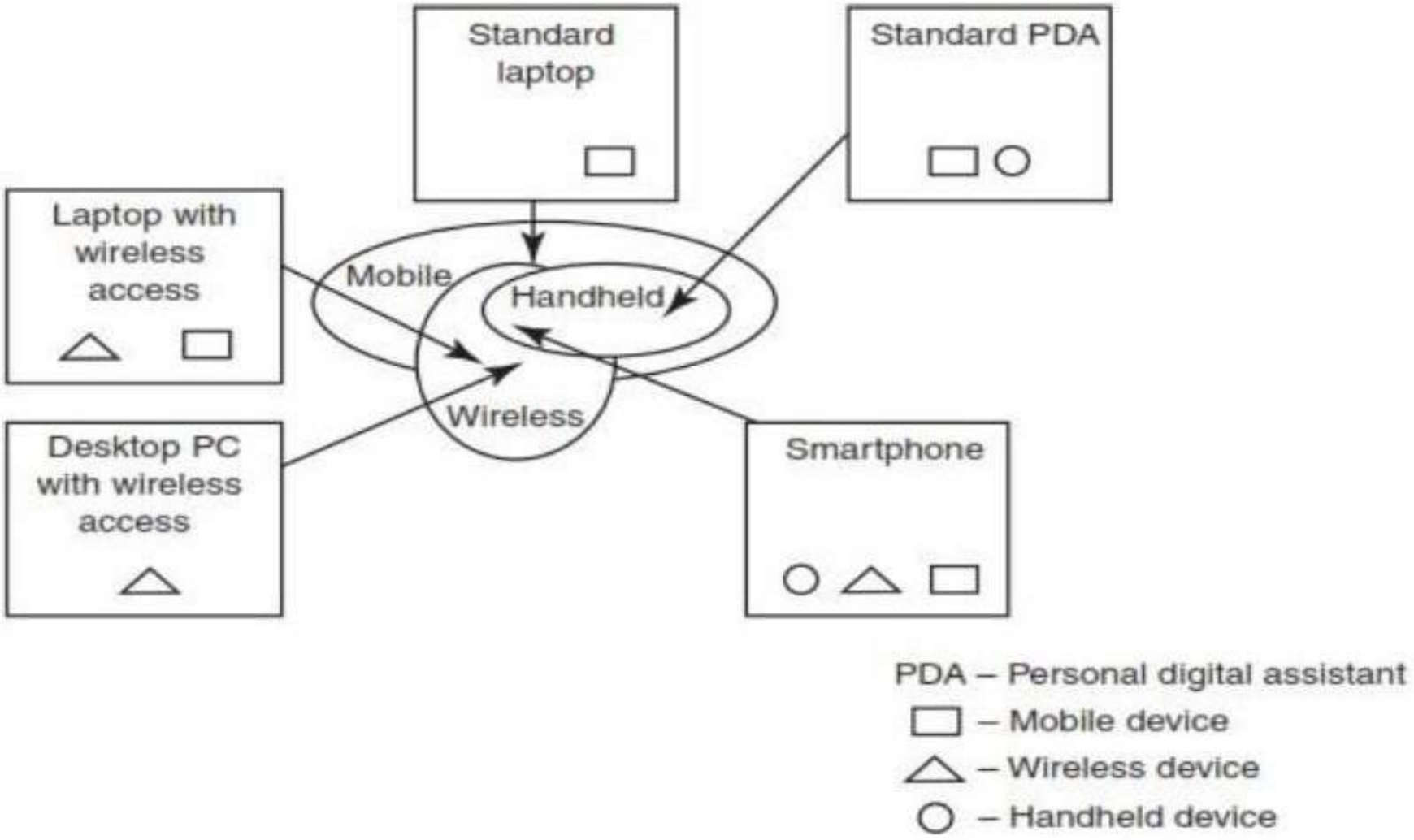
- You see them everywhere: people hunched over their smartphones or tablets in cafes, airports, supermarkets and even at bus stops, seemingly oblivious to anything or anyone around them.
- They play games, download email, go shopping or check their bank balances on the go.
- They might even access corporate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

Types of Mobile Computer

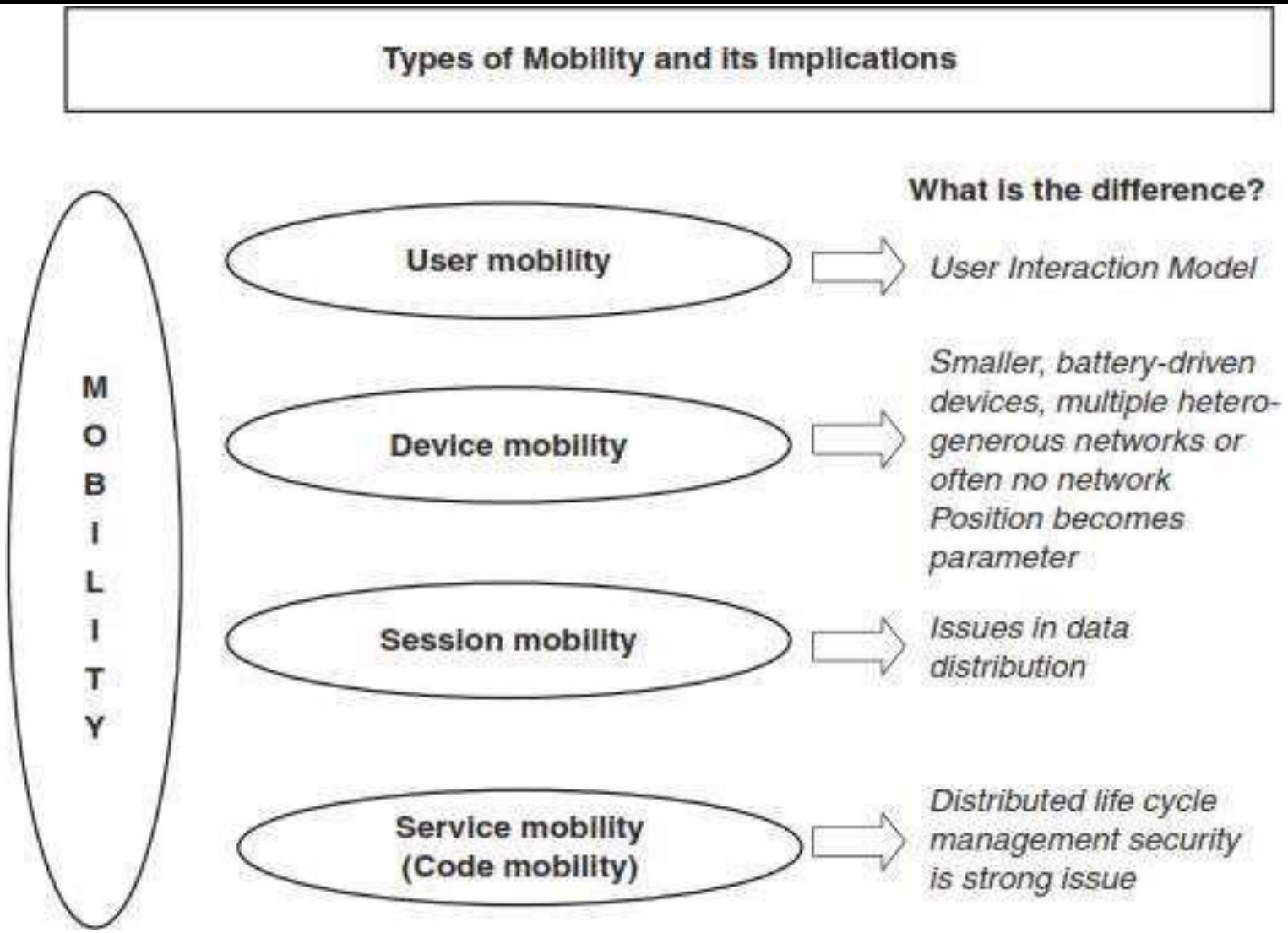
Many types of mobile computers have been introduced since 1990, as follows;

- Portable computer
- Tablet PC
- Internet Tablet
- PDA
- Ultramobile PC
- Smartphone
- Carputer
- Fly fusion Pen top computer

Mobile, Wireless Devices and hand-held devices



Trends in Mobility



Security?

- But as wireless devices become increasingly ingrained into our daily lives, they open the door to heightened security risks.

- Not only do such devices become points of access for cybercriminals, but they also may be more easily breached than personal computers since many consumers do not secure their smartphones or tablets with antivirus software or take simple precautions such as enabling password protection.

Risk factors

The dangers, of course, are plenty;

- Rogue mobile apps can record the information that users type into a device, such as bank account numbers and PINs.
-
- They can read data stored on a handset, such as emails, text messages, attachments, credit card numbers, and log-ins and passwords to corporate networks.

- A phone can even secretly record conversations within earshot.

Risk factors

- Data that leaves a mobile device wirelessly to connect to a Wi-Fi network could be hijacked in mid-air in "man in the middle" attacks.

- Consumers may not be as concerned about securing a wireless device because they do not view it as a small computer. "They think, 'Oh, it's just my phone.

- The risks are transferred to the workplace as more people bring their devices to the office for both personal and professional use, a phenomenon known as BYOD or "Bring Your Own Device."

Key Findings for Mobile Computing Security Scenario

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

Attacks against 3G mobile networks

- Malware, viruses and worms
  - Skull trojans
  - Cabir worm
  - Mosquito worm
- Denial-of-service
- Overbilling attack
- Spoofed policy development process
  - Exploits vulnerabilities of GTP (GPRS Tunneling Protocol)
- Signaling-level attacks
  - Exploits vulnerabilities of SIP (Session Initiation Protocol) used in IP Multimedia Subsystem (IMS) network to provide VoIP services.

Skull trojan

- A trojan horse piece of code that targets mainly Symbian OS.
- Once downloaded, the virus replaces all phone desktop icons with images of a skull.
- It also renders all phone applications useless.
- This malware also tends to mass text messages containing malicious links to all contacts accessible through the device in order to spread the damage.
- This mass texting can also give rise to high expenses.

Cabir worm

- This malware infects mobile phones running on Symbian OS and was first identified in June 2004.
- When a phone is infected, the message 'Caribe' is displayed on the phone's screen and is displayed every time the phone is turned on.
- The worm then attempts to spread to other phones in the area using wireless Bluetooth signals, although the recipient has to confirm this manually.

Mosquito worm

- In June 2004, it was discovered that a company called Ojam had engineered an anti-piracy Trojan virus in older versions of its mobile phone game, *Mosquito*.
- This virus sent SMS text messages to the company without the user's knowledge.
- Although this malware was removed from the game's more recent versions, it still exists in older, unlicensed versions, and these may still be distributed on file- sharing networks and free software download web sites.

Mobile Vulnerabilities

- Mobile devices often do not have passwords enabled.
- Two-factor authentication is not always used when conducting sensitive transactions on mobile devices.
- Wireless transmissions are not always encrypted
- Mobile devices may contain malware.
- Mobile devices often do not use security software.
- Operating systems may be out-of-date.
- Software on mobile devices may be out-of-date
- Mobile devices often do not limit Internet connections.
- Mobile devices may have unauthorized modifications.
- an unsecured WiFi network could let an attacker access personal information from a device, putting users at risk for data and identity theft.

Mobile Users' Tendency

- According to a Harris Interactive survey commissioned by CTIA, a wireless trade group,
  - less than half of all wireless device owners use passwords or personal identification numbers (PINs) on their handsets
  - Among those who conduct online banking on mobile devices, only half encrypt the data or use some form of security software.
  - Moreover, less than one third of users have installed antivirus software on their mobile devices compared to 91% on their laptops.
  - This may explain why: 45% do not see cybersecurity on their mobile devices as a threat in the same way as they see it on their computers

Credit Card Fraud

1. **Traditional technique**
   - **Application fraud**: paper-based fraud, where in a criminal uses stolen or fake document to open an account on someone else name.
   - Application frauds can be divided in to;
     - ID theft
     - Financial Fraud where an individual gives false info about his financial status to acquire credit.

Credit Card Fraud

2. **Modern technique:** sophisticated techniques enables criminals to produce fake and doctored cards. These are those who use skimming.

   - Triangulation
   - Credit Card generators

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(LDAP) Security
- Remote Access Server(RAS) security
- Media Player Control Security
- Network Application Program Interface (API) security

Registry settings for mobile devices

- Microsoft ActiveSync : is meant for synchronization with PCs and MS Outlook
- It acts as Gateway between Windows-Powered PC and Windows mobile-Powered device, enabling transfer of Outlook information, MS Office documents, pictures, music, videos and applications from user's desktop to his device.
- ActiveSync 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”

Authentication Service Security

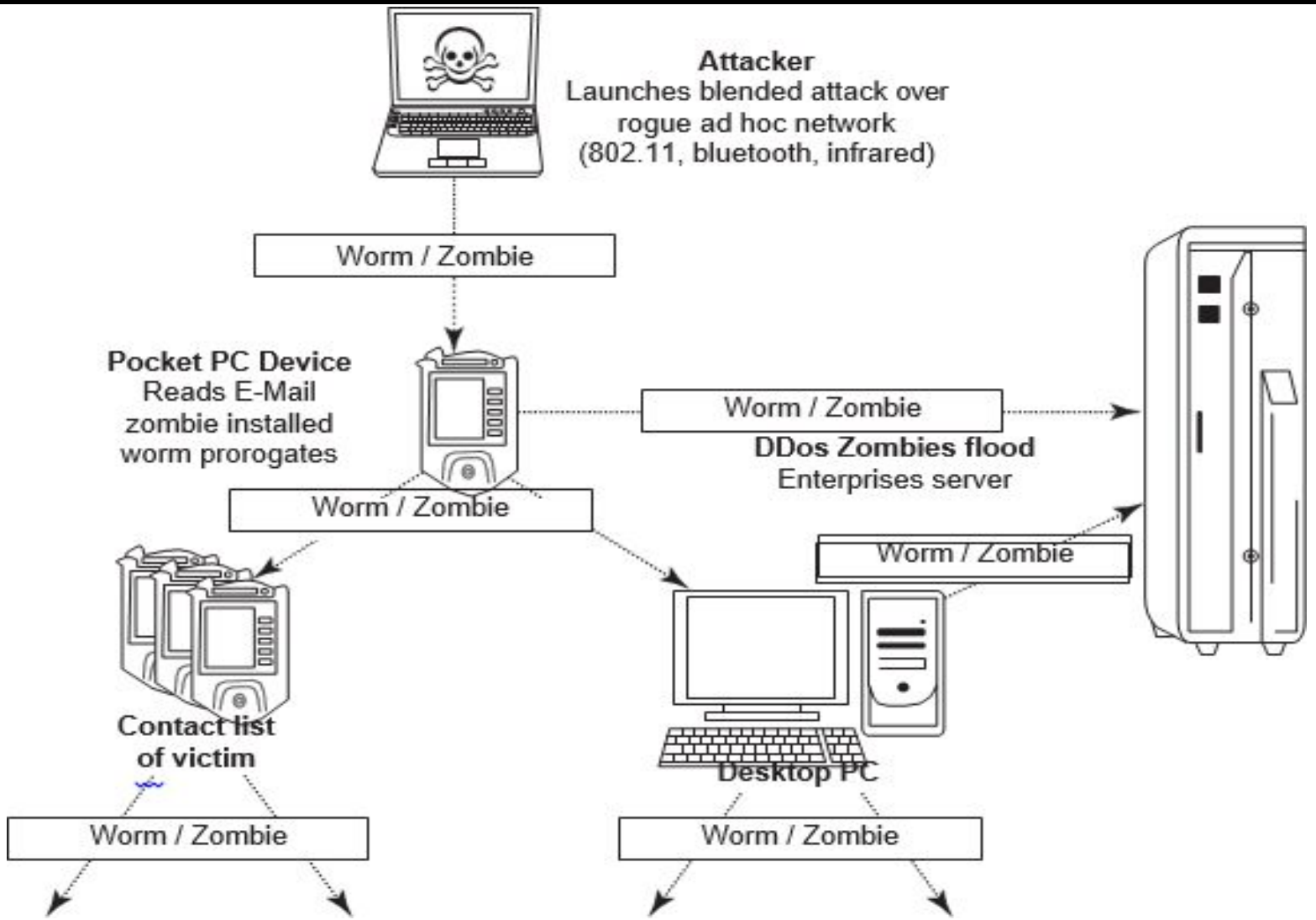
- There are two components of security in mobile computing:
    - security of devices and
    - security in networks.

- 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
- Therefore, no Malicious Code can impersonate the service provider to trick the device into doing something wrong.

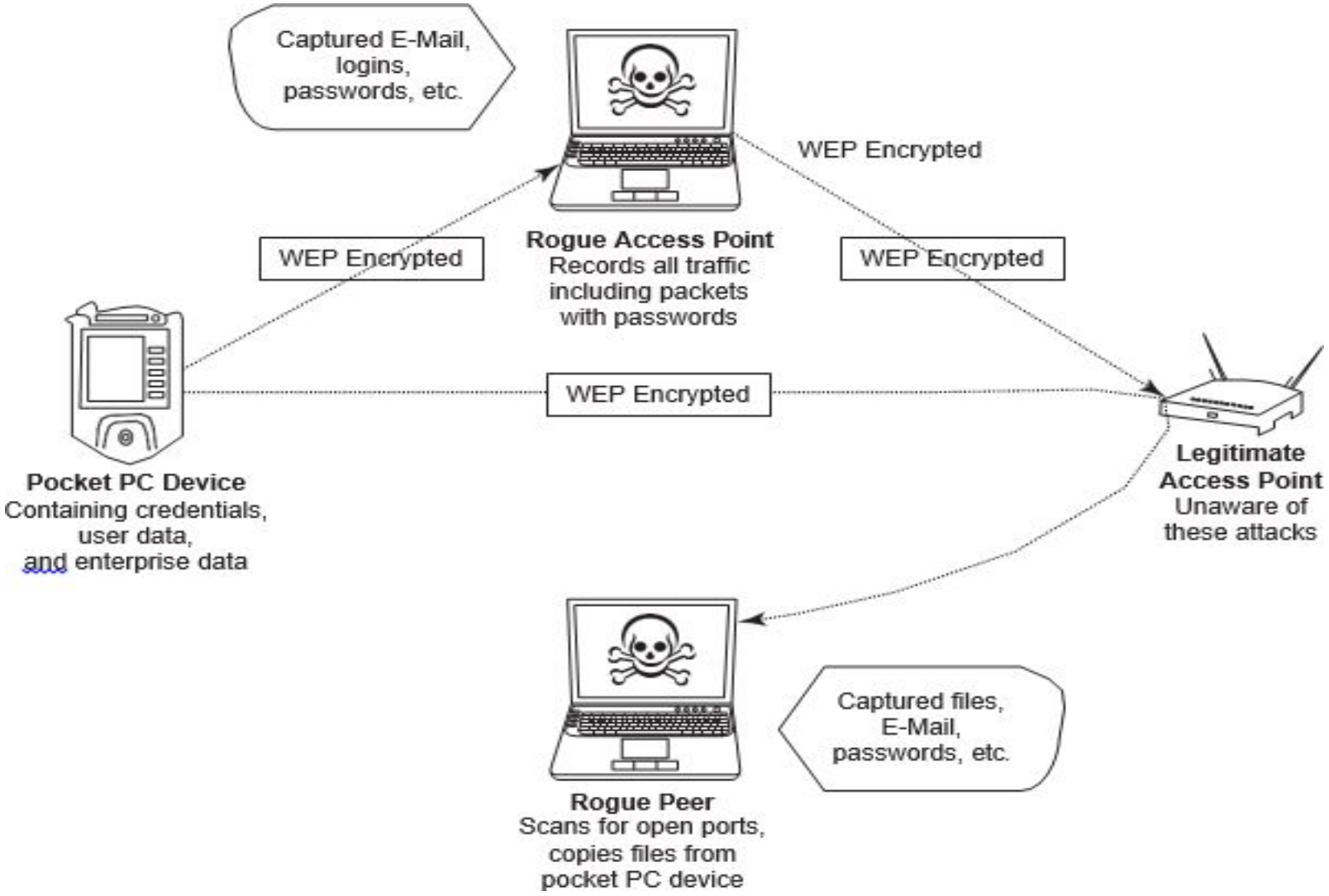
Authentication Service Security

- 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.

Push attack on mobile devices



Pull attack on mobile devices



Authentication Service Security

- 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.

Cryptographic Security for Mobile Devices

- We will discuss a technique known as cryptographically generated addresses (CGA).
- 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.
- To sign messages sent from the address without a Public-Key Infrastructure(PKI)
- CGA-based Authentication can be used to protect IP-Layer signaling protocols
- Also used in key –exchange and create an IPSec security association for encryption and data authentication

Example: Palm OS5

- Cryptographic Provider Manage(CPM) in Palm OS5 is a system-wide suite of cryptographic services for securing data and resources on a Palm- powered device

LDAP security for hand held mobile computing devices

- LDAP is a software protocol for enabling anyone to locate individuals, organizations and other resources like files and devices on the network
- LDAP is light weight version of Directory Access Protocol(DAP) since it does not include security features in its initial version.
- It originated at the University of Michigan
- Endorsed by atleast 40 companies
- Centralized directories such as LDAP make revoking permissions quick and easy.

RAS security for mobile devices

- RAS is important for protecting business sensitive data that is reside on the employee's mobile devices.
- Vulnerable to unauthorized access : resulting in providing a route into the systems with which they connect
  - By impersonating or masquerading to these systems, a cracker is able to steal data or compromise corporate systems in other ways.
- Another threat is by port scanning: DNS server- locate IP address- scan the port on this IP address that are unprotected.
- Precautions: a personal firewall

Media Player Control Security

- Given the lifestyle of today's young generation, it is quite common to expect them embracing the mobile hand-held devices as a means for information access, remote working and entertainment.

- Music and video are the two important aspects in day-to-day aspects for the young generation.

- Given this, it is easy to appreciate how this can be a source for cyber security breaches.

- Various leading software development organizations have been warning the users about the potential security attacks on their mobile devices through the "music gateways."

Media Player Control Security

- 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.

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.

- With the advent of Web services and their use in mobile computing applications consideration.

- Already, there are organizations announcing the development of various APIs to enable software and hardware developers to write single applications that can be used to target multiple security platforms present in a range of devices such as mobile phones, portable media players, set-top boxes and home gateways.

Networking API Security for Mobile Computing Applications

- Most of these developments are targeted specifically at securing a range of embedded and consumer products, including those running OSs such as Linux, Symbian, Microsoft Windows CE and Microsoft Windows Mobile (the last three are the most commonly used OSs for mobile devices).

- Technological developments such as these provide the ability to significantly improve cyber security of a wide range of consumer as well as mobile devices.

- Providing a common software framework, APIs will become an important enabler of new and higher value services.

Attacks on Mobile/ cell phones

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

Mobile phone theft

With mobiles or cellphones 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

How to Protect a Mobile Phone from Being Stolen

- **Add a security mark.** Use an ultra-violet pen to print your post code and house number onto both your mobile handset and battery. This makes it easily identifiable as your property if lost or stolen. It would also be good if you write your alternate contact number or email id on your phone.
- This would help the finder of your handset to contact you if he or she intents to return it. The ultra-violet pen marking will wear off every couple of months, so reapply it when you feel necessary.

How to Protect a Mobile Phone from Being Stolen

- **Use the security lock code, or PIN feature, to lock your phone.** This will make it less valuable to a thief and deny them access to personal numbers stored on your SIM card.

How to Protect a Mobile Phone from Being Stolen

- **Register your phone with your network operator.** If your phone is stolen, report the loss to them immediately.
- Using your IMEI number, they may be able to block your hand set and account details.
- Some wireless carriers are willing to do this, and some aren't.
- If done, this will prevent anyone from using the phone across any network, even if the SIM card is changed.
- Keep in mind that once the phone is disabled, it may not be able to be used again, even if you get it back.
- Keep records of this call--the date, time, name of the person you spoke to, what they said, and their extension.
- Ask for confirmation in writing that your phone has been disabled.
- This is important in case the thief makes fraudulent charges on your account.

How to Protect a Mobile Phone from Being Stolen

- **Have your phone number disabled.** In addition to reporting your phone lost or stolen, you should also disable your phone number (not account) so that no further charges can be applied.
- This is in case the thief figures out how to access your account through another hand set, or in case the carrier is unwilling to block the handset.
- Remember that, as mentioned earlier, many thieves stand to benefit from using your service rather than selling your phone, especially between the moment they steal it and the moment you realize your phone is missing.
- As in the previous step, keep detailed records of when you requested your account to be disabled.

How to Protect a Mobile Phone from Being Stolen

- **Request an immediate, formal investigation from your carrier.** Sometimes this can prevent (or at least delay) the carrier from launching a collections effort and tainting your credit, if things get ugly.
- **File a police report immediately.** Time is money, literally. A thief can add over US$10,000 to your cell phone bill in just hours by making international calls, and you might end up being asked to foot the bill.
- Some phone companies may require proof that the phone was actually stolen, versus it having been lost.
- A police report serves as evidence, which will make your wireless provider more cooperative, especially if insurance is involved.

How to Protect a Mobile Phone from Being Stolen

- **Install anti phone theft software.** There are suppliers that provide modern anti theft software for your phone.
- The software enables you to remotely contact your mobile and stay in control.
- For example, one of the recently published solutions for Symbian and Android is Theft Aware; others provide Windows Mobile or Blackberry support
- **Never let the phone get out of your sight.** Unless you are sleeping of course, always have your eyes on the phone.

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

- 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 (i.e., if Bluetooth is always ENABLED into a mobile phone) whereas MMS virus can send a copy of itself to all mobile users whose numbers are available in the infected mobile phone's address book.

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.

Mobile Phone Virus Hoax

- Forwarded messages claim that a destructive virus will infect your mobile (cell) phone if you receive a call that displays "ACE" or "XALAN" on the screen.

- All mobile users pay attention!!!!!!!!!

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

  PLEASE FORWARD THIS PIECE OF INFORMATION TO ALL YOUR FRIENDS HAVING A MOBILE PHONE.

Mishing

- Mishing is a combination of mobile phone and Phishing Mishing attacks are attempted using mobile phone technology.
- Commerce is fast becoming a part of everyday life. If you use your mobile phone for purchasing goods/services and for banking, you could be more vulnerable to a Mishing scam.
- A typical Mishing attacker uses call termed as Vishing or message (SMS) known as Smishing.
- Attacker will pretend to be an employee from your bank or another organization and will claim a need for your personal details.
- Attackers are very creative and they would try to convince you with different reasons why they need this information from you.

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.

Vishing

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.

How Vishing works?

- A vishing perpetrator (visher) may gain access to a group of private customer phone numbers.
- The visher may then call the group(may use war dialer)
- When a potential victim answers the phone, he or she hears an automated recording informing him that his bank account has been compromised.
- He then calls the specified toll-free number to reset his security settings and hears another automated message requesting the user's bank account number and/or other personal details via the phone keypad..

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.
5. Report incidents to cybercell.

Smishing

- Smishing is a criminal offense conducted by using social engineering techniques similar to Phishing.
- The name is derived from“**SMS**Ph**ISHING**.”
- SMS can be abused by using different methods and techniques other than information gathering under cybercrime.
- 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.

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.

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.

3. Always call on the numbers displayed on the invoice and/or appearing in the bank statements/passbook.

4. 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.

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.

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.

3. Always call on the numbers displayed on the invoice and/or appearing in the bank statements/passbook.

4. 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.

Bluetooth

1. Bluetooth is an open wireless technology standard used for communication (i.e., exchanging data) over short distances between fixed and/or mobile devices.
2. Bluetooth is a short-range wireless communication service/technology that uses the 2.4- GHz frequency range for its transmission/communication.

Bluetooth Hacking

- 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.

Threats of Bluetooth Hacking

- 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.
- Your 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.

Common Bluetooth attacks

- Bluejacking:
- Bluesnarfing
- Bluebugging
- Car wishper

Bluejacking

- *Bluejacking* is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth- enabled device .
- Bluejacking is also known as bluehacking.
- Bluejacking exploits a basic Bluetooth feature that allows devices to send messages to contacts within range.
- Bluejacking is harmless

Bluesnarfing

- Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs (personal digital assistant.).
- This allows access to a calendar, contact list, emails and text messages, and on some phones, users can copy pictures and private videos.
- Both Bluesnarfing and Bluejacking exploit others' Bluetooth connections without their knowledge.
- While Bluejacking is essentially harmless as it only transmits data to the target device, Bluesnarfing is the theft of information from the target device.

Bluebugging

- Bluebugging is a form of Bluetooth attack often caused by a lack of awareness.
- It was developed after the onset of bluejacking and bluesnarfing.
- Similar to bluesnarfing, bluebugging accesses and uses all phone features
- Bluebugging manipulates a target phone into compromising its security, this to create a backdoor attack before returning control of the phone to its owner.
- Once control of a phone has been established, it is used to call back the hacker who is then able to listen-in to conversations.
- The Bluebug program also has the capability to create a call forwarding application whereby the hacker receives calls intended for the target phone.
- Hacker can send messages, read phonebooks, and examine calendars.

Car Whisperer

- Software that intercepts a hands-free Bluetooth conversation in a car.
- Car Whisperer enables an attacker to speak to the driver as well as eavesdrop on a conversation.
- By exploiting the fact that a common security code (passkey) is used by many Bluetooth hands-free system vendors, the Car Whisperer sets up a two-way session with the car and a Linux computer.
- An attacker could access a telephone address book once he has connected with the Bluetooth system,
- May disable airbags or breaks

Bluetooth attack tools

- BTScanner
- Bluesnarfer
- Bluediving
- Blue bugger
- bluesniff

Some dangerous mobile threats to look out

NAME	DISCOVERED?	THREAT TYPE	DESCRIPTION
SpyNote.C	October 2022	Banker Trojan	New variant of the SpyNote malware family that can exfiltrate PII from online banking customers.
Hook	January 2023	Banker Trojan	A fork of the Ermac malware family with RAT capabilities.
MaliBot	June 2022	Banker Trojan	Focuses on stealing financial information, crypto wallets, personal data, and even two-factor authentication codes.
Triada	October 2022 (New version)	Trojan	Found in a modified WhatsApp build. Can display ads, subscribe you to paid services, and download other malicious programs.
Harly	October 2022	Trojan	Imitates legitimate apps on Google Play store. Subscribes you to paid services once installed.
SharkBot	August 2022 (New version)	Trojan	Dropper that poses as a fake Android antivirus and cleaner.

Examples of recent Android malware

Malware is on the rise

1. Open-wifi related threats

When mobile device users connect to a public network, they are vulnerable to cyber threats where cybercriminals can create fake WiFi to snoop on users or steal their data.

2. SpinOk

Spin0k is spyware disguised as an SDK, urging users to play some minigames with promised daily rewards. It infects the mobile device, steals passwords, email ids, and other sensitive data, and emits it to remote servers. It has emerged as one of the fastest-spreading diseases across countries worldwide. What makes it more dangerous is that not many people know about it.

In one research report, security researchers found that over 500 million mobile phone devices were infected with Spin0k. Some of the commonly found apps (more than 101 apps on Playstore!) include CrazyDrop (10,000,00 downloads), VFly video editor (50,000,00 downloads), and Noize video editor (100,000,000 downloads).

Malware is on the rise – Cont.

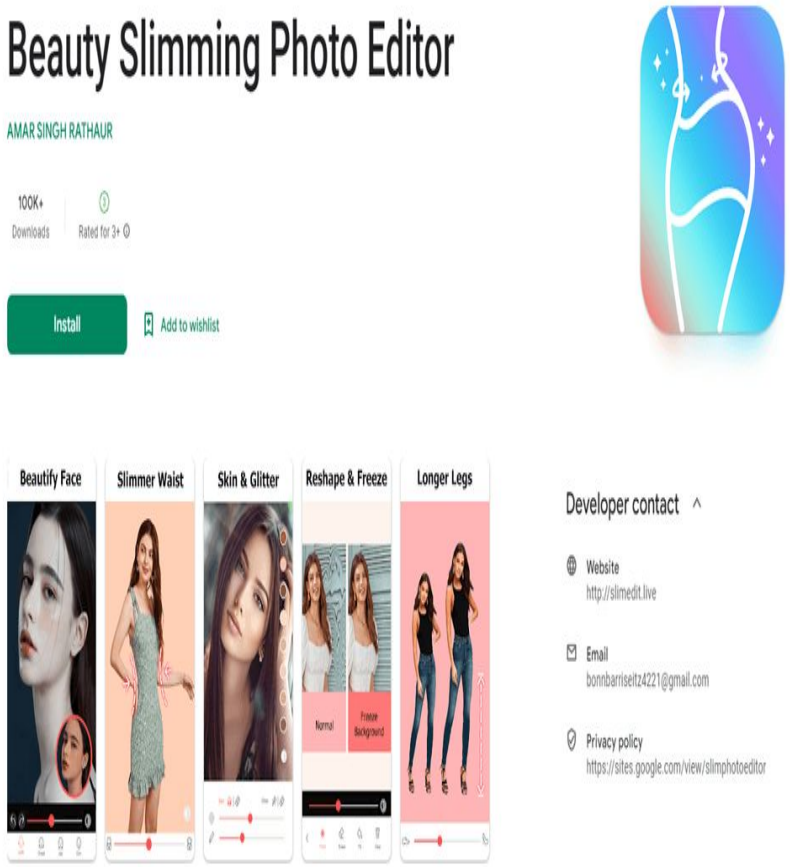
3. Anubis

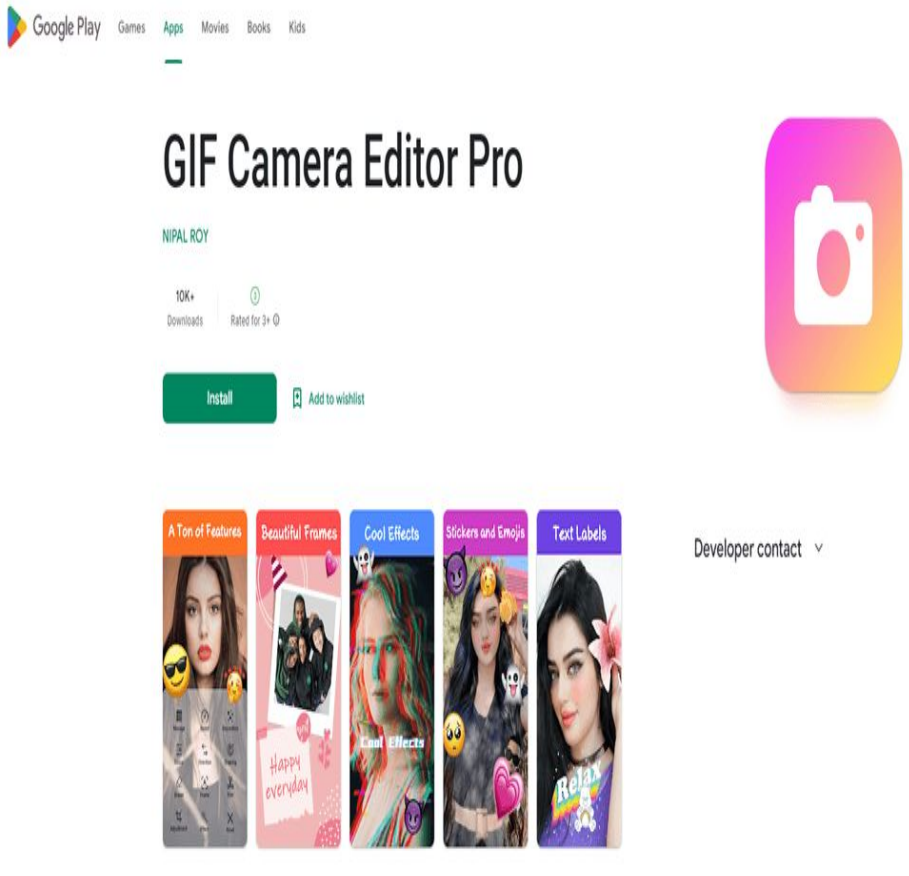
It is a form of open-source malware currently used widely by ransomware groups. It poses a considerable threat to mobile devices. It is used for credential theft, SMS interception to steal OTPs for sensitive transactions, snooping on device audio, engaging in keylogging, and capturing screens. Anubis malware is also used to steal critical company-specific files, depending on the objectives of cyber attackers and their location. It has affected more than 200 baking and finance-related applications worldwide in countries like Australia, Spain, Turkey, Germany, and France.

4. AhMyth

AhMyth is a kind of Remote Administration Tool (RAT) tool that is used by cybercriminals to control devices remotely to steal their data, monitor their location, read their text messages, take control of the camera snapshots, and record audio using the phone's microphone. It is quite a dangerous malicious tool since there are more than 2.5 billion Android users worldwide.

Several mobile photo editors on Google Play, which, besides their legitimate features, contained a dropper hidden inside a heavily obfuscated library. The dropper payload was designed to subscribe the user to paid services and intercept notifications



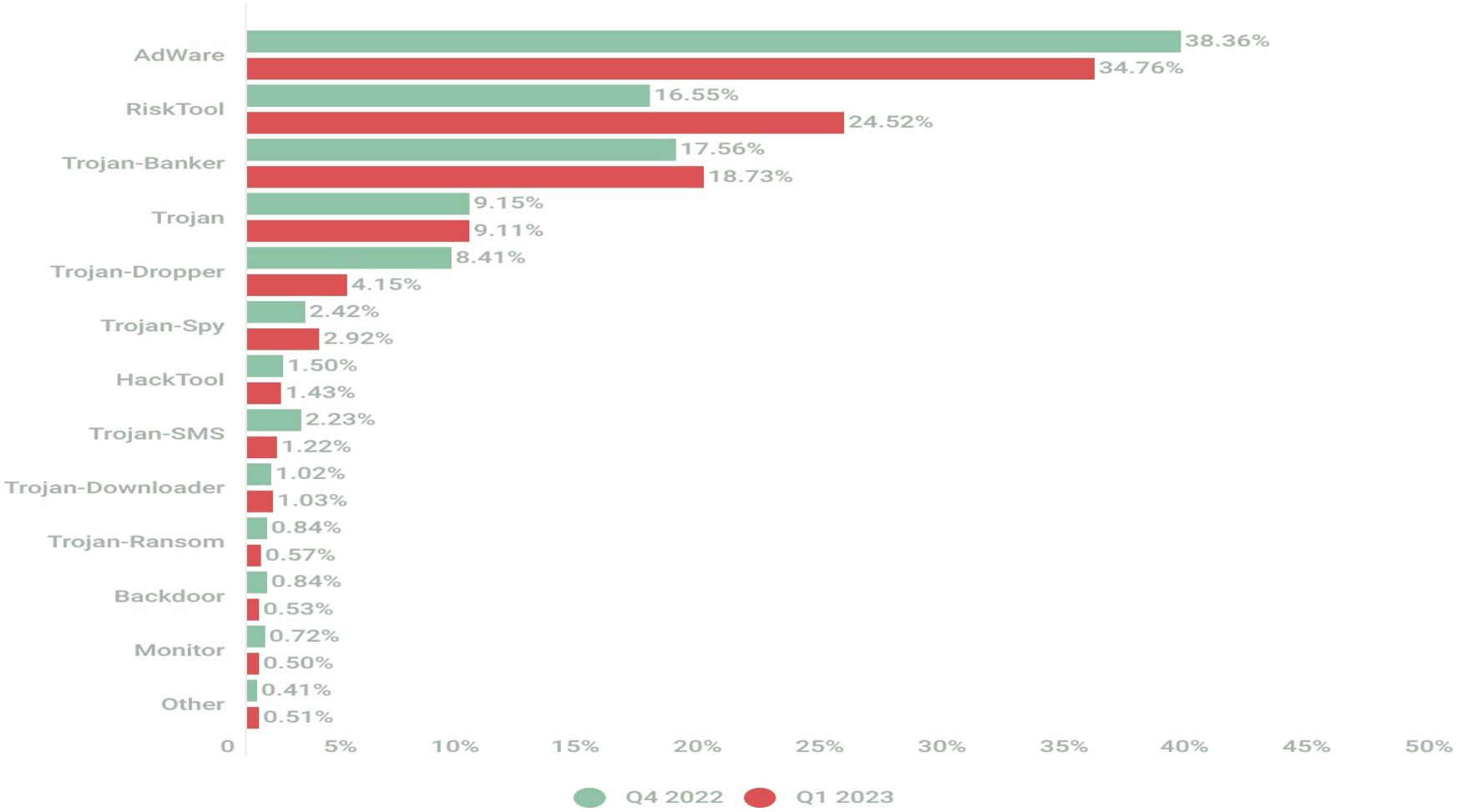


Files associated with this Trojan as Trojan.AndroidOS.Fleckpe.

Number of detected malicious installation packages, Q1 2022–Q1 2023

kaspersky

Distribution of newly detected mobile malware by type, Q4 2022 and Q1 2023



kaspersky

MOBILE SECURITY THREATS PREDICTION FOR 2023

2023 MOBILE SECURITY THREATS

- Increase in Ransomware Attacks Targeting Mobile Devices
- Increase in Malicious Programs Targeting Android Devices
- Increase in Mobile Banking Trojans
- Increase in Phishing Scams Targeting Mobile Devices
- Increase in Network Intrusion Attempts
- Increase in the Use of Machine Learning (ML) and Artificial Intelligence (AI) for Cyber Threats

HOW TO PREVENT MOBILE SECURITY ATTACKS

- Improving Your Mobile Security
- Adhere to Mobile Security Best Practices
- Develop a Mobile Security Plan
- Keep an Eye on Mobile Security Trends
- Stay Agile, Proactive, and Vigilant
- Get Mobile Security Solutions

HOW TO DEVELOP A MOBILE SECURITY PLAN

- Identify the assets that need to be protected.
- Create unique and strong passwords for all of your online accounts.
- Use two-factor authentication whenever possible.
- Install the latest security patches and updates.
- Use a reliable antivirus program and regularly scan your device for malicious software.
- Be aware of the potential risks of public Wi-Fi and unsecured networks.
- Use a Virtual Private Network (VPN) when using public Wi-Fi.
- Avoid connecting to unsecured networks.

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.

1. Managing diversity and proliferation of Hand-Held devices

- 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.

2. Unconventional/ stealth storage devices

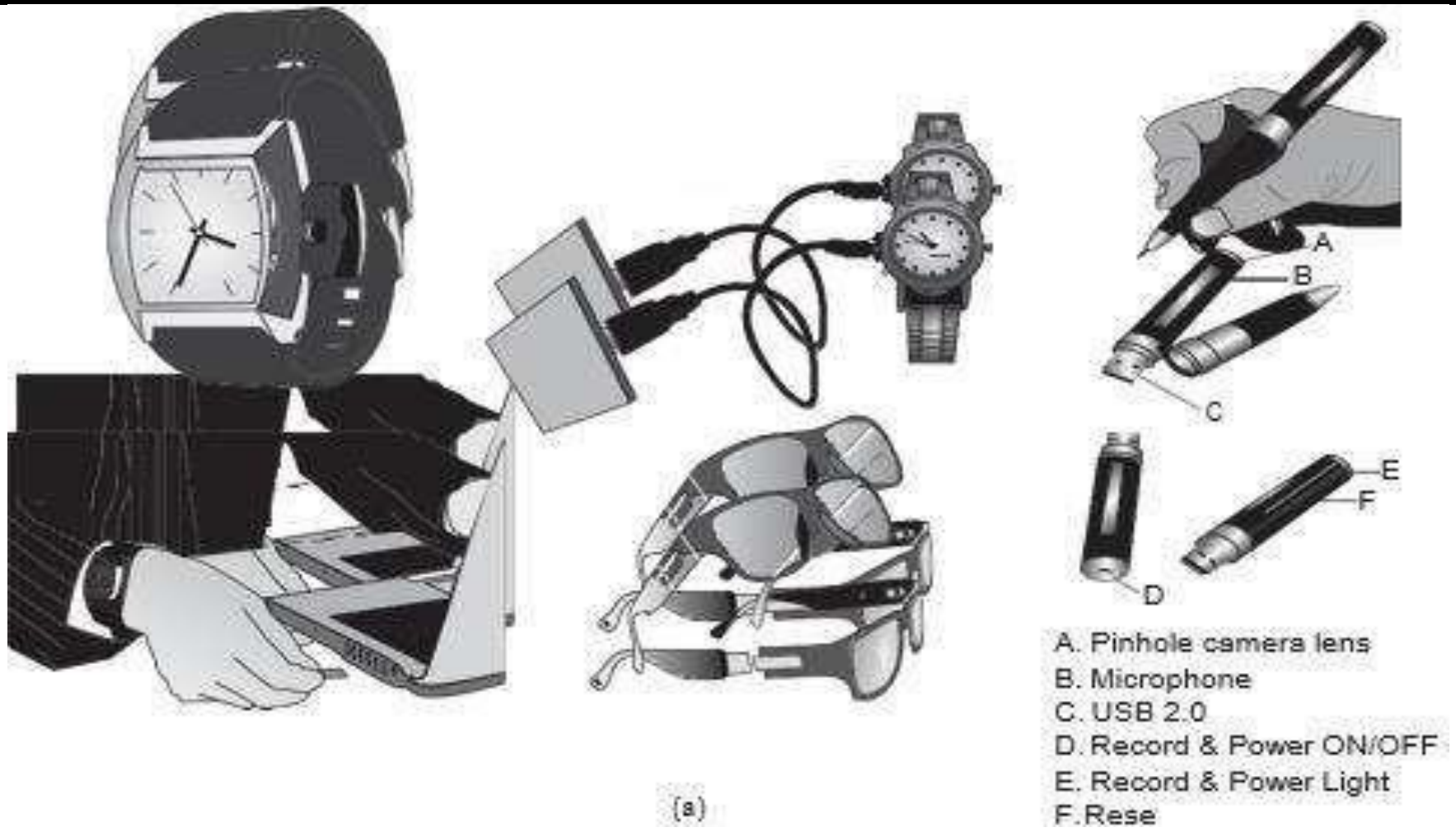


Fig: Unconventional/stealth storage devices.

2. Unconventional/ stealth storage devices

To control over unauthorized access to plug and play devices, solution is “DeviceLock” softwares. The features of the software allows system administrator to:

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

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.

Including Mobile Devices in Security Strategy

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

1. Importance of Security Policies relating to Mobile Computing Devices

- People (especially, the youth) have grown so used to their handhelds that they are treating them like wallets!
- The survey asked the participants about the likelihood of six separate scenarios involving the use of cell phones to communicate sensitive and confidential information occurring in their organizations.

1. Importance of Security Policies relating to Mobile Computing Devices

The scenarios described the following:

1. A CEO's administrative assistant uses a cell phone to arrange ground transportation that reveals the CEO's identity and location.
2. The finance and accounting staff discusses earnings of press release and one participant on the call is using a cell phone.
3. A conference call among senior leaders in the organization in which cell phones are sometimes used.
4. A sales manager conducting business in Asia uses, his/her cell phone to communicate with the home office.
5. An external lawyer asks for proprietary and confidential information while using his cell phone.
6. A call center employee assists a customer using a cell phone to establish an account and collects personal information (including SSN).

2. Operating Guidelines 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.
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.

2. Operating Guidelines for Implementing Mobile Device Security Policies

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.

2. Operating Guidelines for Implementing Mobile Device Security Policies

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). This is to preclude
incidents through which people obtain “old” computing devices that still had confidential company data.
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.

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

- Securing mobile devices is creating company policies that address the unique issues these devices raise.
- Such questions include what an employee should do if a device is lost or stolen.
- 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.

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

Thank You