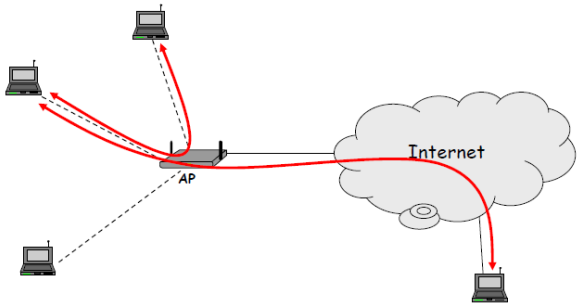
MODULE 5

Security in current domains: Wireless LAN security – WEP details. wireless LAN vulnerabilities – frame spoofing. Cellphone security - GSM and UMTS security. Mobile malware - bluetooth security issues.

INTODUCTION TO WIFI



Wireless network is a network that uses a section of the radio spectrum, so the signals are available to anyone with an effective antenna within range.

A wireless network consists of an **access point** or router that receives, forwards and transmits data, and one or more devices, sometimes called **stations**, such as computers or printers, that communicate with the access point.

The access point is the hub of the wireless sub network. Each device must have a **network interface card**, or **NIC,** that communicates radio signals with the access point.

The NIC is identified by a unique 48- or 64-bit hardware address called a **medium access code**, or **MAC**.

Because wireless computing is so exposed, it requires measures to protect communications between a computer (called the client) and a wireless base station or access point.

Remembering that all these communications are on predefined radio frequencies, you can expect an eavesdropping attacker to try to intercept and impersonate. Pieces to protect are finding the access point, authenticating the remote computer to the access point, and vice versa, and protecting the communication stream.

Wireless communication will never be as secure as wired, because the exposed signal is more vulnerable.

A **Service Set Identifier**, or **SSID**, is the identification of an access point; it is a string of up to 32 characters chosen by the access point's administrator.

WIRELESS LAN SECURITY

WLAN security is a security system designed to protect networks from the security breaches.

This type of security is necessary because WLAN signals have no physical boundary limitations, and are prone to illegitimate access over network resources, resulting in the vulnerability of private and confidential data.

Network operations and availability can also be compromised in case of a WLAN security breech. To address these issues, various authentication, encryption, invisibility and other administrative controlling techniques are used in WLANs.

While wireless networks provide convenience and flexibility, they also increase network vulnerability. Security threats such as unauthorized access, denial of service attacks, IP and MAC spoofing, session hijacking and eavesdropping can all be problems for WLANs.

To counter these threats, various standard authentication and encryption techniques are combined with other access control mechanisms. These protocols, devices and techniques collectively secure the WLAN a level that equals and even exceeds wired LAN security.

Why security is more of a concern in wireless?

- no inherent physical protection
  - physical connections between devices are replaced by logical associations
  - sending and receiving messages do not need physical access to the network infrastructure (cables, hubs, routers, etc.)
- broadcast communications
  - wireless usually means radio, which has a broadcast nature
  - transmissions can be overheard by anyone in range
  - anyone can generate transmissions,
    - which will be received by other devices in range
    - which will interfere with other nearby transmissions and may prevent their correct reception (jamming)

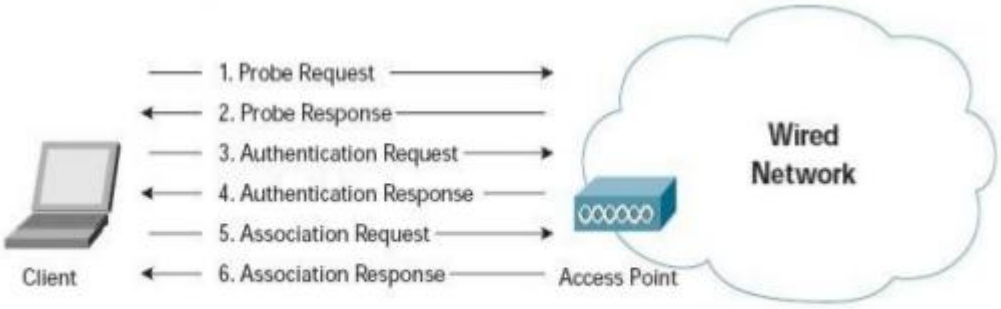
- eavesdropping is easy
- injecting bogus messages into the network is easy
- replaying previously recorded messages is easy
- illegitimate access to the network and its services is easy
- denial of service is easily achieved by jamming

Wireless communication security requirements

- confidentiality
  - messages sent over wireless links must be encrypted
- authenticity
  - origin of messages received over wireless links must be verified
- replay detection
  - freshness of messages received over wireless links must be checked
- integrity
  - modifying messages on-the-fly (during radio transmission) is not so easy, but possible …
  - integrity of messages received over wireless links must be verified
- access control
  - access to the network services should be provided only to legitimate entities
  - access control should be permanent
    - it is not enough to check the legitimacy of an entity only when it joins the network and its logical associations are established, because logical associations can be hijacked
- protection against jamming

WLAN Authentication

- Wireless LANs, because of their broadcast nature, require the addition of:
  - User authentication
  - Data privacy
- Authenticating wireless LAN clients.



Client Authentication Process

WLAN Authentication

- Types Of Authentication
  - Open Authentication
    - The authentication request
    - The authentication response
  - Shared Key Authentication
    - requires that the client configure a static WEP key
  - Service Set Identifier (SSID)
  - MAC Address Authentication
    - MAC address authentication verifies the client's MAC address against a locally configured list of allowed addresses or against an external authentication server

WLAN Authentication Vulnerabilities

- SSID

An eavesdropper can easily determine the SSID with the use of an 802.11 wireless LAN packet analyzer, like Sniffer Pro.

- Open Authentication

Open authentication provides no way for the access point to determine whether a client is valid.

- Shared Key Authentication Vulnerabilities

The process of exchanging the challenge text occurs over the wireless link and is vulnerable to a man-in-the-middle attack

- MAC Address Authentication Vulnerabilities

A protocol analyzer can be used to determine a valid MAC address

How to protect WLAN from security threats

1. ESSID

Chief among these is the ESSID (Extended Service Set ID), or name of the WLAN. By default it's often "101" but it can be any string of up to 256 characters. Don't be obvious and pick the house or road name.

Instead, think of it as a password and use a long name with both letters and numbers, making it harder to hack. Then configure the AP so that it does not broadcast the ESSID. In this way, only authorized clients

can connect to your AP.

2. MAC address filters

Using MAC address filter, the AP maintains a list of MAC addresses and only permits those on the list to connect. No connection means no access to the rest of the network, such as the data on servers and client PCs.

The main drawback to MAC address filtering is the need to discover the MAC address of every client's adapter and enter it into the AP's settings fields. As a one-off task, it might take you half an hour from start to finish for say, half a dozen client machines.

However, if a PC Card gets lost, you buy new ones, or you add or upgrade an AP, it can make for a lot of extra tedious typing. That said, for a small WLAN where such changes are infrequent, this might be almost all the security you need.

3. Encryption :-

The way to protect data in transit is encryption, the WLAN encryption standard being WEP (Wired Equivalence Privacy).

Under WEP, all encrypted packets use the first 24 bits for initialization vector and the rest for data. This means that 64-bit encryption – actually 40 bits of which are data

4. Locking down

The next step is to lock down the AP. You'll notice that you can change the AP's settings over the WLAN. This is not a good idea. If a hacker gets into your network, they can also access your AP, altering the settings to suit them, not you. If they're clever, you might not even notice, even though someone else is accessing your connection. If they're not, your WLAN might even stop working.

Either way, make sure you only configure the AP over a wired connection. If you've got Ethernet use that or, better still, use the serial port connection if it's got one. Don't forget to change the default password where possible.

5. Authentication

The final layer of protection is individual authentication. The standard method of WLAN authentication uses the 802.1X protocol. If the protocol is enabled, unauthenticated users cannot get past the AP to access the rest of the network. It's built into Windows XP already and is embedded in the next-generation WLAN security standard

6. Use a strong administrator password to increase wifi security.

7. Always keep your routers software up to date.

8. Firewall can help to secure your wifi.

WEP – Wired Equivalent Privacy

- part of the IEEE 802.11 specification
- goal
  - make the WiFi network *at least as secure as a wired LAN* (that has no particular protection mechanisms)
  - WEP has never intended to achieve strong security
  - (at the end, it hasn't achieved even weak security)
- services
  - access control to the network
  - message confidentiality
  - message integrity

- It is a protocol used to provide the same level of security as that of wired LAN.
- It provides confidentiality, integrity and protect access to network.
- It protects from unauthorized eavesdropping and restricting access to a wireless network.

WEP operations and Implementation

- Uses RC4 algorithm to encrypt the packets of information.
- Based on 40 or 64 bit secret key that is shared between mobile station and an access point to encrypt or decrypt the data.
- Each byte of data is encrypted using a unique key
- The 64 bit shared key consists of
  - 24 bit master key
  - 40 bit initialization vector(IV)

WEP Services

1. Access control
2. Confidentiality
3. Integrity

WEP – Access control

- before association, the STA needs to authenticate itself to the AP
- authentication is based on a simple challenge-response protocol:

  STA → AP: authenticate request
  AP → STA: authenticate challenge (r) // r is 128 bits long
  STA → AP: authenticate response ($e_K(r)$)
  AP → STA: authenticate success/failure

- once authenticated, the STA can send an association request, and the AP will respond with an association response
- if authentication fails, no association is possible

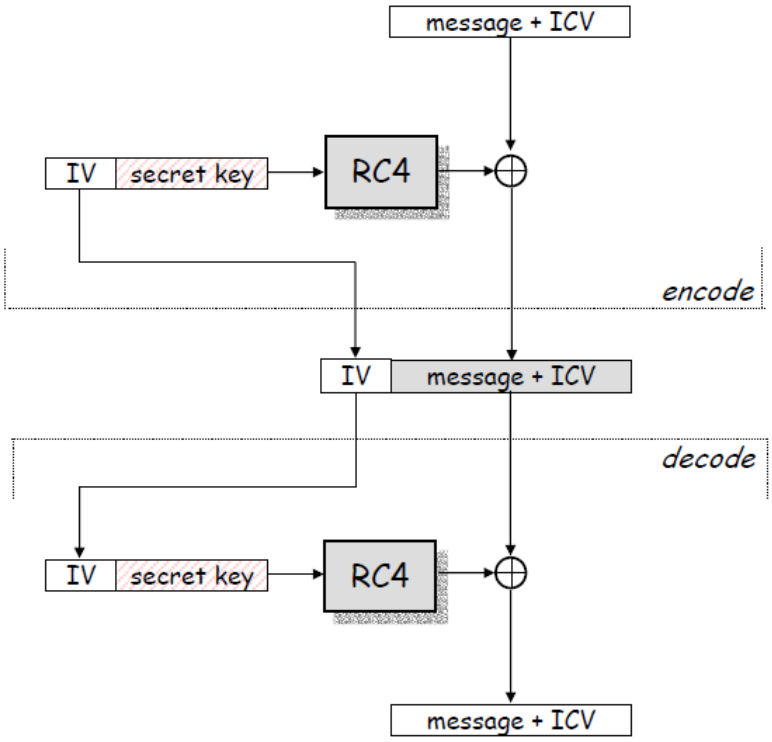
- Station sends authentication request to AP, then AP sends 128 bit random challenge to client
- The client uses shared secret key to sign the challenge and send to AP.
- AP decrypts the signed message using shared secret key and verifies challenges that is sent before.

WEP – Message confidentiality and integrity

- WEP encryption is based on the RC4 stream cipher
  - operation:
    - for each message to be sent:
      - RC4 is initialized with the shared secret (between STA and AP)
      - RC4 produces a pseudo-random byte sequence (key stream)
      - this pseudo-random byte sequence is XORed to the message
    - reception is analogous
  - it is essential that each message is encrypted with a different key stream
    - the RC4 generator is initialized with the shared secret and an IV (initial value) together
      - shared secret is the same for each message
      - 24-bit IV changes for every message

- WEP integrity protection is based on an encrypted CRC value
  - operation:
    - ICV (integrity check value) is computed and appended to the message
    - the message and the ICV are encrypted together

WEP – Message confidentiality and integrity



Working

With WEP enabled, all the data is encrypted using the Ron Rivest Code 4 (RC4) in the purpose to provide secure communication. In addition, WEP protects the wireless traffic with a randomly generated 24-bit Initialization Vector (IV), which is combined with the 40-bit or 104-bit shared secret key (so-called 128 bit in most product implementation). The WEP encryption operation is described below:

1. The 40-bit shared secret key is concatenated with the 24-bit randomly generated Initialization Vector (IV). The IV is used to increased security by introducing cryptographic variance to the Initial Shared Secret Key.
2. The new 64-bit key is fed into the RC4 algorithm to create the Encryption key or key stream
3. Before encrypting the data, an integrity check is performed with the Cyclic Redundancy Check-32 (CRC-32) algorithm. This step intends to protect against data modification. The CRC operation generates a 4 bytes CRC which is concatenated to the initial data to obtain the plaintext that will be used as input in step 4. The shared secret key is not used in this process.
4. The plaintext (data and its concatenated CRC) is encrypted with the encryption key (or key stream) generated in step 2, using the mathematical XOR function to obtain the ciphertext.
5. The encrypted output can now be send to transmission with the Initialization Vector appended to the ciphertext.
6. The client will use the reverse steps to decrypt the ciphertext and recover the original data.

Example

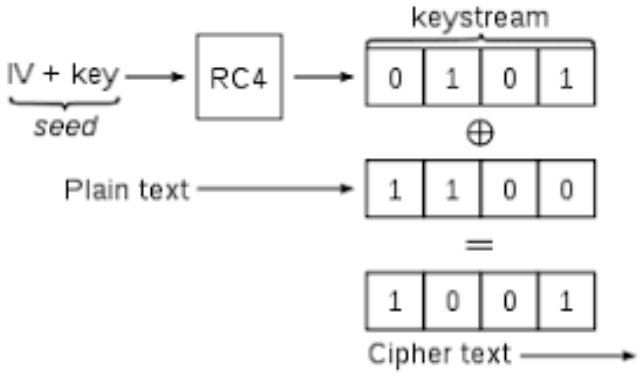
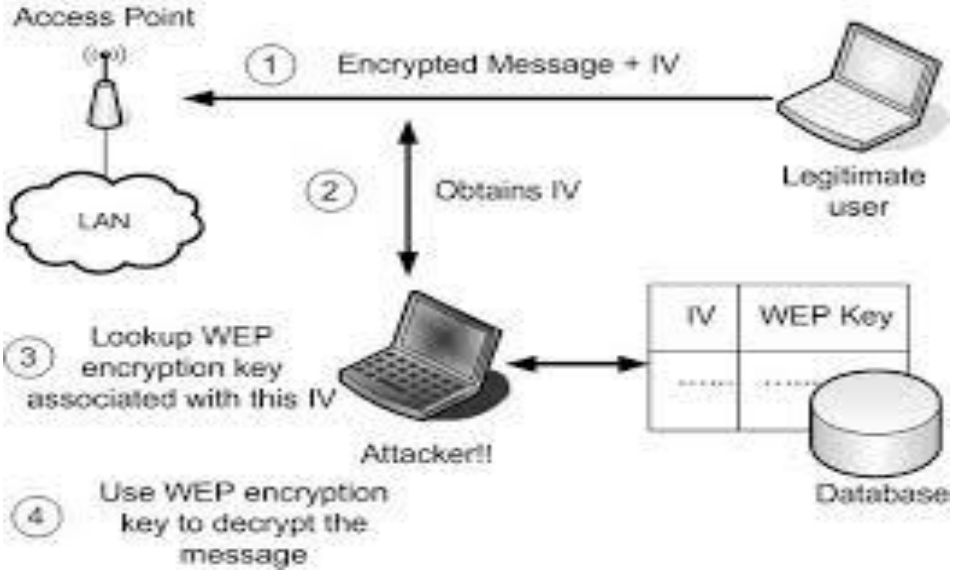


Illustration of WEP weakness



WEP flaws – Authentication and access control

- authentication is one-way only
  - AP is not authenticated to STA
  - STA may associate to a rogue AP
- the same shared secret key is used for authentication and encryption
  - weaknesses in any of the two protocol can be used to break the key
  - different keys for different functions are desirable
- no session key is established during authentication
  - access control is not continuous
  - once a STA has authenticated and associated to the AP, an attacker send messages using the MAC address of STA
  - correctly encrypted messages cannot be produced by the attacker, but replay of STA messages is still possible
- STA can be impersonated

there's no replay protection at all

- IV is not mandated to be incremented after each message

attacker can manipulate messages despite the ICV mechanism and encryption

IV reuse

- IV space is too small
  - IV size is only 24 bits → there are 16,777,216 possible IVs
  - after around 17 million messages, IVs are reused
  - a busy AP at 11 Mbps is capable for transmitting 700 packets per second → IV space is used up in around 7 hours
- in many implementations IVs are initialized with 0 on startup
  - if several devices are switched on nearly at the same time, they all use the same sequence of IVs
  - if they all use the same default key (which is the common case), then IV collisions are readily available to an attacker

weak RC4 keys

- for some seed values (called weak keys), the beginning of the RC4 output is not really random
- if a weak key is used, then the first few bytes of the output reveals a lot of information about the key → breaking the key is made easier
- for this reason, crypto experts suggest to always throw away the first 256 bytes of the RC4 output, but WEP doesn't do that
- due to the use of IVs, eventually a weak key will be used, and the attacker will know that, because the IV is sent in clear

→ WEP encryption can be broken by capturing a few million messages !!!

WPA:- Wifi Protected Access

It is a security protocol designed to create secure wifi networks. It is similar to WPA protocol, but offers improvements in the way it handles security keys and the way users are authorized.

VULNERABILITIES IN WIRELESS NETWORKS

Wireless networks are subject to threats to confidentiality, integrity, and availability just like other computer applications and technologies. The attacker can either join the network of the target and participate in data exchanges, or merely observe the traffic as a bystander.

Confidentiality

If data signals are transmitted in the open, unintended recipients may be able to get the data. The data values themselves are the most sensitive, but A's communicating with access point B or the duration or volume of communication may also be sensitive.

The nature of the traffic, whether web page access, peer-to-peer networking, email, or network management, can also be confidential. Finally, the mode in which two units communicate—encrypted or not and if encrypted, by what algorithm—is potentially sensitive. Thus, the confidentiality of many aspects of a communication can be sensitive.

Integrity

As for integrity, we must consider both malicious and nonmalicious sources of problems. Numerous nonmalicious sources of harm include interference from other devices, loss or corruption of signal due to distance or intervening objects, reception problems caused by weather, and sporadic communication failures within the hardware and software that implement protocol communication.

Availability

Availability involves some potential problems. First, the most obvious, occurs when a component of a wireless communication stops working because hardware fails, power is lost, or some other catastrophe strikes.

A second problem of availability is loss of some but not all access, typically manifested as slow or degraded service. Service can be slow because of interference, for example, if tree leaves in a wind interfere with frame transmission, so the receiving end recognizes loss of some data and must request and wait for retransmission.

Service can also be slow if the demand for service exceeds the capacity of the receiving end, so either some service requests are dropped or the receiver handles all requests slowly.

Types of vulnerabilities in WLAN

1. **War Driving(Access Point Mapping)**

It is the act of searching for wifi networks by a person usually in a moving vehicle, using a laptop or smartphone.

Wireless NIC scans for wireless access points . The computer looks for SSID (wireless network name) which is being constantly transmitted by the access point , letting the computers know of its presence. The wire driver uses some software to scan the airwaves for SSIDs.

Solution for War Driving

- o Do not broadcast your SSID.
- o Change the default password.
- o Encrypt your wireless connection using the encryption schemes.
- o Filter the MAC addresses that are allowed to connect to your router.
- o If you configure file sharing on your computer, make sure it is password protected. o Use personal firewall software.

2. **Eavesdropping**

It is the unauthorized real time interception of private communication.

This involves attacks against the confidentiality of the data that is being transmitted across the network. There are two types of eavesdropping:

I. Passive Eavesdropping: The malicious nodes detect the information by listening to the message transmission in the wireless broadcasting medium.

II. Active Eavesdropping: The malicious nodes actively grab the information via sending queries to transmitters by disguising themselves as friendly nodes.

Solution for Eavesdropping

o The best way to keep your traffic secure while on Wi-Fi hotspots is to connect to a Virtual Private Network (VPN), maybe to your work's network, a server you set up at your home, or a hosted service designed specifically for hotspot security, such as Private Wifi or Hotspot Shield.

o We must make sure any services or sites you use while on the hotspot are secured with SSL encryption.

3. **Denial of Service Attack** A denial-*of*-service (DoS) *is* any type of *attack* where *the* attackers (hackers*) attempt* to prevent *legitimate* users from accessing the *service*

This can come in one of two forms:

I. A huge flood of packets that uses up all of the network's resources and forces it to shut down.

II. A very strong radio signal that totally dominates the airwaves and renders access points and radio cards useless.

Solution for Denial of Service Attack

This type of attack can be prevented by:

o implementing and updating firewalls.

o maintaining updated virus protection.

o ensuring strong passwords and deploy DoS detection tools,

You can protect a WLAN against DoS attacks by making the building as resistive as possible to incoming radio signals.

4. **Rogue Access Points**

A rouge access point is any wireless access point that has been installed on a networks wired infrastructure without the consent of the network administrator or owner , thereby providing unauthorized wireless access to the networks wired infrastructure.

Most of the time , rouge APs are set up by employees who want wireless access when none is available.

Types of Rogue Aps based on security categories:

I. Non-malicious APs: The majority of the cases consist of someone installing a rogue AP with the intent being not to bypass the corporation's security policy but to deploy wireless as a convenience or productivity enhancer.

II. Malicious Aps: the attacker sets up the AP to gain access to the wired network or to disrupt the performance of the WLAN

Prevention of Rogue APs

o Use of commercial tools like AirMagnet and AirDefence to scan for rogue Aps periodically and verify their legitimacy.

o Using network Wireless Intrusion Prevention System (WIPS) to watch the air or by using a host-resident Wireless IPS to monitor client activity.

o Use of WLAN analyzer for Rogue AP detection.

5. **Unauthorized WiFi Access**

An unauthorized device can attempt to establish an association with an access point.

Remember from the WiFi protocols that access basically involves three steps:

1. The access point broadcasts its availability by sending a beacon, an invitation for devices to connect with it.

2. A device's NIC responds with a request to authenticate, which the access point accepts.

3. The device's NIC requests establishment of an association, which the access point negotiates and accepts.

There are threats at each of these points. In step 1, anyone can pick up and reply to a broadcast beacon. In step 2, the authentication is not rigorous; in basic WiFi mode the access point accepts any device, without authentication. In step 3, any access point can accept an association with any device. We can counter these attacks of unauthorized access at any of the three steps.

Authentication in Wireless Networks

Access points can manage lists of MAC addresses of devices with which they will accept connections. Thus, authentication in step 2 could be accomplished by accepting only devices on the positive accept list.

6. **Authentication Vulnerabilities**

a. **Use of SSID**

An eavesdropper can easily determine the SSID with the use of an 802.11 wireless LAN packet analyzer, like Sniffer Pro. Some access-point vendors, including Cisco, offer the option to disable SSID broadcasts in the beacon messages.

b. **Open Authentication Vulnerabilities**

Open authentication provides no way for the access point to determine whether a client is valid. This is a major security vulnerability if WEP encryption is not implemented in a wireless LAN.

Cisco does not recommend deploying wireless LANs without WEP encryption.

c. **Shared Key Authentication Vulnerabilities**

Shared key authentication requires the client use a preshared WEP key to encrypt challenge text sent from the access point.

The access point authenticates the client by decrypting the shared key response and validating that the challenge text is the same. The process of exchanging the challenge text occurs over the wireless link and is vulnerable to a man-in-the-middle attack.

An eavesdropper can capture both the plain-text challenge text and the cipher-text response. WEP encryption is done by performing an exclusive OR (XOR) function on the plain-text with the key stream to produce the cipher-text. It is important to note that if the XOR function is performed on the plain-text and cipher-text are XORed, the result is the key stream.

Therefore, an eavesdropper can easily derive the key stream just by sniffing the shared key authentication process with a protocol analyzer.

d. MAC Address Authentication Vulnerabilities

MAC addresses are sent in the clear as required by the 802.11 specification. As a result, in wireless LANs that use MAC authentication, a network attacker might be able to subvert the MAC authentication process by "spoofing" a valid MAC address.

MAC address spoofing is possible in 802.11 network interface cards (NICs) that allow the universally administered address (UAA) to be overwritten with a locally administered address (LAA).

CELLPHONE SECURITY

Most people have mobile phones today. In the past these devices were primarily used to call and send text messages. In addition, all mobiles have at least an ability to keep an address book. There is a new generation of mobile devices that come with Internet access, built-in video cameras and the ability to install additional software. These smart phones can be very convenient and provide you with very powerful and useful tools. These phones contain a lot of private data and, unfortunately, a phone can be lost easily.

Mobile Security as a concept deals with the protection of our mobile devices from possible attacks by other mobile devices, or the wireless environment that the device is connected to.

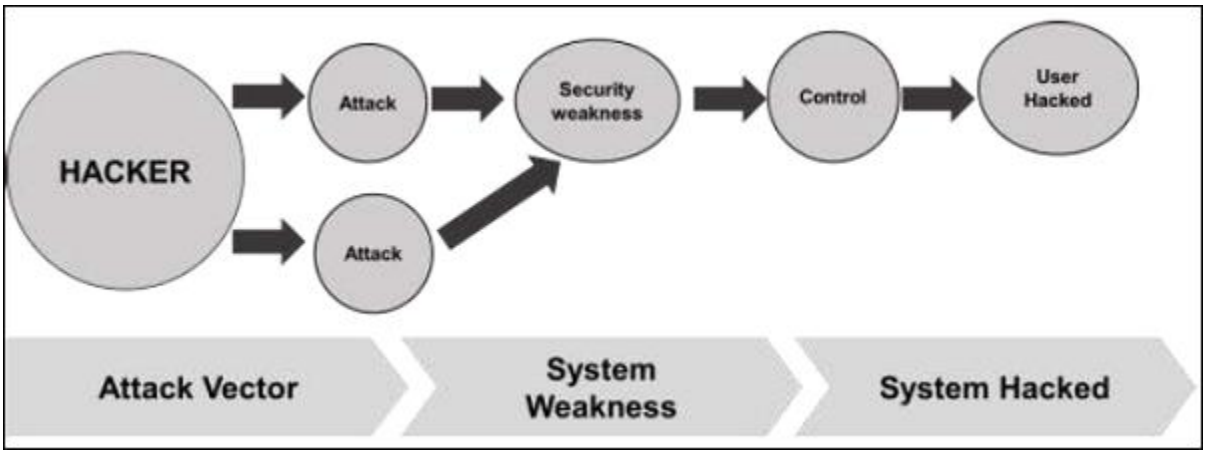
Security issues with mobile phones

- **Physical security** - A phone can be stolen. As a minimum safety measure you should always enable some kind of password protection on your phone .
- **Voice** - Although the voice on a GSM (mobile phone) channel is encrypted, this encryption was hacked some time ago and is not considered safe any more. Furthermore, if you do not trust the network(s) you are using it has never been safe.
- **SMS** - Text messages are sent in plain text over the network, so they are also not considered secure, additionally they are not securely stored at your device, so anyone with access to it will be able to read them.
- **Prepaid sim cards** - In some countries you are still able to use prepaid locally bought SIMcards without identifying yourself. Beware that your phone also has a unique identifier (known as the IMEI number) so switching SIM cards will will not guarantee to protect your privacy.
- **Application hacking or breaching-** Many of us have downloaded and installed phone applications. Some of them request extra access or privileges such as access to your location, contact, browsing history for marketing purposes, but on the other hand, the site provides access to other contacts too. Other factors of concern are Trojans, viruses, etc.
- **Smartphone theft** is a common problem for owners of iPhone or Android devices. The danger of corporate data, such as account credentials and access to email falling into the hands of a tech thief is a threat.

Attack Vector

By definition, an **Attack Vector** is a method or technique that a hacker uses to gain access to another computing device or network in order to inject a "bad code" often called **payload**.

This vector helps hackers to exploit system vulnerabilities. Many of these attack vectors take advantage of the human element as it is the weakest point of this system. Following is the schematic representation of the attack vectors process which can be many at the same time used by a hacker.



Some of the mobile attack vectors are −

- Malware
  - Virus and Rootkit
  - Application modification
  - OS modification
- Data Exfiltration
  - Data leaves the organization
  - Print screen
  - Copy to USB and backup loss
- Data Tampering
  - Modification by another application
  - Undetected tamper attempts
- Data Loss
  - Device loss
  - Unauthorized device access
  - Application vulnerabilities

Consequences of Attack Vectors

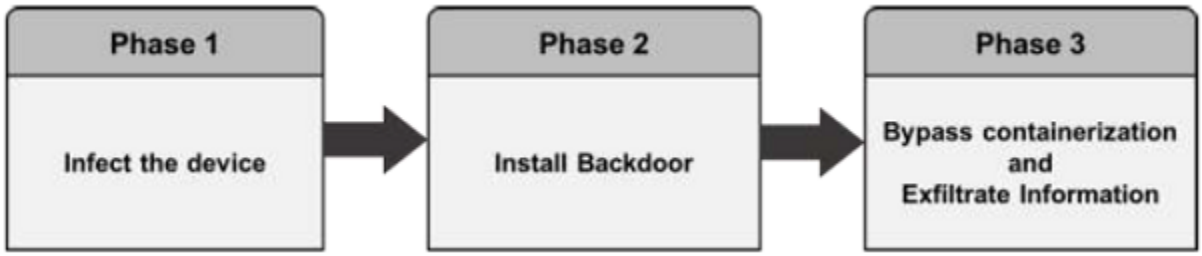
Attack vectors is the hacking process as explained and it is successful, following is the impact on your mobile devices.

- **Losing your data** − If your mobile device has been hacked, or a virus introduced, then all your stored data is lost and taken by the attacker.

- **Bad use of your mobile resources** − Which means that your network or mobile device can go in overload so you are unable to access your genuine services. In worse scenarios, to be used by the hacker to attach another machine or network.
- **Reputation loss** − In case your Facebook account or business email account is hacked, the hacker can send fake messages to your friends, business partners and other contacts. This might damage your reputation.
- **Identity theft** − There can be a case of identity theft such as photo, name, address, credit card, etc. and the same can be used for a crime.

Anatomy of a Mobile Attack

Following is a schematic representation of the anatomy of a mobile attack. It starts with the infection phase which includes attack vectors.



- **Infecting the device**

Infecting the device with mobile spyware is performed differently for Android and iOS devices.

Android − Users are tricked to download an app from the market or from a third-party application generally by using social engineering attack. Remote infection can also be performed through a Man-in-the-Middle (MitM) attack, where an active adversary intercepts the user's mobile communications to inject the malware.

iOS − iOS infection requires physical access to the mobile.

- **Installing a backdoor**

To install a backdoor requires administrator privileges .

A **backdoor** is a means to access a computer system or encrypted data that bypasses the system's customary **security** mechanisms. A developer may create a **backdoor** so that an application or operating system can be accessed for troubleshooting or other purposes.

- **Bypassing encryption mechanisms and exfiltrating information**

Spyware sends mobile content such as encrypted emails and messages to the attacker servers in plain text. The spyware does not directly attack the secure container. It grabs the data at the point where the user pulls up data from the secure container in order to read it. At that stage, when the content is decrypted for the user's usage, the spyware takes controls of the content and sends it on.

Types of Mobile Security

1. Mobile device security.
2. Mobile application security

Mobile Device Security

Different methods for mobile device security are

1. Screen locks.

All mobile devices (e.g., phones, tablets, and laptops) should have the screen lock set.

2. Lockout settings.

   After a specific no. of unsuccessful unlock attempts, the device will get locked which can only be opened through user's ID.

3. GPS.

   Many mobile devices have GPS capabilities, allowing the device to be located if it is lost or stolen.

4. Remote wiping.

   Some mobile devices allow for the device to be wiped (all data and applications are removed) remotely. This can be used if a device is unrecoverable.

5. Application controls.

   Many mobile applications attempt to access unnecessary user information (e.g., the location of the device). Controls should be used to limit the data that applications can access and to restrict the actions that applications may undertake.

Mobile Application Security

1. **Encryption**.

Ensure that mobile applications are encrypting sensitive data that is stored on the device. Encryption keys must also be created and stored securely.

2. **Authentication.**

   A best practice is for the mobile application to authenticate the user and to base access to data on the user's authentication level.

3. **Geotagging**

   Geotagging is most commonly used for photographs and can help people get a lot of specific information about where the picture was taken or the exact location of friend who logged on to service.

4. **Application whitelisting.** It is a device administration practice used to prevent unauthorized application from running. The purpose is primarily to protect device and networks from harmful application.

Mobile Threats

1. Application Based Threats
2. Web Based Threats.
3. Network Threats.

Application Based Threats.- Downloadable applications present many security issues on mobile devices, including both software specifically designed to be malicious as well as software that can be exploited for malicious purposes. It contains (Malware, Spyware, Privacy Threats, Vulnerable application)

Web –Based Threats.- Because mobile devices are often constantly connected to the Internet and used to access web-based services, web-based threats that have historically been a problem for PCs also pose issues for mobile devices It contains (Phishing Scams, Drive-By Download, Browser Exploits).

Network Threats Mobile devices typically support cellular networks as well as local wireless networks. It contains (Network Exploits, Wi-Fi Sniffing).

How to protect mobile devices

1. **Keep Your Operating System Up-to-Date.**

First, it is important to update your operating system as soon as a new version is released. Don't wait on these updates, because they often include security bug fixes

2. **Delete the Apps You Don't Use.**

Next, we recommend going through your phone and deleting any apps that you don't plan on using in the future. Every app has the potential to be infected. Often, the apps you don't use are not receiving regular updates in the app store, so they become more vulnerable to hacking attempts. It is easier to just delete the old apps from your cellphone, rather than updating them and never using them. However, if you have enough space on your hard drive to leave every app installed, make sure that "Automatic Downloads" (iOS) or "Auto-update apps" (Android) is turned on.

3. **Lock Your Phone.**

Every phone has an auto-locking security feature with a 4 or 6 digit passcode. Make sure to turn this setting on as soon as you purchase a new phone. If available, use a 6-digit passcode for a higher level of protection. Secondly, most smartphones allow you to set the length of time before auto-locking. Choose the shortest time possible (i.e. one minute). Sometimes, cell phone "hacking" can be as simple as someone stealing your phone and accessing your accounts through normal means. Make sure that every app and account is password-protected.

4. **Avoid Public WiFi for Sensitive Tasks.**

Public WiFi can be a lifesaver when you need to access Internet and don't have cell service, but these networks are not secure. When anyone can access the same WiFi, it is easy for hackers to capture your personal information, such as your passwords or credit card details. If possible, you should turn your smartphone into a wireless hotspot and use that to access the internet for your laptop instead.

5. **Don't Click on Questionable Links.**

Junk mail and other spam attempts are made all the time. Often, phishing is disguised in such a clever way that even an experienced web surfer accidentally clicks on a compromising link. You may even receive a

text message with a link to malware (called “smishing”). Android smartphones are the most susceptible to this issue. To avoid any potential problems, never click on a link from an unidentifiable source.

6. **Delete Data Remotely to Prevent Theft.**

When setting up a new cell phone, make sure to enable the "Android Device Manager" or "Find My iPhone" feature, so that you can track the phone down if it goes missing. These apps also allow you to delete the phone's hard drive remotely, before the thieves can get to it. Meanwhile, if you decide to sell your current phone or purchase a used phone, we recommend resetting the device to factory settings. This will clean out any sensitive material or malware that is still present.

7. **Be Cautious When Asked to Provide Personal Info.**

Every time you sign up for a new service online, you will probably be asked to provide personal details, such as your name and email address. We do this all the time, but it puts us at risk for spam email and texts. Always think twice before giving out information, and use two or three-factor authentication whenever it is an option.

8. **Avoid Using Unofficial Tools.**

There're many unofficial (and legally murky) software tools that promise to "jailbreak" or "root" your phone, so you can use it with other cell networks. This opens your device to potential security threats. You should be extremely cautious if you decide to use these tools, because some of them can lead to spyware and identity theft. Laws have been put in place to make it easier to officially unlock your phone - Contact your cellular service carrier for details.

9. **Be Careful About Granting Permissions.**

By law, smartphone apps must ask for permission to access your personal data and various phone functions, such as the camera or microphone. Often, an app will need access to work properly, but some apps abuse these permissions. For instance, the Google Play Store has a less rigorous vetting process for accepting new apps. Bad actors can take advantage of these vulnerabilities and create an app that steals your personal data. Think twice before granting permission to an app developer you don't completely trust.

10. **Avoid Auto-Login Features.**

Finally, we recommend turning off your phone's auto-login features, so that it is harder for bad actors to access your accounts. Auto-login can be extremely useful when you don't want to remember or type passwords, but you shouldn't use it for sensitive apps like online banking and email. If a thief somehow figured out your phone's password, they would be able to open any app without signing in. To keep this from happening, you can also enable the setting that erases your phone's contents after 10 failed login attempts. And if you must use an auto-login feature, do it with a secure password manager app that requires a separate password to function.