Network Interface card (NIC):

→ Networking device

→ Also known as N/w Adapter card, ethernet card, LAN card.

→ NIC converts parallel data stream into serial data stream & vice versa.

& Types → (a). Media specific: Different types of NICs are used to connect with different types of media.

(b). N/w design specific: A specific N/w design needs a specific LAN card.

3 Methods to detect Malware:

(a). Signature detection: Detects the pattern.

(b). Change detection: detects change in files.

(c). State Detection: Anomaly based. Detects change in behaviour.

Honeypot: → Honeypot is a trap to detect unauthorized access
→ It is a computer or an IP address space that appears to be a part of n/w unprotected & monitored which seems to contain information but its just a trap for attackers.
Honeynet → network of honeypots.

Cellphone Security

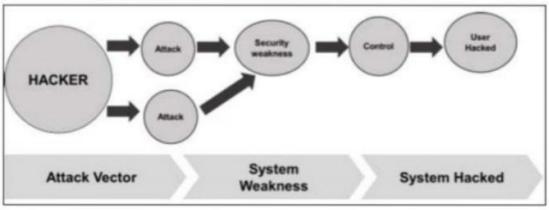
Mobile Security as a concept deals with the protection of our mobile devices from possible attacks by other mobile devices, or the wireless environment that the device is connected to.

Following are the major threats regarding mobile security −

- Loss of mobile device. This is a common issue that can put at risk not only you but even your contacts by possible phishing.
- Application hacking or breaching. This is the second most important issue. 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 highly coveted smartphones such as 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.

Mobile Security - Attack Vectors

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
  - Jail-broken devices
- Data Loss
  - Device loss
  - Unauthorized device access
  - Application vulnerabilities

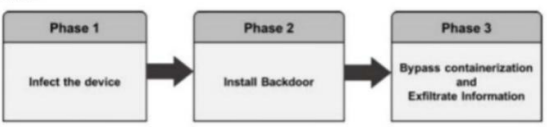
Consequences of Attack Vectors

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. Infecting the device can also be through exploiting a zero-day such as the JailbreakME exploit.

Installing a backdoor

To install a backdoor requires administrator privileges by rooting Android devices and jailbreaking Apple devices. Despite device manufacturers placing rooting/jailbreaking detection mechanisms, mobile spyware easily bypasses them −

Android − Rooting detection mechanisms do not apply to intentional rooting.

iOS − The jailbreaking "community" is vociferous and motivated.

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.

DMZ (Demilitrized Zone Networks).