**Module 2 Technologies & Tools**

**2.5 Mobile Security**

**Mobile Devices**

* Any easily transportable computing systems

1. Laptops, tablets, hybrids, smartphones, watches, IoT (Internet of Things)

**Connection Methods**

* Cellular
* Wi-Fi
* Bluetooth
* NFC (Near-Field Communication)
* SATCOM (Satellite Communication)
* ANT – proprietary multicast wireless
* Infrared – using light in infrared spectrum
* USB/Firewire

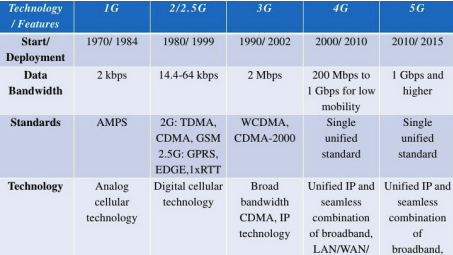
**Cellular Communications**

* Components

1. Cellular layout (towers)
2. Base station (connects to tower)
3. Mobile switching office (centrepiece of operation)
4. Public switched telephone network (PSTN)

* Voice technologies

1. Long-Term Evolution (LTE)
2. Code Division Multiple Access (CDMA)
3. Global Systems Mobile (GSM)



**Bluetooth**

* Personal-Area Network (PAN) – short-range wireless connectivity
* Uses spread spectrum, frequency hopping, full-duplex signal
* Pairing devices forms a *piconet*
* Bluesnarfing/Bluejacking
* If needed, set to non-discoverable

**Near-Field Communications (NFC)**

* Standards for contactless communication between devices
* Chips generate electromagnetic fields
* Modes of operation

1. Peer-to-peer mode – 2 mobile devices exchange data
2. Read/write mode – active device receives data from passive device
3. Card Emulation – device used as contactless credit card

**Mobile Device Management (MDM)**

* Administration of mobile devices in organisation
* Software used to inventory, monitor, manage & secure employees’ mobile devices, deployed across multiple mobile service providers & Operating Systems
* Device enrolment, provisioning & inventory
* Configuration management/updating
* Managing apps
* Enforcing policies

**Mobile Device Management Capabilities**

* Mobile App Management (MAM)

1. Restricting apps
2. Digitally signing apps
3. Distribution from centralised, controlled source
4. Managed through whitelisting/blacklisting

* Mobile Content Management (MCM)

1. Controlling access to data & file storage

* Push notification services

1. Brief message/alert
2. OS push notification service (OSPNS)
3. Allows auto-updating base OS & client apps

* Geo-location

1. Uses devices’ GPS
2. Some apps (Maps, Foursquare)

* Geo-Fencing

1. Defining geographic perimeter
2. Eg. Texting in front seat of car

**Mobile Device Management Concepts**

* Separate personal & business content
* Storage segmentation – segregate business & personal storage
* Containerisation

1. Separate sensitive corporate information from user’s personal use of device
2. Ability to isolate apps & control app functions

* Remote wipe/Sanitisation

1. Sending command from centralised management server to remotely clear data
2. Used when device lost/stolen/employee terminates

* Full device encryption

1. System & application
2. Use TPM (Trusted Platform Module) when available (laptops)

* Screen locks/Lockout – screen configured to automatically lock after set time
* Passwords & Pins – based on corporate policy
* Biometrics
* Context-aware authentication

1. Additional criteria used for authentication/device usage
2. Eg. Location, time, activity etc.

**Deployment Models**

* Bring Your Own Device (BYOD)

1. Employees use own personal device
2. Highest risk
3. Adherence with company policies

* Choose Your Own Device (CYOD)

1. Employees choose from list of approved devices

* Company-Owned Provided Equipment (COPE)

1. Company has complete control over device

* Virtual Desktop Infrastructure (VDI)

**Enforcement & Monitoring**

* Third-party app stores

1. Restrict based on policy
2. Whitelist apps

* Rooting (Android)/Jail-breaking (Apple)

1. User takes full control of device (root)
2. Should be forbidden for corporate devices

* Sideloading – transfer data between 2 devices (side channel)
* USB On-the-Go (OTG)

1. Standard that enables mobile devices communication using USB cable

* Custom Firmware

1. Valid use – forensics acquisition
2. Invalid – bypass policy

* Carrier Unlocking

1. Modifying device to use different cell carrier w/o purchasing new device
2. Now legal in US

* Firmware OTA (Over-the-Air) updates

1. Automatically update device when attached to corporate Wi-Fi/computers
2. Users may have no control over updates