UF1. Seguretat en dispositius mòbils i IoT

UF1. Seguretat en dispositius mòbils i IoT

Índex

- Mòbils
  - Introducció
  - Arquitectura dels dispositius mòbils.
  - Sistemes operatius mòbils.
  - Seguretat en dispositius mòbils: iOS / Android

- IoT
  - Introducció
  - Arquitectura dels dispositius IoT
  - Sistemes operatius per IoT
  - Vulnerabilitats i amenaces
  - Bones pràctiques per la securització

UF1. Seguretat en dispositius mòbils i IoT

- Mòbils
  - Introducció
  - Arquitectura dels dispositius mòbils.
  - Sistemes operatius mòbils.
  - Seguretat en dispositius mòbils: iOS / Android

UF1. Seguretat en dispositius mòbils i IoT

- **Mòbils**
  - **Introducció**
  - Arquitectura dels dispositius mòbils.
  - Sistemes operatius mòbils.
  - Seguretat en dispositius mòbils: iOS / Android

UF1. Seguretat en dispositius mòbils i IoT

Introducció. Dispositius mòbils.

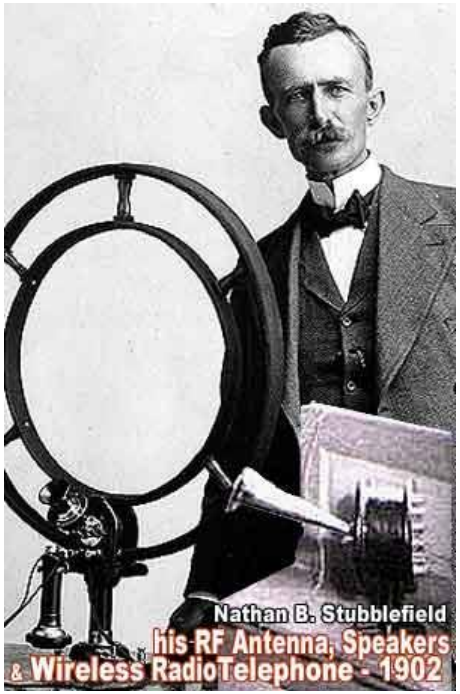
- Segons wikipedia:
  - Un **dispositiu mòbil** és un aparell de mides reduïdes i lleuger que pot ser utilitzat mentre es transporta.
  - Normalment té **capacitat** per a **connectar-se** a **Internet** i sol estar dissenyat per a **realitzar** una **tasca** concreta o **més d'una tasca**.
  - Aquest dispositiu normalment també pot connectar-se a un ordinador per tal de complementar les seves funcions, actualitzar-se, transferir dades, etc.
  - Segons la mateixa wikipèdia trobaríem diversos **tipus de dispositius mòbils**: telèfon mòbil, telèfon intel·ligent, receptor GPS, Organitzador personal (PDA), cercapersones, ordinador portàtil, tauleta tàctil, calculadora, reproductor d'àudio digital, consola portàtil, càmera fotogràfica, càmera de vídeo, …
  - Nosaltres **estudiarem els telèfons mòbils**, ja que pràcticament ha adquirit **totes** les **funcionalitats** de la **resta** de **dispositius mòbils** comentats en el paràgraf anterior.

UF1. Seguretat en dispositius mòbils i IoT

Introducció. Dispositius mòbils.

Història

- En el següent link extret d'Internet, podeu veure un exemple de l'evolució dels dispositius mòbils en el temps.
- Sabíeu que el primer mòbil de la història data de l'any 1902 !!

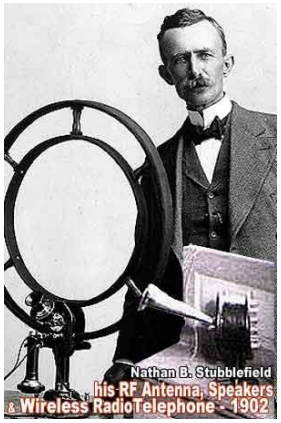


UF1. Seguretat en dispositius mòbils i IoT

Introducció. Dispositius mòbils.

Història

1902



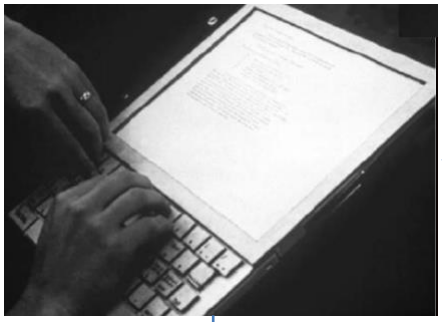
1956

1983

1984

1989

1992



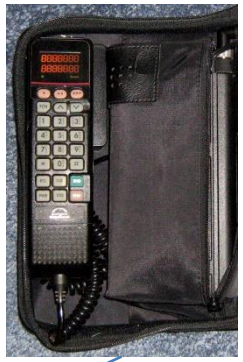
1994

UF1. Seguretat en dispositius mòbils i IoT

Introducció. Dispositius mòbils.

Història

1994



1996

1998

1999

2002

2004

2007

.....

2010

.....

UF1. Seguretat en dispositius mòbils i IoT

Introducció. Dispositius mòbils.

Història

- Al llarg de la història hi ha hagut una gran aparició de dispositius. Per tal de classificar-los es van agrupar en generacions, cadascuna amb una sèrie de característiques. (Això us ho deixaré a vosaltres en una pràctica!!)

UF1. Seguretat en dispositius mòbils i IoT

- **Mòbils**
  - **Introducció**
  - **Arquitectura dels dispositius mòbils.**
  - Sistemes operatius mòbils.
  - Seguretat en dispositius mòbils: iOS / Android

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius mòbils.

Hardware

- El hardware dels dispositius mòbils tindria com a part fonamental els següents elements:

✓ Placa base. ✓ CPU. ✓ GPU. ✓ Memòria RAM. ✓ Memòria d'emmagatzematge. ✓ Sensors. ✓ Antena. ✓ Antena Wifi. ✓ Antena NFC. ✓ Bluetooth. ✓ Port infrarroig.	✓ Càmera. ✓ Pantalla. ✓ Teclat. (Avui en dia en desús en mòbils tàctils) ✓ Micròfon. ✓ Altaveu. ✓ Bateria. ✓ Port de càrrega. (També per passar dades) ✓ Mòdul GPS. ✓ …

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius mòbils.

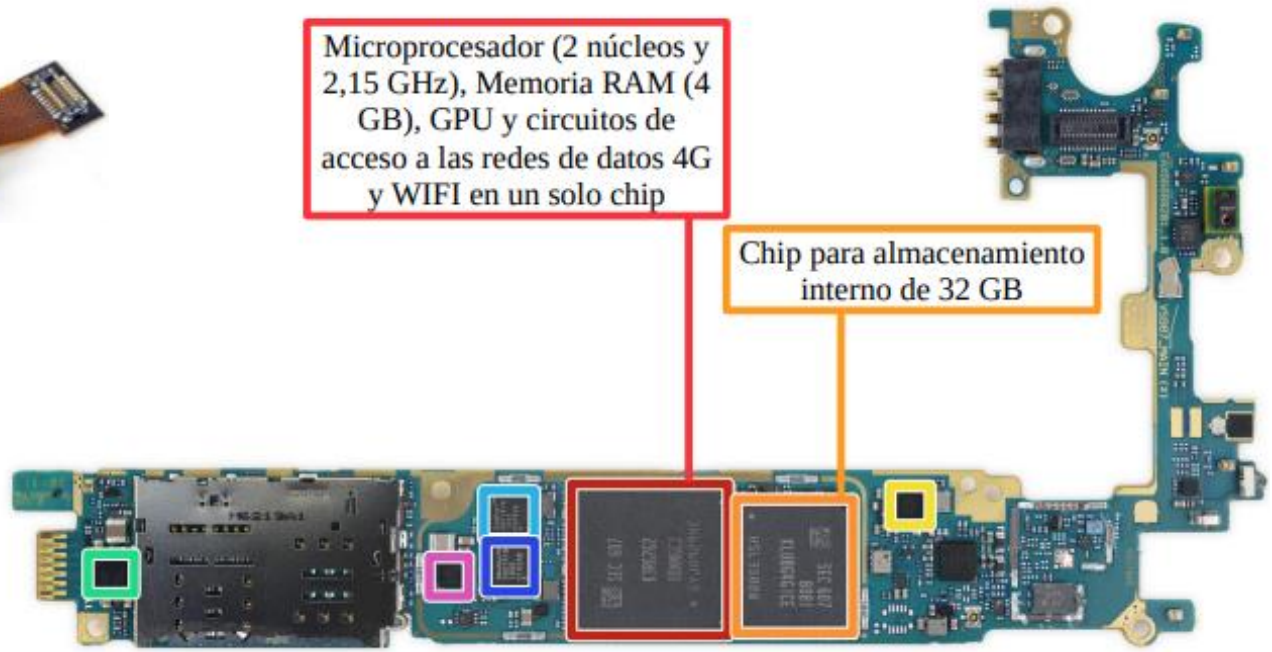
Hardware

- **Placa base**. Microprocessador (la majoria ARM)+GPU.
- **Memòria RAM**.
- **Memòria emmagatzematge. ROM + Tarjeta memòria**.
- **Sensors i connectivitat.** Antena + antena wifi + acceleròmetre + giroscopi + sensor de proximitat + càmeres + connexió Bluetooth + …
- **Pantalla.**
- **Bateria.**
- **Altaveus.**
- **Micròfon.**
- **Conexió micro USB, micro USB-C, …**

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius mòbils.

Hardware



UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius mòbils.

Hardware. Article interessant

- En el següent enllaç hi ha un article prou interessant. Seria recomanable la seva lectura.

  https://www.nobbot.com/pantallas/tecnologia-forense-te-destripamos-smartphone/

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius mòbils.

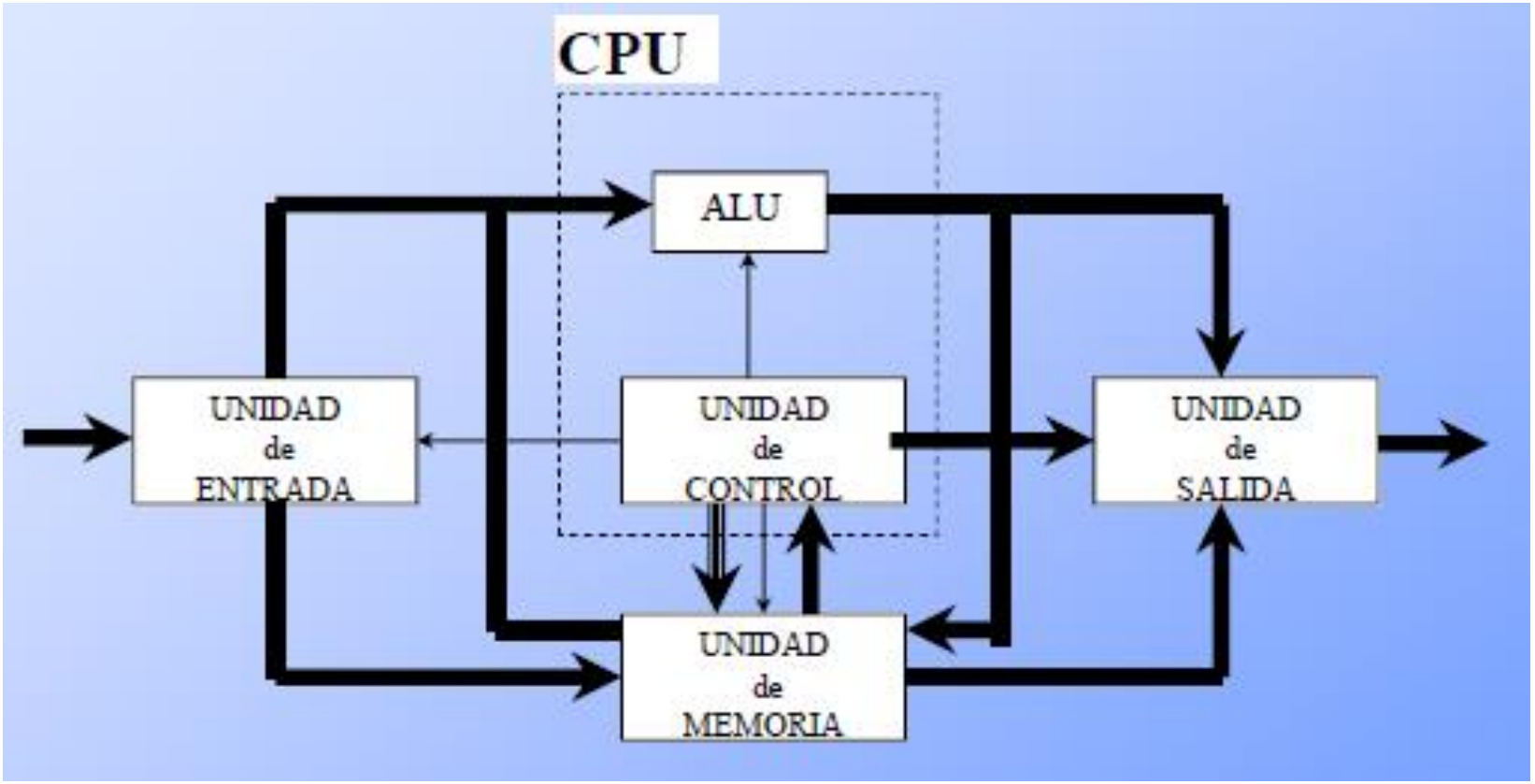
Arquitectura i funcionament bàsic.

- La CPU normalment és ARM. De tipus RISC (Reduced Instruction Set Computing). En els PC's convencionals seria de tipus CISC.
- CPU òptima, consum menor, ràpida, més econòmica, més senzilla, amb major grau d'integració (pot tenir més nuclis).

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius mòbils.

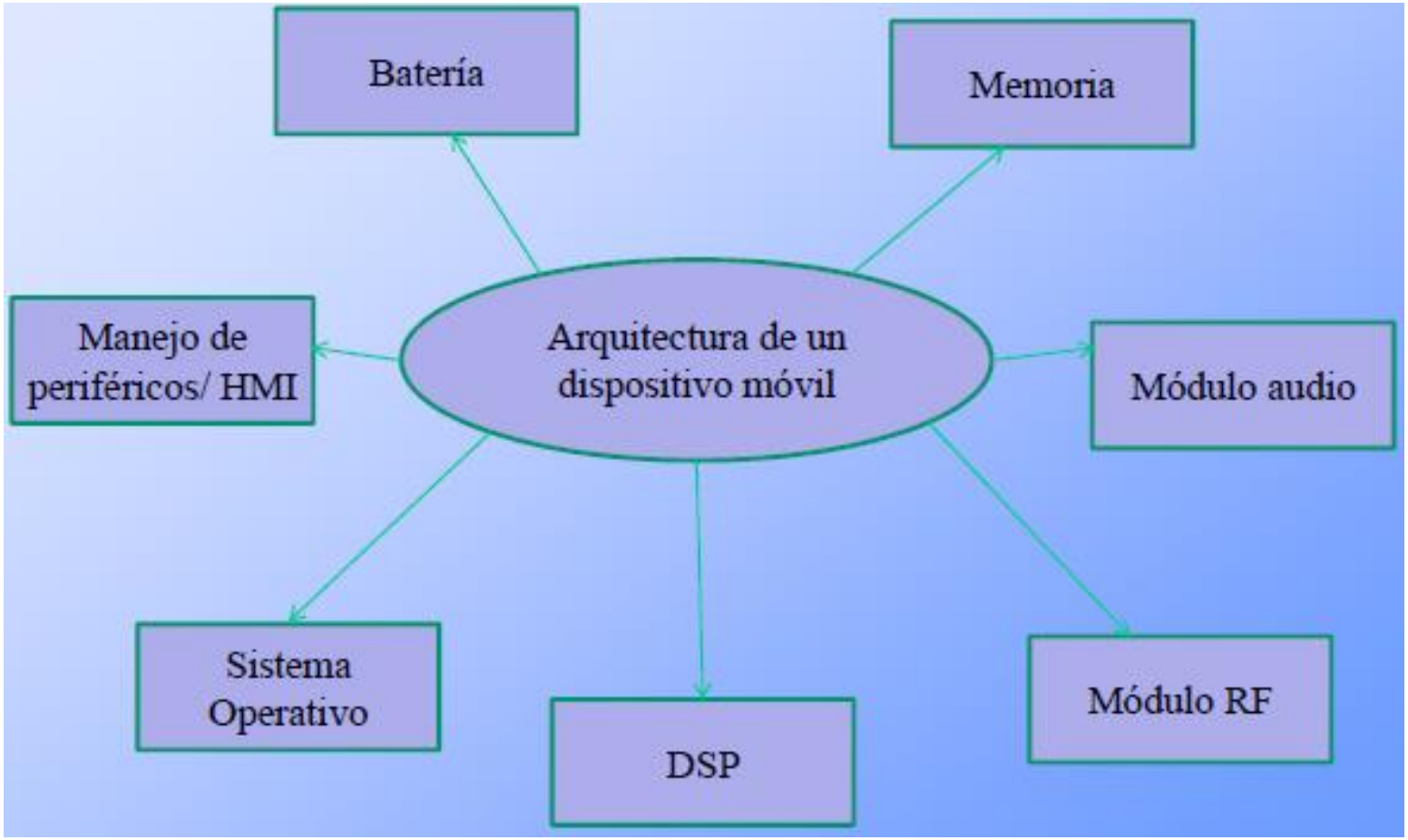
Arquitectura i funcionament bàsic.



UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius mòbils.

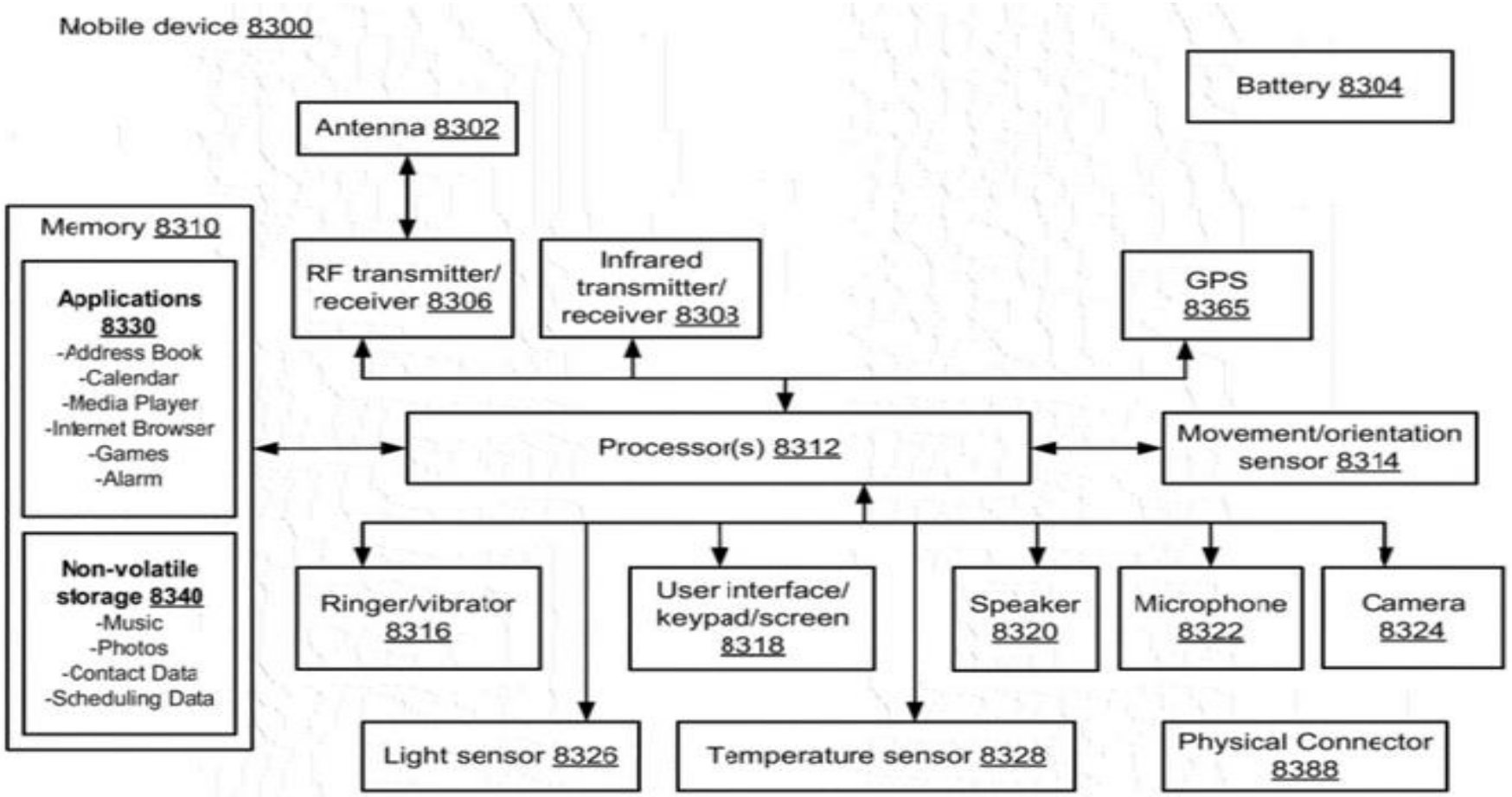
Arquitectura i funcionament bàsic.



UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius mòbils.

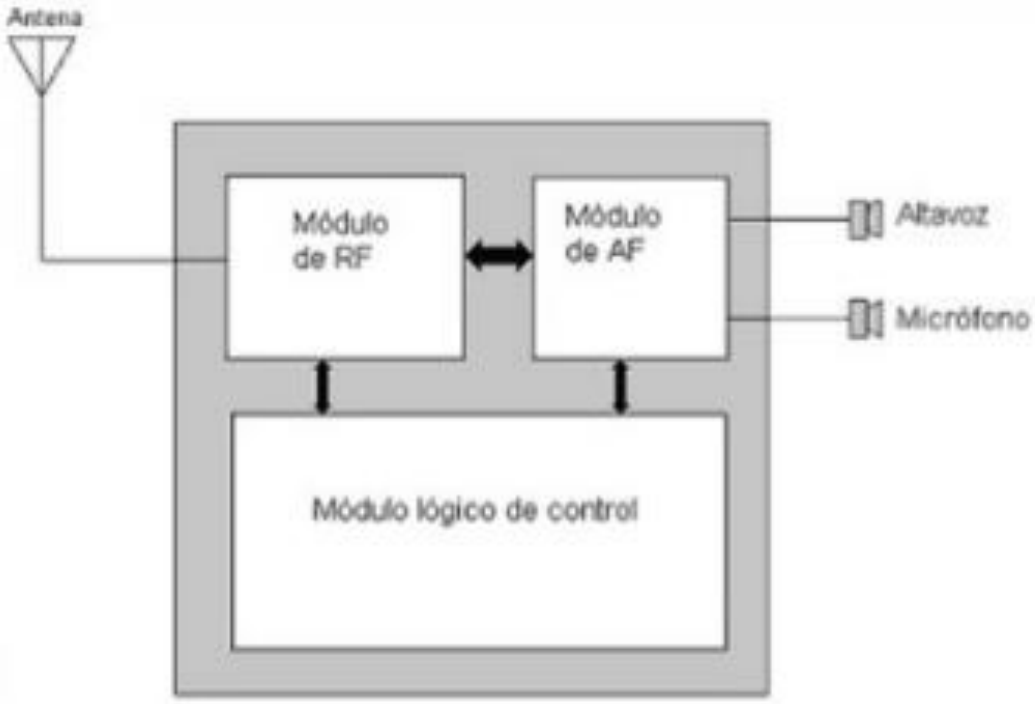
Hardware. Exemple infraestructura.



UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius mòbils.

Arquitectura i funcionament bàsic.



- Mòdul de RF (Ràdio Freqüència).
- Mòdul AF (Àudio freqüència).
- Mòdul lògic de control (CPU).

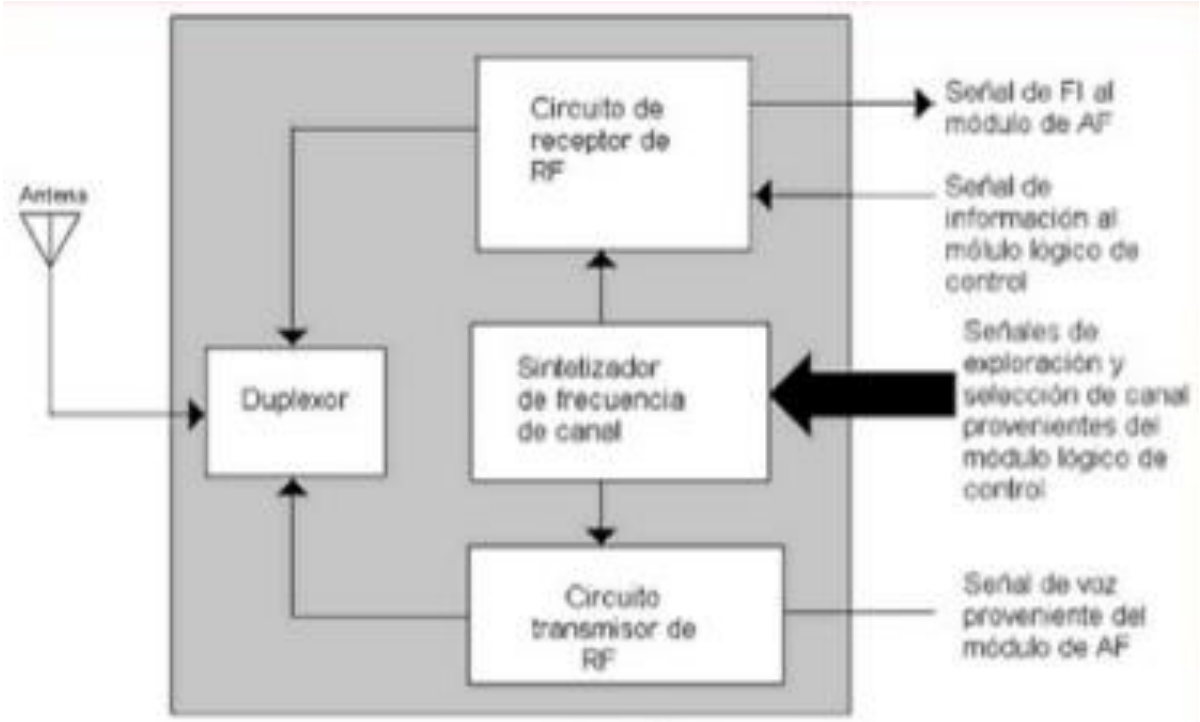
UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius mòbils.

Arquitectura i funcionament bàsic.

Mòdul de RF (Ràdio Freqüència).

- Tracta les senyals que entren o surten del dispositiu mòbil.



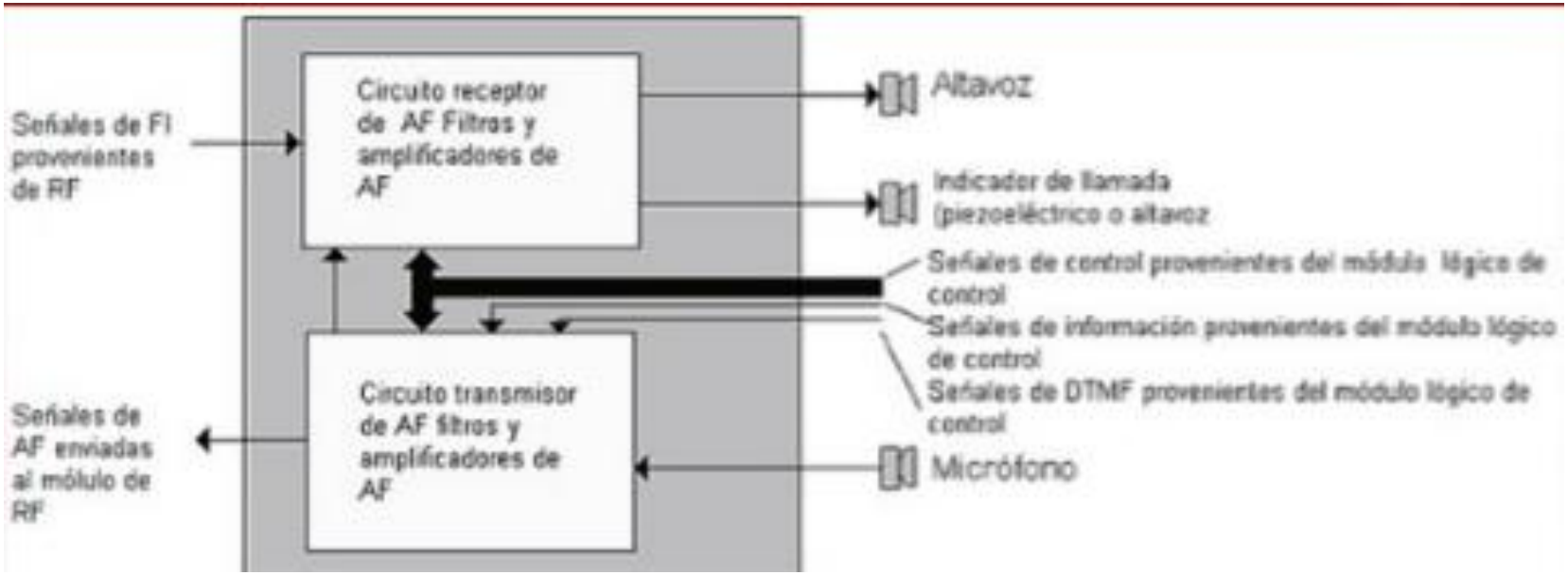
UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius mòbils.

Arquitectura i funcionament bàsic.

Mòdul d'AF (Àudio Freqüència).

- És responsable de la conversió de les senyals de la FI (Freqüència Intermitja) provinents del mòdul RF, en senyals de veu que es puguin escoltar en el receptor del telèfon.

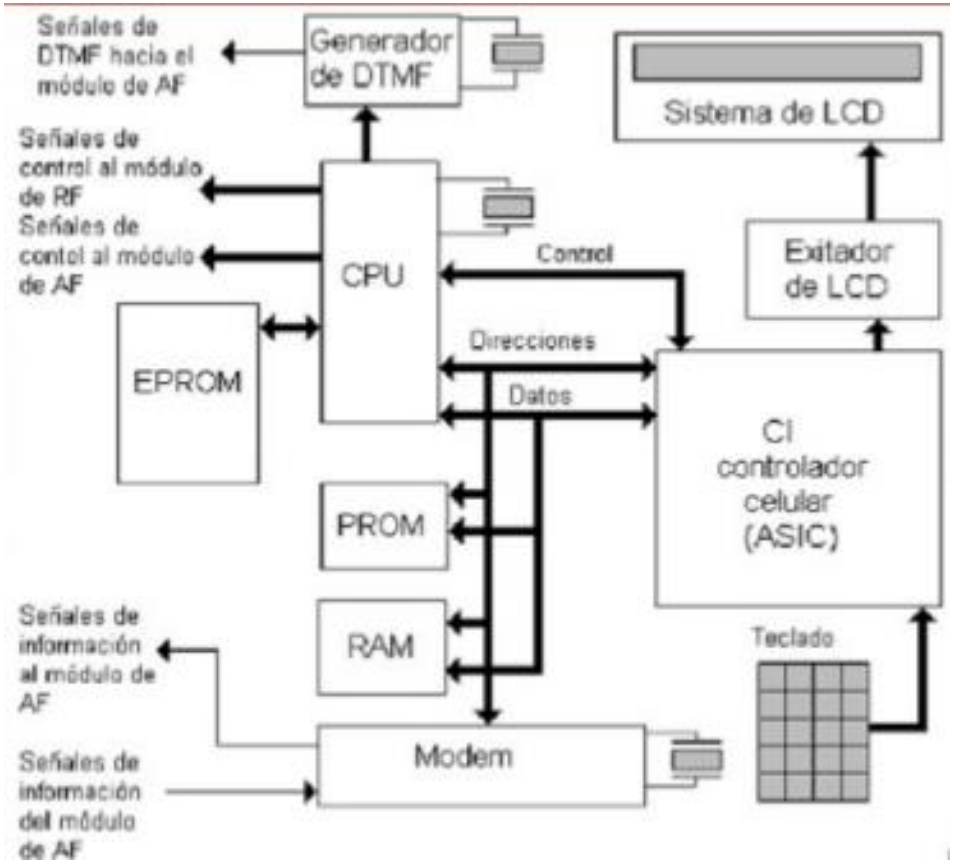


UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius mòbils.

Arquitectura i funcionament bàsic.

Mòdul Lògic de Control. Té una arquitectura semblant a un ordinador convencional.

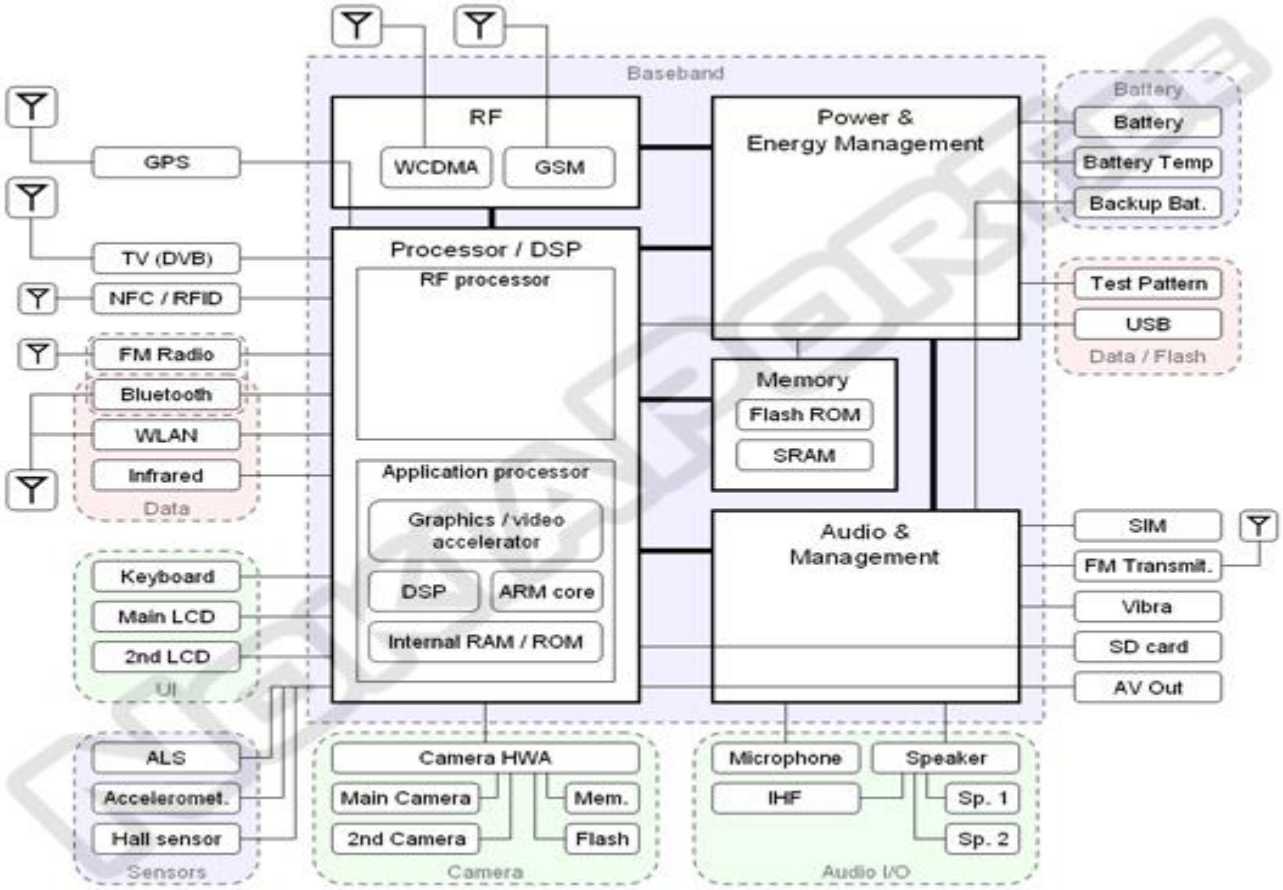


UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius mòbils.

Arquitectura i funcionament bàsic.

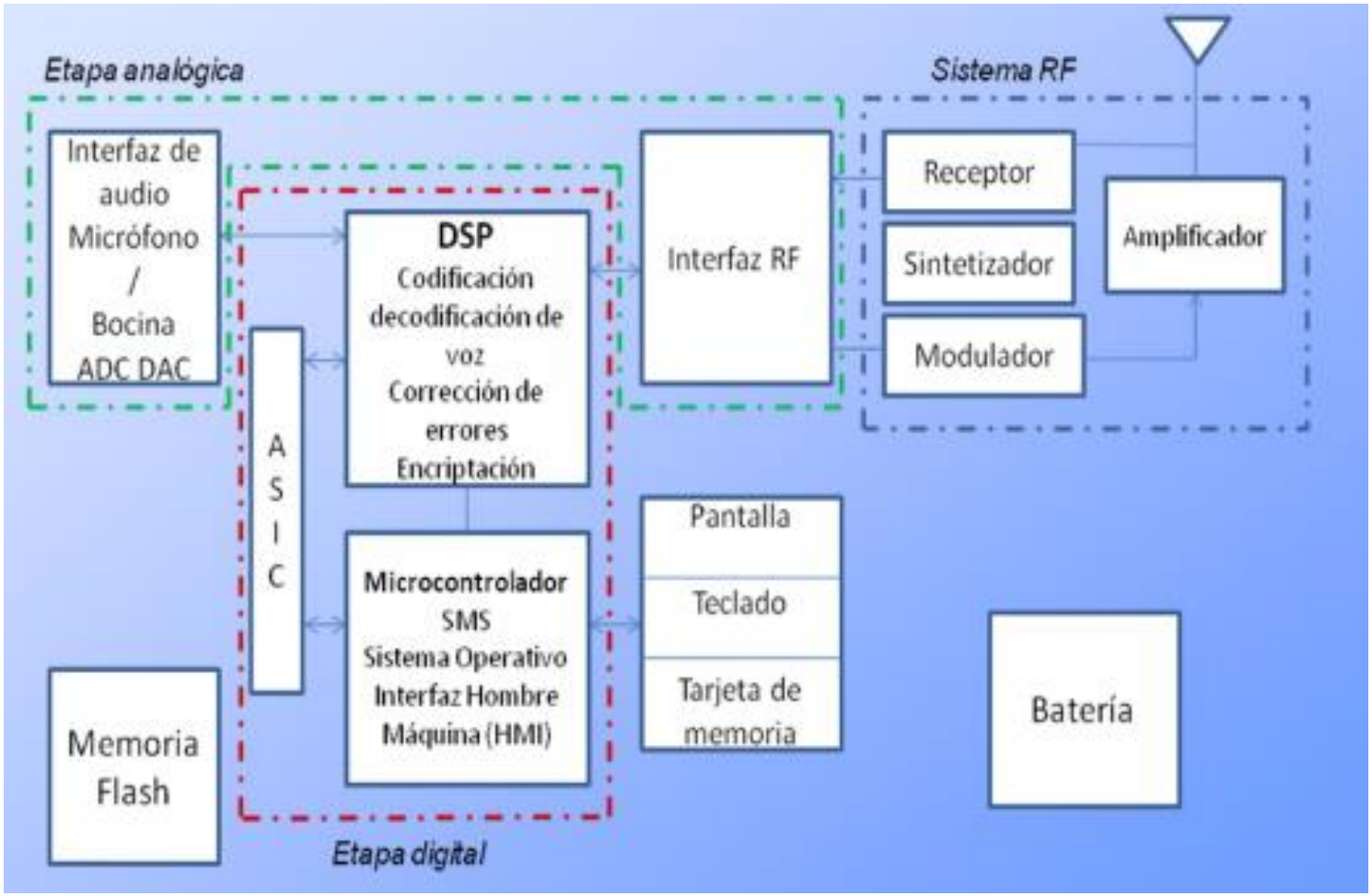
- Segons la marca que dissenya els telèfons hi haurà alguna petita modificació.
- Ex: Nokia



UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius mòbils.

Arquitectura i funcionament bàsic.



UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius mòbils.

Arquitectura i funcionament bàsic.

- El sistema de banda base consta de 2 circuits integrats:
  - 1 digital.
  - 1 analògic.
- El **circuit integrat Digital:**
  - Té un **circuit** de **rellotge** i diversos **ports** i **comportes CMOS** que li permeten **comunicar** amb altres elements.
  - S'encarrega del **processament** del **senyal GSM** (Global System for Mobile communications) **mitjançant** un procés digital (**DSP** o Digital signal processing).
  - A dintre hi ha el **Microcontrolador**, que s'encarrega de realitzar les diferents operacions amb l'ajuda de RAM interna.
  - Com a resum: És un **circuit integrat capaç de realitzar les tasques de codificació i descodificació necessàries per construir les diferents senyals de transmissió i recepció.**

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius mòbils.

Arquitectura i funcionament bàsic.

- El sistema de banda base consta de 2 circuits integrats:
  - 1 digital.
  - 1 analògic.
- El **circuit integrat Analògic:**
  - Té un **sistema A/D – D/A** (analògic-digital i digital/analògic) que li permet **processar senyals de tipus IQ** (I=fase, Q= Quadratura) i **senyals de veu**.
  - Consta de **circuits auxiliars** pel **control RF** (Radio freqüència), control de **càrrega per la bateria**, i el sistema **d'anàlisi d'engegada del mòbil**.

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius mòbils.

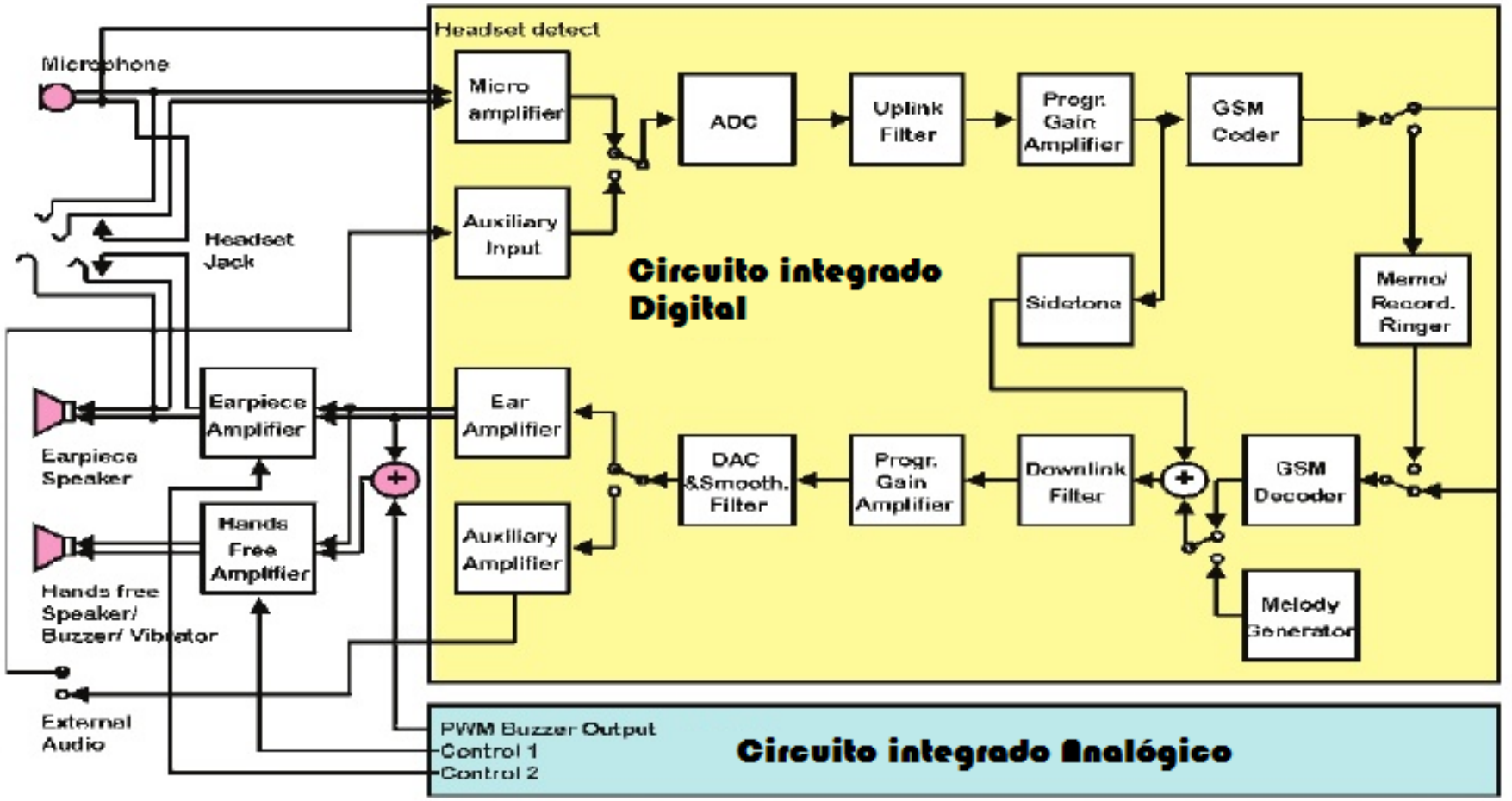
Arquitectura i funcionament bàsic.

- El **circuit integrat Analògic:**
  - Per **comunicar-se amb el circuit digital** té un **port sèrie** en **banda base (BSP)** i un altre **port per la comunicació per veu (VSP)**, que li permeten comunicar-se amb el DSP.
  - Té un **port UPS per comunicar-se amb el microcontrolador** del circuit digital, i un **port TSP per comunicar-se amb el rellotge**, per tal que les etapes digital i analògica estiguin en sincronia.

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius mòbils.

Arquitectura i funcionament bàsic.



UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius mòbils.

Arquitectura i funcionament bàsic.

- Enllaç molt interessant comparativa entre arquitectures mòbils. (Any 2015)

UF1. Seguretat en dispositius mòbils i IoT

- **Mòbils**
  - **Introducció**
  - **Arquitectura dels dispositius mòbils.**
  - **Sistemes operatius mòbils.**
  - Seguretat en dispositius mòbils: iOS / Android

UF1. Seguretat en dispositius mòbils i IoT

Sistemes operatius mòbils.

- Al llarg de la història del mòbils hi ha hagut una gran quantitat de sistemes operatius per a mòbils:

Android	Palm OS
Bada	Symbian OS
BlackBerry OS	Windows CE
EMUI	Windows Mobile
Firefox OS	Windows Phone
iOS	Moblin (proyecto)
MeeGo	Maemo
MIUI	Sailfish OS

UF1. Seguretat en dispositius mòbils i IoT

Sistemes operatius mòbils.

- Nosaltres estudiarem dos dels sistemes operatius més característics i presents actualment. Un de **propietari** , i un de **codi obert**:
  - **Android**. Present en Smartphones, tablets, AndroidTV, …
  - **IOS**. De la companyia Apple. Present en iPhone, iPad, …
- Per cadascun veurem la seva estructura i la seva seguretat.

UF1. Seguretat en dispositius mòbils i IoT

- **Mòbils**
  - **Introducció**
  - **Arquitectura dels dispositius mòbils.**
  - **Sistemes operatius mòbils.**
  - **Seguretat en dispositius mòbils: iOS / Android**

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

- **Sistema de fitxers iOS.**
- FileSystem HFSX (Sistema Jeràrquic d'Arxius)
  - Variació del HFS+ (Sistema Jeràrquic d'Arxius Extès)
  - S'ha substitutït per APFS (Sistema d'Arxius d'Apple)-> Optimitzat per unitats flash i d'estat sòlid. A partir del 2017.
- Conté 2 particions

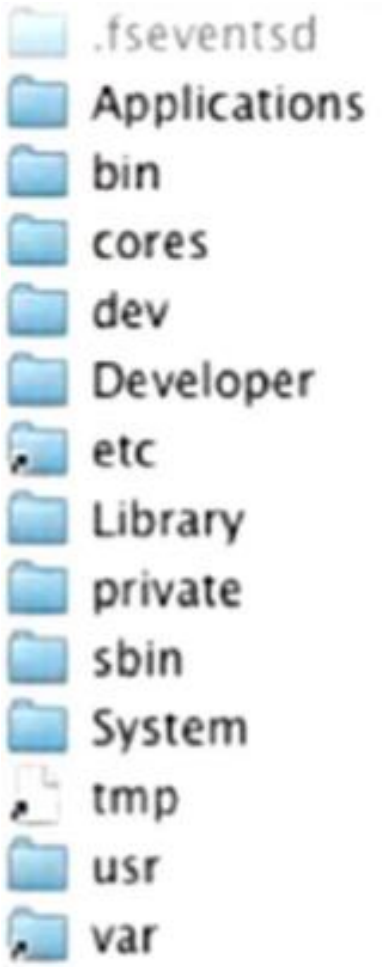
ID	Type	Offset	Size	Name	(3)
0	MBR	0	1		
	Free	1	62		
1	Apple_HFS	63	128000	← OS partition	
2	Apple_HFS	128079	1854342	← Data partition	
	Free	1982421	13877291		

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Sistema de fitxers iOS. Partició OS (Sistema Operatiu)

- **/Library/:**
  - Conté plugins del sistema y de configuració, referents a l'àudio, bluetooth, etc...
- **/private/:**
  - Conté /etc/ y /var/ que inclouen els fitxers fstab (discos y particions) y passwd.
- **/System/:**
  - Conté llibreries core del sistema.
- **/usr/:**
  - Conté binaris executables y dades de la configuració horària.



UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Sistema de fitxers iOS. Partició DATA (Dades)

- **/Keychains /:**
  - Conté "keychain.db" passwords d'usuari de distintes aplicacions.
- **/Logs/:**
  - Logs del sistema.
- **/mobile/:**
  - Informació d'aplicacions i configuració de l'usuari
  - Contactes, Calendari, Cookies, Mail, … .
- **/Preferences/:**
  - Configuració referent als recursos de la xarxa.
- **/Root/:**
  - Informació del GPS i de certificats.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Sistema de fitxers iOS.

Datos	Ubicación
Bases de Datos Aplicaciones	/mobile/Application/
Contactos	/Library/AddressBook/
Call Log	/Library/CallHistory/
Información del Portador	/Library/Carrier Bundles/
Favoritos e Historial	/Library/Safari/
SMS & MMS	/Library/SMS/
Mail	/Library/WebKit/
Fotos	/media/DCIM y /media/PhotoData/

https://norfipc.com/celulares/rutas-ubicacion-archivos-datos-informacion-iphone.html

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

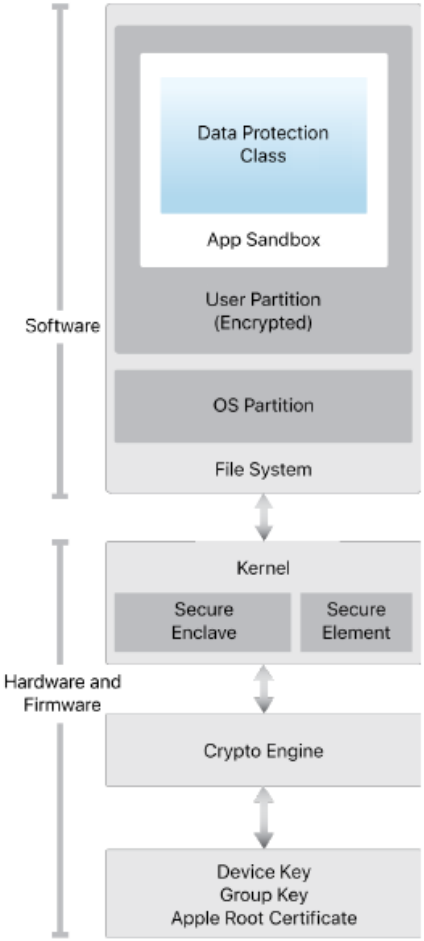
Seguretat iOS. Seguretat del sistema.

- La seguretat del sistema inclou:
  - El procés d'engegada del dispositiu.
  - Les actualitzacions del software.
  - El funcionament del sistema operatiu.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS. Seguretat del sistema.

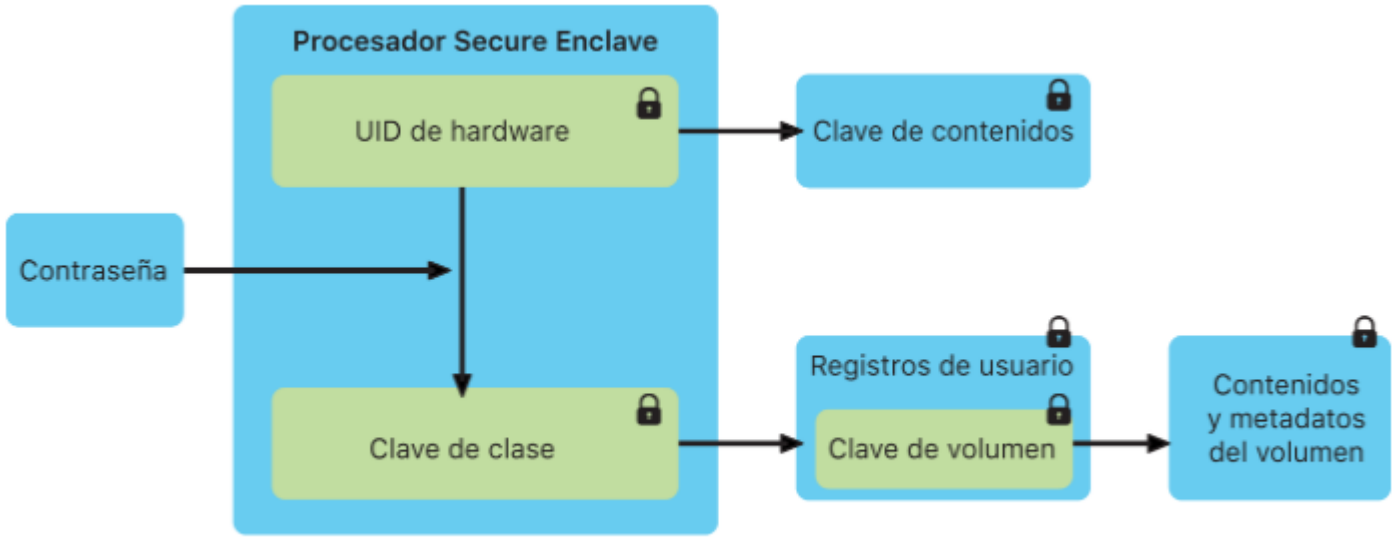


UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS. Característiques de seguretat.

- **Secure Enclave** és un coprocessador que incorpora un gestor de claus basat en hardware aïllat del processador principal.
- Les dades de la clau s'encripten en Secure Enclave amb un sistema en un xip (SoC) que inclou un generador de nombres aleatoris.



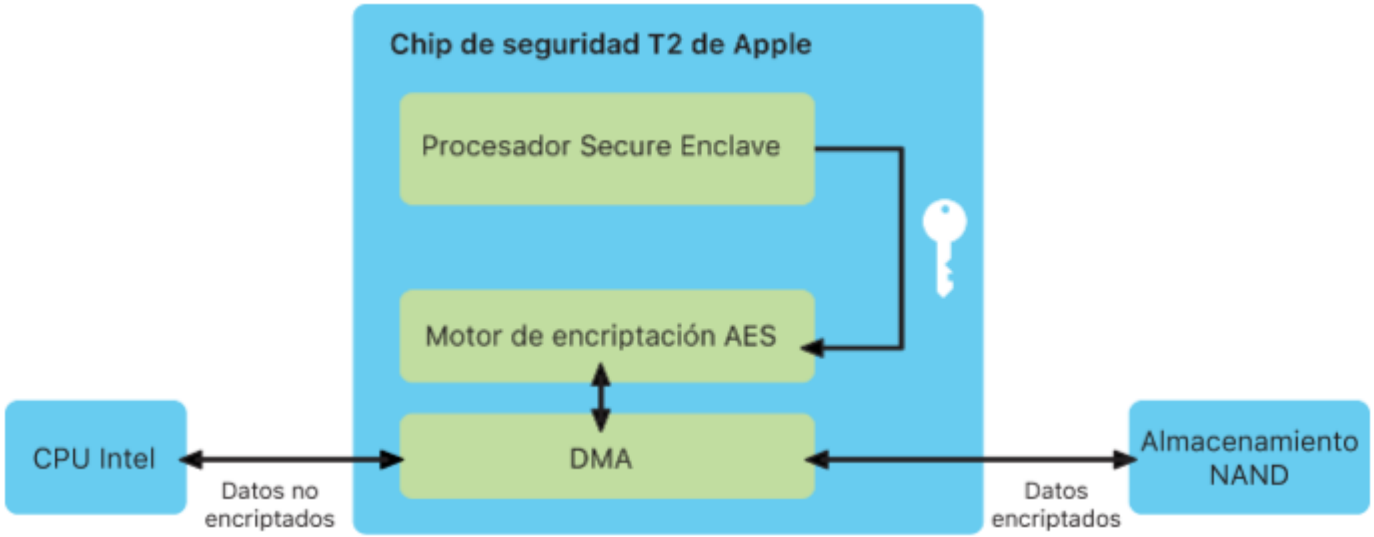
El procesador Secure Enclave.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS. Característiques de seguretat.

- Encriptació dels arxius (Crypto Engine)
  - Sistema de xifrat dedicat AES de 256 bits.
- **Secure Enclave** genera les seves pròpies claus de forma segura i utilitza:
  - UID (unique id) Única per cada dispositiu.
  - GID (device group id) comú per cada familia de processadors A5, A6, etc.
- Les claus s'esborren de forma segura quan és necessari, i es creen durant la fabricació. Cap software ni firmware les pot llegir directament.



UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS. Característiques de seguretat.

- L'UID anirà associat a cada dispositiu de forma que si un dispositiu, com el SSD intern, es trasllada a un altre, no es podrà accedir als arxius, ja que l'altre dispositiu no conté el UID associat al dispositiu inicial.
- A part de l'UID i del GID, es generen altres claus criptogràfiques. Aquestes són creades pel generador de nombres aleatoris (RNG) del sistema mitjançant un algorisme basat en codi font CTR_DRBG.
- L'entropia del sistema es genera a partir de variacions temporals durant l'arrencada, i d'interrupcions de sincronització que es produeixen després d'haver arrencat el dispositiu.
- El procés d'esborrat de les claus que s'han guardat, és igual de segur que el procés de creació.
- Els dispositius iOS inclouen una funció dedicada a esborrar dades segures anomenada **Effaceable Storage** (Emmagatzematge eficaç).

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS. Engegada del dispositiu.

- Es protegeix l'arrancada i execució del SO.
- Es garanteix que el nivell més baix del software no s'ha manipulat.
- Quan s'engega el dispositiu s'executa codi de la Boot ROM. (iBoot)
- En la fabricació del xip, és on s'ha establert que el codi és de confiança i segur. (Arrel de confiança de hardware).
- El codi del Boot ROM conté la clau pública Apple Root CA, que s'utilitza per verificar que Apple ja havia signat el codi abans permetent que es carregui.
- Quan s'acaba l'execució del codi de la Boot ROM (procés iBoot), es verifica i executa el nucli d'iOS.
- En dispositius antics hi ha una etapa addicional LLB (Low-Level Bootloader) abans de verificar i carregar el iBoot.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS. Engegada del dispositiu.

- Quan iBoot acaba de fer les tasques assignades, verifica i executa el kernel de iOS.
- Un error en carregar o verificar les etapes següents es gestiona de manera diferent segons el maquinari:
  - La ROM d'arrencada no pot carregar LLB (dispositius anteriors): mode DFU
  - LLB o iBoot: mode de recuperació
- En qualsevol dels dos casos, el dispositiu s'ha de connectar a iTunes mitjançant USB i restaurar a la configuració predeterminada de fàbrica.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS. Engegada del dispositiu.

- **Secure Enclave** és un coprocessador que incorpora un gestor de claus basat en hardware aïllat del processador principal.
- El Registre de progrés d'arrencada (BPR) l'utilitza Secure Enclave **per limitar accés a les dades de l'usuari** en diferents modes i s'actualitza abans d'entrar en els modes següents:
  - Mode DFU: configurat mitjançant l'arrencada ROM en dispositius amb SoC A12.
  - Mode de recuperació: configurat per iBoot en dispositius amb Apple A10, S2 i en els més nous sistemes en xip (SoCs).

- S'utilitza **l'Autorització de Software de Sistema** per evitar que es tornin a versions anteriors del sistema iOS on hi havia vulnerabilitats, per a que no puguin ser utilitzades per un atacant.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS. Engegada del dispositiu.

- **Després de la inicialització del nucli** iOS, s'activa la **protecció** del nucli (KIP) **per evitar modificacions** del codi de kernel i del controlador. El controlador de memòria proporciona una **regió de memòria física protegida** que l'iBoot **utilitza per carregar el kernel i les extensions del kernel.**
- Un cop **finalitzada l'arrencada**, el controlador de memòria **denega l'escriptura** a la regió de **memòria física protegida**.
- A més, la unitat de gestió de memòria (**MMU**) està configurada per **evitar que el codi privilegiat de mapeig de la memòria física pugui sortir fora de la regió de memòria protegida**, i per **evitar l'escriptura en el mapeig de memòria física** dins la regió de memòria del nucli.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS. Actualització del sistema.

- Només es proporciona software conegut per Apple.
- Per **actualitzar el sistema** s'utilitza **iTunes** per baixar la imatge sencera del iOS, o bé **OTA** per baixar només els components requerits per completar una actualització.
- Durant una actualització d'iOS, iTunes (o el propi dispositiu, en el cas d' actualitzacions en OTA) es **connecta** al **servidor d'autorització d'instal·lació d'Apple** i li **envia** una **llista** de **mesures criptogràfiques** per a cada part del paquet d'instal·lació que es vol instal·lar (per exemple, iBoot, el nucli i la imatge del sistema operatiu), un **valor aleatori anti-reproducció**, i **la identificació única exclusiva de xip** (ECID) del dispositiu.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS. Actualització del sistema.

- El **servidor d'autorització comprova** la **llista** de mesures presentada en contra les versions per a les quals es permet la instal·lació i, **si troba** una **coincidència**, **afegeix** la versió **ECID** a la mesura i **signa** el **resultat**.
- El servidor passa un complet conjunt de dades signades al dispositiu com a part del procés d'actualització. Afegint el ECID "personalitza" l'autorització del dispositiu sol·licitant.
- **Autoritzant** i **signant** només per a mesures conegudes, el servidor **assegura** que **l'actualització s'efectua** tal **com proporciona Apple**.
- L'avaluació de la cadena de confiança d'arrencada **comprova** que la **signatura** prové **Apple** i que la mesura de l'element carregat des del disc, combinada amb l'ECID del dispositiu coincideix amb el que estava cobert amb la signatura.
- El coprocessador Secure Enclave utilitzarà el procés d'arrancada segura per comprovar que el software està signat i verificat epr Apple.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS.

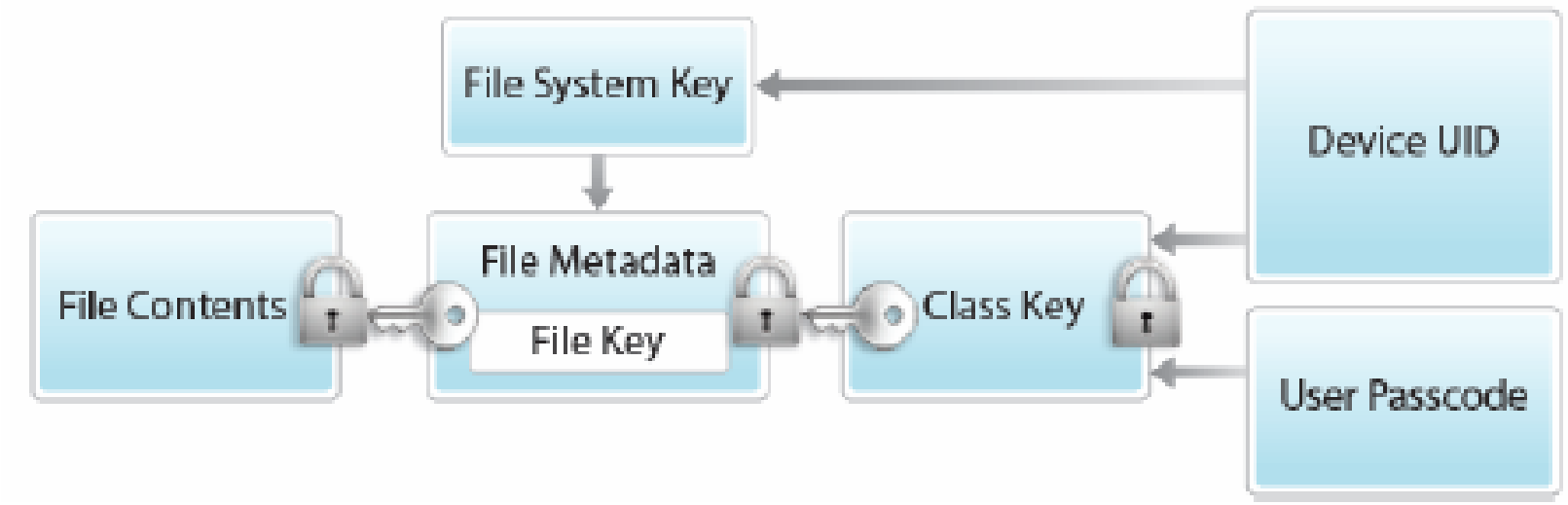
- Format: .ipa (**i**OS **A**pp Store **P**ackage)
- Programades en Objective-C. (Swift)
- Només origen en l'AppStore.
  - Totes les Apps estan xifrades.
  - Desxifra l'app quan l'executa.
- Estan Verificades manualment per Apple.
- Excepte en el mode de desenvolupament.
  - L'execució en sandbox es realitza amb l'user "mobile".
- Les apps estan aïllades de forma que no puguin accedir a les dades no autoritzades.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS. Característiques de seguretat.

- Quan es crea un fitxer en la partició de dades, es crea una clau de 256 bits, per tal de xifrar el fitxer. A cada fitxer també se li assigna així la clau de classe.
- Per desxifrar el fitxer es necessita:
  - Clau de classe de fitxer
  - Codi de desblocatge del telefon (**Passcode**)



UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS. Característiques de seguretat.

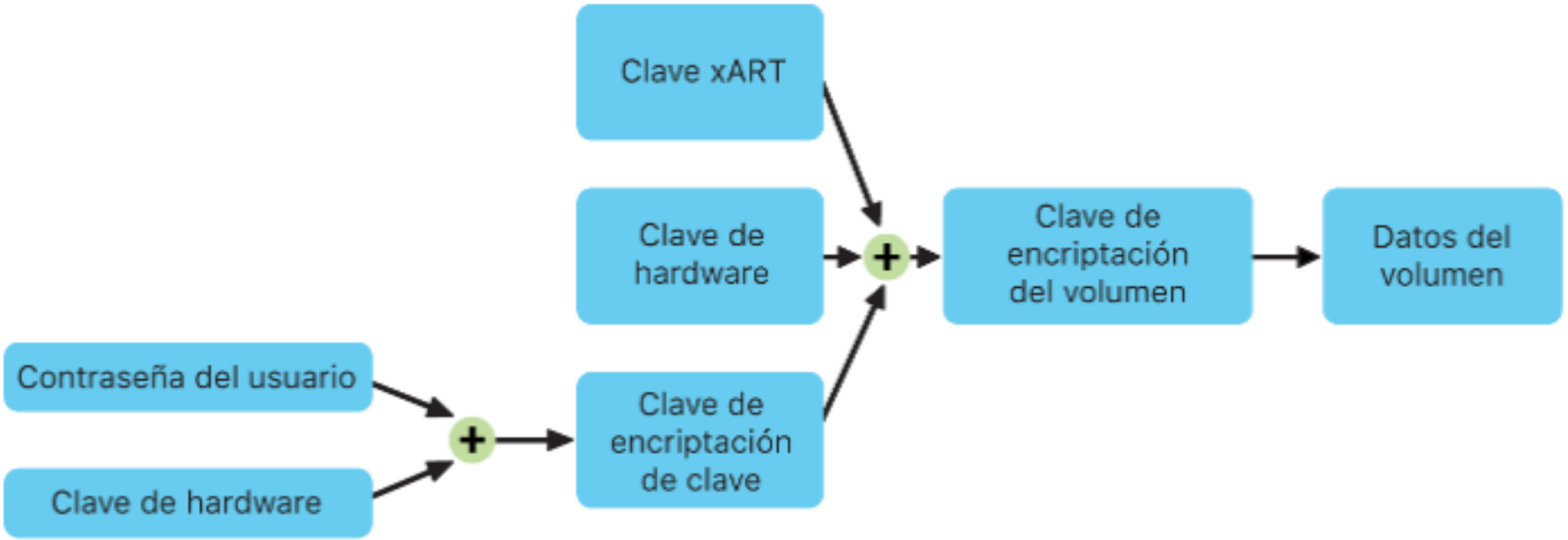
- Es pot encriptar tot el volum intern amb **FileVault** activat.
- Usa l'algoritme AES-XTS per protegir volumns complets en dispositius interns i extraibles.
- Tot el volum APFS intern estarà encriptat i protegit de l'accés no autoritzat. (També si s'agafa el disc dur i es posa en un altre dispositiu).
- Usa el xip T2.
- Aconsegueix cuatre objectius:
  - Contrassenya d'usuari per desxifrar.
  - Atac per força bruta sobre un dispositiu d'emmagatzematge extret del dispositiu no es pot realitzar.
  - Proporciona un mètode ràpid i segur per borrar contingut amb l'eliminació del material d'encriptació necessari.
  - Permetre als usuari canviar la contrassenya sense tornar a encriptar tot el volum.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS. Característiques de seguretat.

- **FileVault activat**

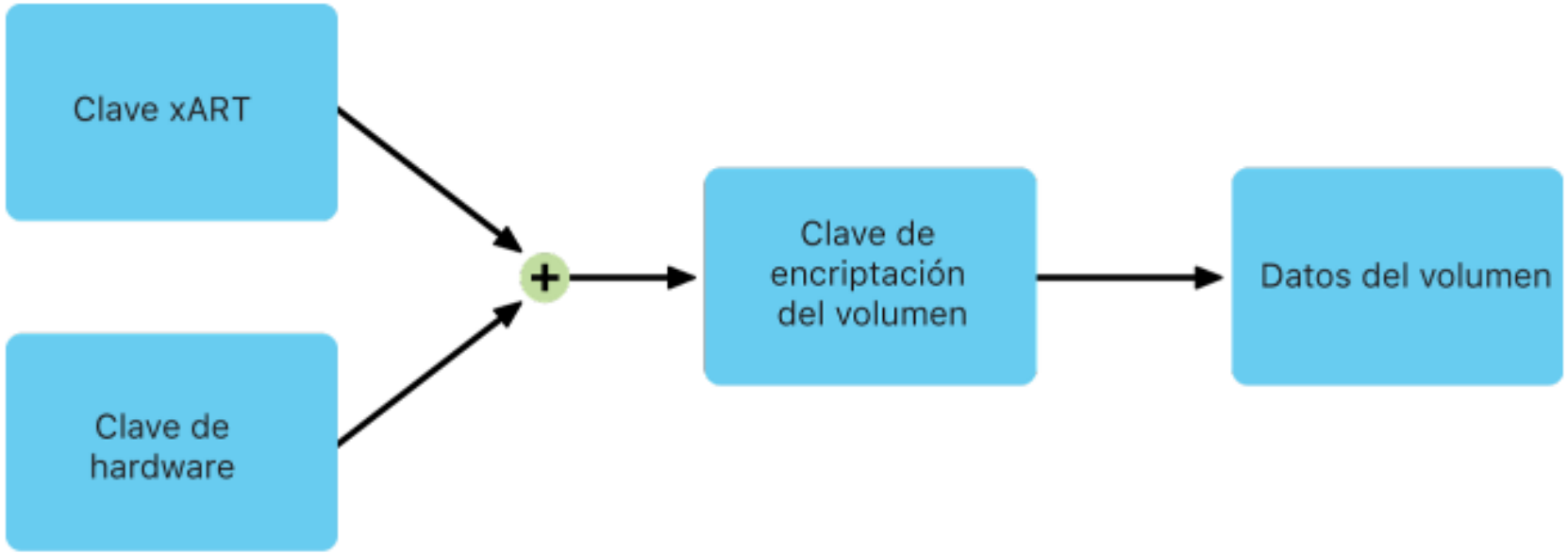


UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS. Característiques de seguretat.

- **FileVault desactivat**



UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS. Característiques de seguretat.

- **Seguretat segons hagin d'estar disponibles els fitxers:**

Clase	Descripción
Protection Complete	Accesible cuando el dispositivo se desbloquea.
Protection Complete Unless Open	Accesible cuando se desbloquea y cuando está bloqueado si el fichero se está utilizando.
Protection Complete Until First User Authentication	Accesible después del primer desbloqueo.
Protection None	Accesible aún si el dispositivo está bloqueado.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS.

- **Passcode**
  - Per defecte 4 dígits (força bruta: 18 min aprox)
  - Més de 4 dígits (més de 18 min)
  - Alfanumèrics (força bruta: entre 8 i 13k anys)
  - Cada intent per força bruta triga 80 mil·lisegons. Es va afegint retard entre intent i intent. 5 anys i mig per provar les combinacions d'un password alfanumèric amb majúscules i números de 6 caràcters.
  - Es pot millorar la seguretat de la contrasenya afegint el Touch ID i el Face ID.
  - Quan passa 1 hora des de l'últim desbloqueig, el dispositiu es torna a bloquejar.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS.

- **Passcode**
  - Es demana quan:
    - S'actualitza el software.
    - S'esborra el dispositiu.
    - Es visualitzen o canvien característiques del passcode.
    - S'instal·len perfils de configuració de l'iOS.
    - Es para o reinicia el dispositiu.
    - No s'ha desbloquejat el dispositiu des de fa 48 hores.
    - No s'ha usat el passcode per desbloquejar el dispositiu en els últims sis dies i mig, o no ha estat desbloquejat de forma biomètrica en les últimes 4 hores.
    - El dispositiu ja rebut una comanda de bloqueig remota.
    - Després de 5 intents de desbloqueig biomètric fallits.
    - Després d'iniciar power off/ Emergència SOS.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS.

- **Passcode**
  - Si s'intenta connectar un accessori desconegut per obrir una connexió de dades durant el període de desbloqueig, es bloquejaran totes les connexions de dades fins que es torni a desbloquejar el dispositiu.
- Esborrar dades del telèfon després de 10 intents (opcional)
- Retard segons el nombre d'intents.

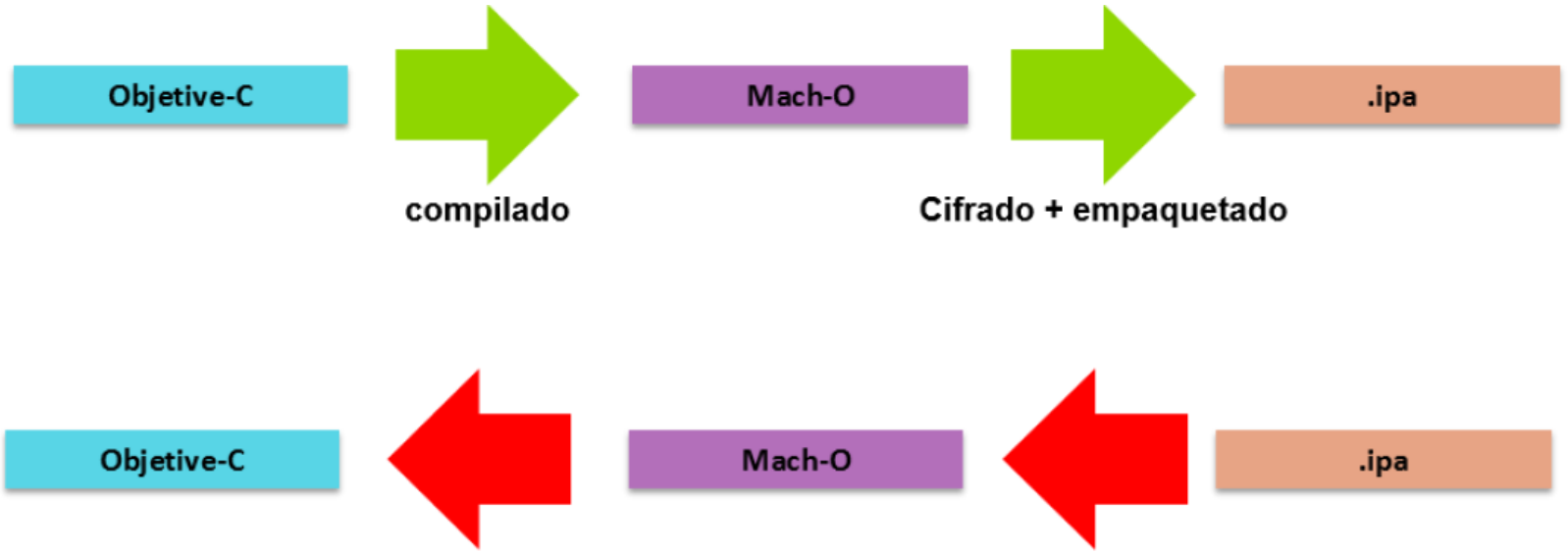
INTENTS	RETARD
1 - 4	Cap
5	1 minut
6	5 minuts
7-8	15 minuts
9	1 hora

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS.

- **Reversing iOS apps.**
  - Com les apps estan xifrades, el millor és volcar des de memòria quan s'estan executant.
  - S'ha de disposar d'un iPhone amb jailbreak (root).



UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS.

- https://www.youtube.com/watch?v=qzYyt9xGtlQ
- https://www.youtube.com/watch?v=DbqkBAjId_U
- https://www.redseguridad.com/actualidad/detectadas-dos-graves-vulnerabilidades-en-ios_20200424.html
- https://support.apple.com/es-es/guide/security/secf020d1074/web

UF1. Seguretat en dispositius mòbils i IoT

- **Mòbils**
  - **Introducció**
  - **Arquitectura dels dispositius mòbils.**
  - **Sistemes operatius mòbils.**
  - **Seguretat en dispositius mòbils: iOS / Android**

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Sistema Android.

- Basat en el **kernel de linux** i amb **software obert**.
- Codi font AOSP. (Android Open Source Project) sota **llicència d'Apache.**
- **Google** n'és el **propietari**.
- A l'any 2018 hi havia 2 milions d'aplicacions al Google Play.
- Existeixen altres **tendes de codi obert** amb aplicacions compatibles. (F-Droid)
- Les aplicacions s'executaven en un framework Java, sobre una màquina virtual (Dalvik) amb compilació en temps d'execució. (**Cada cop que s'obria l'aplicació es compilava**) JIT
- El sistema operatiu consta de 12 milions de línies de codi. (3 milions de línies XML, 2,8 milions de línies en C, 2,1 milions de línies en Java i 1,75 milions de línies en C++)

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

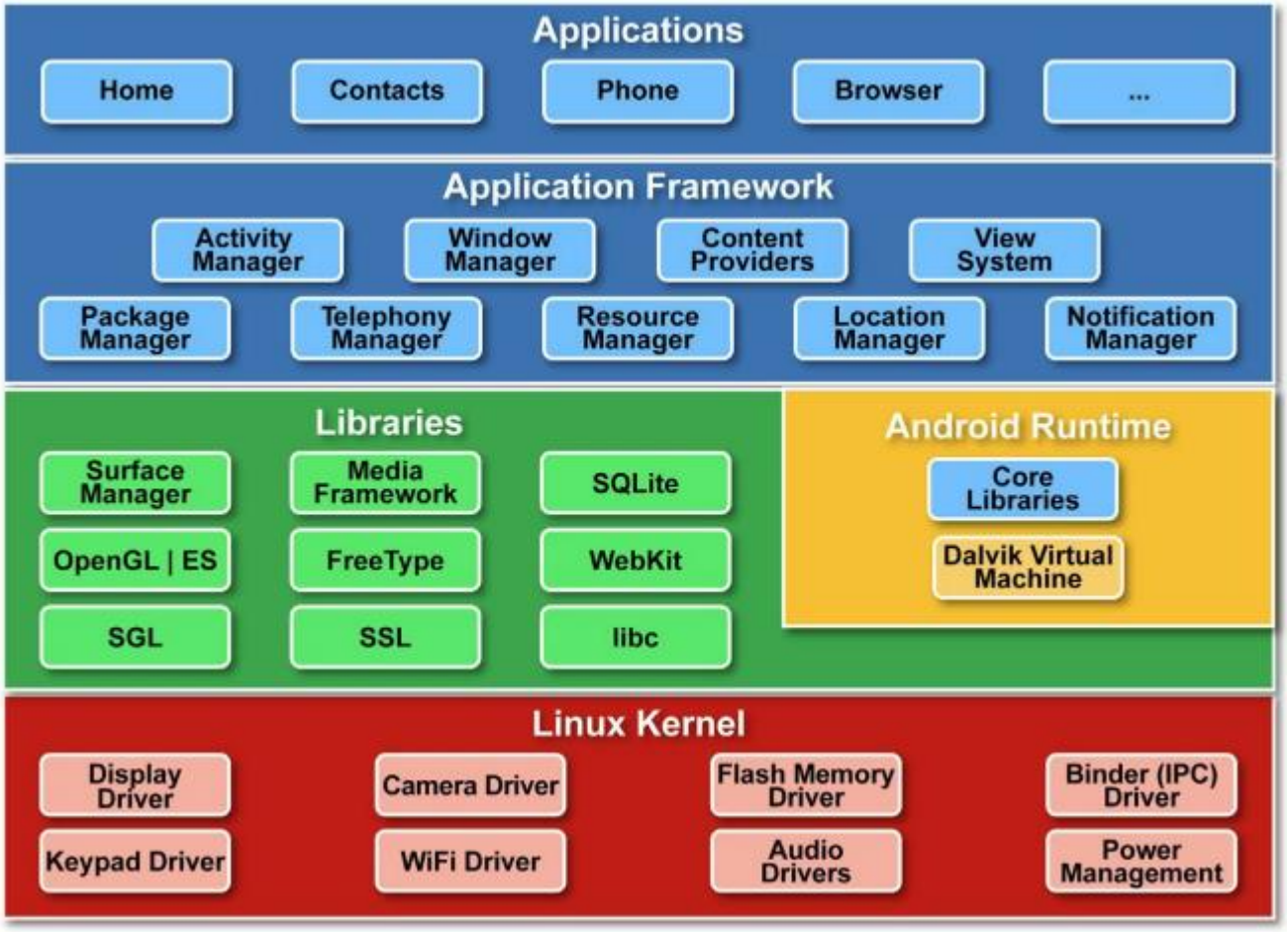
Sistema Android.

- Es va **substuir** la **màquina virtual** per **l'Android Runtime** (ART) https://es.wikipedia.org/wiki/Android_Runtime
- Es crea un arxiu de compilació quan s'instal·la l'aplicació i ja **no s'ha de compilar cada cop** quan s'executi l'aplicació.
- Es crea a partir d'Android 4.4 "Kit Kat", però substitueix completament a l'anterior màquina virtual en la versió 5.0 "Lollipop".
- Android apareix al setembre del 2008.
- Utilitza una base de dades SQLite per guardar les dades.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Sistema Android. Arquitectura.



UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Sistema Android. Arquitectura.

- **Aplicacions**. Escrites en Java. De base té un client de correu electrònic, un programa d'SMS, calendari, mapes, navegador, contactes,…
- **Framework de les aplicacions**. Els desenvolupadors tenen accés complet a les API de l'entorn de treball utilitzat per les aplicacions.
- **Biblioteques**. Conté biblioteques C/C++ . Ex: System C library, biblioteques de mitjans, de gràfics, 3D, SQLite, …
- **Runtime d'Android**. Dalvik substituïda per ART. Compila quan instal·la l'aplicació.
- **Nucli linux**. La base d'Android és linux, que gestiona la memòria, processos, pila de xarxa, model de controladors, …

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Sistema Android. Versions.

Letra	Nombre	Versión	Traducción
A	Apple Pie	1.0	Tarta de manzana
B	Banana Bread	1.1	Pan de plátano
C	Cupcake	1.5	Magdalena
D	Donut	1.6	Donut
E	Éclair	2.0 / 2.1	Palo de crema
F	Froyo	2.2	Yogur helado
G	Gingerbread	2.3	Pan de jengibre
H	Honeycomb	3.0 / 3.1 / 3.2	Panal
I	Ice Cream Sandwich	4.0	Sándwich de helado
J	Jelly Bean	4.1 / 4.2 / 4.3	Gominola
K	KitKat	4.4	Kit Kat
L	Lollipop	5.0 / 5.0.1 / 5.0.2 / 5.1	Piruleta[55]
M	Marshmallow	6.0 / 6.0.1	Malvavisco[56]
N	Nougat	7.0 / 7.1 / 7.1.1 / 7.1.2	Turrón
O	Oreo	8.0 / 8.1	Oreo
P	Pie	9.0	Pastel
Q	Android 10	10.0	Android 10

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Sistema Android. Aplicacions.

- En llenguatge Java.
- Es poden realitzar amb l'Android SDK (kit de desenvolupament de software), Google App Inventor, …
- Format: .APK (**A**ndroid A**p**plication Pac**k**age).
  - Variant del format JAR de java.
- Tendes d'aplicacions: Google Play (Play Store), Amazon Appstore, …

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

- **Sistema de fitxers Android.**
- FileSystem YAFFS (Yet Another Flash File System).
  - Primer sistema de fitxers per a **memòria Flash NAND**. (pendrive)
  - Utilitzat en molts dispositius Android.
  - Proveeix wear leveling per perllongar la vida útil de les memòries Flash.
  - Robustesa davant fallades d'energia.
  - Redueix la sobrecàrrega de la memòria RAM.
- Versions
  - YAFFS1 (limitat a 1GiB el sistema de fitxers), 2^{18} fitxers, 2^{22} (512 MiB) tamany màxim del fitxer.
  - YAFFS2(limitat a 8GiB)

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

- **Sistema de fitxers Android.**
- FileSystem EXT4
  - Seguretat de dades i velocitat lectura/escriptura.
  - Utilitzat des de la versió 2.3 (Gingerbread)
  - Molt més ràpid que YAFFS.
- FileSystem F2FS
  - Flash-Friendly FileSystem. Per memòries SSD o targetes SD.
  - Utilitzat per dispositius Samsung, Motorola,, …
  - 5 vegades més ràpid que EXT4 en accés a BBDD i escriptures aleatòries.
  - 20% més lent en lectura seqüencial.
- https://www.androidpit.es/que-son-sistemas-de-archivos-android (Desembre de 2014)
- https://www.xataka.com/moviles/por-que-el-sistema-de-ficheros-de-tu-telefono-android-es-mas-importante-de-lo-que-crees

UF1. Seguretat en dispositius mòbils i IoT

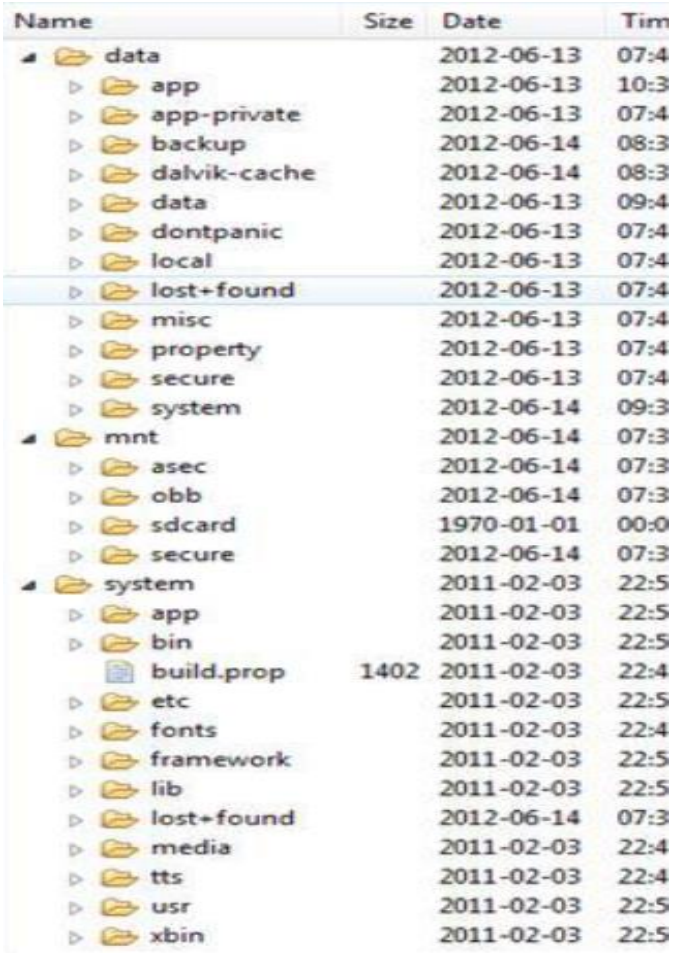
Seguretat en dispositius mòbils: iOS / Android

- **Sistema de fitxers Android.**
- **/system/:** sistema operatiu.
- **/mnt/sdcard/ o /sdcard/:**
  - Targetes SD montades al sistema (fitxers, música, fotos, …)
- **/data/**:
  - Dades de l'usuari i aplicacions.
  - **/data/app/**: Emmagatzema les aplicacions.
  - **/data/data/**: Guarda dades de les aplicacions. Inclou un subdirectori per aplicació amb els permisos de l'aplicació.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

- **Sistema de fitxers Android.**



Name	Size	Date	Tim
data		2012-06-13	07:4
app		2012-06-13	10:3
app-private		2012-06-13	07:4
backup		2012-06-14	08:3
dalvik-cache		2012-06-14	08:3
data		2012-06-13	09:4
dontpanic		2012-06-13	07:4
local		2012-06-13	07:4
lost+found		2012-06-13	07:4
misc		2012-06-13	07:4
property		2012-06-13	07:4
secure		2012-06-13	07:4
system		2012-06-14	09:3
mnt		2012-06-14	07:3
asec		2012-06-14	07:3
obb		2012-06-14	07:3
sdcard		1970-01-01	00:0
secure		2012-06-14	07:3
system		2011-02-03	22:5
app		2011-02-03	22:5
bin		2011-02-03	22:5
build.prop	1402	2011-02-03	22:4
etc		2011-02-03	22:5
fonts		2011-02-03	22:4
framework		2011-02-03	22:5
lib		2011-02-03	22:5
lost+found		2012-06-14	07:3
media		2011-02-03	22:4
tts		2011-02-03	22:4
usr		2011-02-03	22:5
xbin		2011-02-03	22:5

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

- **Sistema de fitxers Android.**
- Particions estándar interna:
  - /boot
  - /system
  - /recovery
  - /data
  - /cache
  - /misc
- Particions tarjeta SD:
  - /sdcard
  - /sd-ext

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

- **Sistema de fitxers Android.**
- Partició **/boot:**
  - Conté el bootloader i el kernel.
  - És necessària. On arrenca el dispositiu.
- Partició **/system:**
  - Conté el sistema operatiu excepte el kernel i bootloader.
  - Hi ha les aplicacions pre-instal·lades.
  - Hi ha la interfície d'usuari.
  - Es podria eliminar la carpeta i conseguir engegar en mode de recuperació, però no és gens recomanable.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

- **Sistema de fitxers Android.**
- Partició **/recovery:**
  - Per recuperació (Factory reset).
  - Es pot iniciar el sistema en mode recovery.
  - Es fa servir per manteniment i recuperació de dades.
- Partició **/data:**
  - Conté dades que l'usuari ha creat o modificat, és a dir, les dades pròpies de l'usuari. (correus, contactes, xarxes wifi a les que ha tingut accés, …)

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

- **Sistema de fitxers Android.**
- Partició **/sdcard:**
  - Es guarden les configuracions i dades de les aplicacions.
  - Pot ser una tarjeta SD o el sitema de fitxers montats. (Es pot accedir mitjançant USB OTG).
  - Es poden tenir diverses montades, per exemple la interna i l'externa.
- Partició **/cache:**
  - Es guarda la informació d'ús habitual que se li dóna a l'usuari al dispositiu mòbil tant referent a les aplicacions com al propi sistema operatiu Android.
  - Podem esborrar el seu contingut sense cap problema.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

- **Sistema de fitxers Android.**

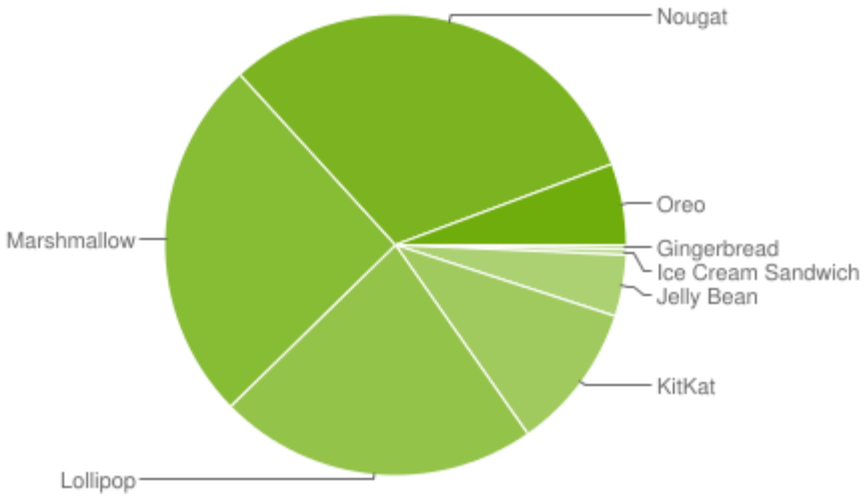
Datos	Ubicación
Calendario	/data/data/com.android.providers.calendar/
Browser Data	/data/data/com.android.providers.browser/
Download History	/data/data/com.android.providers.downloads/
Location Cache	/data/data/com.google.android.location/
Gmail	/data/data/com.google.android.providers.gmail/
SMS & MMS	/data/data/com.android.providers.telephony/
Contactos	/data/data/com.android.providers.contacts/
Whatsapp	/data/data/com.whatsapp/databases Backup: /sdcard/WhatsApp/databases/

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	0.3%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.3%
4.1.x	Jelly Bean	16	1.2%
4.2.x		17	1.5%
4.3		18	0.5%
4.4	KitKat	19	6.9%
5.0	Lollipop	21	3.0%
5.1		22	11.5%
6.0	Marshmallow	23	16.9%
7.0	Nougat	24	11.4%
7.1		25	7.8%
8.0	Oreo	26	12.9%
8.1		27	15.4%
9	Pie	28	10.4%



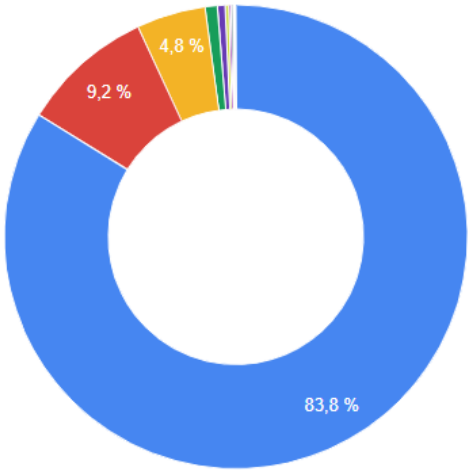
UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

abr. 2020-jun. 2020

Google Play



Categoría	Porcentaje de descargas de aplicaciones potencialmente dañinas
Software espía	0,05880071 %
Fraude telefónico	0,0064762375 %
DoS	0,0033851833 %
Suplantación de identidad	0,0006023021 %
Apropiación de privilegios	0,0003683153 %
Puerta trasera	0,0001811936 %
Troyano	0,000106876 %
Descargador hostil	0,0000912197 %
Software espía comercial	0,0000711425 %
Fraude por SMS	0,0000660227 %
Rooteo	0,0000083795 %
Software malicioso de Windows	0,0000024783 %
Spam	0,0000000802 %
Fraude de llamadas	0,0000000123 %
Software de secuestro	0,0000000028 %

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

- **Com funciona?**
  - Cada **aplicació** està en la seva **pròpia zona de proves de seguretat** i està protegida per les següents característiques de seguretat:
    - Android és un sistema Linux multiusuari, i **cada aplicació** és un **usuari diferent**.
    - El sistema assigna a **cada aplicació un ID d'usuari** de linux **únic**. El sistema estableix permisos per tots els arxius en una aplicació, de manera que **només el ID d'usuari assignat** a aquella **aplicació podrà accedir** a ells.
    - **Cada procés** té la **seva pròpia màquina virtual (VM)**. El codi d'una **aplicació s'executa de forma independent** d'altres aplicacions.
    - **Cada aplicació executa el seu propi procés** linux.
    - El sistema **Android inicia el procés quan es requereix** l'execució **d'algun dels components** de l'aplicació i, **el tanca quan ja no és necessari o quan** el sistema **ha de recuperar memòria** per altres aplicacions.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

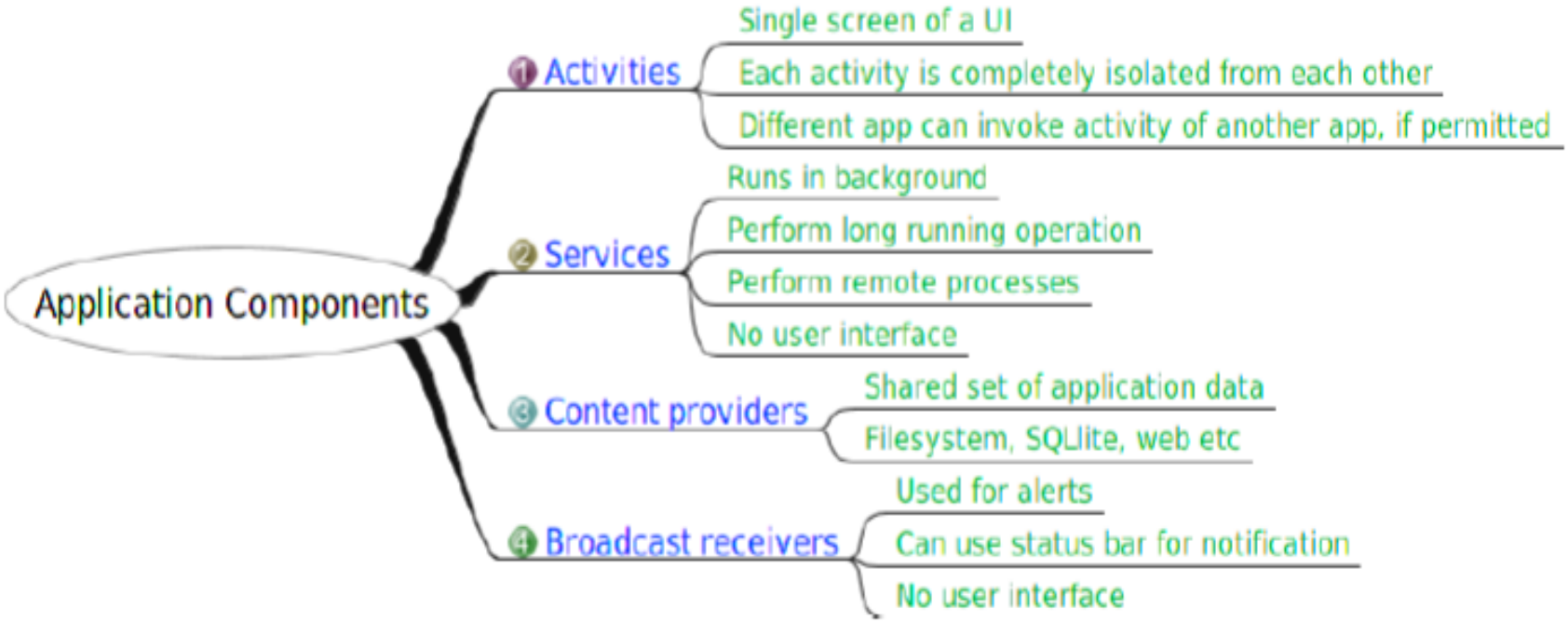
- **Com funciona?**
  - S'implementa el **principi de mínim privilegi**. Cada aplicació té **accés només als components que necessita** per fer la seva funció.
  - Una aplicació **no pot accedir a parts del sistema** per les **quals no té permisos**.
  - Hi ha maneres en les que **una aplicació pot compartir dades amb altres aplicacions** i en les que una aplicació pot **accedir a serveis del sistema**:
    - Han de compartir **mateix ID i estar signades** amb el **mateix certificat**.
    - **L'aplicació pot sol·licitar permís per accedir a dades del dispositiu**, com els contactes, missatges de text, targeta SD, càmera, bluetooth,...

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

- **Com funciona?**
  - Les **aplicacions** tenen **quatre tipus de components** diferents, amb una funció específica i un cicle de vida que defineix com es crea i destrueix el component.



UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

- **Com funciona?**
  - **Activity.** (Activitat)
    - **Punt d'entrada d'interacció amb l'usuari**. Pantalla individual amb interfície d'usuari. **Cada activitat és independent una de l'altra.**
    - Exemple: Activitat principal->correu electrònic.
      - Activitat per llegir correu.
      - Activitat per escriure correu.
      - Activitat del correu electrònic entrada.
      - ...
    - **Una activitat es pot iniciar per una altra**. Per exemple enviar foto feta amb la càmera del mòbil per correu.
    - https://developer.android.com/guide/components/activities/intro-activities?hl=es-419

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

- **Com funciona?**
  - **Services.** (Serveis)
    - Punt d'entrada general que **permet mantenir l'execució d'una aplicació en segon pla** per diversos motius.
    - **No** proporciona **interfície d'usuari**.
    - Exemple: un servei pot proporcionar **música** en segon pla **mentre l'usuari es troba en una altra aplicació**.
    - **Una altra activitat pot iniciar el servei** i permetre que s'executi o enllaçar-se en ell per poder interactuar.
      - La reproducció de música és una cosa que l'usuari sap que hi és, i per tant l'aplicació li envia permís al sistema, qui envia notificació a l'usuari.
      - **Un servei es pot interrompre si es necessita memòria RAM** en processos més urgents per l'usuari.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

- **Com funciona?**
  - **Services.** (Serveis)
    - **Gestionats pel sistema.**
    - Els **serveis enllaçats** s'executen perquè una altra aplicació o el sistema ha indicat que vol usar-los.
    - El **sistema** sap que hi haurà una **dependència entre els processos**, per tant **no podrà tancar els processos** ja que s'estan **usant serveis** d'aquests.
    - Exemple: **fons de pantalla animats**, els **receptors de notificacions**, els **protectors de pantalla**, etc. Aquests serveis són vinculats pel **sistema**, que **decideix quan s'han d'executar**.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

- **Com funciona?**
  - **Content providers.** (Proveïdors de continguts)
    - **Administra un conjunt compartit de dades** de l'aplicació que es poden guardar en el sistema d'arxius, en una base de dades SQLite, en la Web o en qualsevol altre lloc on tingui accés l'aplicació.
    - Altres **aplicacions poden consultar o modificar les dades si el proveïdor de contingut ho permet.**
    - Android proporciona un **proveïdor de contingut** que **administra la informació de contacte de l'usuari**, de forma que qualsevol aplicació amb els permisos adequats podrà consultar la informació.
    - **Poden llegir i escriure dades privades de l'aplicació i que no es comparteixin.**

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

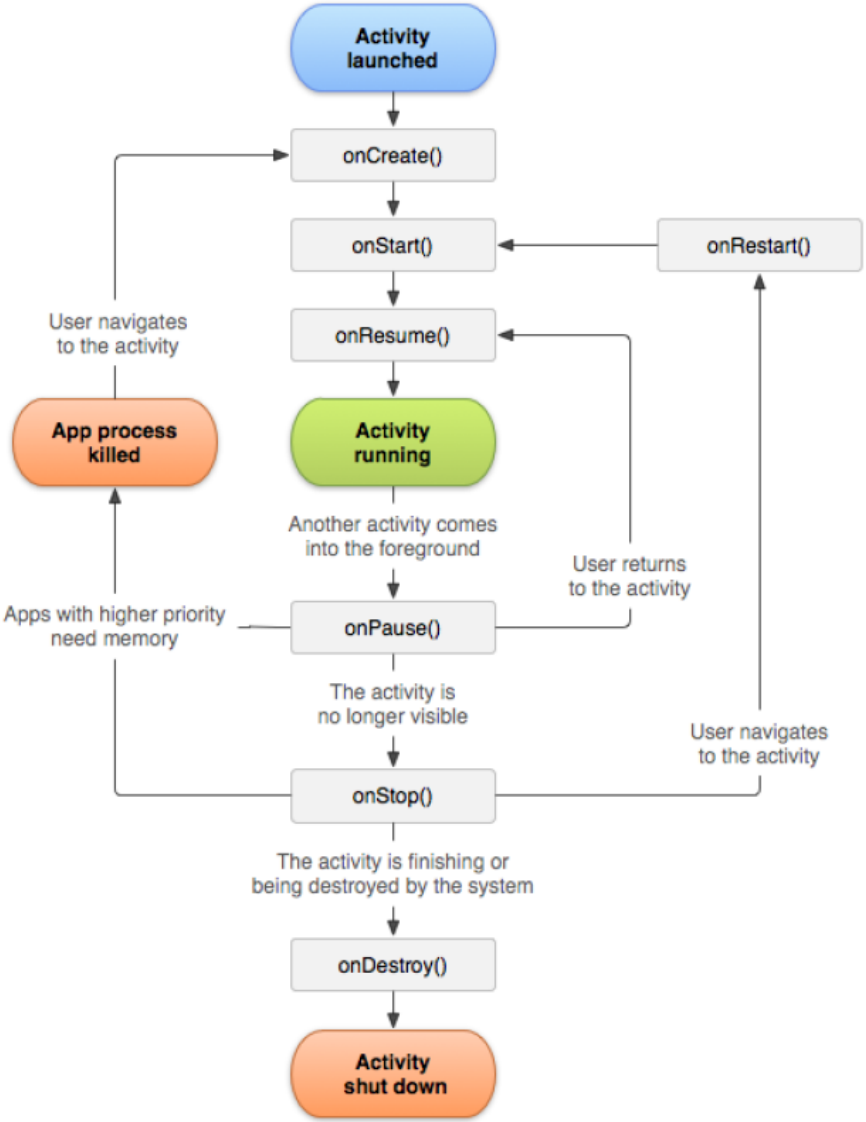
- **Com funciona?**
  - **Broadcats receivers.** (Receptors d'emissions)
    - Un receptor d'emissió és un component que possibilita que **el sistema entregui events a l'aplicació fora del flux d'usuaris habitua**l, és a dir, l'aplicació respondrà a tots els anuncis d'emissió del sistema.
    - **El sistema pot entregar emissions a aplicacions que no estan en execució**.
    - Per **exemple**, una aplicació pot **programar una alarma per publicar una notificació** sobre un futur event destinat a l'usuari. Quan el receptor d'emissió de l'aplicació rep l'alarma per part de l'aplicació, no fa falta que l'aplicació continuï executant-se fins que s'activi l'alarma.
    - Hi ha **moltes emissions** que provenen del sistema, com les **de nivell baix de bateria, que s'apagarà la pantalla, que s'ha fet captura de pantalla**,...
    - Les aplicacions també inicien **emissions per avisar d'altres aplicacions que s'han descarregat dades** que ja estan disponibles per utilitzar-les.
    - Els **receptor d'emissions** no tenen interfície d'usuari, però **poden crear una notificació a la barra d'estat**.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

- Activity-lifecycle.
- El sitema operatiu gestiona l'execució de les activities.
- Callbacks per especificar què es fa a cada esdeveniment.
- Al tancar una app, no es tanca! El S.O. ho decideix.

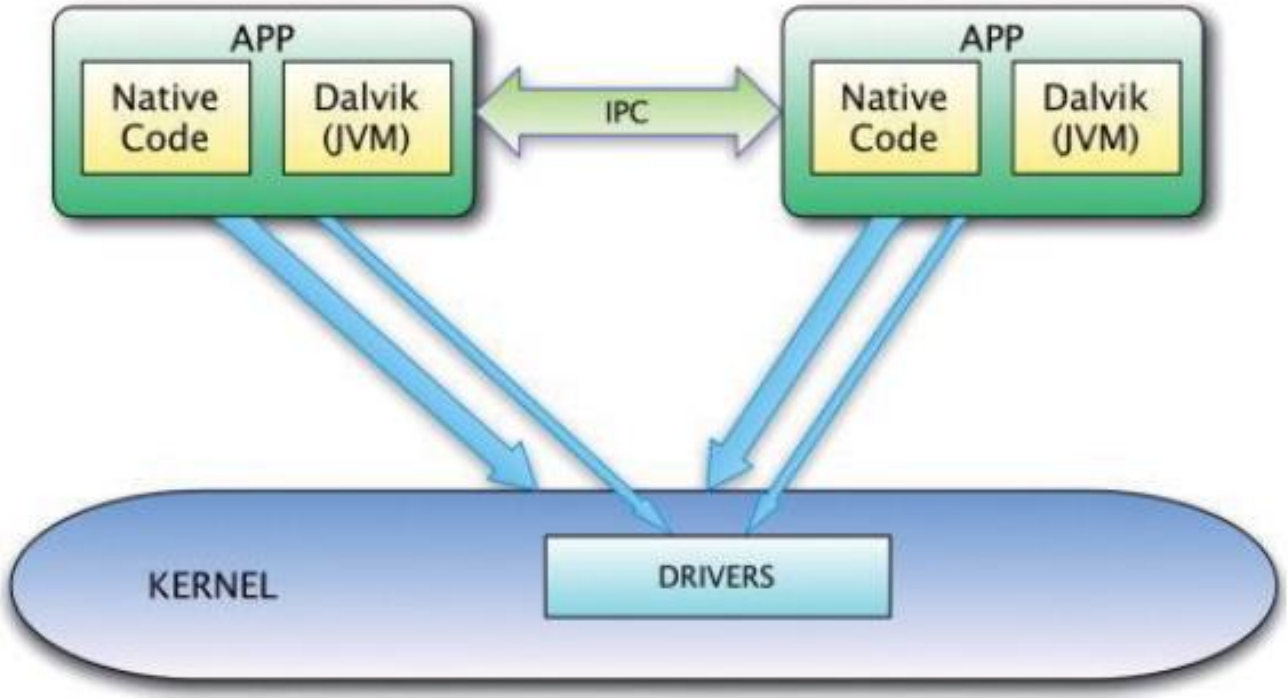


UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

- **Entorn execució:**
  - C++ natiu.
  - Java (JVM)

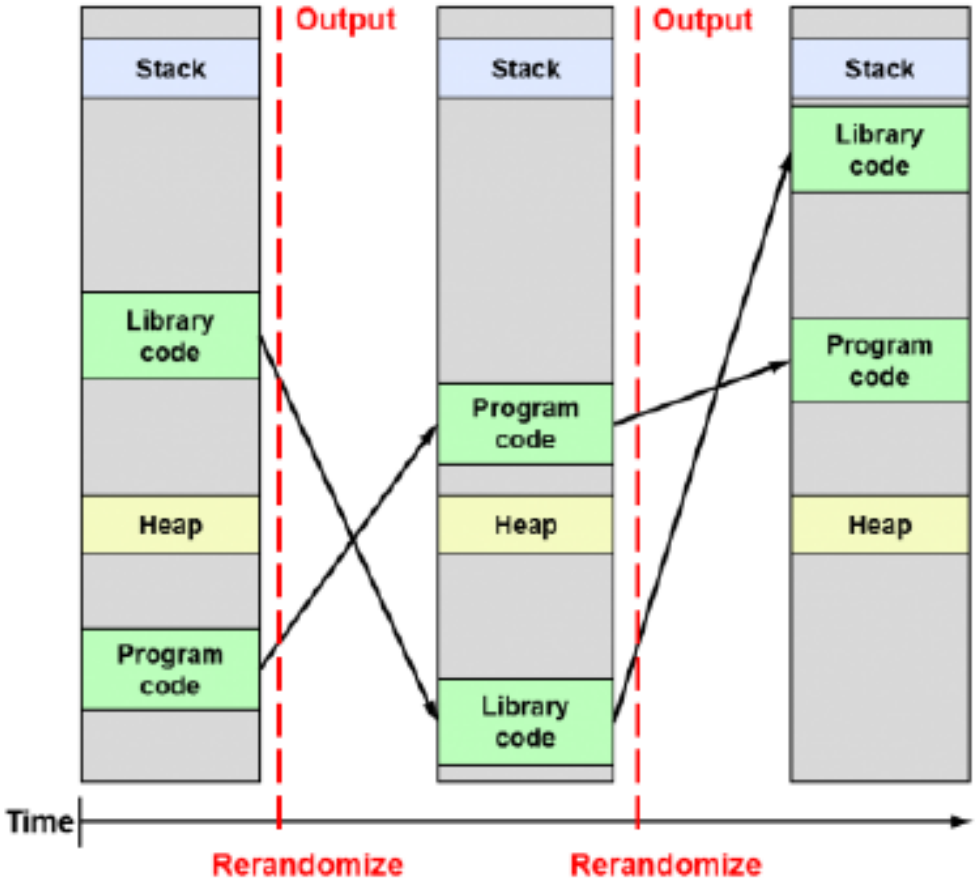


UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

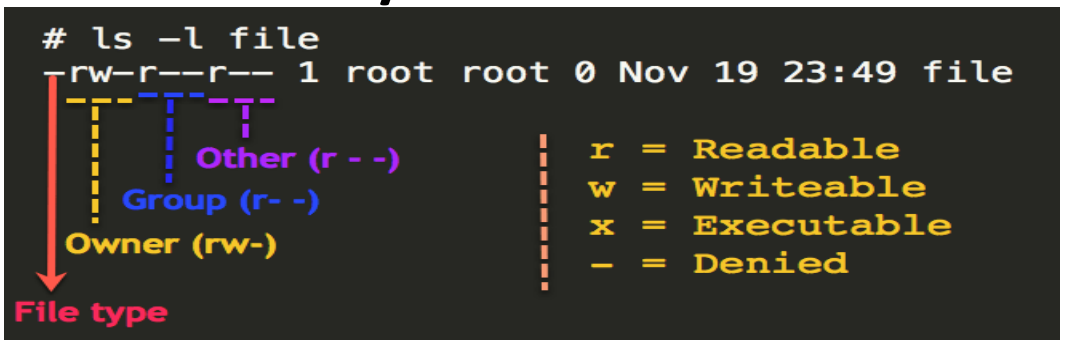
Seguretat Android.

- **Memòria.**
  - DEP (Data execution prevention). Permet no executar en regió de memòria no executable.
  - ASLR (Address space layout randomization)
- El mode Debug permet accedir a memòria, per desenvolupament.



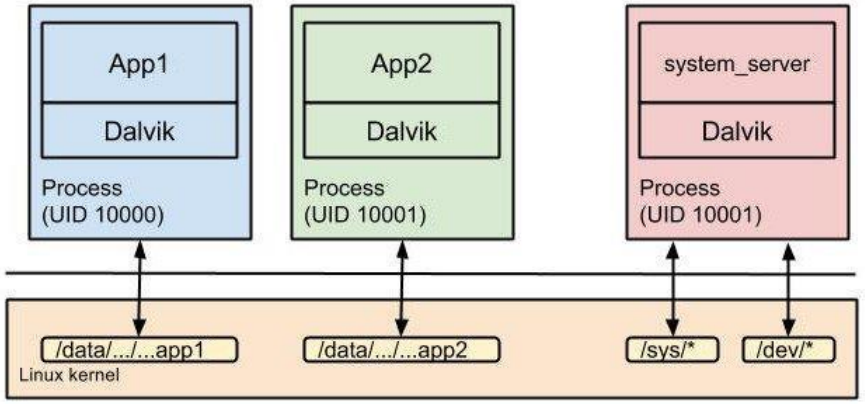
UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android



Seguretat Android.

- Permisos: Linux!
  Propietari, grup, altres
- Sandboxing:
  Cada Activity té un usuari diferent (no root ni system)
- MAC (Mandatory Access Control)
- Granularitat SEAndroid (basat en SELinux)
- Sistema de fitxers xifrat.

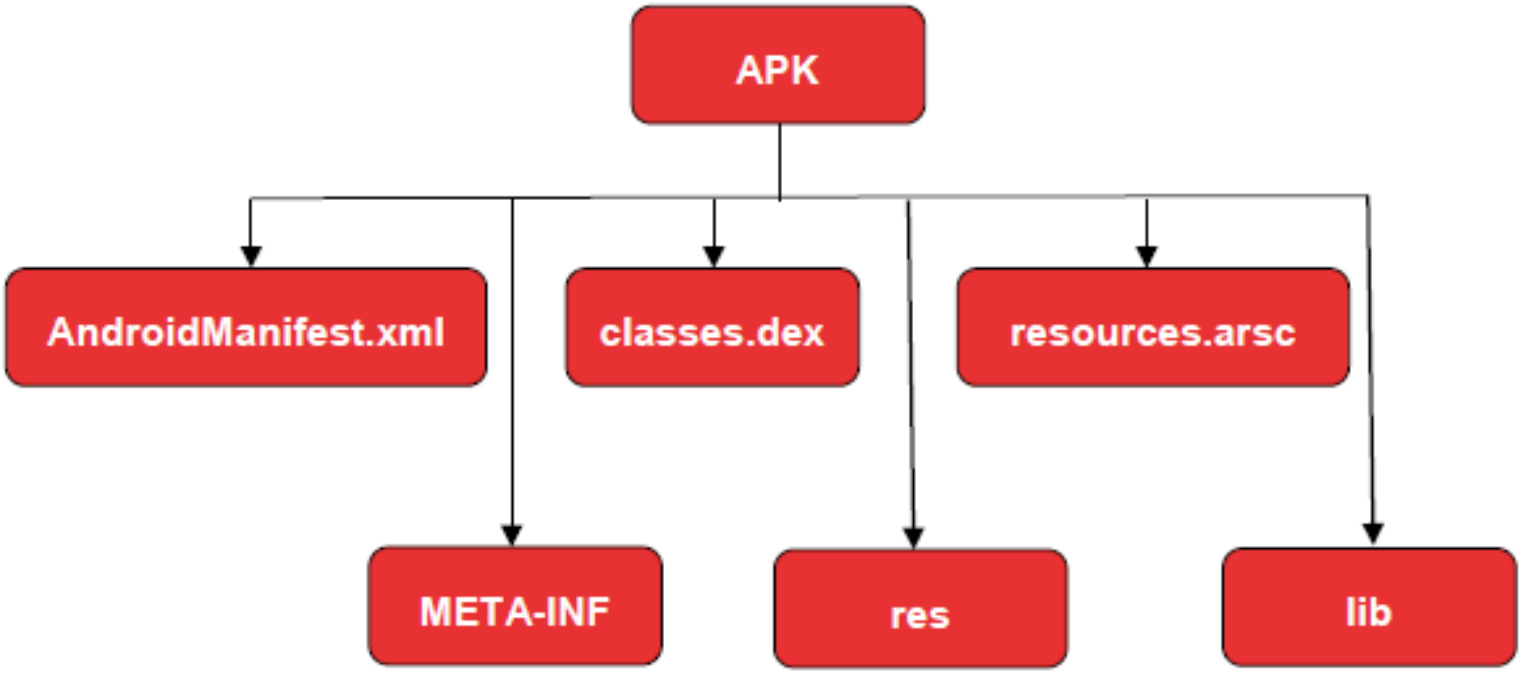


UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

- **APK (Android Application Package**
  - Aplicació + Metadades



UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

APK (Android Application Package

- **AndroidManifest.xml**
  - Arxiu de **configuració** de l'aplicació.
  - Descriu el **nom**, la **versió**, els **drets** d'accés i els arxius de biblioteques referenciats per l'aplicació.
  - Punt **d'entrada d'execució (Activity**).
  - **Permisos** de l'aplicació.
    - Al instal·lar /on demand()
  - Sol estar en Android binari XML.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

APK (Android Application Package

- **AndroidManifest.xml**

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.deneme2.uygulama1">

    <application
        android:allowBackup="true"
        android:icon="@mipmap/ic_launcher"
        android:label="Uygulama1"
        android:supportsRtl="true"
        android:theme="@style/AppTheme">
        <activity android:name=".MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />

                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
        <activity android:name=".CustomList"></activity>
    </application>

</manifest>
```

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

APK (Android Application Package

- **META-INF**
  - Directori que conté:
    - MANIFEST.MF: l'arxiu manifest.
    - CERT.RSA: el certificat de l'aplicació.
    - CERT.SF: la llista de recursos i un resum SHA-1 de les línies corresponents en l'arxiu MANIFEST.MF; per exemple:

      Signature-Version: 1.0

      Created-By: 1.0 (Android)

      SHA1-Digest-Manifest: wxqnEAI0UA5nO5QJ8CGMwjkGGWE=

      ...

      Name: res/layout/exchange_component_back_bottom.xml

      SHA1-Digest: eACjMjESj7Zkf0cBFTZ0nqWrt7w=

      ...

      Name: res/drawable-hdpi/icon.png

      SHA1-Digest: DGEqylP8W0n0iV/ZzBx3MW0WGCA=

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

APK (Android Application Package

- **Classes.dex**
  - Les **classes compilades en** el **format** d'arxiu **dex**, comprensible per la màquina virtual Dalvik i per Android Runtime.
- **Res**
  - Directori que **conté recursos no compilats** en resources.arsc.
- **resources.arsc**
  - Arxiu que conté **recursos precompilats** com XML binari.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

APK (Android Application Package

- **lib**
  - Directori que **conté el codi compilat** que és específic d'una capa de software d'un processador. **Conté altres subdirectoris**:
    - Armeabi. Codi compilat per processadors ARM.
    - Armeabi-v7a. Codi de compilació només per processadors ARMv7 o superiors.
    - Arm64-v8a. Codi compilat per tots els processadors ARMv8 asrm64 i superiors.
    - X86. Codi compilat només per processadors x86.
    - X86_64. Codi compilat només per processadors x86_64.
    - Mips. Codi compilat només per processadors MIPS.

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

- **Permisos.**

- ACCESS_LOCATION_EXTRA_COMMANDS
- ACCESS_NETWORK_STATE
- ACCESS_NOTIFICATION_POLICY
- ACCESS_WIFI_STATE
- BLUETOOTH
- BLUETOOTH_ADMIN
- BROADCAST_STICKY
- CHANGE_NETWORK_STATE
- CHANGE_WIFI_MULTICAST_STATE
- CHANGE_WIFI_STATE
- DISABLE_KEYGUARD
- EXPAND_STATUS_BAR
- FOREGROUND_SERVICE
- GET_PACKAGE_SIZE
- INSTALL_SHORTCUT
- INTERNET
- KILL_BACKGROUND_PROCESSES
- MANAGE_OWN_CALLS
- MODIFY_AUDIO_SETTINGS
- NFC
- READ_SYNC_SETTINGS
- READ_SYNC_STATS
- RECEIVE_BOOT_COMPLETED
- REORDER_TASKS
- REQUEST_COMPANION_RUN_IN_BACKGROUND
- REQUEST_COMPANION_USE_DATA_IN_BACKGROUND
- REQUEST_DELETE_PACKAGES
- REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
- SET_ALARM
- SET_WALLPAPER
- SET_WALLPAPER_HINTS
- TRANSMIT_IR
- USE_FINGERPRINT
- VIBRATE
- WAKE_LOCK
- WRITE_SYNC_SETTINGS

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

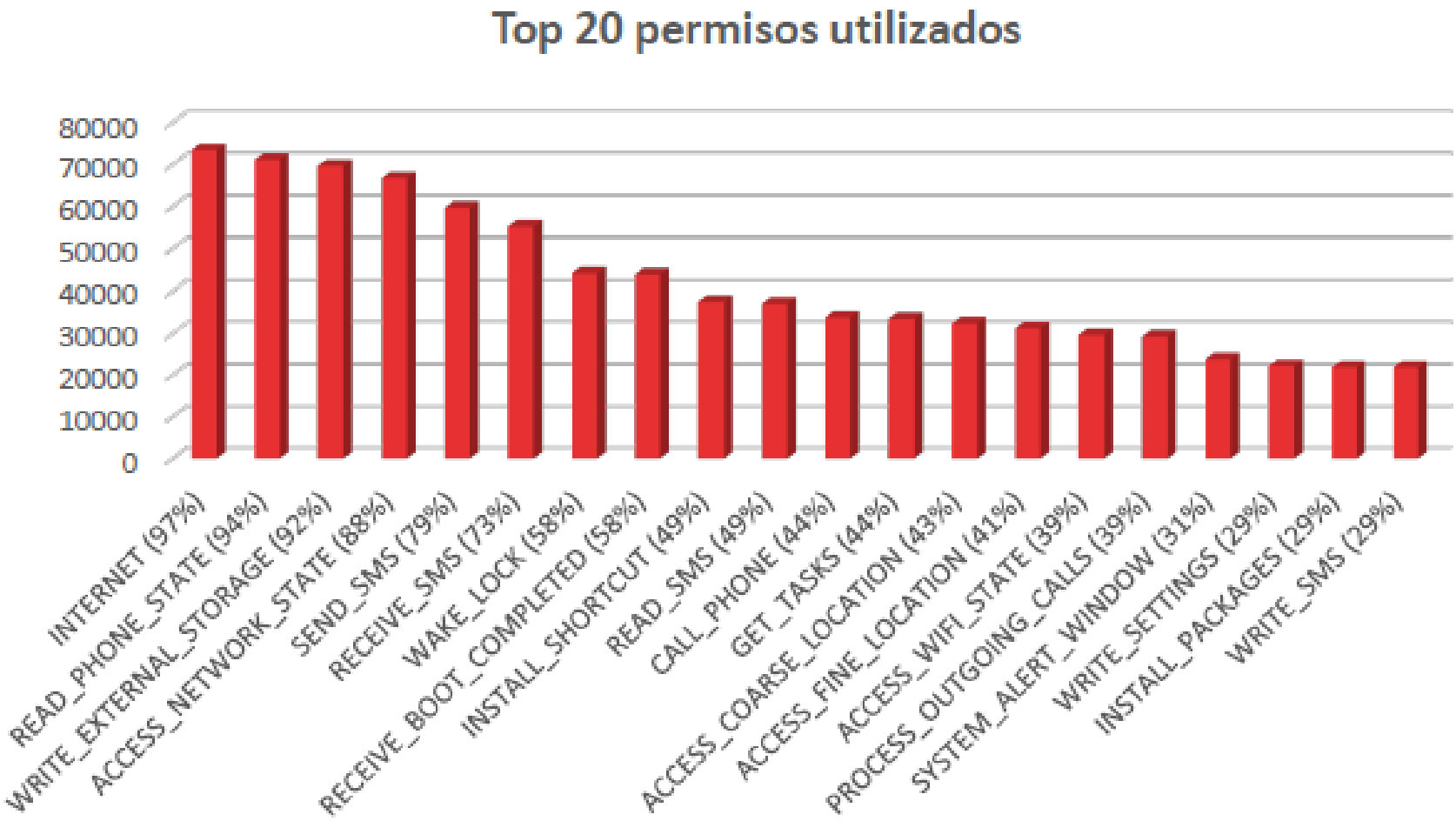
- **Permisos.**

- ❑ **CALL_PHONE PROCESS_OUTGOING_CALLS**
- ❑ **INTERNET**
- ❑ **ACCESS_GPS •**
- ❑ **ACCESS_COARSE_LOCATION**
- ❑ **ACCESS_COARSE_UPDATES**
- ❑ **ACCESS_FINE_LOCATION READ_PHONE_STATE READ_CONTACTS WRITE_CONTACTS ACCESS_WIFI_STATE**
- ❑ **SEND_SMS**
- ❑ **READ_SMS**
- ❑ **WRITE_SMS**
- ❑ **WAKE_LOCK**
- ❑ **RECORD_AUDIO**
- ❑ **WRITE_EXTERNAL_STORAGE**

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

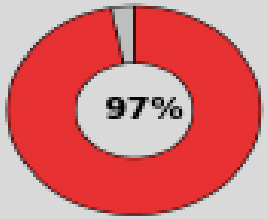
Seguretat Android.



UF1. Seguretat en dispositius mòbils i IoT

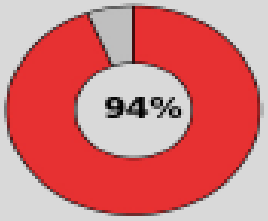
Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.



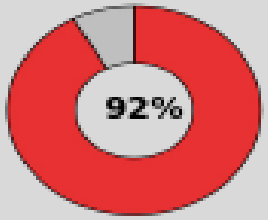
android.permission.INTERNET

- Permite a las aplicaciones acceso total a Internet.
- Dangerous



android.permission.READ_PHONE_STATE

- Permite el acceso de sólo lectura al estado del teléfono.
- Dangerous



android.permission.WRITE_EXTERNAL_STORAGE

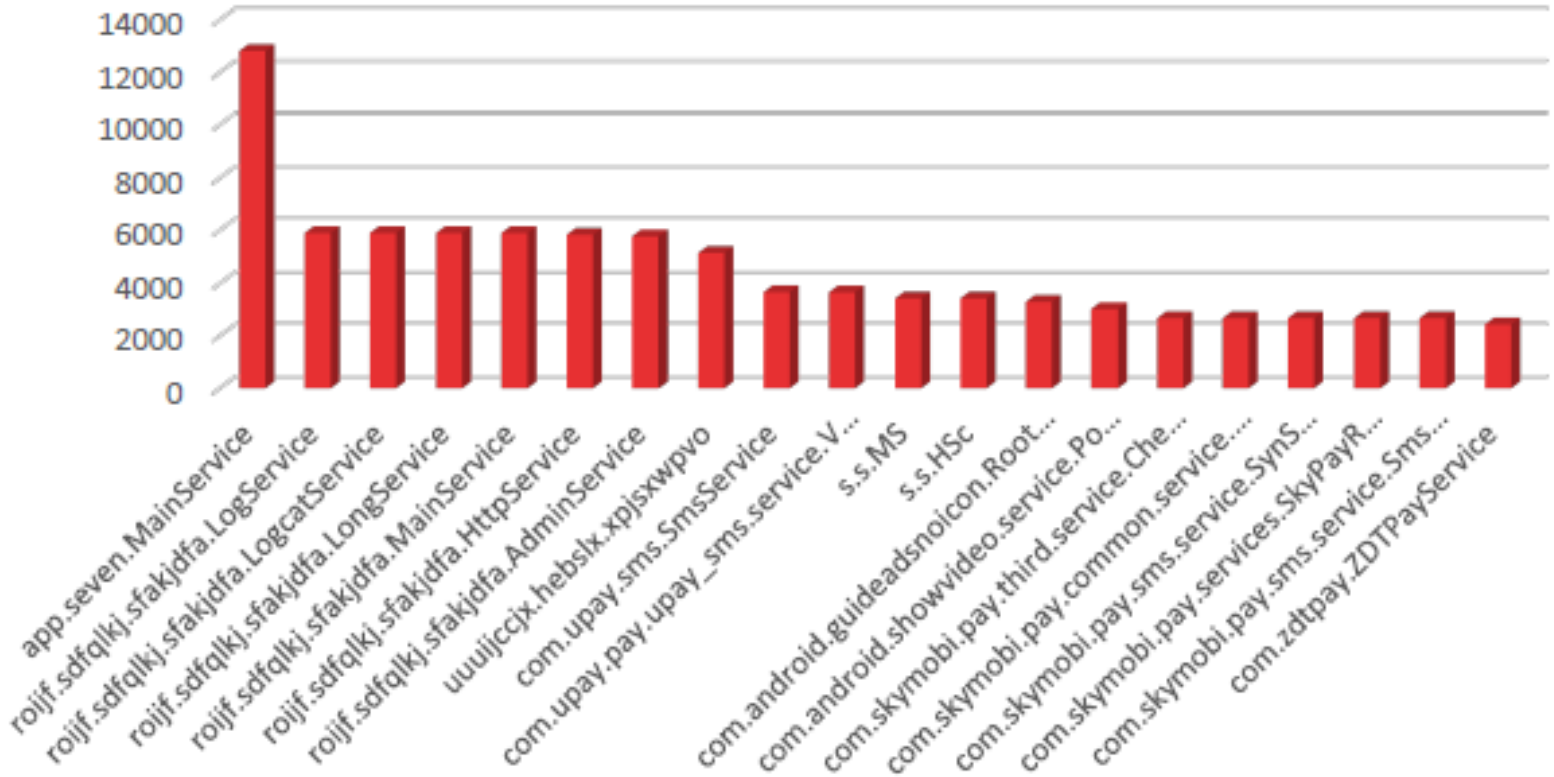
- Permite a una aplicación escribir en el almacenamiento externo.
- Dangerous

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

- Serveis:
  - Corren en background
  - 2,66 serveis per app



UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

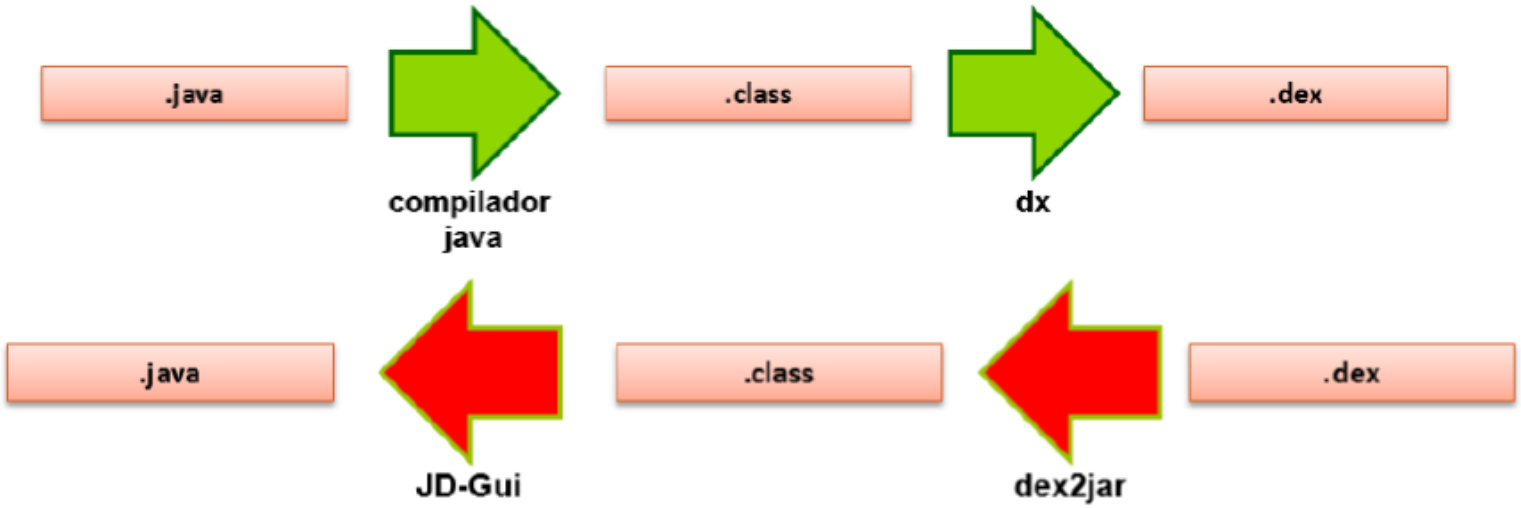
- **Signatura**
  - Permet verificar que l'app no ha estat modificada.
- **Authorities.**
  - Google Play (només confia en google)
  - Altres Stores (qualsevol o per store)
  - Qualsevol… (" orígenes desconocidos")

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android. Reversing Android.

- Les apps Android s'executen en la màquina Dalvik
  - Format dex (dalvik executable)
  - Codi Font en JAVA
  - En el procés de compilació es duen a terme optimitzacions:
    - Memòria
    - Reutilització de codi
    - Gestió d'errors



UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

- **Android hacks examples**
  - Self sign app
  - cryo root
  - Links whatsapp
  - Pin pantalla visible
  - Desbloquejar amb foto
  - AndroidTV exposat sense pwd
  - Bar spoofing
  - Man in the middle a llocs publics
  - Enginyeria social…

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat Android.

- https://www.android.com/intl/es_es/security-center/
- https://transparencyreport.google.com/android-security/overview
- https://andro4all.com/2019/04/guia-seguridad-android
- https://elandroidelibre.elespanol.com/2016/05/seguridad-de-google-en-android.html
- https://androidayuda.com/category/seguridad/

UF1. Seguretat en dispositius mòbils i IoT

Seguretat en dispositius mòbils: iOS / Android

Seguretat iOS vs Android.

- https://www.movilzona.es/2019/09/04/seguridad-iphone-mala-hackear-android/
- https://www.adslzone.net/2019/09/04/android-ios-mas-seguro-zerodium/
- https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3464-ccn-cert-ia-04-19-informe-anual-2018-dispositivos-moviles/file.html
- https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4625-ccn-cert-ia-03-20-informe-anual-2019-dispositivos-y-comunicaciones-moviles-1/file.html
- https://www.ccn-cert.cni.es/documentos-publicos/ix-jornadas-stic-ccn-cert/1234-m1-07-laboratorio-de-analisis-de-aplicaciones-android-mirojo/file.html