Dispositius IoT

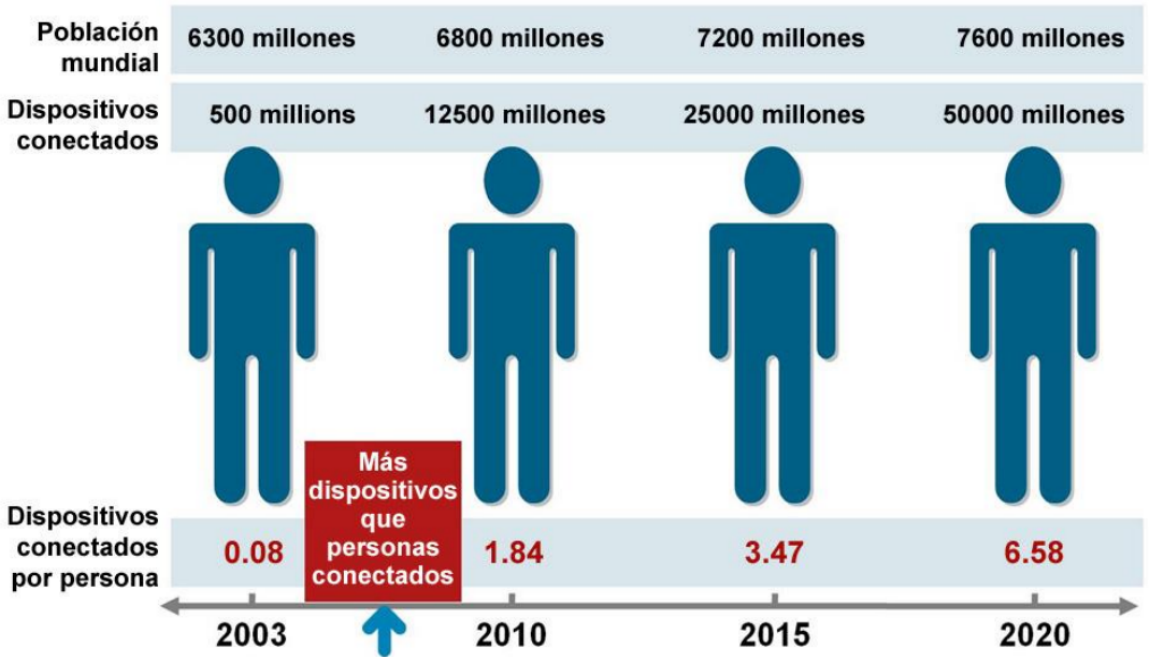
Que es un dispositiu IoT:
Internet of Things és la xarxa d'objectes físics que contenen tecnologia incrustada per comunicar-se i sentir o interactuar amb els seus estats interns o amb l'entorn extern.

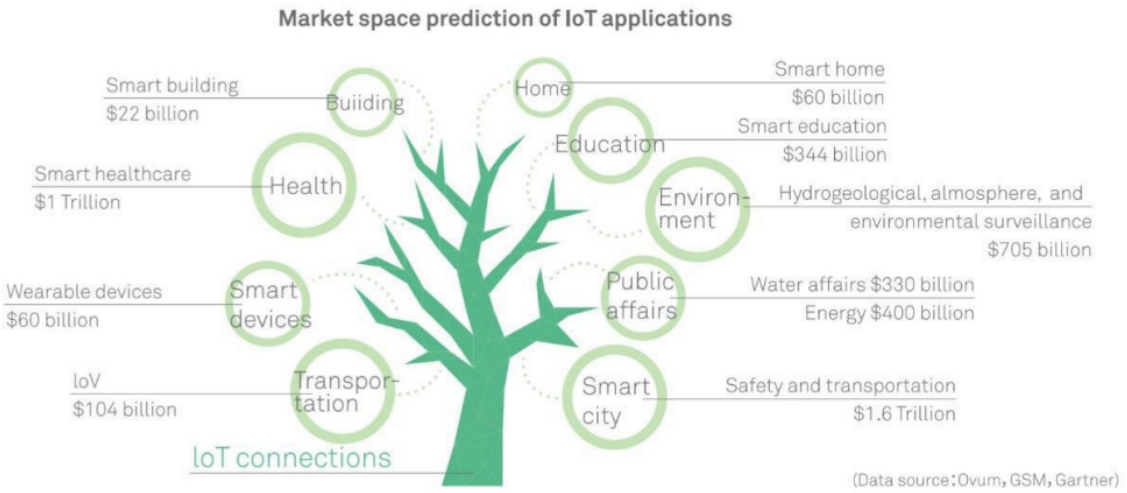
La persona que li va donar nom va ser el tecnòleg Kevin Ashton als anys 90.

- És un sistema on Internet està connectat al món físic a través desensors omnipresents.

Segons CISCO, la IoT es defineix com el moment on es va detectar que hi haurien més objectes que persones connectades a Internet.

- IoT segons Cisco. (Abril del 2011). A partir de l'any 2008 comença a haver-hi més dispositius que persones connectades a Internet.
- Calculaven que hi hauria 25000 milions de dispositius connectats a Internet l'any 2015 i 50000 l'any 2020, però sense tenir en compte els avenços tecnològics que poguessin haver a partir de l'any 2011 en que es va fer el càlcul.





On es troben

Està present a tots els àmbits: la casa, les ciutats, la indústria, l'automoció, els jocs, ...

Casos d'ús de l'IoT

- **Automòbils:** sensors per tenir en temps real la màxima informació.
- **Ciutats:** semàfors, enllumenat, contenidors d'escombraries, transports públics, ...
- **Casa:** càmeres TV's, mòbils, assistència, neveres, rentadores, routers, ...
- **Industria (IIoT):** controladors, robots, sistemes de monitorització,...
- **Agricultura:** sensors per la presa de decisions sobre la humitat, aigua, per recopilar i analitzar les dades, ...
- **Hospitals:** control de tovalloles utilitzades en operacions, càmeres, escanners, control de medicaments en stock, …

Exemples per Sector

- Agricultura
    - Drons per a la Imatge Agrícola
    - Sensors de Humitat del Sòl
    - Automatització de la Cosecha
    - Sistemes de Reg Intel·ligent
- Medicina i Salut
    - Dispositius Vestibles de Monitorització de la Salut
    - Telemedicina
    - Implants Intel·ligents
    - Sistemes de Gestió d'Hospitals
- Transport
    - Vehicles Autònoms
    - Sistemes de Gestió del Trànsit Intel·ligents
    - Rastreig GPS per a Flotes
    - Apps de Mobilitat Compartida
- Indústria
    - Manteniment Predictiu amb IoT
    - Robotització de la Producció
    - Sistemes de Control de Qualitat Automatitzats
    - Monitorització de la Cadena de Producció
- Casa
    - Termostats Intel·ligents
    - Sistemes de Seguretat Domèstica
    - Electrodomèstics Connectats
    - Assistents de Veu Intel·ligents
- Ciutats
    - Il·luminació Pública Intel·ligent
    - Gestió de Residus Intel·ligent
    - Sistemes de Transport Públic Eficients
    - Xarxes Elèctriques Intel·ligents (Smart Grids)

Aplicacions de tipus Empresarial EIoT

S'anomenen EIoT, i són tots els dispositius en l'ambient corporatiu o dels negocis.

Es recol·lecta la informació dels individus mitjançant la segmentació per comportament, que és un conjunt de tècniques i tecnologies utilitzades per publicistes i editors d'un lloc web per tal d'augmentar l'efectivitat de la publicitat usant la informació del comportament de l'usuari a l'utilitzar el navegador web. (pàgines visitades, cerques realitzades, nombre de clics del ratolí, ...)

DEKA

DEKA va crear un braç alimentat per bateries que utilitzava l'activitat elèctrica dels músculs esquelètics per controlar-lo.

S'anomenava Luke Arm (en honor a Luke Skywalker d'Star Wars)

Tipus d’aplicacions industrials

Enfocament: Aquestes aplicacions es centren en la producció i manufactura, així com en la millora dels processos industrials.

Exemples: Inclouen la robotització en les línies de muntatge, sistemes de gestió de la producció, manteniment predictiu en fàbriques, i aplicacions de monitorització i control de processos.

Objectiu: L'objectiu principal és augmentar l'eficiència, la productivitat i la seguretat en els entorns de producció i manufactura.

Problemes de seguretat

Una gran part venen amb passwords per defecte que són molt simples o coneguts per tothom, i que moltes vegades no és obligatori canviar amb els conseqüents problemes de seguretat.

Les actualitzacions és un altre dels problemes. O bé no es contemplen, o bé no es fan per no tenir mecanismes fàcils i ben definits.

El problema de la securització de IoT és que afecta a molts àmbits:

- Securitzar el dispositiu
- El Cloud
- La xarxa
- Aplicacions mòbils per accedir hi i utilitzar-la.
- Xifrat.
- Mecanismes d’autenticació.
- Seguretat física.
- Ports i interfícies físiques accessibles

Top 10 vulnerabilitats OWASP

- **Injecció:** Aquesta vulnerabilitat es produeix quan un atacant pot inserir un codi maliciós en el programa.
- **Trencament d'Autenticació:** Succeeix quan les implementacions d'autenticació i gestió de sessions no són segures, permetent als atacants comprometre contrasenyes, claus o tokens de sessió.
- **Exposició de Dades Sensibles:** Aquest risc es refereix a la protecció inadequada de dades sensibles com dades financeres, sanitàries o personals.
- **Entitats Externes XML:** Aquesta vulnerabilitat permet als atacants explotar aplicacions processant XML de manera insegura, sovint per a realitzar atacs de Servei Denegat Distribuït (DDoS), exposició de dades internes, entre altres.
- **Trencament de Control d'Accés:** Succeeix quan els usuaris poden accedir a dades o funcions per a les quals no tenen permís.
- **Configuració de Seguretat Incorrecta:** Això es produeix quan la configuració de seguretat no està definida, està definida incorrectament o és incompleta.

- **Cross-Site Scripting (XSS):** Aquesta vulnerabilitat permet als atacants injectar scripts maliciosos en contingut vist per altres usuaris, podent robar informació de sessió, vandalejar llocs web, o redirigir l'usuari a llocs maliciosos.
- **Deserialització Insegura:** Aquesta vulnerabilitat pot permetre als atacants realitzar atacs com l'execució remota de codi, injeccions, i més.
- **Ús de Components amb Vulnerabilitats Conegudes:** Això es refereix a l'ús de llibreries, frameworks i altres components de programari amb vulnerabilitats conegudes.
- **Monitorització i Registre Insuficients:** La falta de registre i monitorització adequats pot impedir o retardar la detecció d'atacs, augmentant el risc de danys.

Arquitectura dels dispositius IoT

Un sistema IoT està format per capes o nivells.

El model compta amb 7 nivells. Va des del nivell 1 dels dispositius físics i controladors, fins la col·laboració i processos del nivell 7.

Nivell		Descripció
7	**Col·laboració i processos**	Comunicació i col·laboració entre persones i processos empresarials.
6	**Aplicació**	Interpretació de la informació basada en les dades del dispositiu i les necessitats empresarials.
5	**Abstracció de dades**	Representació i emmagatzematge de dades per al desenvolupament d'aplicacions.
4	**Acumulació de dades**	Conversió de dades en moviment en dades en repòs, preparació per a l'ús en nivells superiors.
3	**Edge (fog) Computing**	Anàlisi i transformació de dades per a emmagatzematge i processament de nivell superior.
2	**Connectivitat**	Gestió de la transmissió de dades entre dispositius i xarxes, i entre la xarxa i el processament de dades.
1	**Dispositius físics i controladors**	Dispositius de punt final que envien i reben informació en una xarxa IoT.

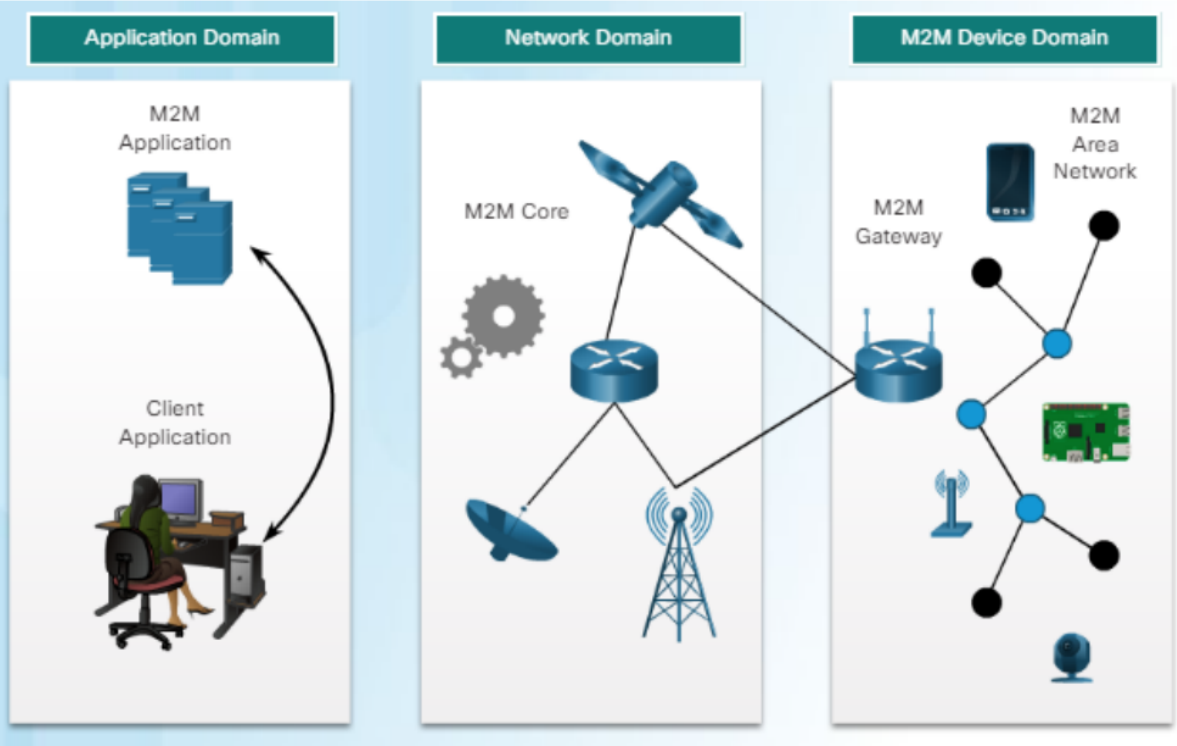
Model ETSI

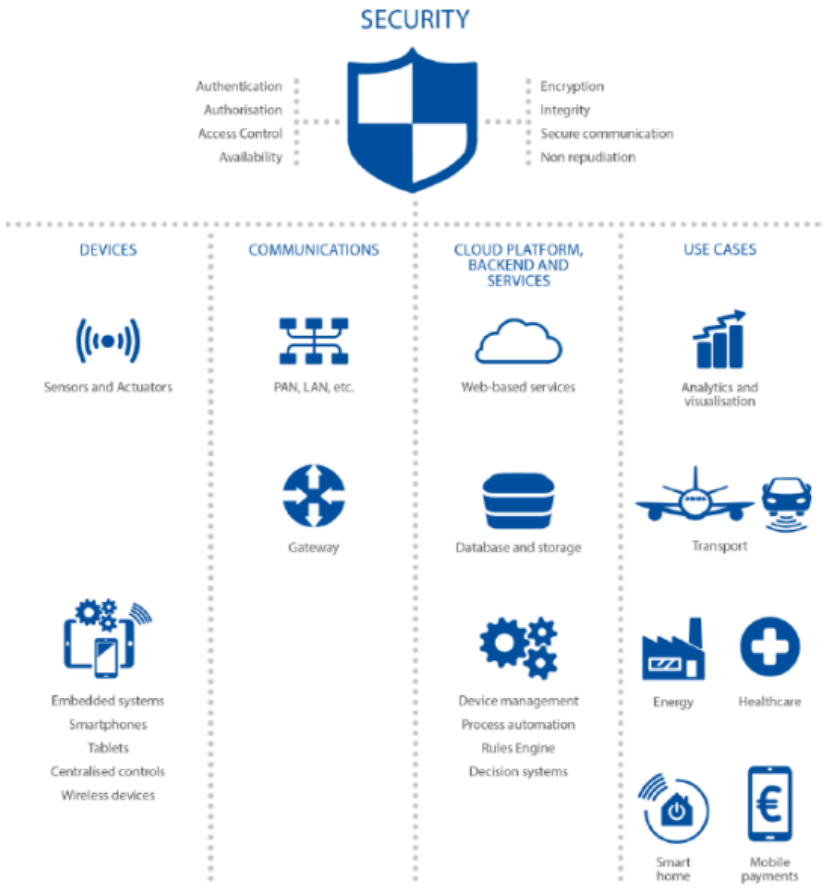
L'European Telecommunications Standards Institute (ETSI) va crear una arquitectura per a comunicacions màquina a màquina (M2M), que també inclou dispositius IoT.

El propòsit del model era proporcionar un marc comú per entendre la col·locació de diversos estàndards i protocols en un sistema IoT.

El model ETSI inclou tres dominis:

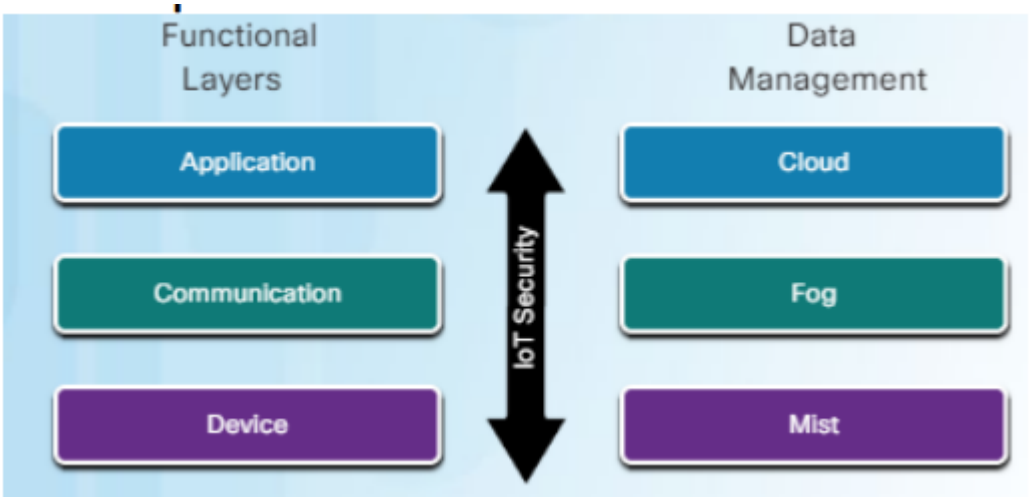
- Domini de l'aplicació: aquí es poden produir funcions de gestió com ara l'anàlisi de dades, la gestió de connectivitat, la gestió intel·ligent de l'energia, la gestió de flotes o qualsevol aplicació que consumeixi les dades dels dispositius IoT.
- Domini de xarxa: aquí és on les dades surten a la xarxa local i es transporten al domini de l'aplicació mitjançant protocols per cable i sense fils, com ara el canvi d'etiquetes multiprotocol (MPLS), l'evolució a llarg termini (LTE) i la interoperabilitat mundial per a l'accés a microones (WiMax).
- Domini de dispositiu M2M: aquí és on els dispositius finals, com ara sensors, actuadors i controladors, es connecten a la xarxa a través de passarel·les M2M mitjançant diversos protocols, com IEEE 802.15.4 i Bluetooth.



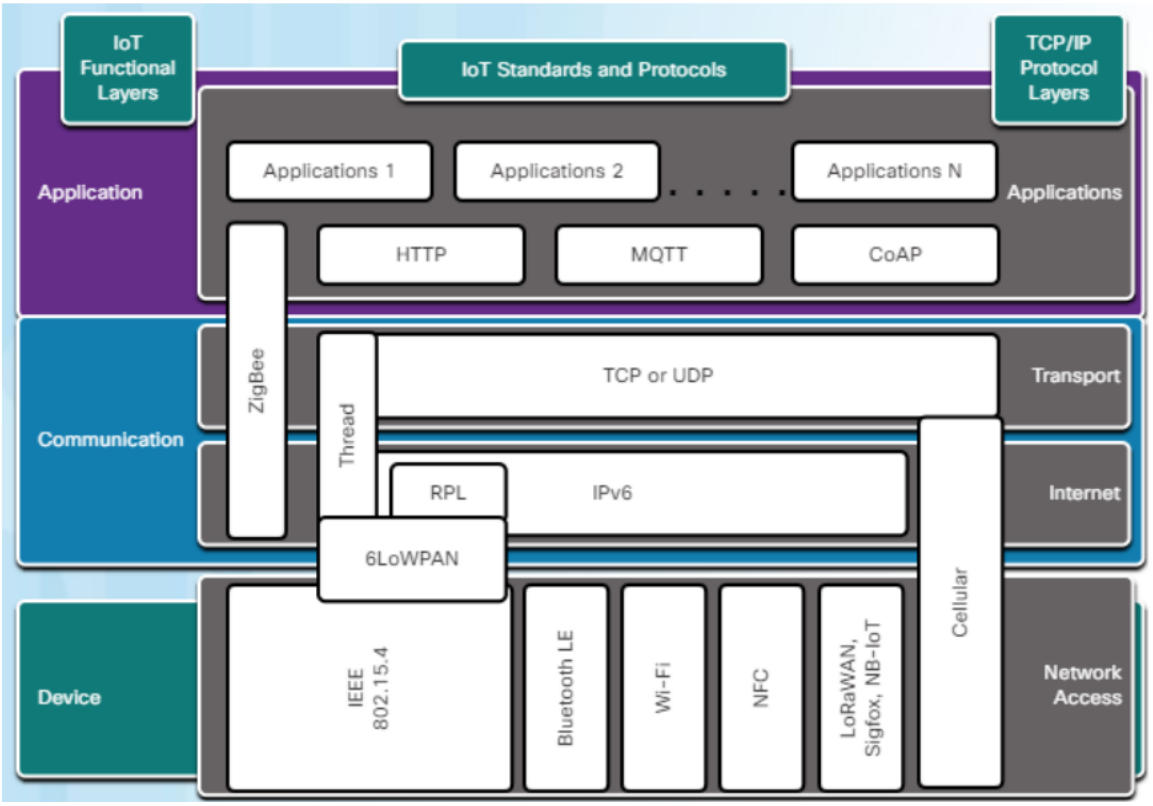


Model Simplificat

- La capa de dispositiu d'un sistema de reg pot incloure capçals d'aspersors individuals, sensors d'humitat, sensors de temperatura i actuadors.
- A la capa de comunicació, tots aquests dispositius podrien estar connectats a un tauler de control de reg local que supervisa l'estat del sistema.
- A la capa d'aplicacions, el tauler de control es pot connectar a un centre de dades remot on s'agrupen tots els taulers de control de múltiples sistemes de reg.



Protocols



A quin tipus dispositiu correspon MQTT CoAP

MQTT:

- Dispositius Mòbils:
- Gateways i Brokers

CoAP:

- Entorns de Xarxa Restringits:
- Aplicacions que Requereixen Interacció amb HTTP
- Sistemes que Requereixen Comunicació M2M

Que es doble factor autentificació

El doble factor d'autenticació és un mètode de seguretat que requereix que l'usuari proporcioni dos tipus diferents de proves d'identitat abans d'obtenir accés a un recurs, com un compte en línia, un sistema informàtic, o una porta segura.

Que es MQTT

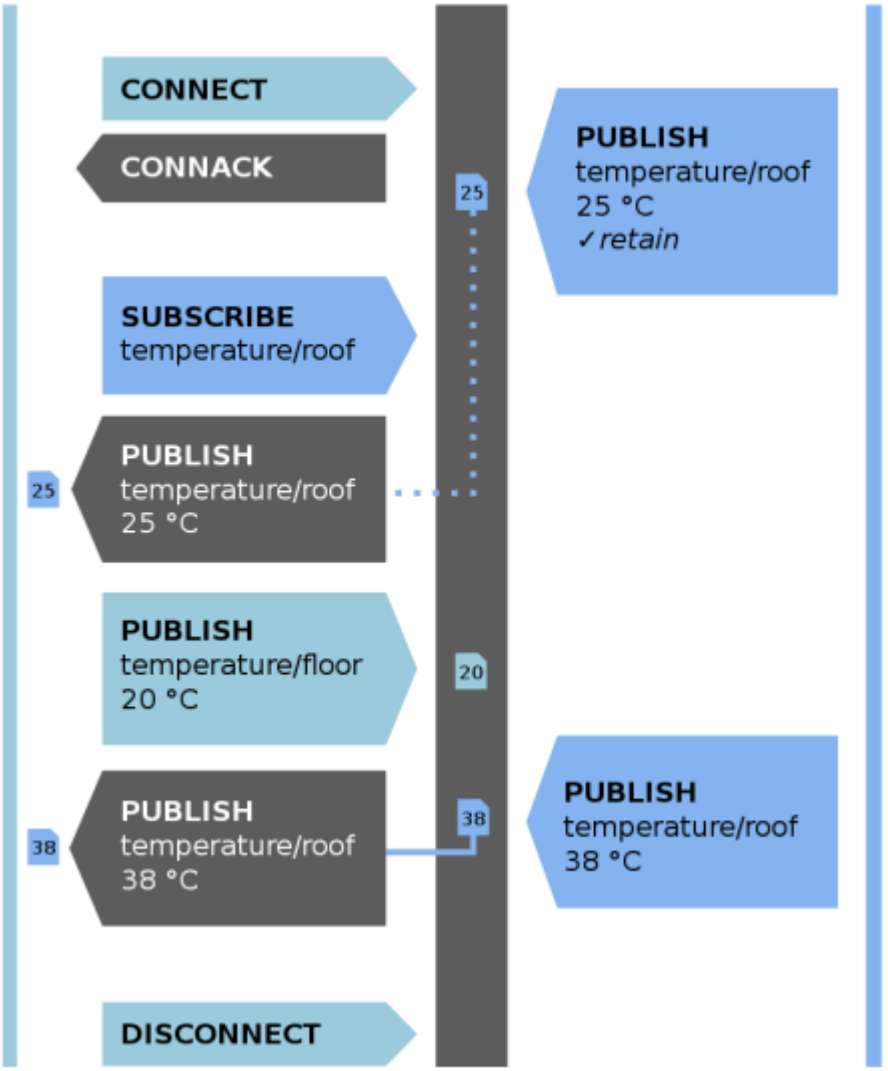
Message Queue Telemetry Transport Protocol

És un sistema de publicació de subscripció basat en un model d'intermediari i en el protocol TCP/IP.

- Es va dissenyar per donar suport a xarxes amb connexió amb llocs remots i on es produeixen pèrdues intermitents de dades.
- Funciona sobre TCP.
- S'utilitza el mínim nombre de bytes per cada missatge.
- És molt fiable, ja que existeix la funció QoS (Quality of Service) que informa de l'estat de la comunicació.

Tipus de missatges

- Connect
- Disconnect
- Publish



Que es CoAP

Constrained Application Protocol

- És un model client/servidor.
- Protocol de la capa d'aplicació d'internet.
- Proporciona un protocol de sol·licitud RESTful .
- Funciona sobre UDP.
- Utilitza seguretat DTLS, que és la implementació del protocol SSL sobre el protocol UDP.
- Permet comunicar-se amb diferents nodes al mateix temps (Multicast). Per exemple per apagar o encendre totes les llums alhora.

Sistema Operatiu

Podem tenir dispositius sense sistema operatiu, però la tendència és tenir-los, ja que ajuden a la gestió de la complexitat creixent dels dispositius.

Podem dir que un dispositiu que consumeix menys de 16 K de RAM i Flash/ROM no requereix un sistema operatiu.

Caracteristiques

- **Empremta:** mínims requisits hardware, memòria, per a evitar sobrecarregues.
- **Escalabilitat:** escalable per qualsevol tipus de dispositiu.
- **Portabilitat:** aïllar les aplicacions de les característiques específiques del hardware.
- **Modularitat:** disposar d'un kernel i la resta de funcions modulars.
- **Connectivitat:** suport per diferents tipus de protocols de connectivitat com Ethernet, Bluetooth, WiFi, LoRaWAN, IEEE 802 15 4, RFID, etc.
- **Temps real:** dispositius mèdics, dispositius per control de la seguretat o controls de tràfics són essencials que funcionin en temps real.
- **Seguretat:** proporcionar nivells de seguretat, com suport per SSL, inici segur amb autenticació, mòduls o components pel xifrat, etc.
- **Fiabilitat:** aquesta característica és obligatòria per dispositius crítics, per exemple aquells que s'utilitza en sistemes crítics industrials, o que han d'estar en ubicacions físiques especials.
- **Eficiència energètica:** Estalviar bateria pot suposar un avantatge econòmic ja que de vegades és molt costós fer els canvis.

Requeriments de seguretat

- **Referents al sistema**
    - Assegurar la privacitat de les dades. Confidencialitat.
    - Minimitzar els atacs de superfície. Tots els llocs o punts d'entrada que poden ser explotats per un hacker.
- **Referents a la capa dispositiu**
    - Sistema endurit i segur. El SO dels dispositius IoT no han d'executar serveis de xarxa innecessaris. Podrien permetre als actors d'amenaça un camí cap al sistema i potser a la xarxa IoT.
    - Assegurar el firmware i les actualitzacions del sistema operatiu. Molts dispositius no disposen d'un accés continuat per poder actualitzar-los, ja que es troben en lloc remots. S'ha d'intentar trobar un mètode per fer-ho.
- **Referents a la capa comunicació**
    - Comunicacions segures. Els sistemes IoT han d'usar mesures que evitin la intercepció i falsificació de dades. Han d'utilitzar tècniques per verificar que les dades que es reben provenen de fonts autèntiques.
- **Referents a la capa d'aplicació**
    - Credencials predeterminades o febles. Tots els dispositius IoT han d'utilitzar un fort procés d'autenticació. Molts productes IoT s'inclouen amb credencials predeterminades que faciliten la configuració del propietari del dispositiu. Les credencials predeterminades s'han de canviar abans de posar el dispositiu en servei. Les contrasenyes s'han d'ajustar a les polítiques de seguretat quant a longitud i composició.
    - Interfícies web segures. Les interfícies web orientades a Internet tenen instal·lacions d'inici de sessió que poden ser vulnerables a diversos tipus de ciberatacs. Aquestes interfícies haurien d'estar protegides contra atacs.

Vulnerabilitats del OWASP

- **Inseguretat en les aplicacions webs de gestió d'IOT**
    - Obstacles
        - Noms d'usuari i passwords per defecte.
        - No bloqueig del compte.
    - Solucions
        - Permetre canviar els noms d'usuari i passwords per defecte.
        - Habilitar el bloqueig del compte.
- **Mecanismes febles d'autenticació i autorització**
    - Obstacles
        - Passwords febles.
        - Els mecanismes de recuperació de passwords són insegurs
    - Solucions
        - Demanar passwords forts i complexos.
        - Verificar que els mecanismes de recuperació de passwords siguin segurs.
- **Falta de xifrat a totes els comunicacions implicades**
    - Obstacles
        - Informació sensible es passa en text en clar.

        - No està habilitat o no hi ha SSL/TLS.
    - Solucions
        - Encriptar la comunicació entre els components del sistema.
        - Mantenir les implementacions SSL/TLS.
- **Privacitat de les dades**
    - Obstacles
        - Es recopila molta informació personal.
        - La informació recollida no està correctament protegida.
    - Solucions
        - Reduir la recol·lecció de dades.
        - Anonimitzar la recol·lecció de dades

Dispositius Mobils

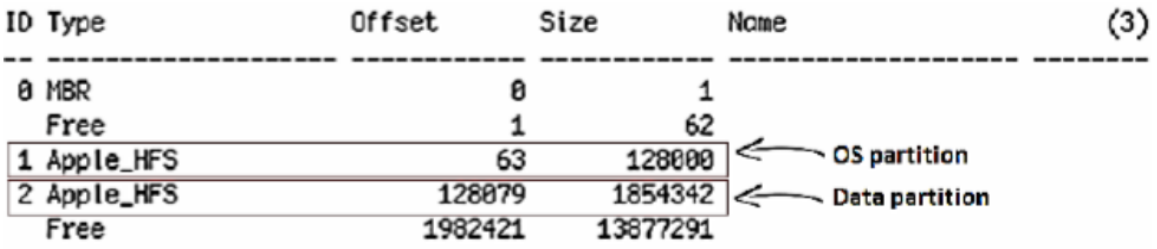
Arquitectura Mobils

- 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, …

Sistema de fitxers iOS - particions

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.



- **/Library/:** Conté plugins del sistema y de configuració, referents a l'àudio, bluetooth, etc… (Llibreries Apple no segures)
- **/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.
- **/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.

Secure Enclave

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.

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 lafabricació. Cap software ni firmware les pot llegir directament.

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.

Procés d'engedada iOS

1. Es protegeix l'arrancada i execució del SO.
2. Es garanteix que el nivell més baix del software no s'ha manipulat.
3. Quan s'engega el dispositiu s'executa codi de la Boot ROM. (iBoot)
4. En la fabricació del xip, és on s'ha establert que el codi és de confiança i segur.
5. 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.
6. Quan s'acaba l'execució del codi de la Boot ROM (procés iBoot), es verifica i executa el nucli d'iOS.
7. En dispositius antics hi ha una etapa addicional LLB (Low-Level Bootloader) abans de verificar i carregar el iBoot.
8. Quan iBoot acaba de fer les tasques assignades, verifica i executa el kernel de iOS.
9. Un error en carregar o verificar les etapes següents es gestiona de manera diferent segons el maquinari: o La ROM d'arrencada no pot carregar LLB (dispositius anteriors): mode DFU o LLB o iBoot: mode de recuperació
10. En qualsevol dels dos casos, el dispositiu s'ha de connectar a iTunes mitjançant USB i restaurar a la configuració predeterminada de fàbrica
11. Secure Enclave és un coprocessador que incorpora un gestor de claus basat en hardware aïllat del processador principal.
12. 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:
    a. Mode DFU: configurat mitjançant l'arrencada ROM en dispositius amb SoC A12.
    b. Mode de recuperació: configurat per iBoot en dispositius amb Apple A10, S2 i en els més nous sistemes en xip (SoCs).
13. 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.

14. 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.
15. Un cop finalitzada l'arrencada, el controlador de memòria denega l'escriptura a la regió de memòria física protegida.
16. 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.

Que pasa quan es produeix error arrancada iOS

El dispositiu entra en mode de recuperació o DFU automàticament.

Actualització en iOS

1. 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.
2. 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 antireproducció, i la identificació única exclusiva de xip (ECID) del dispositiu.
3. 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.
4. 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.
5. Autoritzant i signant només per a mesures conegudes, el servidor assegura que l'actualització s'efectua tal com proporciona Apple.
6. 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.
7. El coprocessador Secure Enclave utilitzarà el procés d'arrencada segura per comprovar que el software està signat i verificat per Apple.

Claus Clau de fitxer o Clau de classe

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

TOUCH ID

- Què és: Touch ID és un sistema d'identificació d'empremtes digitals.
- Com Funciona: Utilitza un sensor d'empremtes digitals que permet als usuaris desbloquejar el seu dispositiu, realitzar compres i iniciar sessió en aplicacions simplement posant el dit sobre el sensor.
- Seguretat: Les dades de l'empremta digital s'emmagatzemen de manera segura en un component del dispositiu anomenat "Secure Enclave", i no es comparteixen amb Apple ni es guarden en els servidors d'Apple.

FACE ID

- Què és: Face ID és un sistema de reconeixement facial.
- Com Funciona: Utilitza una càmera de profunditat avançada amb sensors per mapejar i reconèixer la cara de l'usuari. Això permet als usuaris desbloquejar el seu dispositiu, realitzar compres i iniciar sessió en aplicacions simplement mirant el dispositiu.
- Seguretat: Com amb Touch ID, les dades biomètriques recollides per Face ID s'emmagatzemen de manera segura en el Secure Enclave del dispositiu. Face ID també utilitza l'aprenentatge automàtic per adaptar-se als canvis en l'aparença de l'usuari, com el creixement de la barba o l'ús de maquillatge.

Sistema Android

Es va substuir la màquina virtual per l'Android Runtime (ART)

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.

Aplicacions Android

- En llenguatge Java.
- Es poden realitzar amb l'Android SDK (kit de desenvolupament de software), Google App Inventor, …
- Format: .APK (Android Application Package).

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), 218 fitxers, 222 (512 MiB) tamany màxim del fitxer.
        - YAFFS2(limitat a 8GiB)
- 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. o 20% més lent en lectura seqüencial.
- **/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.
- **/boot:**
    - Conté el bootloader i el kernel.
    - És necessària. On arrenca el dispositiu.
- **/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
- **/recovery:**
    - Per recuperació (Factory reset).
    - Es pot iniciar el sistema en mode recovery.
    - Es fa servir per manteniment i recuperació de dades.
- **/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, …)
- **/sdcard:**
    - Es guarden les configuracions i dades de les aplicacions.

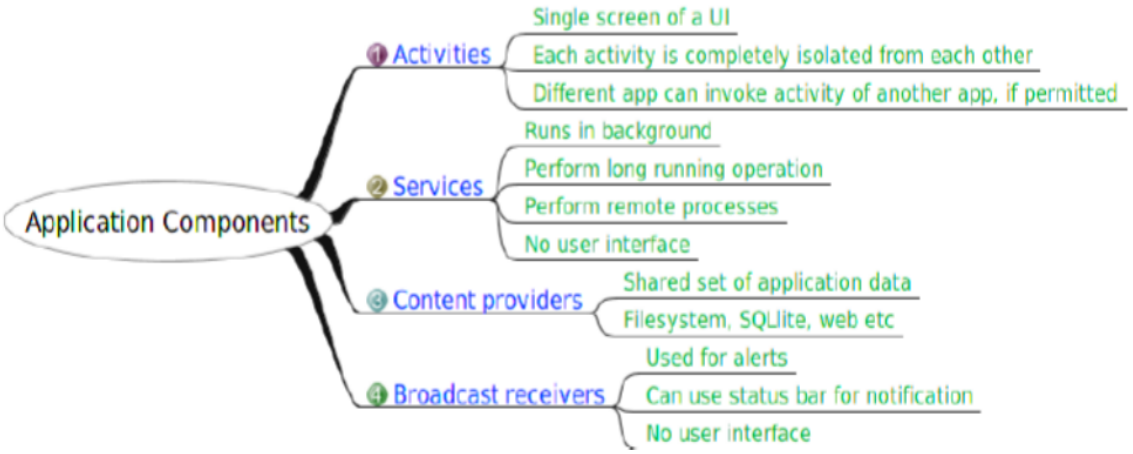
    - Pot ser una tarjeta SD o el sitema de fitxers montats. (Es pot accedir mitjançant USB OTG).
    - Es poden tenir diverses montades, per exemple la interna i l'externa
- **/cache:**
    - Es guarda la informació d'ús habitual que se li dóna a l'usuari al dispositiu mòbil tant referent a les aplicacions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

Com arranca Android

- **Power On:** Quan s'encén el dispositiu, el primer que s'activa és el bootloader, un programa de baix nivell emmagatzemat en la memòria ROM del dispositiu.
- **Bootloader:** El bootloader és el primer codi que s'executa quan un dispositiu s'encén. La seva funció principal és inicialitzar el maquinari i carregar el sistema operatiu.
- **Carregament del Kernel:** El bootloader carrega el kernel de Linux. El kernel és el nucli del sistema operatiu i gestiona la interacció entre el maquinari i el programari.
- **Inicialització del Sistema:** Un cop el kernel està carregat, s'inicia el procés d'inicialització del sistema. Això inclou la configuració de diversos paràmetres del sistema i la preparació del dispositiu per a carregar el sistema operatiu Android.
- **Daemon 'init':** El procés 'init' és el primer procés que s'executa en l'espai d'usuari. Aquest procés llegeix els scripts d'inicialització i configura els serveis necessaris per al funcionament del sistema operatiu.
- **Zygote:** El procés Zygote s'inicia com a part de l'arrancada del sistema. Aquest procés és la base per a totes les aplicacions Android que s'executen en l'espai d'usuari. Zygote carrega la màquina virtual de Java (Dalvik o ART, depenent de la versió d'Android) i altres biblioteques comunes.
- **System Server:** Aquest procés s'inicia des de Zygote i inicialitza els serveis de nivell superior d'Android, com el gestor de finestres, el gestor de telefonia, etc.
- **Carregament de la Interfície d'Usuari:** Un cop els serveis de sistema estan en marxa, el sistema carrega la interfície d'usuari, permetent a l'usuari interactuar amb el dispositiu.
- **Aplicacions d'Inici:** Finalment, s'inicien les aplicacions d'arrancada, com ara llançadors d'aplicacions, serveis de sincronització, etc.

Seguretat Android

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.



- **Activity**
  - Punt d'entrada d'interacció amb l'usuari. Pantalla individual amb interfície d'usuari. Cada activitat és independent una de l'altra.
  - Una activitat es pot iniciar per una altra. Per exemple enviar foto feta amb la càmera del mòbil per correu.
- **Services**
  - 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.
  - 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 processosja que s'estan usant serveis d'aquests.
- **Content providers**
  - 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..
- **Broadcats receivers**
    - Un receptor d'emissió és un component que possibilita que el sistema entregui events a l'aplicació fora del flux d'usuaris habitual, 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.

Memoria

- 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.

APK

- 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.
- Classes.dex
    - Les classes compilades en el format d'arxiu dex, comprensible per la màquina virtual Dalvik i per Android Runtime.