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: Android / iOS

- 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

- 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

- **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

Introducció. Què és IoT?

- Segons l'empresa Gartner:
  - 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 de sensors omnipresents.

UF1. Seguretat en dispositius mòbils i IoT

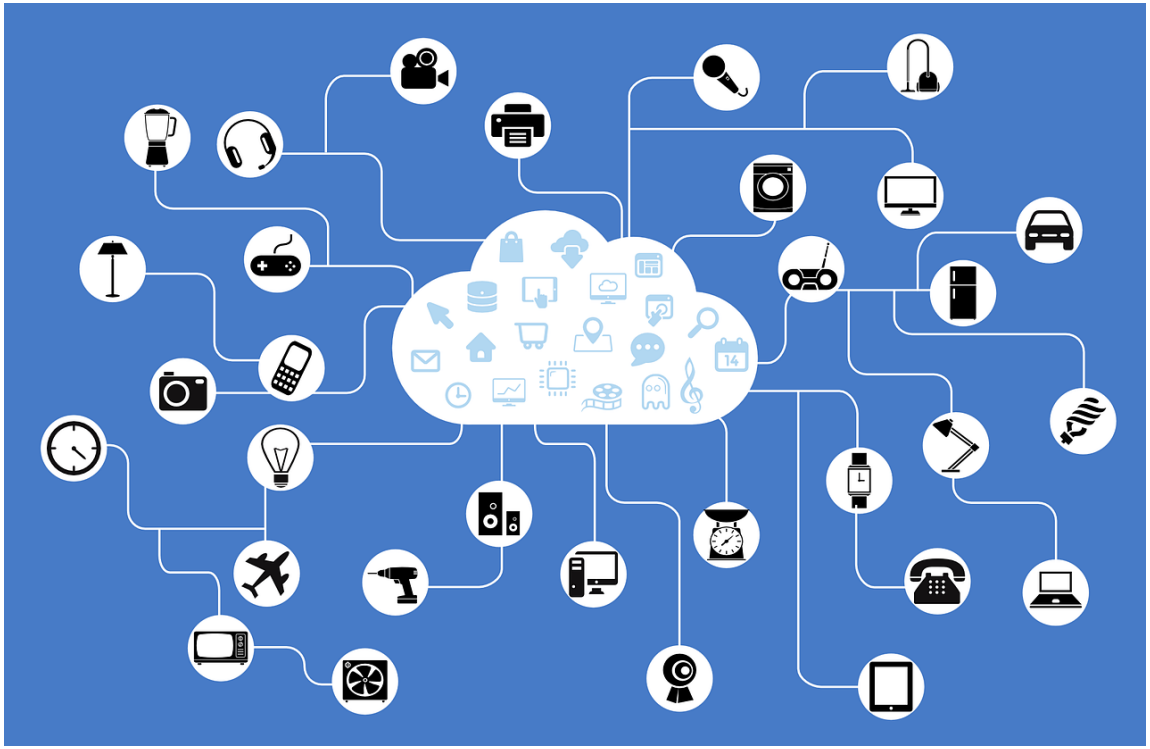
Introducció. Què és IoT?

- El concepte va sorgir del MIT concretament del Centre “Auto ID”, del que Kevin Asthon va ser el cofundador.
- En aquest centre treballaven amb la definició e implementació del que seria el RFID (identificació per radiofreqüència) i en el disseny de sensors per realitzar diferents tipus de deteccions.
- Aquest centre que estava repartit per 7 universitats de 4 continents es va encarregar de definir l’arquitectura del que seria la IoT.

UF1. Seguretat en dispositius mòbils i IoT

Introducció. Què és IoT?

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

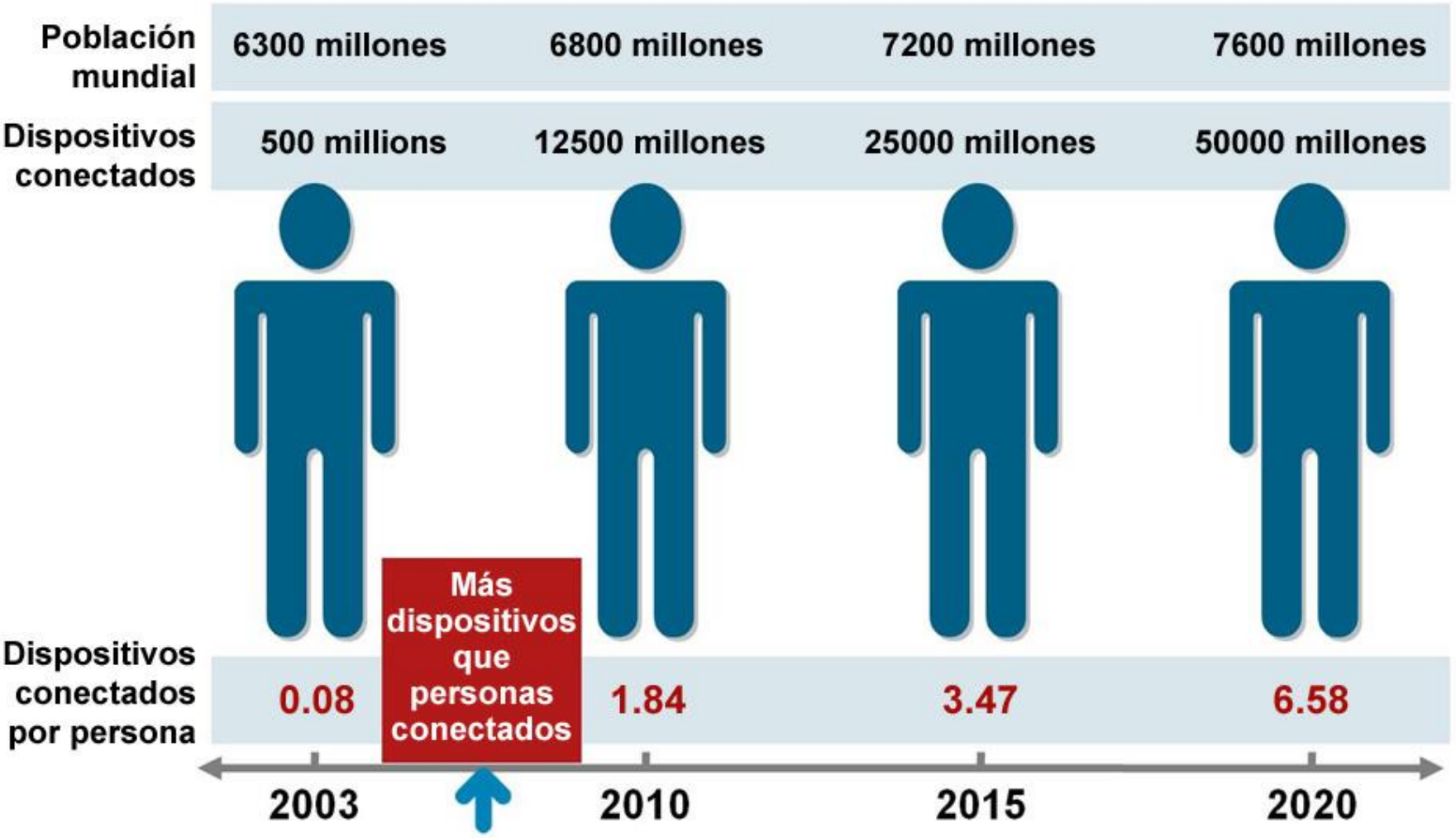


UF1. Seguretat en dispositius mòbils i IoT

Introducció. Què és IoT?

- L'empresa CISCO, darrera de la iniciativa de la IoT , va crear un comptador de connexions dinàmic, que permetia estimar el nombre de *"coses"* connectades des del juliol del 2013 fins al 2020.
- 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.

UF1. Seguretat en dispositius mòbils i IoT



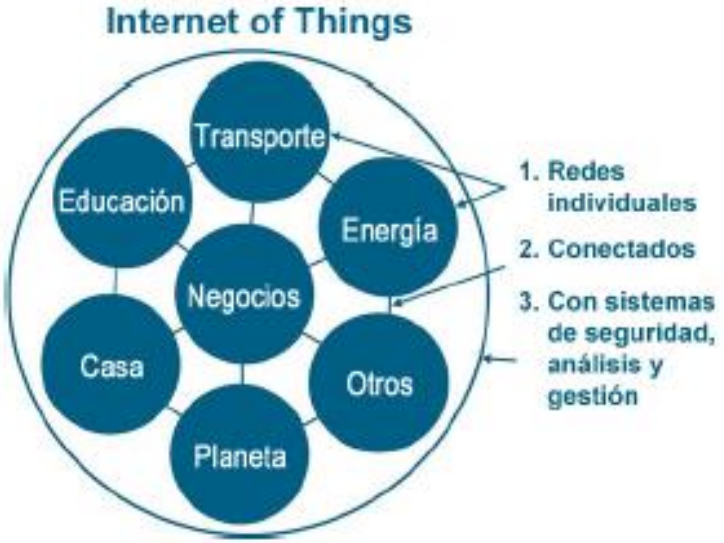
Ref.https://www.cisco.com/c/dam/global/es_es/assets/executives/pdf/Internet_of_Things_IoT_IBSG_0411FINAL.pdf

UF1. Seguretat en dispositius mòbils i IoT

Introducció. Què és IoT?

- El càlcul que es realitza de dispositius connectats segons persones, es fa tenint en compte tota la població mundial.
- El IoT pot ser vista com una xarxa de xarxes.
  - Exemple: Sensors d'un cotxe, casa o edifici domòtic, …

Figura 2. El IoT puede considerarse una red de redes



Fuente: IBSG de Cisco, abril de 2011

UF1. Seguretat en dispositius mòbils i IoT

Introducció. Dades IoT.

Table 1: IoT Units Installed Base by Category (Millions of Units)

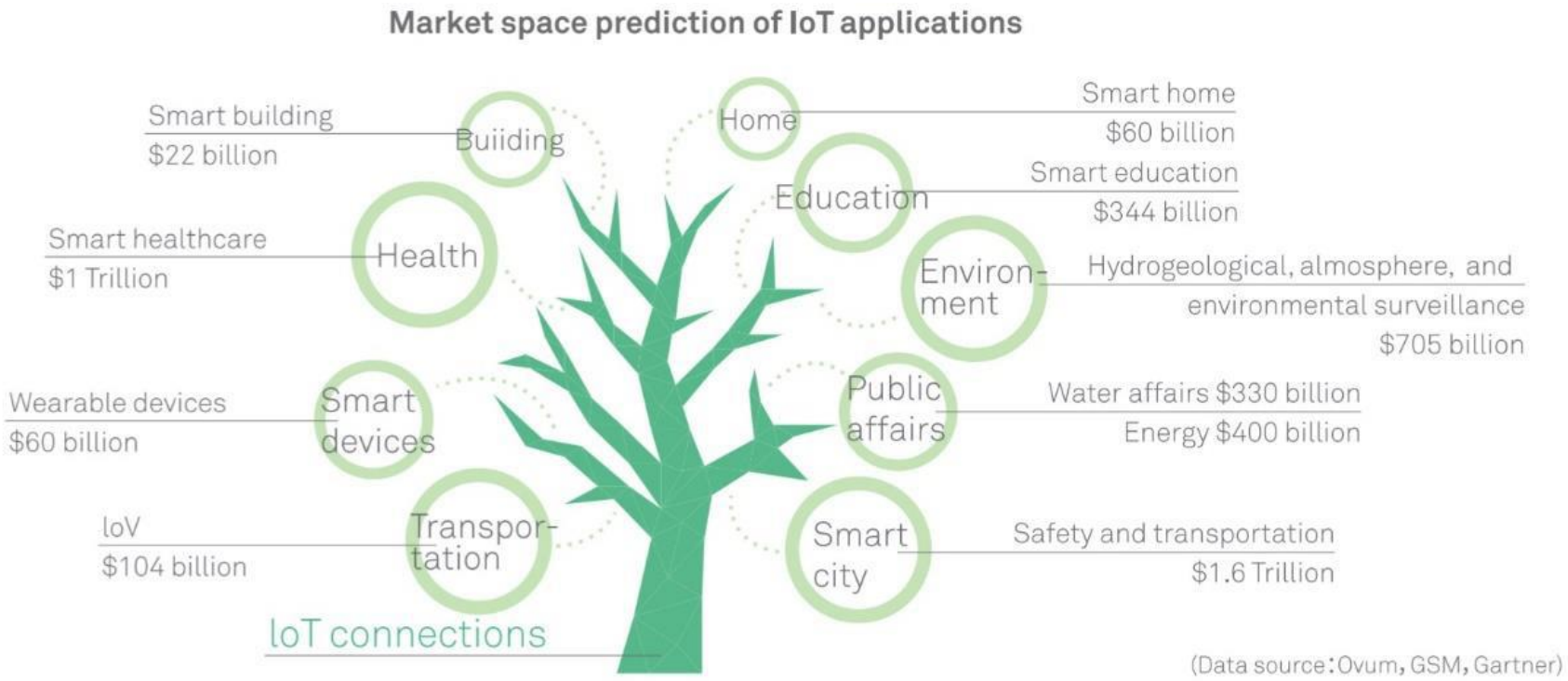
Category	2016	2017	2018	2020
Consumer	3,963.0	5,244.3	7,036.3	12,863.0
Business: Cross-Industry	1,102.1	1,501.0	2,132.6	4,381.4
Business: Vertical-Specific	1,316.6	1,635.4	2,027.7	3,171.0
Grand Total	6,381.8	8,380.6	11,196.6	20,415.4

Source: Gartner (January 2017)

Ref. https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

UF1. Seguretat en dispositius mòbils i IoT

Introducció. Dades IoT.



UF1. Seguretat en dispositius mòbils i IoT

Introducció. Dades IoT.

- La major part de les comunicacions a internet són degudes a IoT.
- Qualsevol " *objecte* " pot estar connectat, enviant i/o rebent informació.
- Al 2020 segons Gartner estima que hi haurà 26 bilions d'unitats interconnectades.
- Està present a tots els àmbits: la casa, les ciutats, la indústria, l'automoció, els jocs, ...
- La principal característica dels dispositius que formen part de la IoT és la seva ubiqüitat o omnipresència.
- Uns dels principals objectius és l'anàlisis de la multitud de dades que ens proporciona.
- https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/infographic-c82-741491.html

UF1. Seguretat en dispositius mòbils i IoT

Introducció. 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, …

UF1. Seguretat en dispositius mòbils i IoT

Introducció. Aplicacions de l'IoT.

- Hi ha 3 categories o camps d'aplicació suggerides, tot i que n'hi ha d'altres d'importants:
  - Consum.
  - Empresarial.
  - Infraestructura.
- Exemples:
  - Dispositius embeguts amb CPU, memòria i energia limitats. -> Recol·lecció d'informació en diferents entorns (ecosistemes naturals, edificis, fàbriques, …)
  - Hàbits de compra d'un usuari rastrejant el telèfon mòbil. (Es fan ofertes especials amb els productes preferits pels usuaris)
  - Neveres intel·ligents amb stock dels productes.
  - Sistemes intel·ligents de transport per evitar retencions, i millorar l'operació i seguretat del transport terrestre, tan en carreteres urbanes i rurals com per ferrocarrils.
  - Seguretat i automatització en la llar.

UF1. Seguretat en dispositius mòbils i IoT

Introducció. Aplicacions de consum de l'IoT.

- Són molts els dispositius IoT creats per al consum:
  - automòbils connectats,
  - entreteniment,
  - automatització de la llar (domòtica),
  - tecnologia vestible (rellotges digitals, videojocs, moda, ….),
  - Electrodomèstics amb connexió wifi (rentadora, secadora, forns, nevera,…), …

UF1. Seguretat en dispositius mòbils i IoT

Introducció. Aplicacions de tipus empresarial de l'IoT.

- S'anomenen EIoT, i són tots els dispositius en l'ambient corporatiu o dels negocis.
- Utilitzen l'IoT pel mercadeig i estudi dels hàbits dels consumidors.
- 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, ...)
- https://bits.blogs.nytimes.com/2008/03/09/aol-brings-out-the-penguins-to-explain-ad-targeting-ok-saul-and-louise-post-with-article/

UF1. Seguretat en dispositius mòbils i IoT

Introducció. Aplicacions de infraestructura de l'IoT.

- Permeten fer el seguiment i control d'operacions d'infraestructura urbana i rural, com ponts, vies de ferrocarril, parcs eòlics, abocadors d'escombraries ...
- Permeten portar un control sobre sistemes que poden comprometre la seguretat o incrementar el risc en certs llocs.
- Control dels ponts en rius per permetre el pas de grans embarcacions.
- Control de les vies de ferrocarril.

UF1. Seguretat en dispositius mòbils i IoT

Introducció. Altres tipus d'aplicacions de l'IoT.

- **Agricultura**.
  - Permet reduir els residus i millora la productivitat, des de la quantitat de fertilitzant utilitzat fins al combustible usat en la maquinària agrícola.
  - S'instal·len sensors de llum, humitat, temperatura, humitat del sòl, i s'automatitza el sistema de reg, tenint en compte les hores on hi ha més temperatura a l'ambient, per tal d'estalviar aigua.

UF1. Seguretat en dispositius mòbils i IoT

Introducció. Altres tipus d'aplicacions de l'IoT.

- **Medicina i salut**.
  - Permet rastrejar remotament pacients i sistemes de notificació d'emergències.
  - Exemples: Monitors de pressió sanguínia, control de pulsacions, marcapassos, polseres electròniques, audiòfons sofisticats.
  - Alguns hospitals utilitzen llits intel·ligents per saber quan estan ocupats, quan un pacient s'intenta aixecar del llit, o per ajustar la posició del llit segons les necessitats del pacient, sense estar-hi present.
  - 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)
  - https://www.cleveroad.com/blog/iot-in-healthcare-industry--see-why-it-has-a-promising-future

UF1. Seguretat en dispositius mòbils i IoT

Introducció. Altres tipus d'aplicacions de l'IoT.

- **Transport**.
  - Permet gestionar tot el relacionat amb els vehicles, la infraestructura, i els conductors o usuaris.
  - Exemples:
    - Control intel·ligent del trànsit.
    - Estacionament intel·ligent.
    - Cobrament electrònic dels petges.
    - Control de velocitat.
    - Logística i manegament de flota, seguiment de la ubicació i les condicions de la carga i els actius, mitjançant sensors inalàmbrics que envien alertes en cas d'events com retrassos, danys, robatoris, …

UF1. Seguretat en dispositius mòbils i IoT

Introducció. Altres tipus d'aplicacions de l'IoT.

- **Indústria**.
  - Anomenat IIoT.
  - Utilitzat en entorns relativament tancats.
  - Exemples:
    - Mesura de concentració de pols en entorns industrials.
    - Automatització de robots.
    - …

UF1. Seguretat en dispositius mòbils i IoT

Introducció. Seguretat de l'IoT.

- La seguretat és un dels problemes principals quan parlem de la IoT.
- No hi ha una regulació clara i explícita pels fabricants. Existeixen certes normatives específiques per àmbits concrets (dispositius per ITS energia).
- 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.

UF1. Seguretat en dispositius mòbils i IoT

Introducció. Seguretat de l'IoT.

- Al 2015 quasi la meitat de les aplicacions dels dispositius mòbils no encriptaven les comunicacions, i el 70% dels dispositius IoT tenia vulnerabilitats de seguretat en les seves contrasenyes.
- Una càmera de vigilància per a nadons podia ser hackejada per robar el vídeo, i en una cafetera amb contrasenya no encriptada es podia arribar a saber la contrasenya de la xarxa WIFI on estava connectada.
- Els dispositius IoT guarden dades sobre els hàbits dels usuaris.
- Una solució seria usar el xifratge i encriptació de les dades en el moment de pujar-los al núvol.

UF1. Seguretat en dispositius mòbils i IoT

Introducció. Seguretat de l'IoT.

- Segons OWASP, la seguretat en IoT NO és el mateix que la seguretat als dispositius.
- El problema de la securització de IoT és que afecta a molts àmbits:
  - Securitzar el dispositiu (S.O., firmware, interficie de gestió,…).
  - El Cloud (on s'emmagatzemen les dades).
  - La xarxa (com viatgen les dades, ports oberts..)
  - Aplicacions mòbils per accedir hi i utilitzar-la.
  - Xifrat.
  - Mecanismes d'autenticació.
  - Seguretat física.
  - Ports i interfícies físiques accessibles (USB, Bluetooth , xarxa, ...).

UF1. Seguretat en dispositius mòbils i IoT

Introducció. Seguretat de l'IoT.

Ref. https://www.kaspersky.es/blog/internet-de-las-cosas-problemas-de-seguridad/1045/

UF1. Seguretat en dispositius mòbils i IoT

- **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

Arquitectura dels dispositius IoT.

- Un **sistema IoT** està format per **capes o nivells**.
- El model de referència d'**IoT** conté **7 capes** semblant al model de referència del model OSI.
- Les parts acostumen a dir-se nivells en lloc de capes. El model de referència d'IoT va ser desenvolupat com un framework comú per guiar i ajudar a accelerar els desplegaments d'IoT.
- La intenció del **model de referència** IoT és proporcionar una **terminologia comuna** i ajudar a aclarir com la informació flueix i es processa per a una indústria IoT unificada.
- 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**.

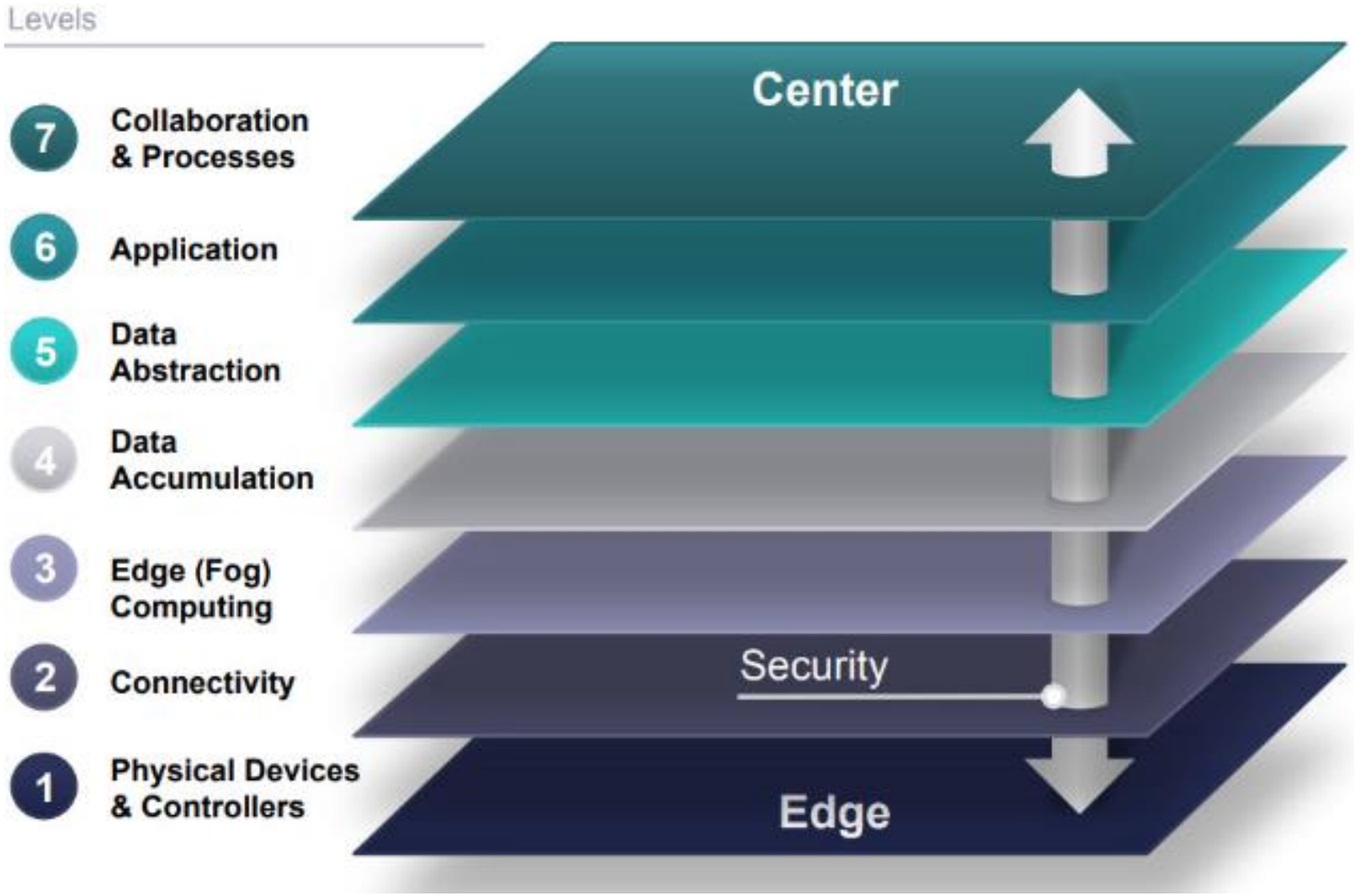
UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius IoT.

Nivell		Descripció
7	Col·laboració i processos (Implicació de persones i processos empresarials)	Trascendeix múltiples aplicacions per incloure la comunicació i la col·laboració necessàries entre les persones i els processos empresarials.
6	Aplicació (Informes, anàlisi, control)	Interpretació de la informació basada en la naturalesa de les dades del dispositiu i les necessitats empresarials.
5	Abstracció de dades (Agregació i accés)	Centrat en la representació de les dades i el seu emmagatzematge per permetre el desenvolupament d'aplicacions.
4	Acumulació de dades (emmagatzematge)	Les dades en moviment es converteixen en dades en repòs. Les dades també es transformen perquè puguin ser consumides pels nivells superiors.
3	Edge (fog) Computing (Anàlisi i transformació d'elements de dades)	Converteix les dades en informació adequada per a emmagatzematge i processament de nivell superior.
2	Connectivitat (Unitats de processament i comunicació)	Responsable de la transmissió de dades fiable i oportuna entre els dispositius i la xarxa, a través de xarxes i entre la xarxa i el processament de dades al nivell 3.
1	Dispositius físics i controladors (Les "coses" d'IoT)	Inclou una àmplia gamma de dispositius de punt final que envien i reben informació.

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius IoT.



UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius IoT.

- Les mesures de seguretat del model inclouen:
  - **Securitzar el hardware i software de cada dispositiu** o sistema connectat a la xarxa IoT.
  - Proveir **seguretat a tots els processos** que succeeixin a cada nivell en la xarxa.
  - **Securitzar el moviment de els dades i comunicacions entre cada nivell.**

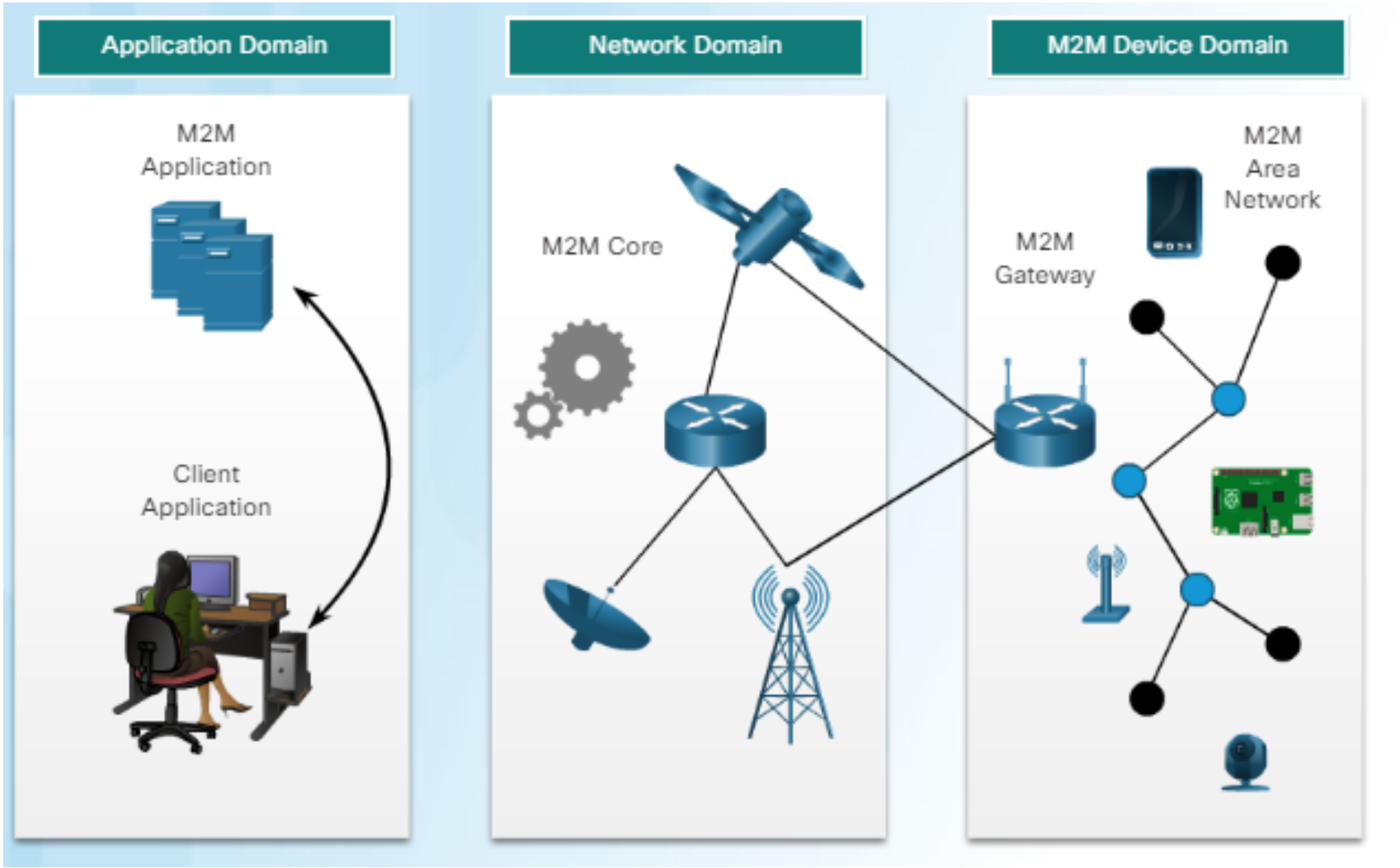
UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius IoT. El model ETSI.

- El 2008, 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
- 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**.

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius IoT. El model ETSI.

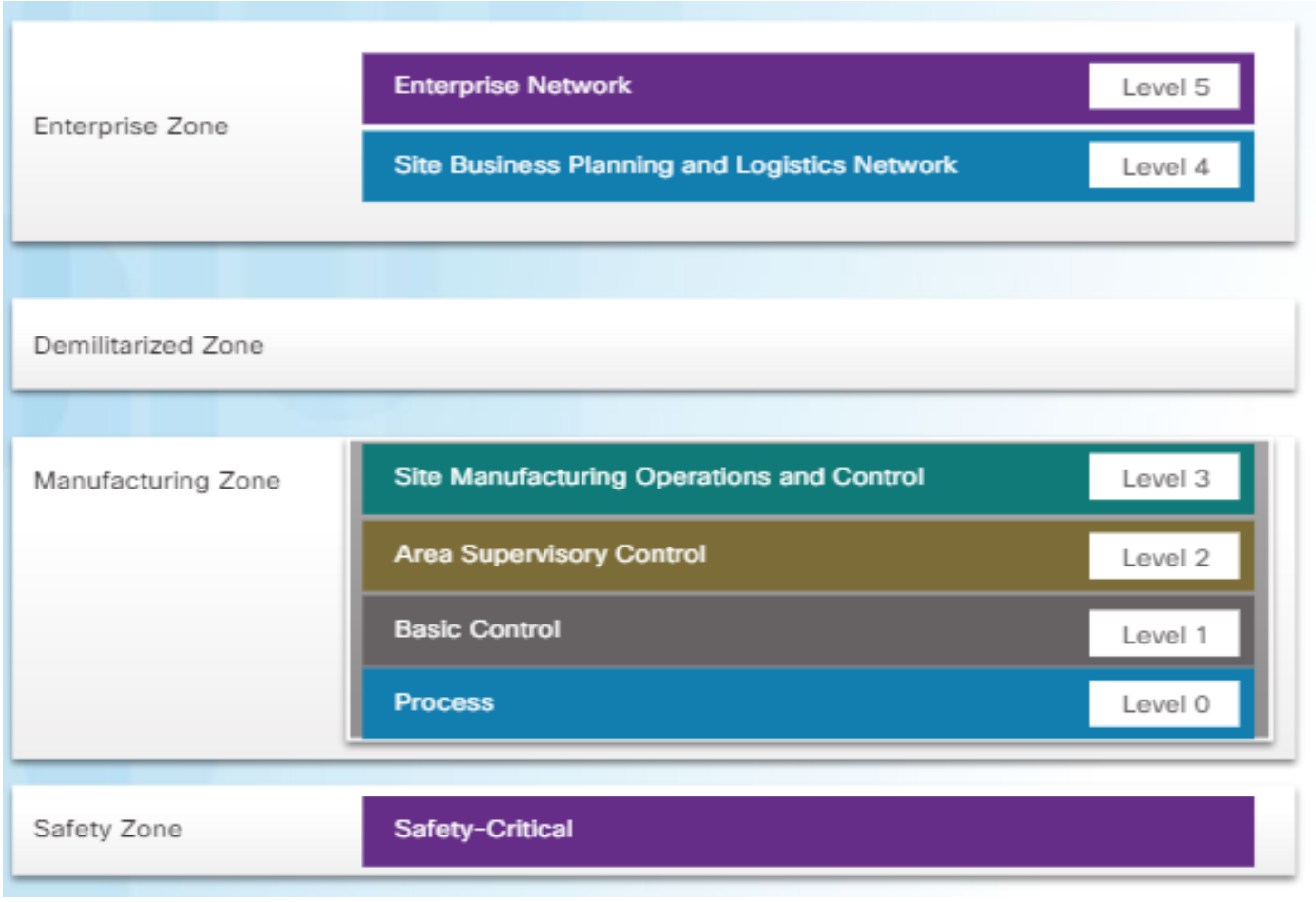


UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius IoT. Altres models.

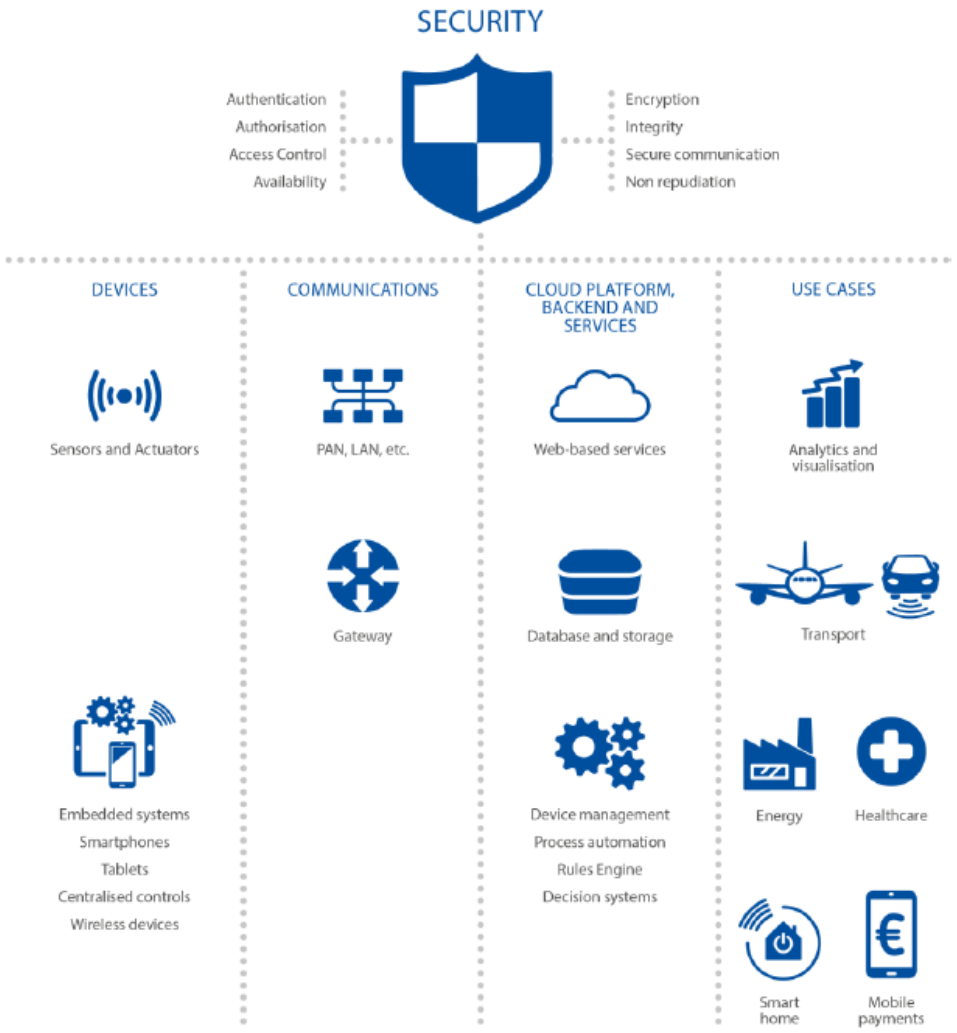
- Hi ha una gran varietat de models IoT amb usos especials:

Model Purdue per a la jerarquia de control



UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius IoT.



UF1. Seguretat en dispositius mòbils i IoT

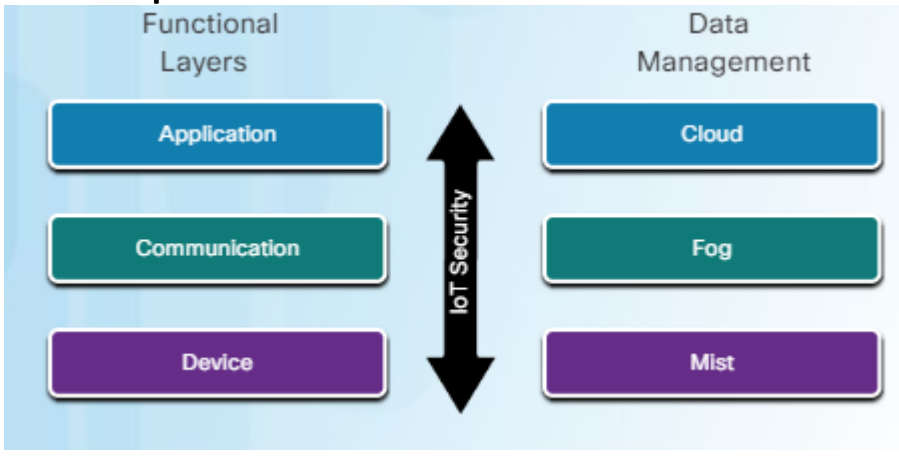
Arquitectura dels dispositius IoT. Altres models.

- Hi ha una gran varietat de models Iot amb usos especials:
  - **Model Purdue per a la jerarquia de control:** es tracta d'un model comú i ben entès a la **indústria manufacturera** que **segmenta dispositius i equips en funcions jeràrquiques**. S'ha incorporat a molts altres models i estàndards de la indústria.
  - **Industrial Internet Reference Architecture (IIRA):** creat pel Consorci d'Internet Industrial (IIC), l'IIRA és un marc basat en estàndards utilitzat pels arquitectes de sistemes per dissenyar sistemes industrials.
  - **Internet de les Coses - Arquitectura (IoT-A):** aquest model es coneix habitualment com a IoT-A, més conegut formalment com a Model de referència arquitectònica (**ARM**) per a Internet de les coses. El fòrum IoT-A manté el model IoT-A.

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius IoT. Model Simplificat IoT.

- Els **sistemes IoT** poden ser molt **grans i complexos**. Milers de **sensors, actuadors i passarel·les** poden estar presents en un sistema IoT.
- Els dispositius IoT es poden **connectar** a passarel·les **mitjançant** diversos **protocols** i les passarel·les es poden **connectar** a **Internet** i a **aplicacions en núvol mitjançant** un nombre similar de **protocols**.
- Per assegurar un sistema IoT, és important **entendre on existeixen vulnerabilitats al sistema**.
- Simplificar el sistema dividint-lo en **àrees funcionals** és una manera molt útil d'entendre els sistemes complexos.
- Dividim els nivells en capes:
  - **d'aplicacions,**
  - **comunicacions, i**
  - **dispositius**



UF1. Seguretat en dispositius mòbils i IoT

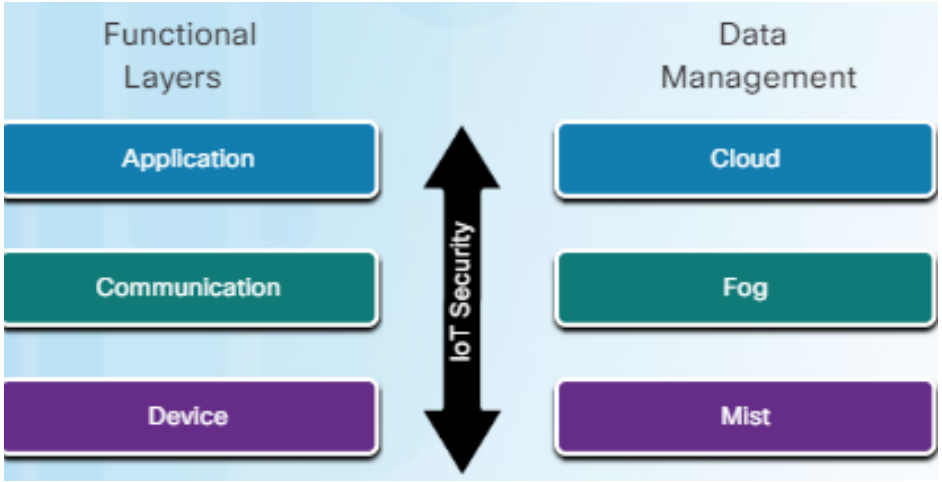
Arquitectura dels dispositius IoT. Model Simplificat IoT.

- Funcionalment, ens interessa com es connecten les coses a la xarxa.
- Per exemple:
  - 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.

UF1. Seguretat en dispositius mòbils i IoT

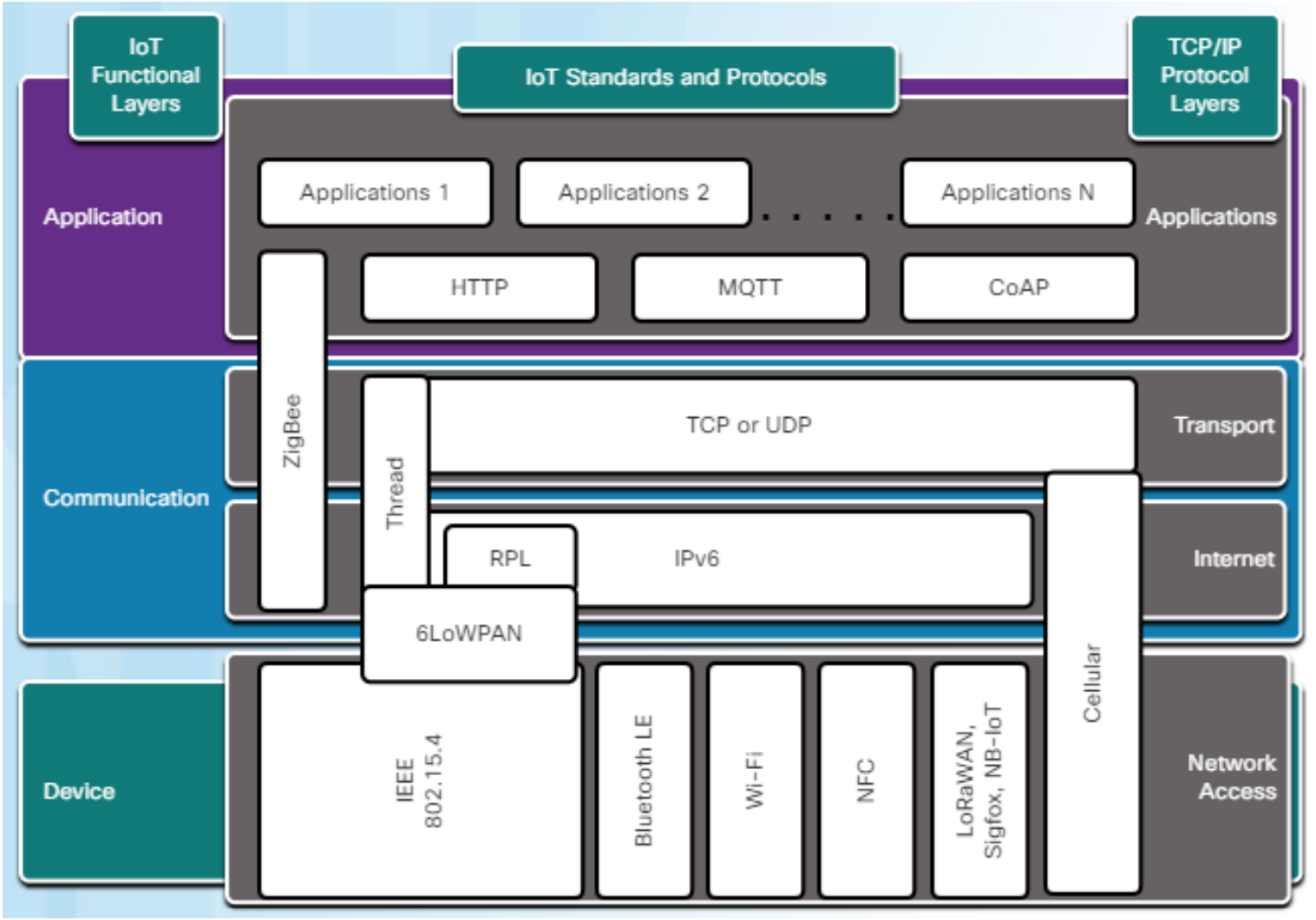
Arquitectura dels dispositius IoT. Model Simplificat IoT.

- Per a la **gestió de dades**, ens interessa saber **quan i on es processen les dades**.
- Es processa a la capa **Mist**, a prop del terra on hi ha coses connectades a la xarxa? Per exemple, l'aspersor d'un sistema de reg pot detectar la temperatura i la humitat del sòl i activar-se de forma autònoma?
- O les dades processades a la capa **Fog** en un dispositiu local que té més energia, com ara el tauler de control del sistema de reg? El supervisor pot anul·lar remotament les accions autònomes del tauler de control mitjançant una aplicació mòbil o d'escriptori al **Cloud**?
- Independentment dels aspectes de connectivitat funcional i gestió de dades del sistema IoT, **la seguretat ha d'impregnar-se a tot arreu**, tal com mostra la fletxa del gràfic.



UF1. Seguretat en dispositius mòbils i IoT

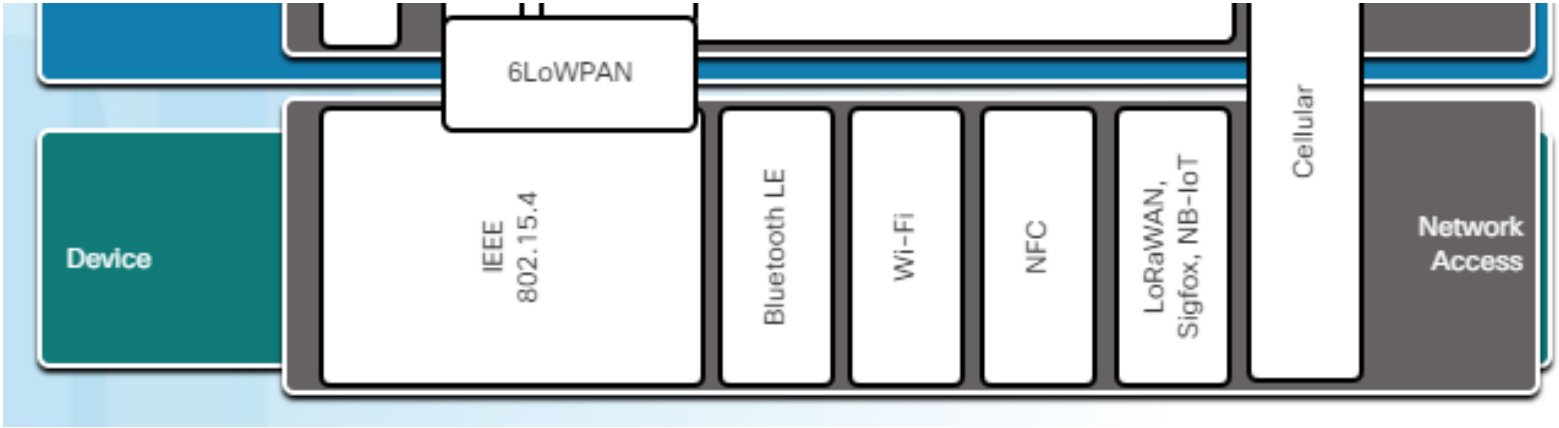
Arquitectura dels dispositius IoT. Model Seguretat IoT.



UF1. Seguretat en dispositius mòbils i IoT

Arquitectura IoT. Capa dispositiu.

- Podem trobar:

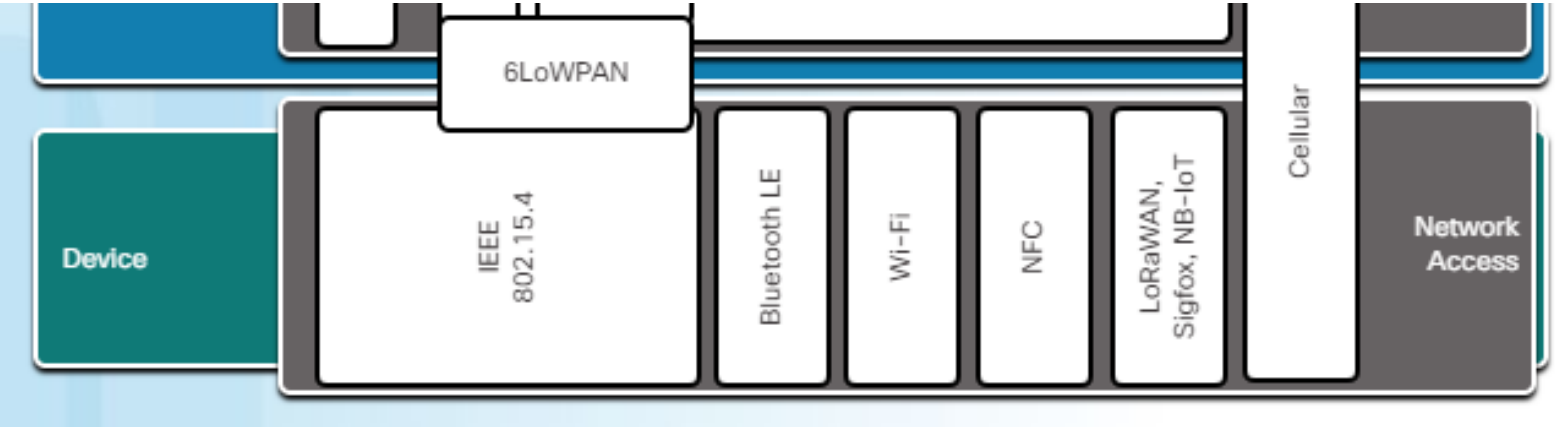


  - **IEEE 802.15.4:** es tracta de l'estàndard de l'Institut d'Enginyers Elèctrics i Electrònics per a **xarxes d'àrea personal sense fils de baix rate(LR-WPAN**) que ha de ser utilitzat per **dispositius de baix cost i baixa velocitat**.
  - **Bluetooth Low Energy (BLE):** es tracta d'un protocol de xarxa d'àrea personal sense fils (**WPAN**) que utilitza la **freqüència de ràdio de 2,4 GHz**. La versió LE proporciona un **consum d'energia molt reduït** sense sacrificar l'abast.
  - **Wi-Fi:** es tracta d'una col·lecció de protocols o estàndards **IEEE 802.11** per a xarxes d'àrea local sense fils (**WLAN**) que funcionen a les **freqüències de 2,4 GHz i 5 GHz.**

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura IoT. Capa dispositiu.

- Podem trobar:

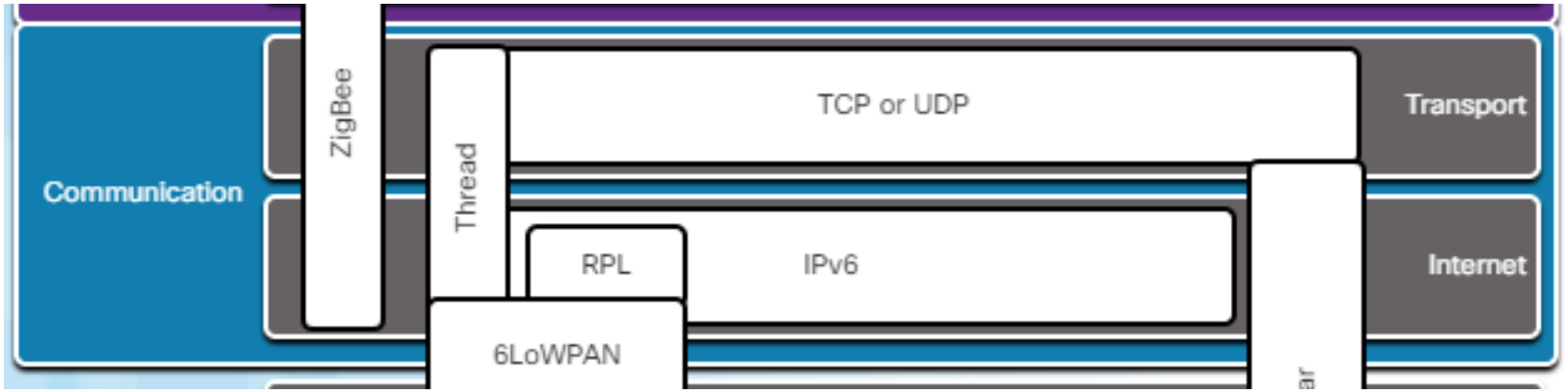


  - **Comunicació de camp proper (NFC):** es tracta d'una col·lecció de protocols per a **comunicacions de dispositiu a dispositiu** quan els **dispositius** estan **molt a prop** els uns dels altres (**a menys de 4 cm** o 1,6 polzades).
  - **Mòbil:** inclou totes les tecnologies mòbils cobertes pel Projecte de col·laboració de tercera generació (**3GPP**), com ara la quarta generació (**4G**), **LTE** i la 5a generació (**5G**).
  - **LoRaWAN, Sigfox, NB-IoT:** protocols de **xarxa d'àrea ampla de baixa potència (LPWAN)** dissenyats per transportar **petites càrregues útils de dades a llargues distàncies a taxes de transferència baixes**.

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura IoT. Capa comunicació.

- Podem trobar:

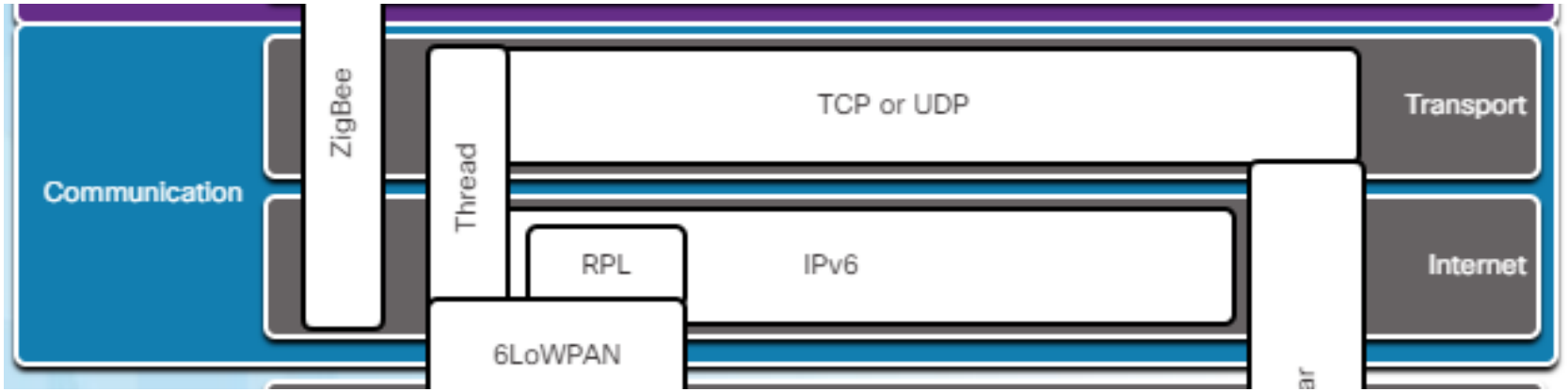


  - **Thread** (fil): aquest és un estàndard per a la domòtica que utilitza el **protocol d'Internet versió 6 (IPv6)** per encaminar a sobre d'una xarxa sense fils IEEE 802.15.4.
  - **Protocol de control de transport (TCP):** es tracta d'un protocol de **transport fiable** que **garanteix l'enviament de dades** mitjançant un sistema de **sincronització** i **missatges de confirmació**.
  - **UDP:** es tracta d'un protocol de **transport lleuger i poc fiable** que **no té cap mecanisme per a l'enviament de dades garantit.**

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura IoT. Capa comunicació.

- Podem trobar:

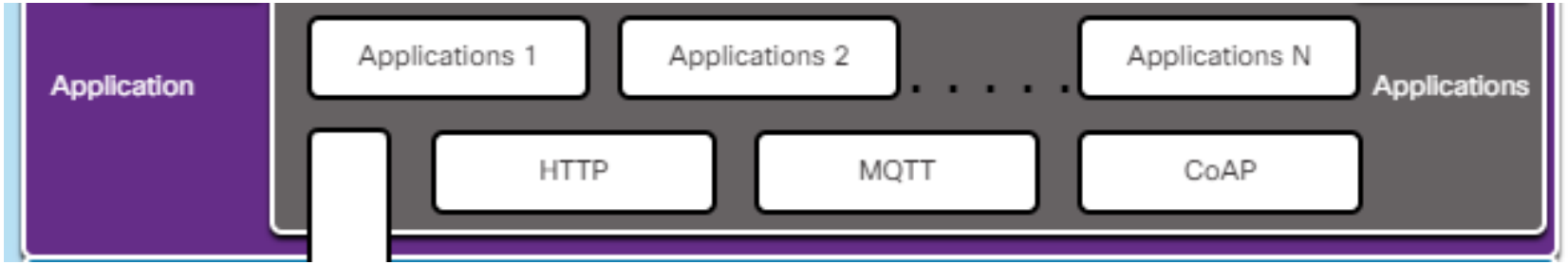


  - **RPL:** es tracta d'un **protocol d'encaminament** per a **xarxes de baix consum** i **pèrdues que utilitza IPv6**. Les xarxes amb pèrdues es classifiquen com aquelles amb dispositius que solen tenir taxes de pèrdues altes, taxes de dades baixes i inestabilitat.
  - **IPv6:** es tracta d'un espai d'adreces de 128 bits que proporciona $3{,}4 \times 10^{38}$ adreces úniques, que són més que suficients per a qualsevol nombre imaginable de dispositius IoT.
  - **6LoWPAN:** es tracta d'un estàndard Internet Engineering Task Force (IETF) per a **dispositius sense fils de baixa potència IPv6 en una xarxa d'àrea personal** que proporciona una manera perquè IPv6 s'adapti a l'estàndard IEEE 802.15.4. És per això que 6LoWPAN es mostra com a **encreuament entre les capes de xarxa de comunicacions i dispositius.**

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura IoT. Capa aplicació.

- Podem trobar:

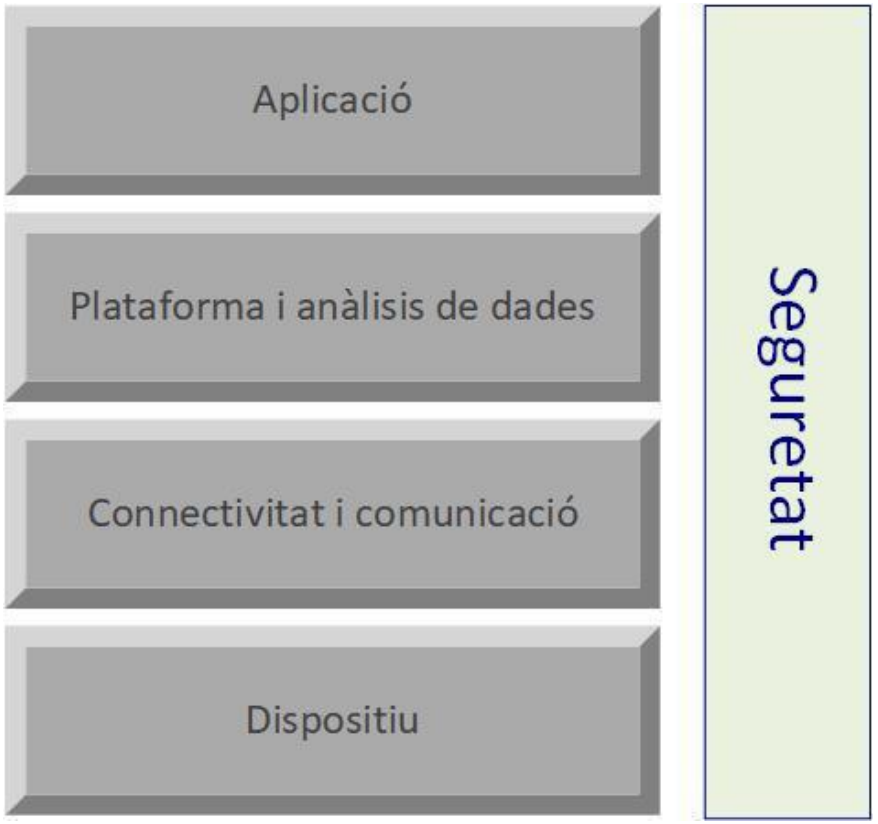


  - **Zigbee:** inclou un conjunt de protocols i utilitza **ràdios digitals de baixa potència basades en l'estàndard sense fils IEEE 802.15.4**. Inclou protocols a les capes d'aplicació i comunicació. La majoria dels components de l'especificació Zigbee existeixen a la capa d'aplicació.
  - **Protocol de transferència d'hipertext (HTTP / HTTPS):** són **protocols** d'aplicació **robustos** per **obtenir** i **publicar dades**.
  - **Message Queueing Telemetry Transport (MQTT):** es tracta d'un **protocol de missatgeria de publicació i subscripció lleuger** dissenyat per a **dispositius restringits de recursos** que **utilitzen TCP**.
  - **Protocol d'aplicació restringida (CoAP): protocol d'aplicació especialitzat dissenyat per a la transmissió de dades per dispositius restringits a xarxes M2M.**

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura dels dispositius IoT. Un altre model.

- Un altre model de sistema IoT seria el format per 4 capes o nivells.
- Pràcticament té els mateixos nivells que l'anterior.



UF1. Seguretat en dispositius mòbils i IoT

Arquitectura IoT. Capa dispositiu.

- És la **capa inferior de l'arquitectura**, l'element **hardware** que ha de tenir comunicació directa o indirecta amb Internet per considerar-ho un dispositiu IoT.
  - Dispositius amb **connexions directes a internet** poden ser: **arduino amb connexió Ethernet o wifi.**
  - Dispositius **connectats indirectament**: dispositius que **comunica a través de ràdios de baixa potència a Raspberry Pi o arduino**.
- Han de tenir un **identificador únic(UUID)**, que pot ser un UUID del sistema de ràdio (**Identificador de Bluetooth, adreça MAC Wi Fi, un token d'OAuth2**, ...)
- Trobem els **sensors o actuadors** que usen uns protocols per connectar-se a xarxa.

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura IoT. Connectivitat/Comunicacions.

- Aquesta capa **permet la comunicació entre els diferents elements** d'un sistema IoT **per l'intercanvi de dades i informació**, i també la **comunicació amb Internet**.
- Seria la capa dels **punts d'accés**.
- Hi ha diferents tipus de xarxes segons la cobertura que necessitem (**LANs,WANs PANs**).
- Tenim els diferents protocols de xarxa i en funció del tipus de comunicació utilitzarem uns o altres (**ZigBee, CoAP, BLE, Ethernet, Bluetooth, WiFi, LoRaWAN, MQTT, AMQP, DDS, RFID, USB, etc**).
- La **infraestructura necessària** per realitzar les comunicacions forma part també d'aquesta capa (**routers, gateway, firewalls**, ...).

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura IoT. Connectivitat/Comunicacions.

- Els dos protocols més coneguts que estan optimitzats per a l'ús de IoT són **MQTT** i **CoAP**.
- **MQTT**: Message Queue Telemetry Transport Protocol (Protocol de transport de telemetria de cua de missatges)
  - Va ser inventat el 1999 per resoldre problemes en sistemes incrustats i sistemes SCADA.
  - 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.

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura IoT. Connectivitat/Comunicacions.

- MQTT:

Tipus de missatge	Valor	Descripció
CONNECT	1	Petició del client per a connectar-se al servidor (vegeu Fig1)
CONNACK	2	Reconeixement de la connexió
PUBLISH	3	Edició missatge
PUBACK	4	Reconeixement de l'edició
PUBREC	5	Edició rebuda (part 1)
PUBREL	6	Edició alliberada (part 2)
PUBCOMP	7	Edició completa (part 3)
SUBSCRIBE	8	Petició de subscripció de client
SUBACK	9	Reconeixement de subscripció
UNSUBSCRIBE	10	Petició de desubscripció de client
UNSUBACK	11	Reconeixement de desubscripció
PINGREQ	12	Petició de PING
PINGRESP	13	Resposta de PING
DISCONNECT	14	Client deconnectant

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura IoT. Connectivitat/Comunicacions.

- MQTT:

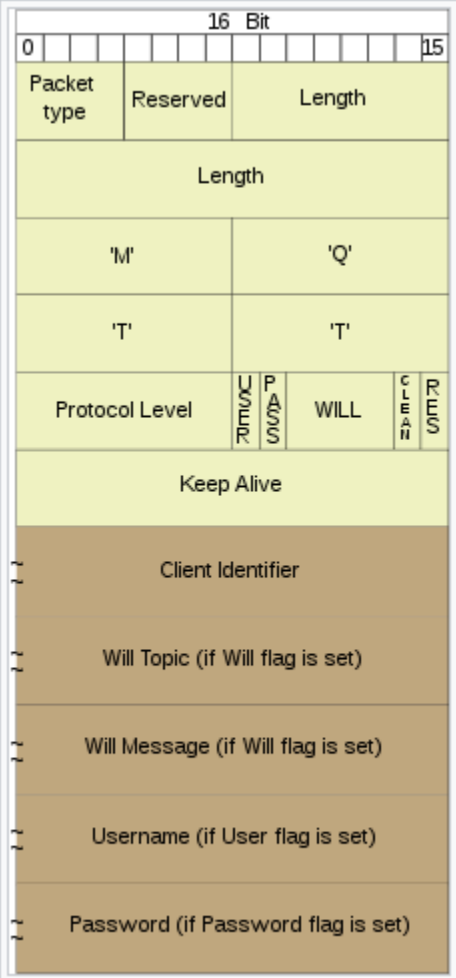


Fig.1 Missatge tipus CONNECT

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura IoT. Connectivitat/Comunicacions.

- **MQTT. Comparativa MQTT vs HTTP**:

Acció	Protocol HTTP	Protocol MQTT	Relació HTTP/MQTT
Rebre una unitat de dades (la mínima)	320 bytes	69 bytes	4,6
Enviar una unitat de dades (la mínima)	320 bytes	47 bytes	6,8
Rebre 100 unitats de dades (la mínima)	12600 bytes	2445 bytes	5,1
Enviar 100 unitats de dades (la mínima)	14100 bytes	2126 bytes	6,6

UF1. Seguretat en dispositius mòbils i IoT

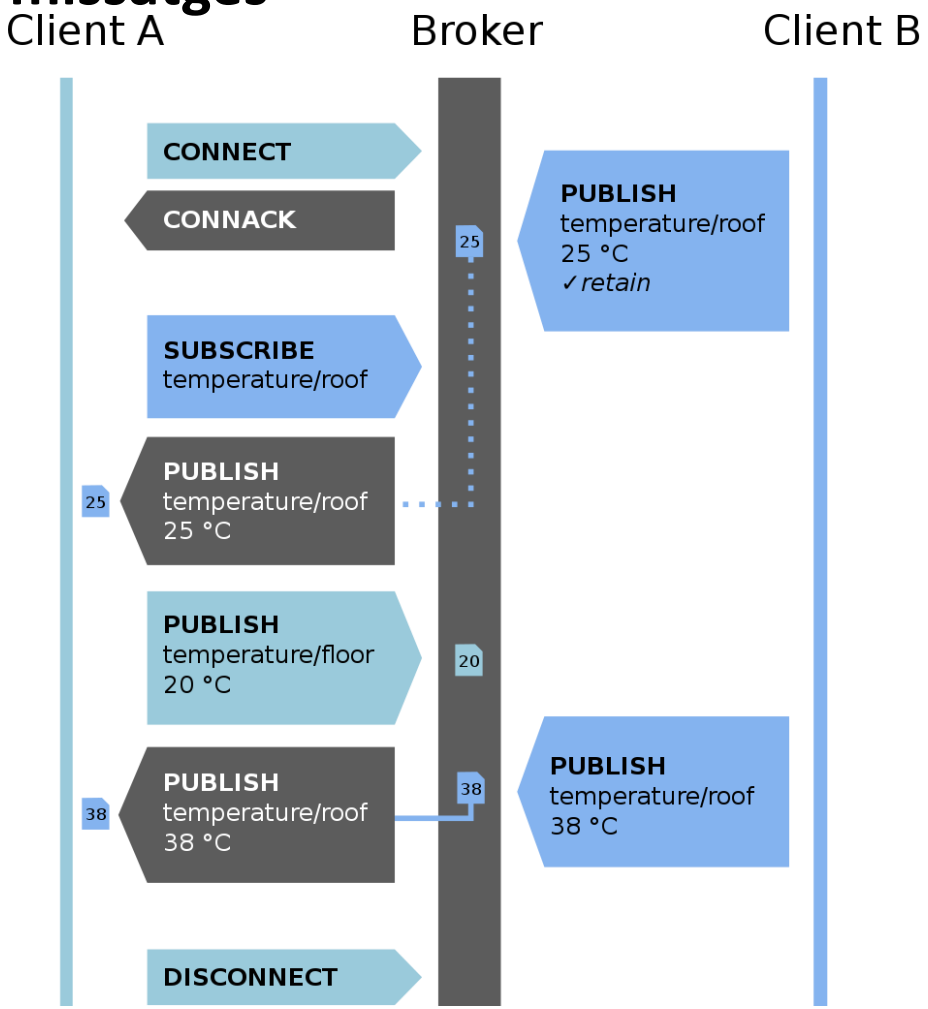
Arquitectura IoT. Connectivitat/Comunicacions.

- **MQTT.**
- Els **clients** es comuniquen amb un **servidor** anomenat **broker**.
- Un **client** pot ser un **publisher** o un **subscriber**.
- Cada client es pot connectar al broker.
- La **informació** està organitzada en una **jerarquia de temes o tòpics**.
  - Quan un **client publisher** vol distribuir informació, **envia** un **missatge** de **control** amb les **dades, al broker** connectat.
  - El **broker distribueix** la **informació** als **clients** que estan **subscrits** al **tema** o tòpic. **Si no té cap subscriptor a aquell tòpic, el broker no farà res**.
  - **Quan un client de publicació es connecta per primera vegada al broker o intermediari, pot configurar un missatge predeterminat que s'enviarà als subscriptors** si l'intermediari detecta que el client de publicació s'ha desconnectat inesperadament del broker.
  - **Els clients només interactuen amb un broker,** però un sistema pot contenir diversos servidors de Broker que intercanvien dades basant-se en els temes o tòpics dels seus subscriptors actuals.

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura IoT. Connectivitat/Comunicacions.

- **MQTT. Tipus de missatges**
- Connect.
- Disconnect.
- Publish.



UF1. Seguretat en dispositius mòbils i IoT

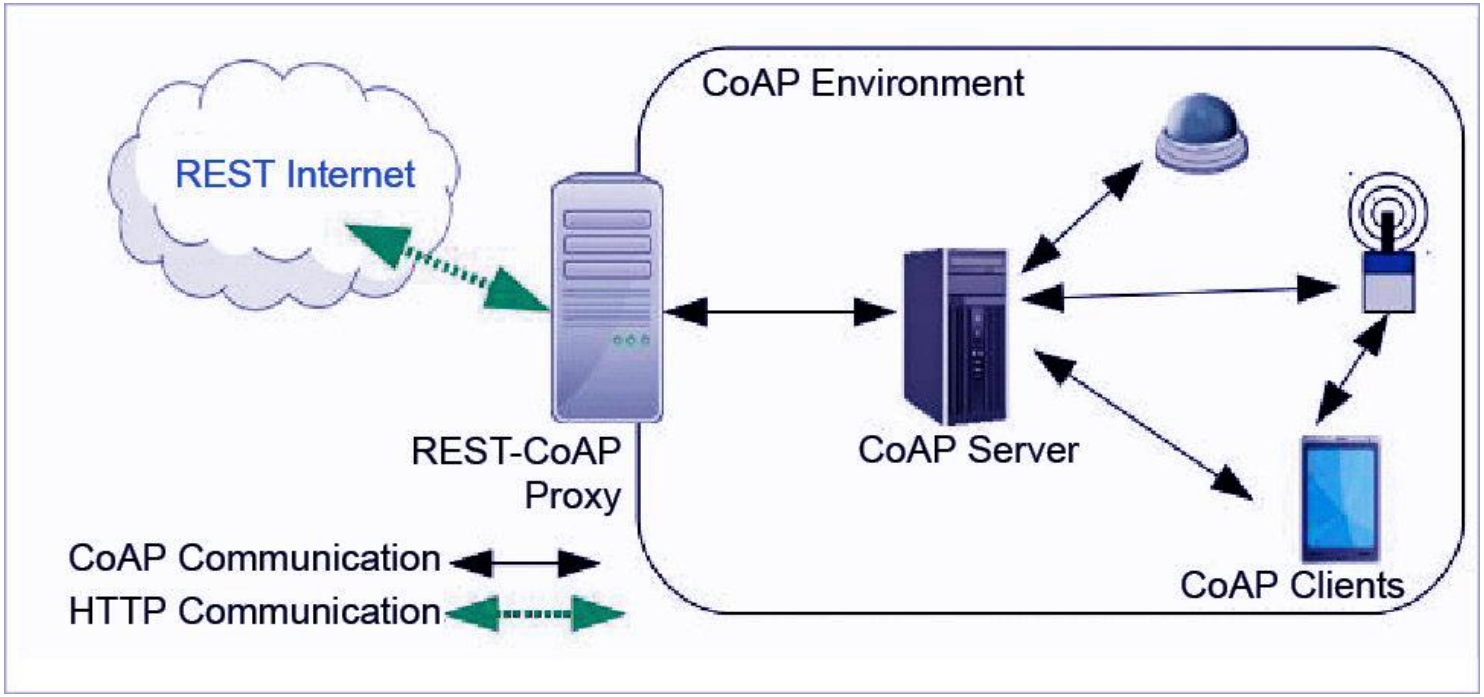
Arquitectura IoT. Connectivitat/Comunicacions.

- **CoAP**: Constrained Application Protocol (Protocol d'aplicació Restringit)
  - 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.
  - Els nodes sovint tenen **microcontroladors de 8 bits amb petites quantitats de ROM i memòria RAM**, mentre que les xarxes limitades com IPv6 a través de les xarxes d'àrea personal sense fils de baix consum (6LoWPANs) sovint tenen altes taxes d'error de paquet i un rendiment típic de 10s de kbit/s.
  - El protocol està **dissenyat per a aplicacions Machine-to-Machine (M2M**) com **l'energia intel·ligent i l'automatització en els edificis**.

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura IoT. Connectivitat/Comunicacions.

- CoAP:



UF1. Seguretat en dispositius mòbils i IoT

Arquitectura IoT. Connectivitat/Comunicacions.

- CoAP. Format del missatge.
  - El **missatge** més petit de CoAP és de **4 bytes de longitud** si s'omet el testimoni, les opcions i la càrrega útil.
  - CoAP fa ús de **dos tipus de missatge, peticions i respostes**, utilitzant un format de capçalera simple, binari.
  - La capçalera de la base pot ser seguida per opcions en un format optimitzat de longitud i valor.
  - **CoAP** és per defecte lligat a **UDP i opcionalment a DTLS**, proporcionant un **alt nivell de seguretat de les comunicacions**.
  - Qualsevol **byte després de les capçaleres** del paquet es considera el **cos del missatge**.
  - La longitud del cos del missatge s'implica amb la llargada del datagrama. Quan està **lligat a UDP, el missatge sencer ha d'encaixar dins d'un únic datagrama**.

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura IoT. Connectivitat/Comunicacions.

- CoAP. Format del missatge.

CoAP Header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
4	32	VER		Type		Token Length				CoAP Request/Response Code								Message ID															
8	64	Token (0 - 8 bytes)																															
12	96																																
16	128	Options (If Available)																															
20	160	1	1	1	1	1	1	1	1	Payload (If Available)																							

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura IoT. Plataforma i Anàlisi de Dades.

- Aquesta capa és el mitjà per **obtenir i tractar la informació** que ens donen els dispositius connectats.
- Tot l'intercanvi i recollida de dades per que sigui útil s'ha de fer un tractament. Caldran **aplicacions**, possiblement de **gestió de** grans volums de **dades** (**Big Data**), així com **plataformes al núvol** on tindrem aquesta informació.
- Termes com " exaflood " o " data deluge " han sorgit per parlar de **l'explosió de dades**. Aquestes es defineixen com l'intercanvi d'exabytes produïts per la quantitat d'objectes connectats.
- Aquesta capa engloba les **aplicacions e infraestructures** necessàries per les comunicacions **entre humans i màquines** (H2M) **i** per a **màquines i maquines** (M2M, API's).

UF1. Seguretat en dispositius mòbils i IoT

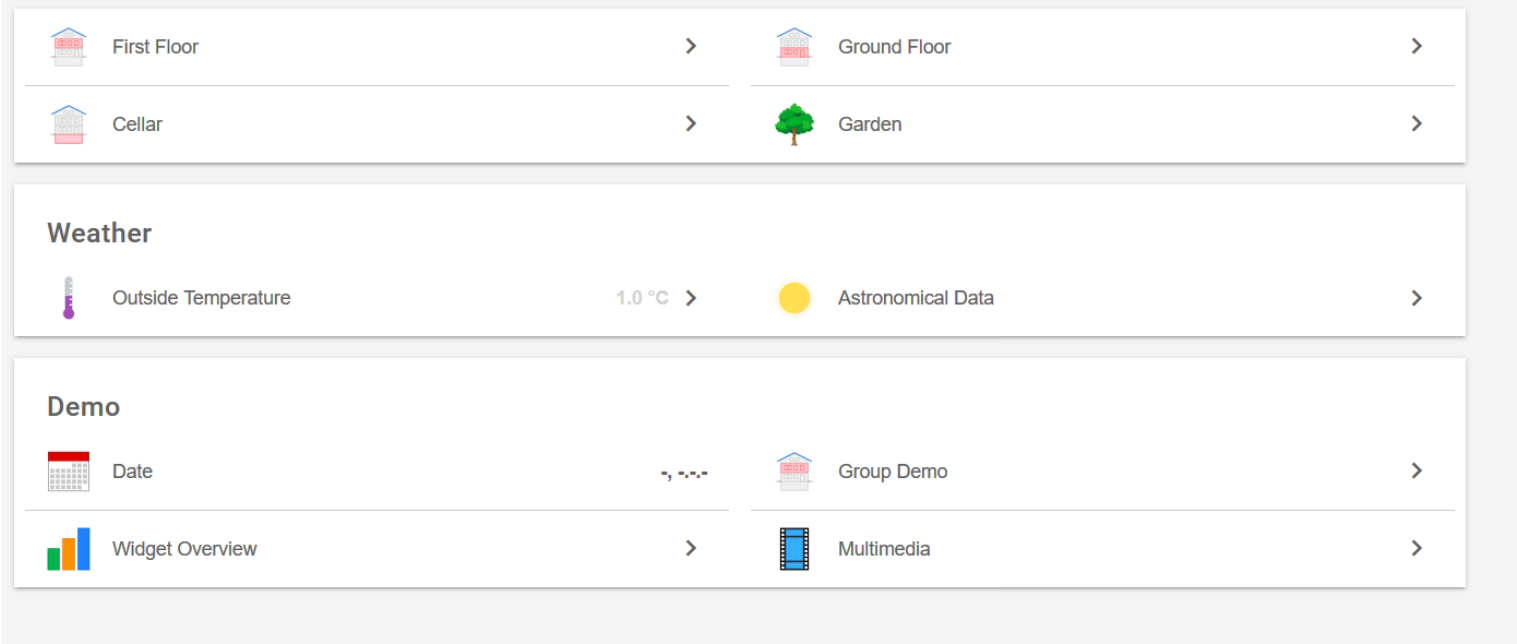
Arquitectura IoT. Plataforma i Anàlisi de Dades.

- Generalment es faran servir "**serveis del núvol**" que ajuden a **agregar i processar dades** des de dispositius dispersos i diversos, a més d'altres serveis com emmagatzematge, escalabilitat, etc.
- Es realitzarà **l'anàlisi de les dades recollides per obtenir informació útil** que pot **ajudar a prendre certes decisions**, a **mostrar resultats**, a **automatitzar processos**, **quadres de comandaments**, etc.

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura IoT. Aplicació.

- És la **capa superior**, i ens dona els **serveis finals** que generalment seran **orientats a persones** però també poden ser **orientats a màquines**.
- Apps per mòbils, aplicacions webs, panells específics, tàctils, etc.



Ref. Openhab.org

UF1. Seguretat en dispositius mòbils i IoT

Arquitectura IoT. Resum.

- Els punts claus a tenir en compte quan es defineix l'arquitectura d'un sistema IoT són:
  - El dispositiu.
  - Les comunicacions i connectivitat.
  - L'emmagatzemament i anàlisis dels dades.
  - La seguretat.
  - L'escalabilitat i alta disponibilitat.
  - La integració.
  - Les aplicacions.

UF1. Seguretat en dispositius mòbils i IoT

IoT. Video resum. Webgrafia.

- http://www.rtve.es/alacarta/videos/torres-y-reyes/masterclass-bricolaje-informatico-david-cuartielles/2252260/
- https://programarfacil.com/podcast/arduino-wifi-proyectos-iot/
- https://aprendiendoarduino.wordpress.com/2018/11/11/arquitecturas-iot/

UF1. Seguretat en dispositius mòbils i IoT

- **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

Sistemes operatius IoT.

UF1. Seguretat en dispositius mòbils i IoT

Sistemes operatius IoT.

- 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**.
- És deduïble que hi hauran **molts sistemes operatius** que s'utilitzaren en els múltiples dispositius IoT que hi ha al mercat.
- La **selecció** d'un o un altre **dependrà** dels **requisits** del **dispositiu**, de les **dades a recopilar**, de **l'aplicació**, de la **seguretat**, ...

UF1. Seguretat en dispositius mòbils i IoT

Sistemes operatius IoT. Característiques.

Característiques, a tenir en compte, per la selecció d'un S.O. serien:

- **Empremta** (footprint): 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.

UF1. Seguretat en dispositius mòbils i IoT

Sistemes operatius IoT. Característiques.

- **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. Generalment per tenir aquesta característica **hi haurà normatives o Estàndards** que haurà de complir (exemple IEC 61508 per sistemes de control industrials o ISO 62304 per dispositius mèdics)
- **Eficiència energètica:** Estalviar bateria pot suposar un **avantatge econòmic** ja que de vegades és molt costós fer els canvis.

UF1. Seguretat en dispositius mòbils i IoT

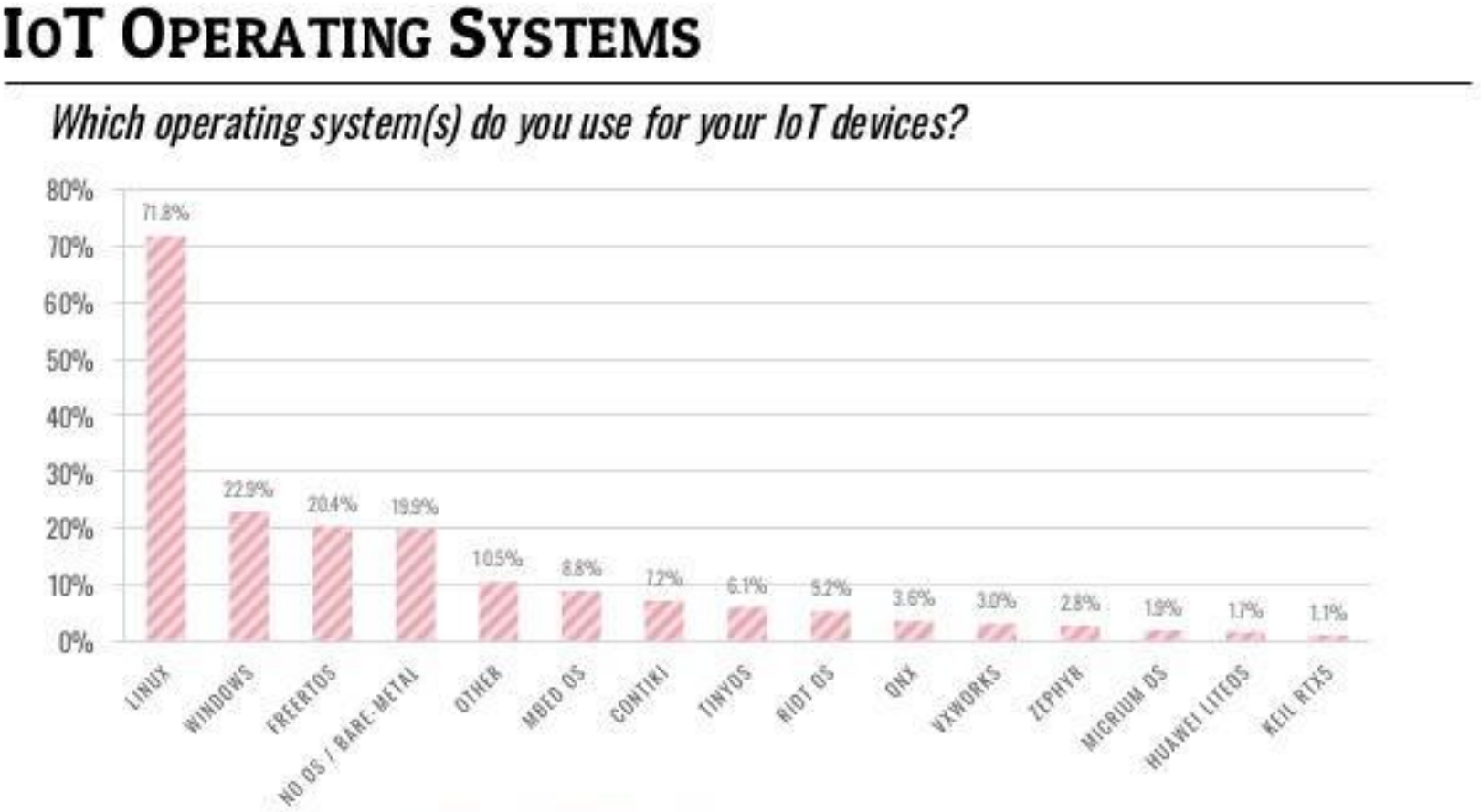
Sistemes operatius IoT. Tipus.

- **Open Source:**
  - TinyOS, Contiki, Raspbian, Mantis OS, Nano RK, LiteOS, FreeRTOS, Apache Mynewt, Zephyr OS, Ubuntu Core 16 (Snappy), ARM mbed, RIOT, ...
  - El TinyOS i Contili són els més vells, RIOT (Real time OS) és dels més moderns.
- **Comercials:**
  - Android Things, Express Logic ThreadX, Windows 10 IoT, Micro Digital SMX RTOS, WindRiver VxWorks, MicroEJ OS, TI RTOS, Mentor Graphics Nucleus RTOS, Micrium µC/OS, Green Hills Integrity…

UF1. Seguretat en dispositius mòbils i IoT

Sistemes operatius IoT. Tipus.

- **Sistemes operatius més usats.**



UF1. Seguretat en dispositius mòbils i IoT

- **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

Vulnerabilitats i amenaces.

- La tríada CIA, guia els requeriments fonamentals de qualsevol operació de ciberseguretat.
- Confidencialitat, integritat i disponibilitat.
- **Confidencialitat**. Control d'accés a la informació. La informació transmesa i guardada s'encripta per privacitat.
- **Integritat**. Addició, modificació o destrucció de les dades i informació. Es crea un hash de les dades a transmetre per comprovar posteriorment la integritat de les dades.
- **Disponibilitat**. S'assegura que es transmetrà la informació en el moment que es demani.

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces.

- 10 requeriments de seguretat IoT crítics:
  - **Referents al sistema**
  1. **Assegurar la privacitat de les dades.** Confidencialitat.
  2. **Minimitzar els atacs de superfície**. Tots els llocs o punts d'entrada que poden ser explotats per un hacker.
  3. **Registrar els events crítics**. Registrar els events en el sistema, incloent mesures d'operacions de xarxa normals i alertes per activitats en la xarxa inusuals.
  4. **Suport a operacions de seguretat mínimes**. El personal de seguretat requereix formació i gestió, per tal de controlar els sistemes per detectar incidents, tractar les vulnerabilitats descobertes i investigar incompliments de seguretat.

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces.

- 10 requeriments de seguretat IoT crítics:
  - **Referents a la capa dispositiu**

5. **Seguretat d'arrencada i integritat del sistema.** Els dispositius IoT haurien de tenir mesures per garantir que els sistemes operatius i el programari no siguin manipulats per hackers o programari maliciós. Es poden utilitzar components de maquinari, per assegurar-vos que els dispositius funcionen de la manera prevista, que la identitat del dispositiu és vàlida i que les dades relacionades amb la seguretat, com ara les claus de xifratge, estan protegides contra manipulacions o pèrdues.
6. **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.
7. **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.

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces.

- 10 requeriments de seguretat IoT crítics:
  - **Referents a la capa comunicació**

La comunicació IoT és bidireccional. Els sensors transmeten dades a les aplicacions a través de passarel·les i els actuadors controlen les aplicacions a través de la xarxa. Les dades transmeses es poden robar, alterar o destruir. Les comunicacions de control es poden alterar o falsificar completament. Els resultats poden ser desastrosos.

8. **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.

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces.

- 10 requeriments de seguretat IoT crítics:
  - **Referents a la capa d'aplicació**

Un administrador configura els dispositius IoT mitjançant una interfície de línia d'ordres (CLI) o una interfície gràfica d'usuari (GUI).

9. **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.
10. **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. A més, els dispositius IoT utilitzen interfícies de programa d'aplicacions (API) per interactuar directament amb aplicacions web. Les credencials que s'utilitzen entre dispositius IoT i aplicacions web s'han de protegir contra atacs.

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces.

Algunes vulnerabilitats segons Microsoft: https://docs.microsoft.com/es-es/azure/iot-fundamentals/iot-security-architecture

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

ANY 2014

HELPING SECURE THE INTERNET OF THINGS WITH THE

OWASP

INTERNET OF THINGS

VULNERABILITY CATEGORIES

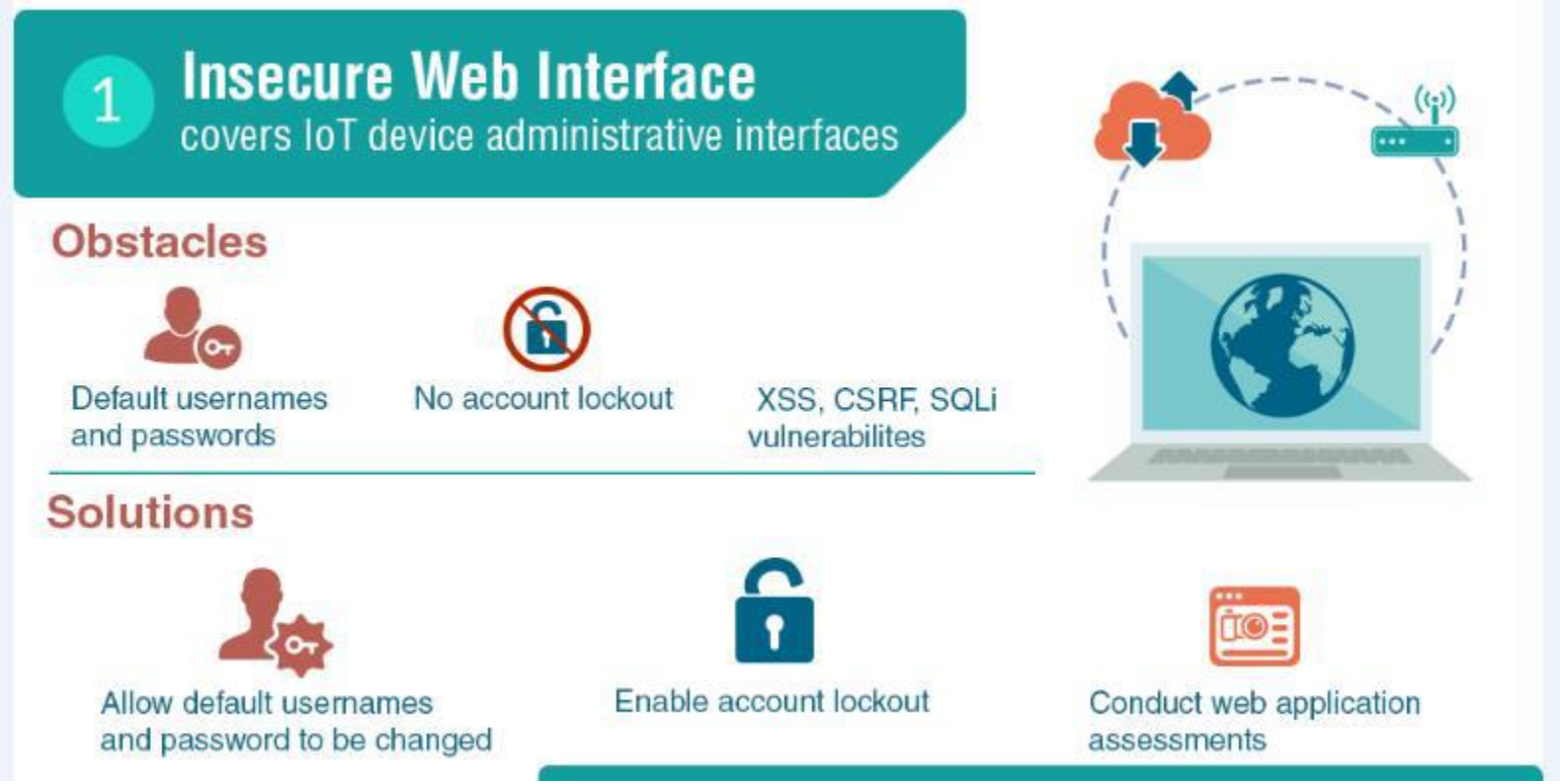
TOP 10

https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

1. Inseguretat en les aplicacions webs de gestió d'IOT.



Ref. https://www.owasp.org/images/8/8e/Infographic-v1.jpg

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

1. Inseguretat en les aplicacions webs de gestió d'IOT.

Obstacles

- Noms d'usuari i passwords per defecte.
- No bloqueig del compte.
- Vulnerabilitats XSS, CSRF, SQLi

Solucions

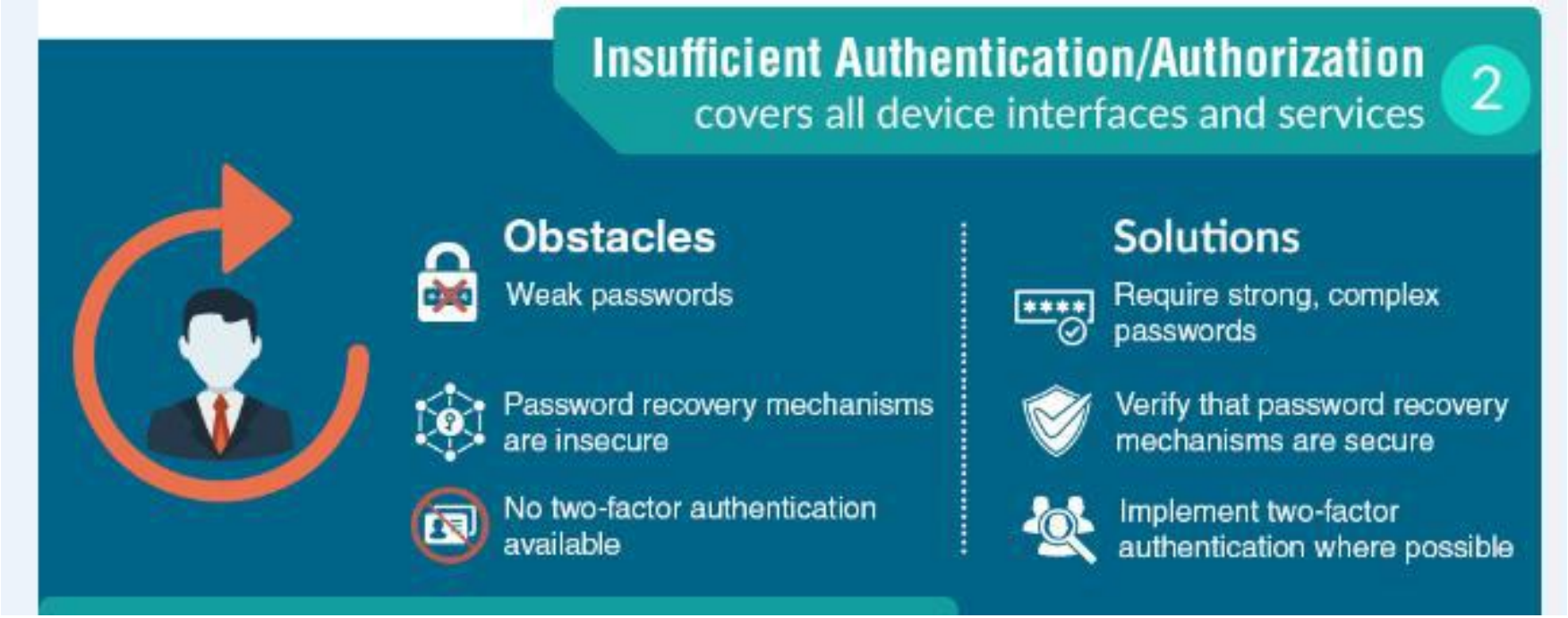
- Permetre canviar els noms d'usuari i passwords per defecte.
- Habilitar el bloqueig del compte.
- Realitzar avaluacions de les aplicacions web.

- https://wiki.owasp.org/index.php/Top_10_2014-I1_Insecure_Web_Interface

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

2. Mecanismes febles d'autenticació i autorització.



Ref. https://www.owasp.org/images/8/8e/Infographic-v1.jpg

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

2. Mecanismes febles d'autenticació i autorització.

Obstacles

- Passwords febles.
- Els mecanismes de recuperació de passwords són insegurs.
- No està habilitat el doble factor d'autenticació.

Solucions

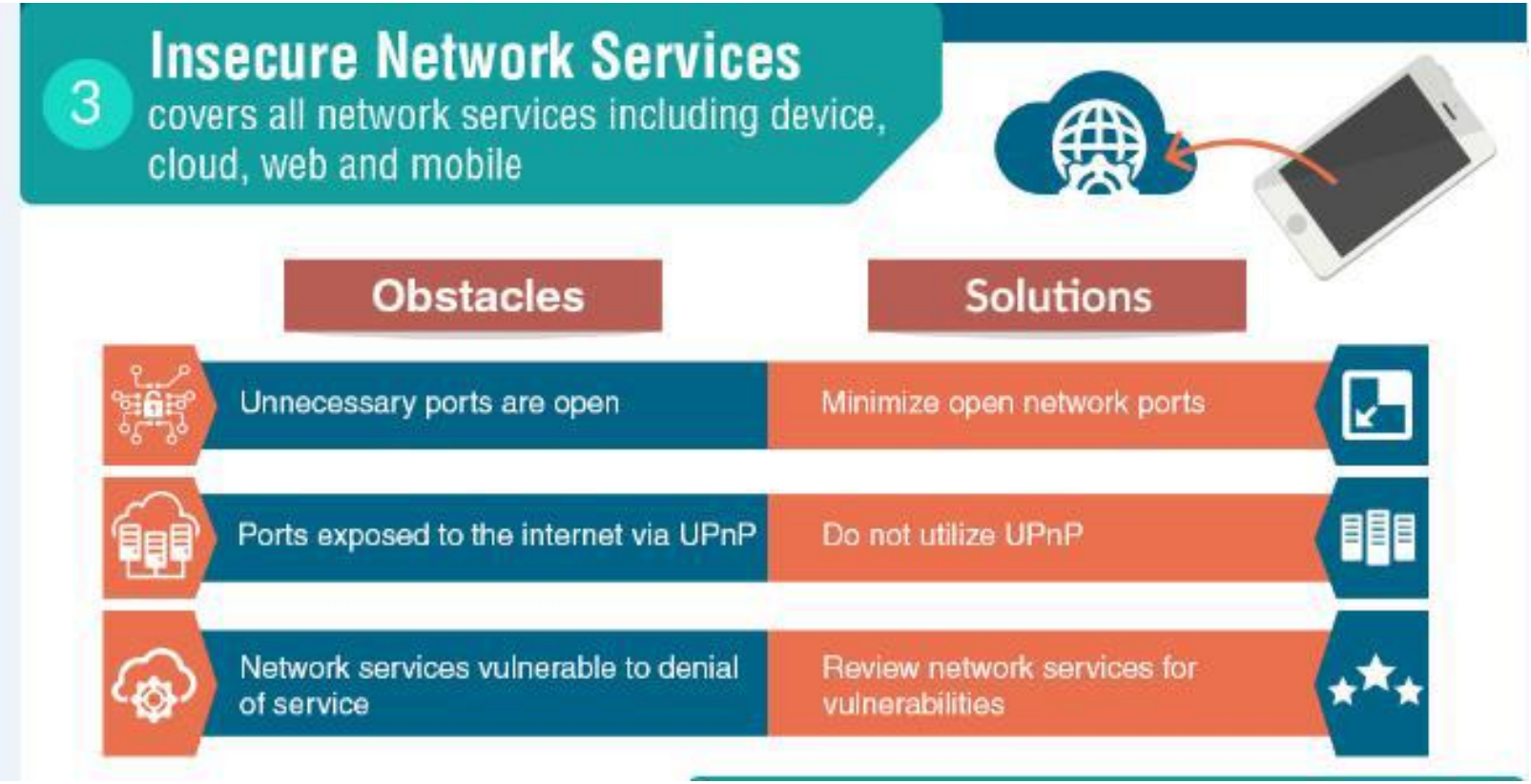
- Demanar passwords forts i complexos.
- Verificar que els mecanismes de recuperació de passwords siguin segurs.
- Implementar el doble factor d'autenticació sempre que sigui possible.

- https://wiki.owasp.org/index.php/Top_10_2014-I2_Insufficient_Authentication/Authorization

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

3. Inseguretat en els serveis de xarxa.



Ref. https://www.owasp.org/images/8/8e/Infographic-v1.jpg

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

3. Inseguretat en els serveis de xarxa.

Obstacles

- Ports innecessaris estan oberts.
- Ports exposats a internet via UPnP.
- Serveis de xarxa vulnerables a denegació de servei.

Solucions

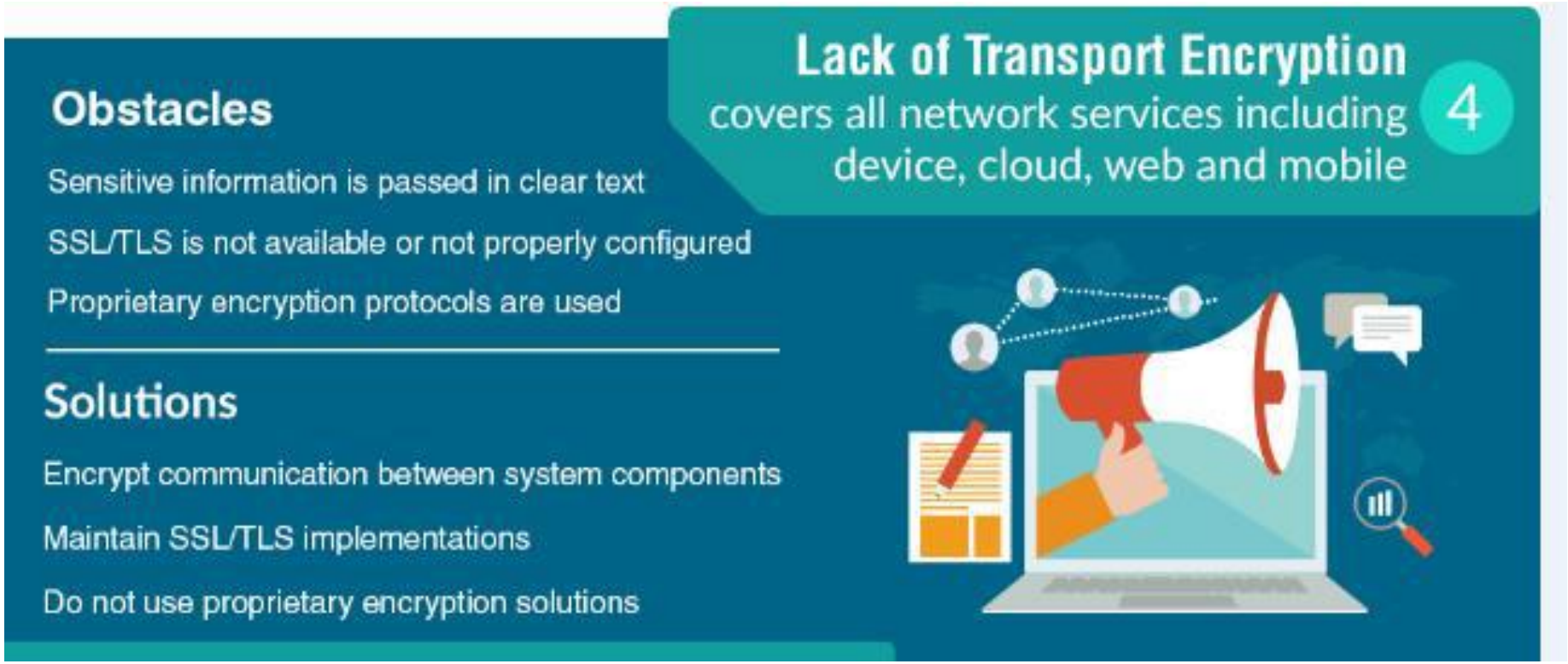
- Minimitzar els ports oberts de la xarxa.
- No utilitzar UPnP.
- Revisar els serveis de xarxa en busca de vulnerabilitats.

- https://wiki.owasp.org/index.php/Top_10_2014-I3_Insecure_Network_Services

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

4. Falta de xifrat a totes els comunicacions implicades.



Ref. https://www.owasp.org/images/8/8e/Infographic-v1.jpg

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

4. 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.
- S'utilitzen protocols d'encriptació propietaris.

Solucions

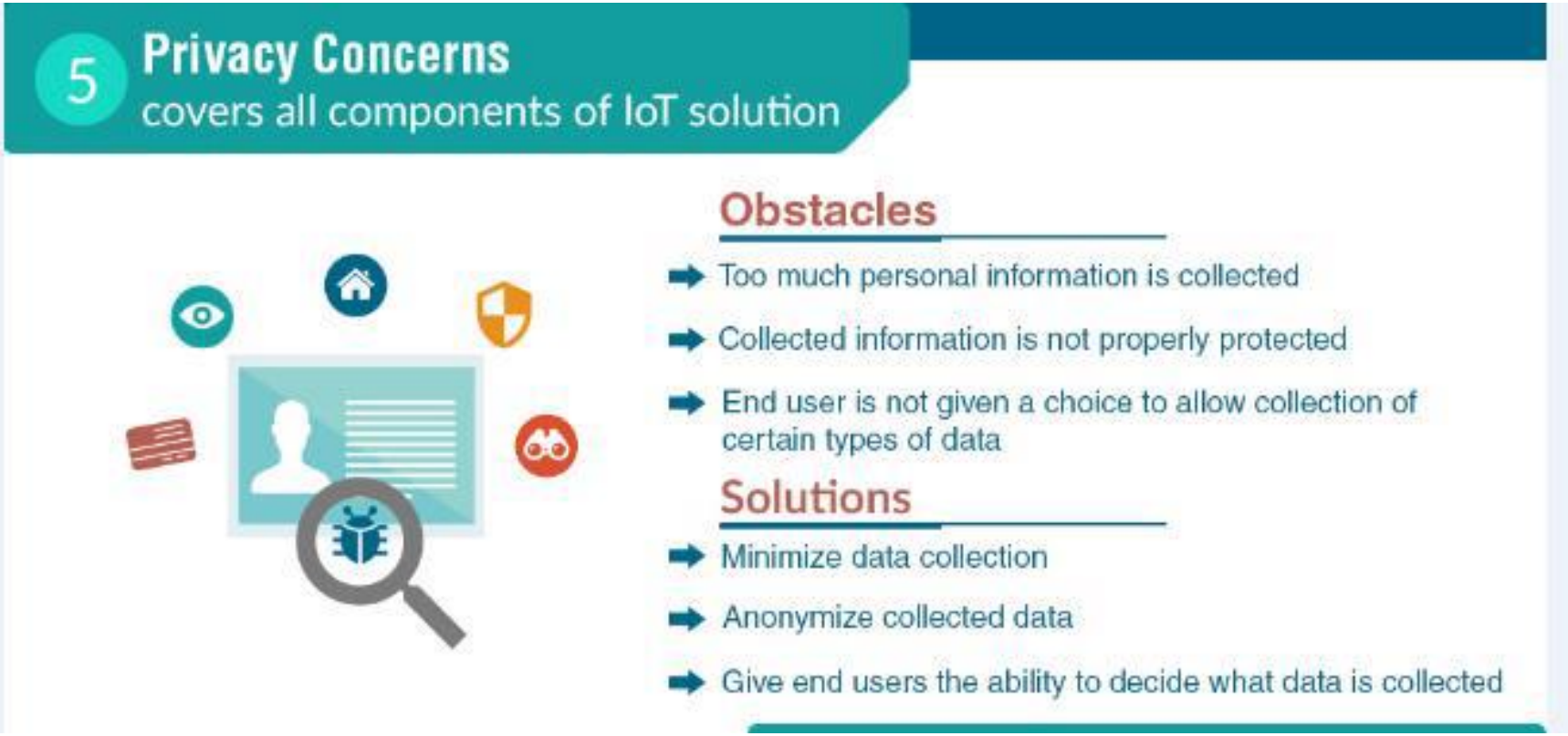
- Encriptar la comunicació entre els components del sistema.
- Mantenir les implementacions SSL/TLS.
- No utilitzar solucions d'encriptació propietàries.

- https://wiki.owasp.org/index.php/Top_10_2014-I4_Lack_of_Transport_Encryption

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

5. Privacitat de les dades.



Ref. https://www.owasp.org/images/8/8e/Infographic-v1.jpg

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

5. Privacitat de les dades.

Obstacles

- Es recopila molta informació personal.
- La informació recollida no està correctament protegida.
- A l'usuari final no se li dóna l'opció de permetre la recol·lecció de determinats tipus de dades.

Solucions

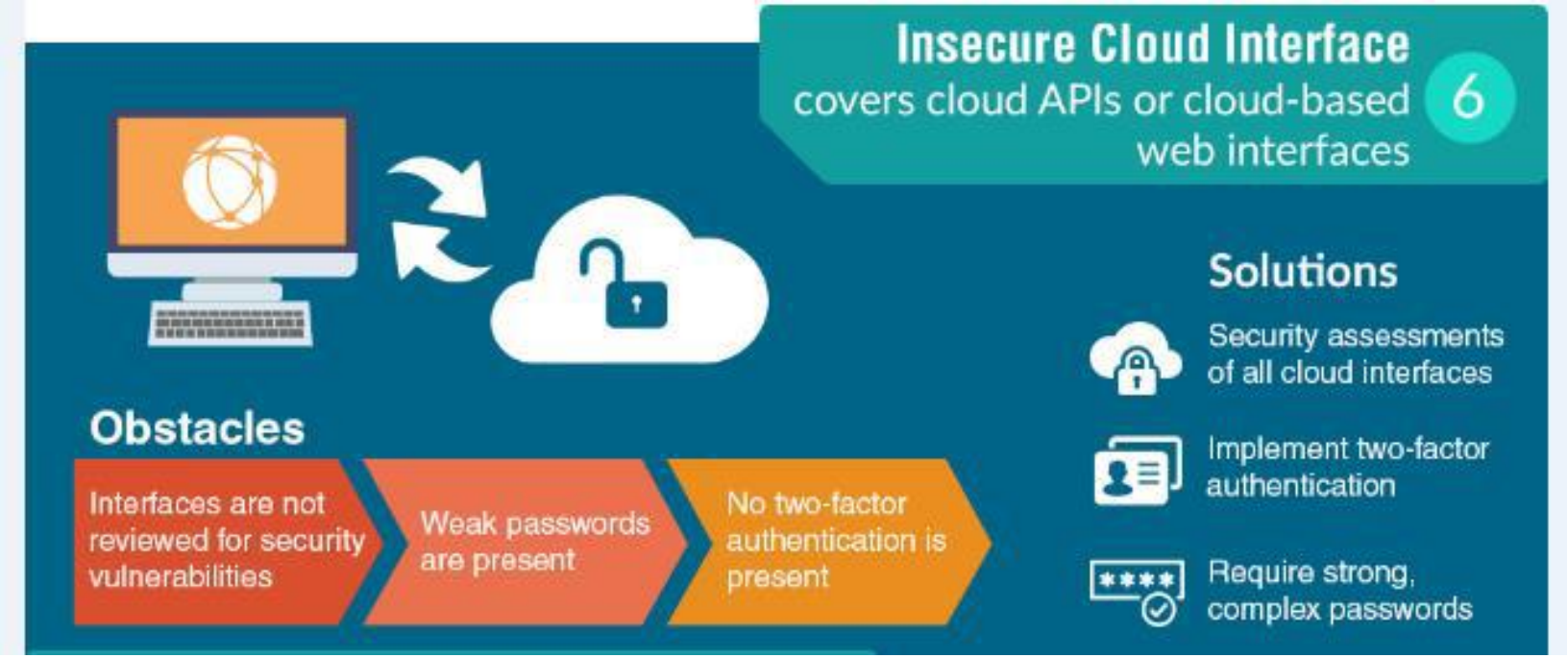
- Reduir la recol·lecció de dades.
- Anonimitzar la recol·lecció de dades.
- Donar als usuaris finals la capacitat de decidir quines dades es recullen

- https://wiki.owasp.org/index.php/Top_10_2014-I5_Privacy_Concerns

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

6. Inseguretat al núvol.



Ref. https://www.owasp.org/images/8/8e/Infographic-v1.jpg

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

6. Inseguretat al núvol.

Obstacles

- Les interfícies no es revisen per vulnerabilitats de seguretat
- Hi ha presents passwords febles.
- No hi ha doble factor d'autenticació.

Solucions

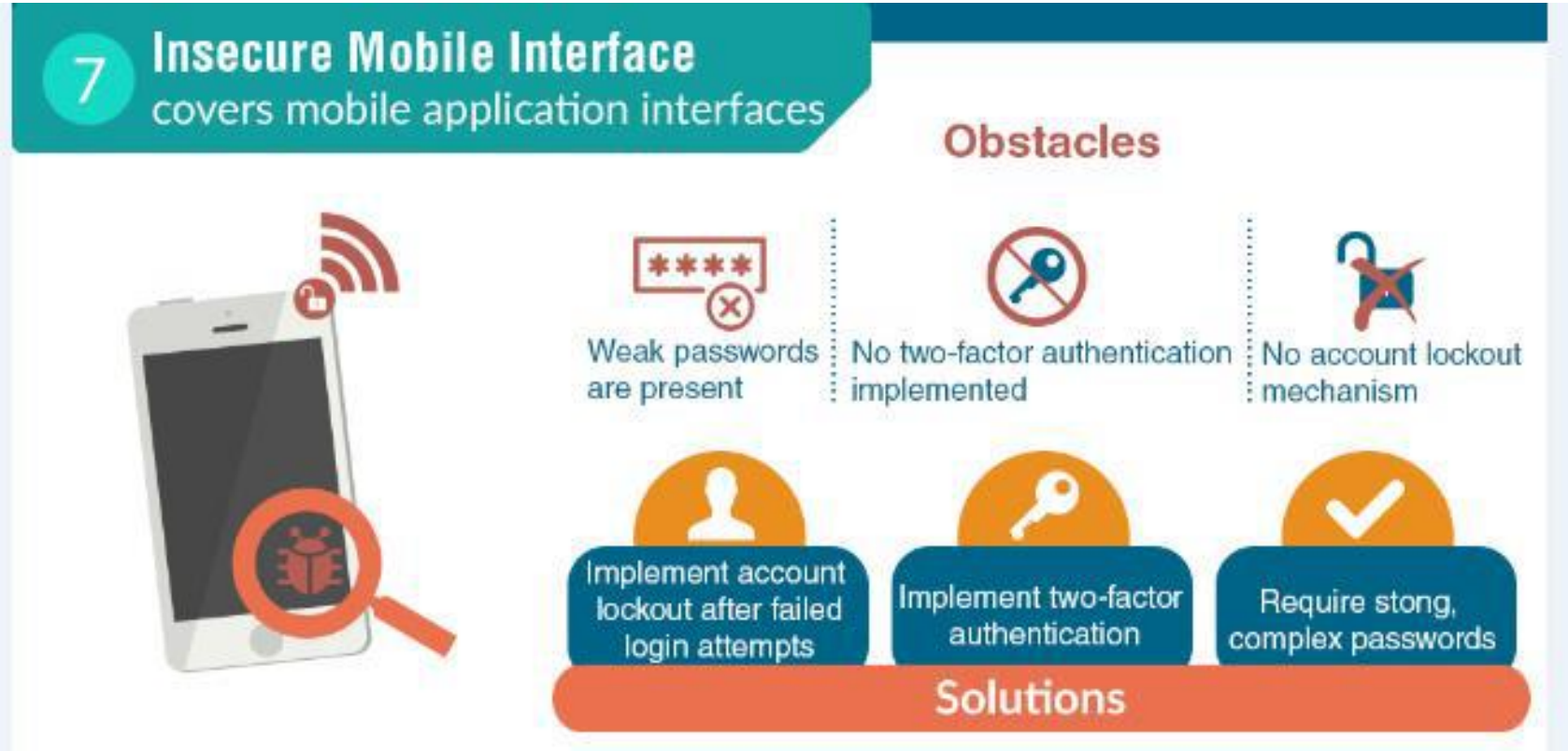
- Avaluacions de seguretat de totes les interfícies del núvol.
- Implementar doble factor d'autenticació.
- Requerir passwords forts i complexos.

- https://wiki.owasp.org/index.php/Top_10_2014-I6_Insecure_Cloud_Interface

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

7. Inseguretat en les aplicacions mòbils.



Ref. https://www.owasp.org/images/8/8e/Infographic-v1.jpg

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

7. Inseguretat en les aplicacions mòbils.

Obstacles

- Hi ha passwords febles.
- No hi ha implementat factor de doble autenticació.
- No hi ha cap mecanisme de bloqueig del compte.

Solucions

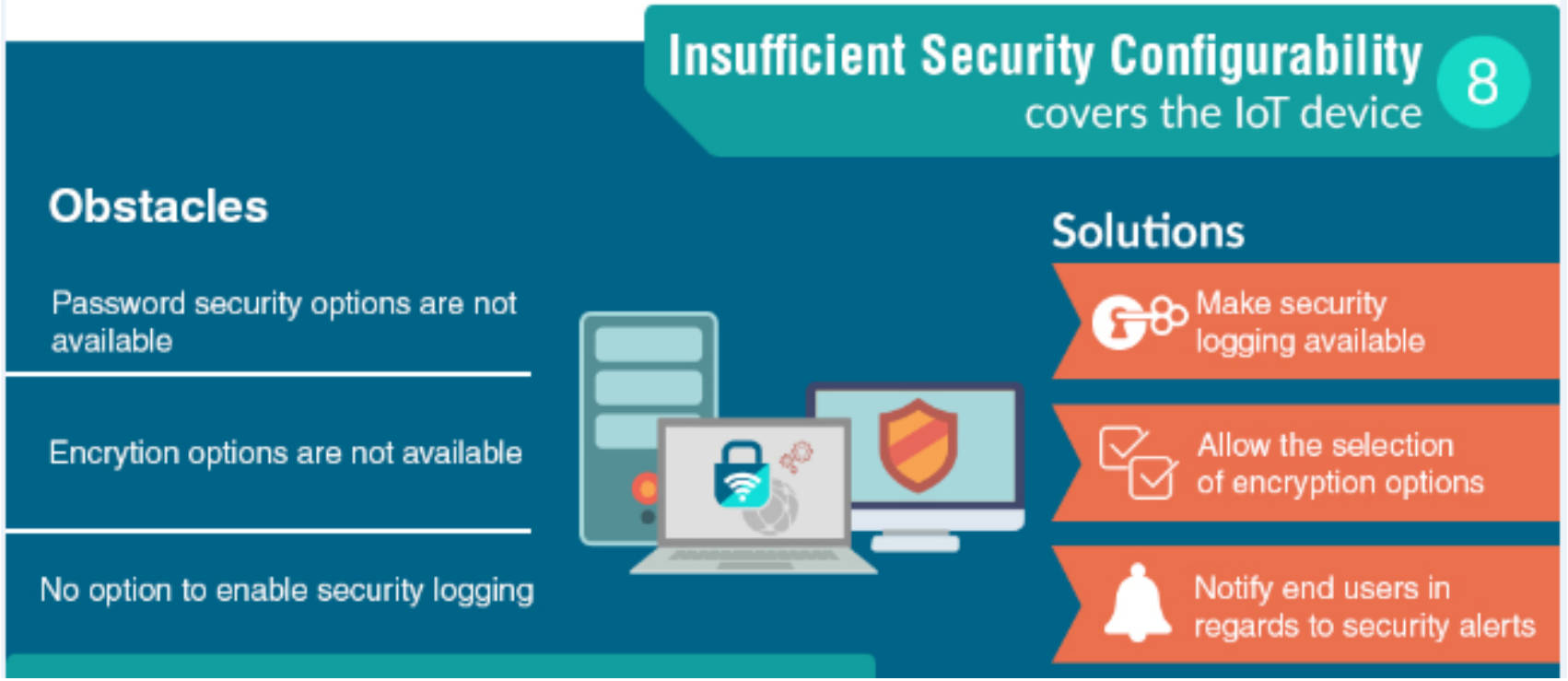
- Implementar el bloqueig del compte després d'intents de connexió erronis.
- Implementar doble factor d'autenticació.
- Requerir passwords forts i complexos.

- https://wiki.owasp.org/index.php/Top_10_2014-I7_Insecure_Mobile_Interface

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

8. Inseguretat en els dispositius IoT.



Ref. https://www.owasp.org/images/8/8e/Infographic-v1.jpg

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

8. Inseguretat en els dispositius IoT.

Obstacles

- Les opcions de seguretat de contrasenya no estan disponibles.
- Opcions d'encriptació no disponibles.
- No hi ha opció per habilitar el registre de seguretat

Solucions

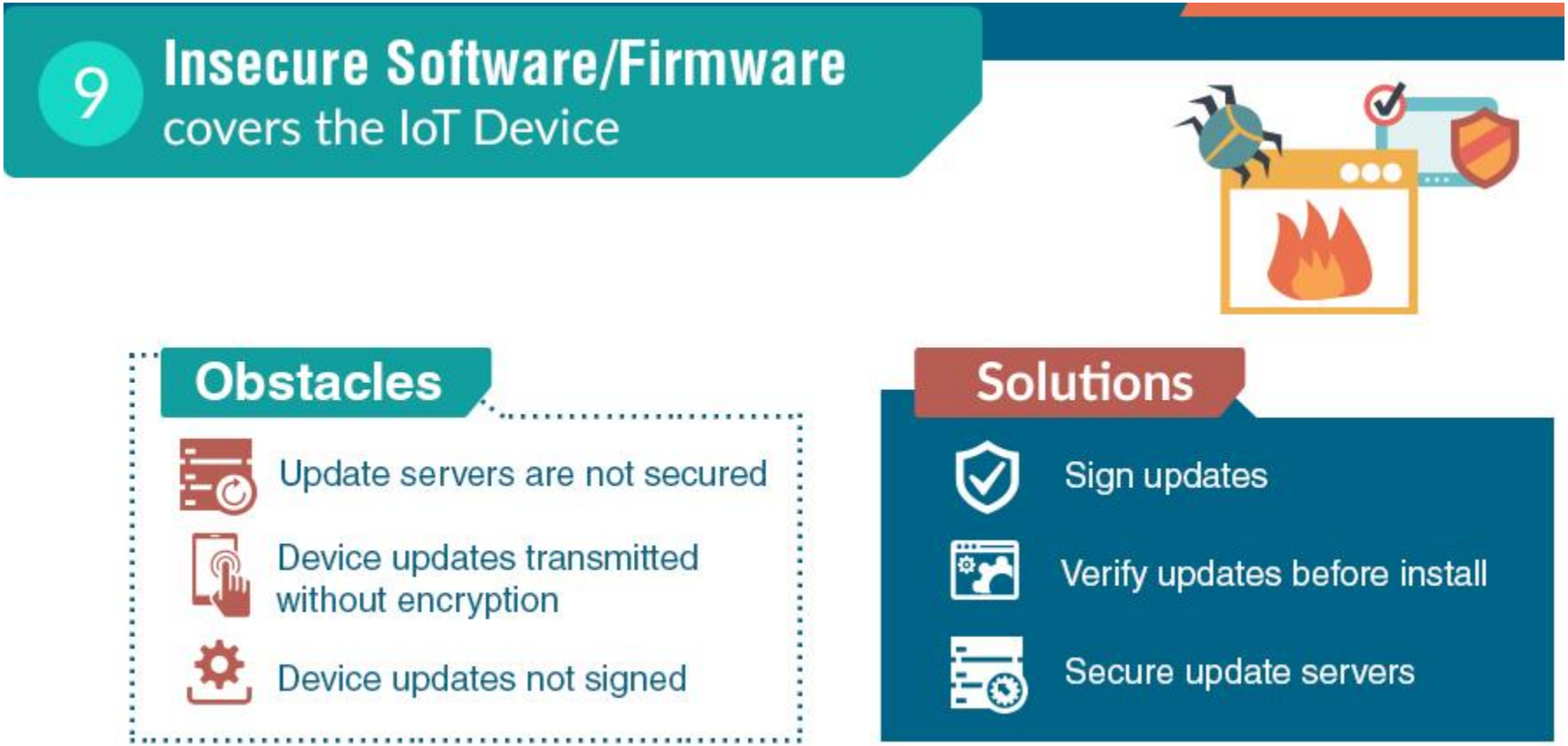
- Fer que el registre de seguretat estigui disponible
- Permetre la selecció d'opcions de xifratge.
- Notificar als usuaris finals pel que fa a alertes de seguretat.

- https://wiki.owasp.org/index.php/Top_10_2014-I8_Insufficient_Security_Configurability

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

9. Inseguretat al software dels dispositius IoT.



Ref. https://www.owasp.org/images/8/8e/Infographic-v1.jpg

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

9. Inseguretat al software dels dispositius IoT.

Obstacles

- Els servidors d'actualitzacions no són segurs.
- Les actualitzacions del dispositiu es transmeten sense encriptació.
- Les actualitzacions del dispositiu no estan signades.

Solucions

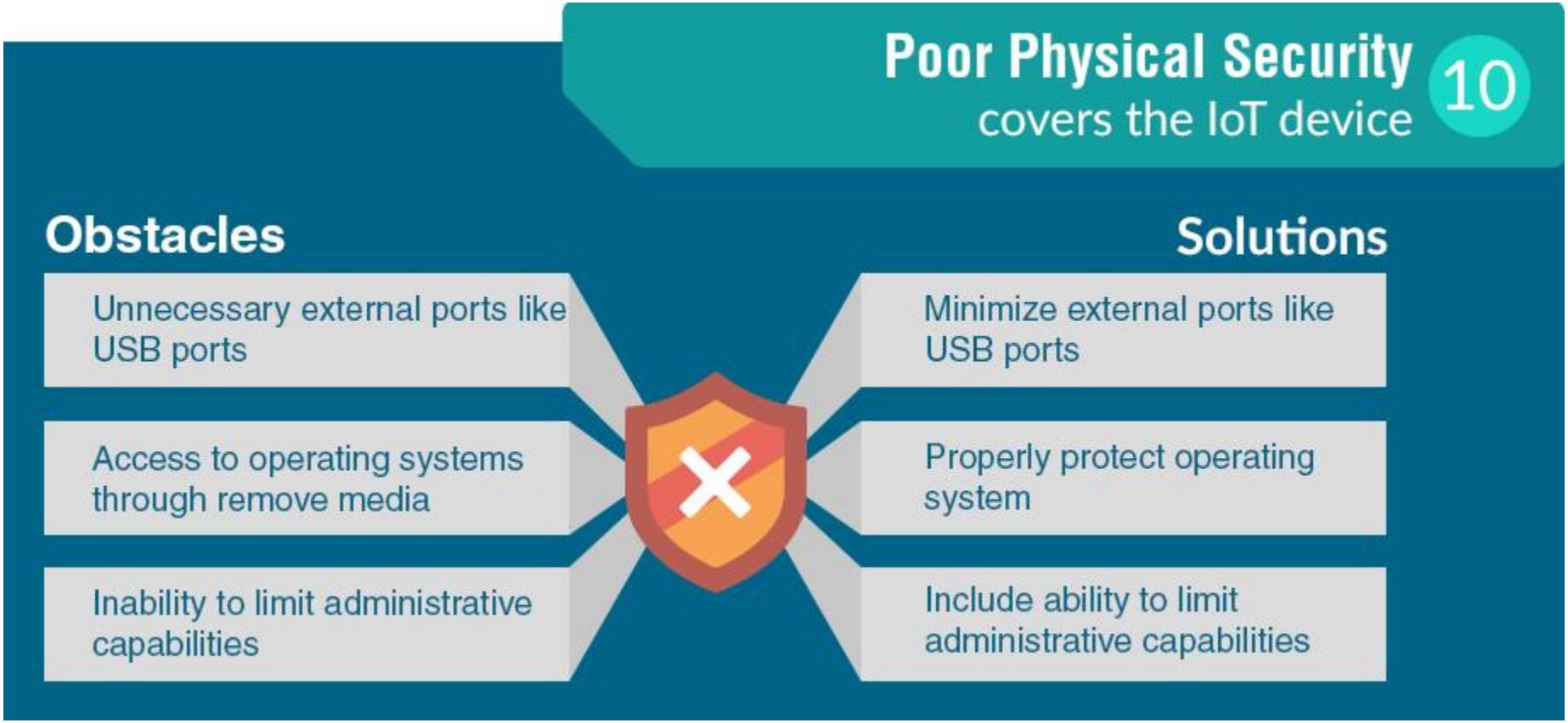
- Signar les actualitzacions.
- Verificar les actualitzacions abans d'instal·lar-les.
- Fer segurs els servidors d'actualitzacions.

- https://wiki.owasp.org/index.php/Top_10_2014-I9_Insecure_Software/Firmware

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

10. Inseguretat física.



Ref. https://www.owasp.org/images/8/8e/Infographic-v1.jpg

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

10. Inseguretat física.

Obstacles

- Ports externs innecessaris com els ports USB.
- Accés als sistemes operatius a través de dispositius extraïbles.
- Incapacitat per limitar les capacitats administratives.

Solucions

- Minimitzar els ports externs com els USB.
- Protegir adequadament el sistema operatiu.
- Incloure la capacitat per limitar les capacitats administratives.

- https://wiki.owasp.org/index.php/Top_10_2014-I10_Poor_Physical_Security

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

- Última llista Top 10 2018. https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10
- https://www.incibe-cert.es/blog/importancia-seguridad-iot-principales-amenazas

- IoT Top 10 2018 Mapping Project. https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=OWASP_IoT_Top_10_2018_Mapping_Project

- Vulnerabilitats IoT. https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#IoT_Vulnerabilities

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. (Segons OWASP)

OWASP IoT Top 10 2014	OWASP IoT Top 10 2018 Mapping
I1 Insecure Web Interface	I3 Insecure Ecosystem Interfaces
I2 Insufficient Authentication/Authorization	I1 Weak, Guessable, or Hardcoded Passwords I3 Insecure Ecosystem Interfaces I9 Insecure Default Settings
I3 Insecure Network Services	I2 Insecure Network Services
I4 Lack of Transport Encryption/Integrity Verification	I7 Insecure Data Transfer and Storage
I5 Privacy Concerns	I6 Insufficient Privacy Protection
I6 Insecure Cloud Interface	I3 Insecure Ecosystem Interfaces
I7 Insecure Mobile Interface	I3 Insecure Ecosystem Interfaces
I8 Insufficient Security Configurability	I9 Insecure Default Settings
I9 Insecure Software/Firmware	I4 Lack of Secure Update Mechanism I5 Use of Insecure or Outdated Components
I10 Poor Physical Security	I10 Lack of Physical Hardening

UF1. Seguretat en dispositius mòbils i IoT

Vulnerabilitats i amenaces. Exemples

- **2013 : Foscam IP baby cam hijacked actualment aquest proveïdor continua amb vulnerabilitats)**
  - https://nvd.nist.gov/vuln/detail/CVE-2013-2560
  - https://www.computerworld.com/article/2878741/hacker-hijacks-wireless-foscam-baby-monitor-talks-and-freaks-out-nanny.html
- **2015: BMW'sConnectedDrive vulnerable:**
  - https://www.cs.bu.edu/~goldbe/teaching/HW55815/presos/bmw.pdf
- **2016: DDoSon building blocks' central heating system(Finlandia):**
  - https://www.ibtimes.co.uk/hackers-leave-finnish-residents-cold-after-ddos-attack-knocks-out-heating-systems-1590639
- **2018:Critical vulnerabilityin Sony BraviaSmart TV:**
  - https://www.securitynewspaper.com/2018/10/09/critical-vulnerability-in-sony-bravia-smart-tv/
- **2018:Satori IoTBotnet Variant :**
  - https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/satori-iot-botnet/

UF1. Seguretat en dispositius mòbils i IoT

- **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

Bones pràctiques per la securització. Eines.

- Anàlisis de xarxa:
  - Caparser: Un analitzador de PCAP, analitza tràfic de xarxa i mostra quines aplicacions envien dades confidencials:
    - https://github.com/danielmiessler/caparser
- Web vulnerabilitys scanner:
  - Burp suite:
    - https://portswigger.net/burp
  - OWASP Zed Attack Proxy (ZAP) :
    - https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

UF1. Seguretat en dispositius mòbils i IoT

Lectures recomanades.

- Articles sobre aplicacions i recursos IoT:
  - https://data-flair.training/blogs/iot-applications/
  - https://iot-analytics.com/10-internet-of-things-applications/
  - https://mobilephonesecurity.org/2016/11/iot-security-resources.html/
- Projecte OWASP sobre IoT:
  - https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
- ENISA:
  - https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport

UF1. Seguretat en dispositius mòbils i IoT

Lectures recomanades.

- Eines anàlisi IoT:
  - https://gurudelainformatica.es/analisis-y-visualizacion-grafica-de-seguridad-de-redes-de-dispositivos-iot
  - https://gurudelainformatica.es/herramienta-para-pruebas-de-seguridad-y-explotacion-de-productos-iot-e-infraestructura-iot
  - https://expliot.readthedocs.io/en/latest/#
  - https://gurudelainformatica.es/herramienta-para-iniciarse-en-test-de-penetracion-de-dispositivos-iot
  - https://gurudelainformatica.es/herramienta-de-analisis-y-comparacion-de-vulnerabilidades-de-firmware-de-dispositivos-iot
  - https://gurudelainformatica.es/sandbox-multiplataforma-para-analisis-automatizado-de-malware-para-iot
  - https://gurudelainformatica.es/herramientas-para-probar-y-auditar-redes-zigbee-e-ieee-802-15-4
  - https://gurudelainformatica.es/seguridad-en-dispositivos-iot
  - https://gurudelainformatica.es/firmware-para-aprender-las-principales-vulnerabilidades-iot-documentadas-por-owasp
  - https://gurudelainformatica.es/test-de-penetracion-de-dispositivos-iot
  - https://gurudelainformatica.es/herramienta-de-analisis-de-codigo-malicioso-en-imagenes-de-firmware

UF1. Seguretat en dispositius mòbils i IoT

Lectures recomanades.

- Prova hackeig IoT:
  - https://noticiasseguridad.com/tutoriales/como-hackear-y-auditar-dispositivos-iot-internet-de-las-cosas/