Anàlisis de les actualitzacions del firmware dels dispositius *IoT*

Pedro Ferré Galván

MÀSTER INTERUNIVERSITARI EN SEGURETAT DE LES TIC (MISTIC)
Seguretat en la Internet de les coses

Helena Rifà Pous

Data Lliurament: 2 de juny de 2020

FITXA DEL TREBALL FINAL

Títol del treball:	Anàlisis de les actualitzacions del firmware dels dispositius IoT
Nom de l'autor:	Pedro Ferré Galván
Nom del consultor/a:	Helena Rifà Pous
Nom del PRA:	Helena Rifà Pous
Data de lliurament:	06/2020
Titulació o programa:	MÀSTER INTERUNIVERSITARI EN SEGURETAT DE LES TIC (MISTIC)
Àrea del Treball Final:	Seguretat en la Internet de les coses
Idioma del treball:	Català
Paraules clau	*IoT*, firmware, vulnerabilitat, seguretat, estadística, actualitzacions.

Resum del Treball

El treball es fixa en els dispositius *IoT*, que formen part d'aquesta munió de camps tecnològics incipients. Aquests dispositius acostumen a estar proveït de pocs recursos, poca memòria, processador poc potent, poca amplada de banda, que els fa molt més vulnerables que els dispositius tradicionals d'Internet que hem fet servir fins a l'actualitat doncs aquesta economia de recursos no els permet implementar grans mesures de seguretat com per exemple la criptografia. Intento demostrar la hipòtesi que una de les causes de la seva vulnerabilitat és el poc actualitzat que té el firmware que fan servir.

Abstract

The work focuses on *IoT* devices, which are part of this multitude of emerging technology fields. These devices are usually low on resources, low memory, low processor, low bandwidth, which makes them much more vulnerable than traditional Internet devices we have used to date because this resource economy does not it allows them to implement large security measures such as cryptography. I try to prove the hypothesis that one of the causes of their vulnerability is how little updated the firmware they use is.

ÍNDEX

FIGURES / TAULES / FITXES

Pàgina

FIGURES

TAULES

FITXES

1. Introducció

1.1 Context i justificació del Treball

En l'actualitat la *Internet de les Coses* (*IoT*) representa la connexió de milions de dispositius intel·ligents i sensor que recopilen i comparteixen dades d'usuaris i organitzacions (empreses i institucions). Hi ha estimacions que als pròxims anys arribaran a 30 mil milions de dispositius connectats a escala mundial, es calcula que un terç seran computadores, telèfons intel·ligents, tauletes i televisors intel·ligents i els altres dos terços seran sensors, actuadors i altres dispositius inventats fa molt poc temps.

Molts d'aquests dispositius tenen capacitat de ser programats (implementen un processador) i poden executar per exemple programes. Això té un **impacte** i unes conseqüències com poden ser:

- Poden executar programes d'**Intel·ligència Artificial**, per tant, poden "aprendre" i modificar el comportament dels actuadors segons els paràmetres que reben.
- Aquest dispositius generen una enorme quantitat de dades cosa que els fa formar part del mon de la **Big Data**. Dades que a més són de diferents tipus i es mouen amb diferents velocitats (amplades de banda).
- Es pot considerar aquests dispositius IoT com un sistema de **processament distribuït** que computen dades tant estructurades com no estructurades.
- Aquesta profusió de dispositius *IoT* dóna lloc i/o facilita l'**automatització** per exemple amb l'àmbit de la llar (domòtica, edificis intel·ligents), de la indústria, xarxes de distribució elèctrica, smarts cities, conducció autònoma o assistida a l'àmbit de l'automòbil, medicina, aviònica, etc.
- També aquest tipus de dispositius tenen protagonisme a l'**aprenentatge automàtic** (*Machine learning*) en casos com el reconeixement de veu, facial i de forma, recomanació de productes segons client, etc.

Aquests dispositius *IoT*, que tenen aquesta incidència tan alta i que a la vegada formen part d'aquesta munió de camps tecnològics incipients, **són molt més vulnerables que els dispositius tradicionals d'Internet** que hem fet servir fins a l'actualitat. A més tenen la **dificultat** afegida de:

- Per a seva distribució espacial, per la llar, per la fàbrica, per la ciutat, es difícil accedir a ells de manera física cosa que a l'hora d'actualitzar en programari i el *firmware* en línia, aquesta actualització es fa en banda (paquets de dades i d'actualitzacions i d'administració circulen per la mateixa xarxa).
- No acostumen a tenir connexió amb fil a la xarxa fan servir prioritàriament connexions sense fil, intrínsecament més insegures, la qual cosa queda reflectida en aquest tipus de dispositius.
- Acostumen a disposar de pocs recursos: poca capacitat de processament, emmagatzematge, poca amplada de banda, etc.
- Compten amb els avantatges d'un sistema de computació destruïda però també els seus inconvenients.
- Els hackers els acostumen a fer servir com a plataformes des d'on llançar atacs tipus distribuïts (per exemple *DDos*) actuant com si fossin una *botnet*.

Dins d'aquesta varietat de dificultats (segur que falten moltes) que pateixen els dispositius *IoT* en centro en la dificultat per a l'actualització de firmware. Aquests tipus de dispositius ubicats en llocs remots o inaccessibles, on en molts casos la intervenció humana és pràcticament impossible, on moltes vegades estan dissenyats de manera intencionada sense capacitat de ser actualitzats.

Sota aquest escenari es de suposar que si a un dispositiu *IoT* es descobreix una nova vulnerabilitat que afecta al seu *firmware* i aquest no té capacitat d'actualització o no té implementat un servei de xarxa per fer-ho, romandrà aquesta vulnerabilitat per a la resta de la seva vida útil. En cas de tindre la possibilitat de fer-ho caldria que es fes d'una manera automatitzada sense la intervenció necessària d'un usuari amb poca formació tècnica per dur-ho a terme d'altre manera.

Això planteja el dubte següent: ***els dispositius IoT són molt més vulnerables que els dispositius tradicionals d'Internet?***

1.2 Objectius del Treball

Els principals objectius a aconseguir en el *Treball de Final de Màster* són:

Objectius d'investigació

- Demostrar la hipòtesi que els dispositius *IoT* són molt més vulnerables que els dispositius tradicionals d'Internet.
- Validar si realment els dispositius de *IoT* tenen un *firmware* més desactualitzat que la resta d'elements connectats a Internet.
- Demostrar si els dispositius de *IoT* són molt vulnerables a ciberatacs a partir de l'anàlisi dels riscos associats a tenir software no actualitzat.
- Definir com es podria millorar la situació de vulnerabilitat de la *IoT*.

Objectius d'implementació

El llistat de les contribucions fetes pel treball:

- Estudi de l'antiguitat mitjana del software que fan servir els dispositius *IoT*.
- Estudi comparatiu dels protocols de seguretat de xarxes que fan servir els dispositius *IoT* i els dispositius de la Internet tradicional amb menció dels riscos associats als protocols propis fets servir a la *IoT*.
- Anàlisi crític de la situació i propostes per a millorar-la.

Objectius d'entrega

- Desenvolupar les successives entregues del *Treball de Final de Màster*.
- Entregar de la Memòria final.

1.3 Enfocament i mètode seguit

El treball tracta un tema que es desenvolupa en un context molt heterogeni per dues raons principals:

- La primera, atès que la *IoT,* es troba molt estesa per molt tipus diferents de dominis d'aplicació com poden ser: l'entorn del habitat urbà de les persones com la llar (domòtica), entorn d'edificis intel·ligents (*Building Management System*), entorns de ciutats intel·ligents, etc; també una altra gran categoria pot-ser l'entorn industrial l'automatització, controls de qualitat, sistemes gestors, robòtica, etc. Trobarien molts dominis més on s'aplica la *IoT*.

- La segona raó és la gran diversitat de dispositius que poden estar connectats amb una xarxa com poden ser: panys de seguretat, termòstats, webcam, electrodomèstics, sensors en general, vàlvules, actuadors, robots, aparells multimèdia, punts d'accés sense fil, wearables, dispositius mòbils, equips de control potència elèctrics, equips de telecomunicacions, equips de monitoratge mèdic, equips de rendiment esportiu, etc.

Per tant una part de la feina seria d'investigació dels diferents dispositius segons el firmware, el sistema operatiu, els protocols de comunicació, les estratègies de seguretat, etc. També diferenciar els diversos dominis d'aplicació amb els sistemes de control que acostumen a fer servir.

Una altra part serà, mitjançant motors de cerca i altres tipus de programari, explorar la Internet per a fer mostrejos sobre els diferents dispositius *IoT* que es poden trobar connectats a la xarxa. Parlo de programes tipus *Shodan*, *FOFA*, *Censys*, etc.

També cal cercar estudis, fets par a institucions solvents, referents a aquest tipus d'estadístiques. Tant sobre l'estat actual de la xarxa com de projeccions de futur.

Una altra part de la feina pot-ser cercar propostes per a aconseguir una millora en la implantació de sistemes d'actualitzacions per a dispositius IoT. Tant ressenyar les diferents implementacions actuals com quines serien les millors pràctiques. Per últim cal investigar sobre les tendències en els propers anys sobre aquest tipus d'operacions.

1.4 Planificació del Treball

Per a planificar, el *TFM*, primer elaboro una taula amb el detall de totes les tasques i subtasques que penso necessitaré durant el desenvolupament del treball. Estar clar que això serà una estimació tant del tipus de feina com del temps necessari per a cadascuna d'aquestes feines.

Per a articular el temps d'entrega tinc en compte com a fites les entregues programades a l'aula del projecte però segons avanci s'entregarà els productes elaborats al llarg del projecte de manera total o parcial. A la *Taula 1* es pot veure la planificació de tasques.

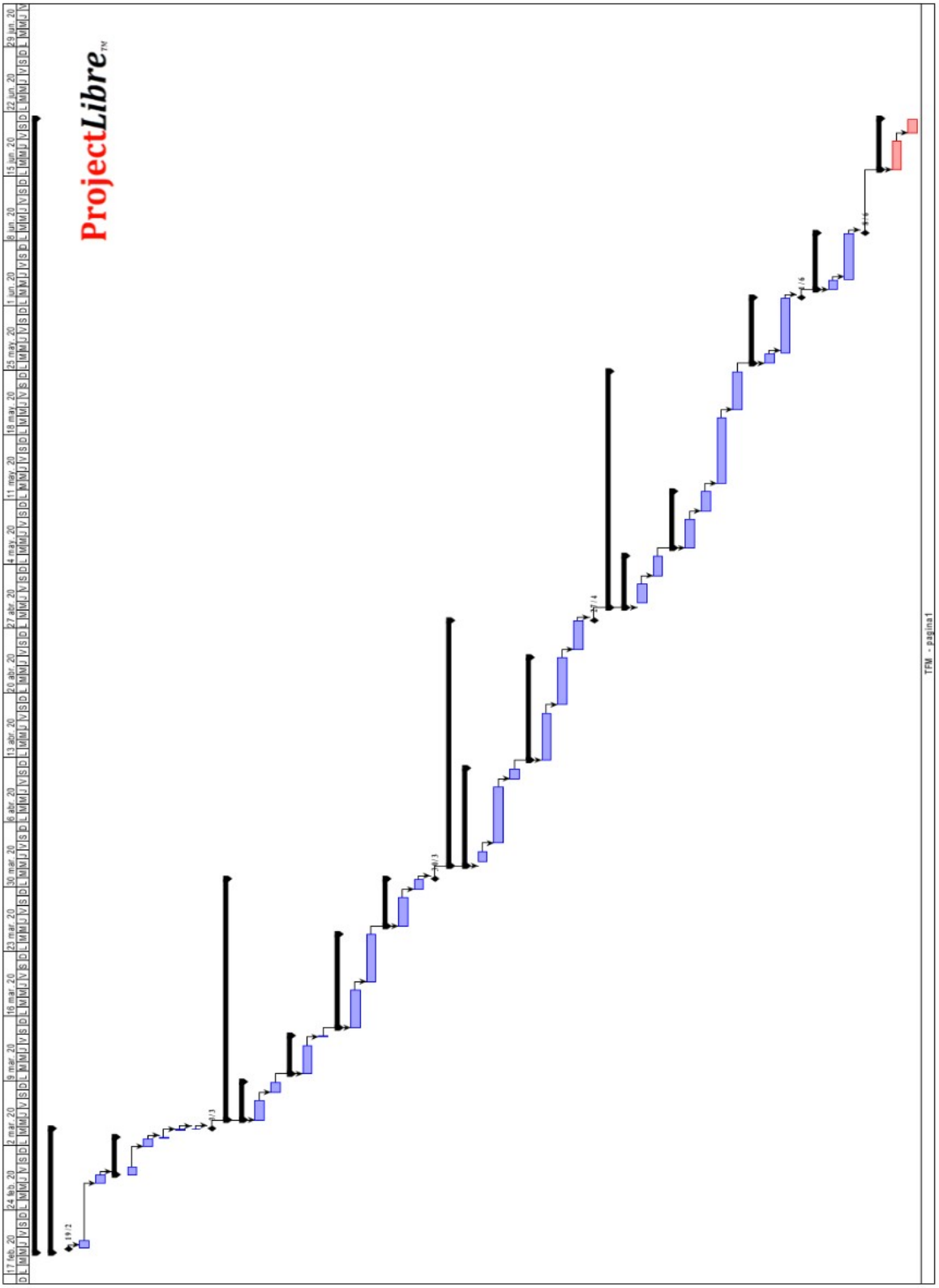

Figura 1: Diagrama de *Gantt* produït amb *ProjectLibre*.

Codi	Definició	Data inici	Data fi	hores
1	**Pla de treball**			
1.1	Establir el problema a resoldre elaborar el context i justificació del treball	19/02/20	22/02/20	3
1.2	Definir els objectius del treball	22/02/20	25/02/20	2
1.3	Definir l'enfocament i mètode seguit	26/02/20	29/02/20	3
1.4	**Elaborar la planificació del treball**			
1.4.1	Definir les diferents tasques de que es compon el treball	29/02/20	01/03/20	3
1.4.2	Càlcul temps d'entrega de les tasques	01/03/20	01/03/20	2
1.4.3	Elaborar cronograma *Gantt*	01/03/20	01/03/20	3
1.5	Elaborar un sumari de productes obtinguts	02/03/20	02/03/20	1
1.6	Fer una descripció dels altres capítols de la memòria	02/03/20	03/03/20	1
1.7	**FITA - Entrega 1 - Pla de Treball**	**19/02/20**	**03/03/20**	**18**
2	**Investigació i cerca estudis**			
2.1	**Elaborar taxonomia de dispositius IoT**			
2.1.1	Obtenir documentació (Web, UOC: Rec. electrònics, Revist. i llibres i BBDD)	04/03/20	07/03/20	5
2.1.2	Elaborar una síntesi recopilatori del material obtingut a las tasca anterior	07/03/20	09/03/20	2
2.2	**Estudi dels diferents dominis d'aplicació**			
2.2.1	Obtenir documentació (Web, UOC: Rec. electrònics, Revist. i llibres i BBDD)	10/03/20	13/03/20	4
2.2.2	Elaborar una síntesi recopilatori del material obtingut a las tasca anterior	14/03/20	14/03/20	2
2.3	**Estudi protocols comunicació, seguretat, SO i firmware**			
2.3.1	Obtenir documentació (Web, UOC: Rec. electrònics, Revist. i llibres i BBDD)	15/03/20	19/03/20	8
2.3.2	Elaborar una síntesi recopilatori del material obtingut a las tasca anterior	20/03/20	25/03/20	2
2.4	**Investigació d'estudis solvents que siguin rellevants per aquest treball**			
2.4.1	Obtenir documentació (Web, UOC: Rec. electrònics, Revist. i llibres i BBDD)	26/03/20	29/03/20	8
2.4.2	Elaborar una síntesi recopilatori del material obtingut a las tasca anterior	30/03/20	31/03/20	2
2.5	**FITA – Entrega 2 -**	**04/03/20**	**31/03/20**	**35**
3	**Elaboració d'estadístiques**			
3.1	**Estudi d'alternatives de software per cerca estadístiques de dispositius**			
3.1.1	Cercar diferent software tipus motor de cerca, detecció heurística, etc	01/04/20	03/04/20	8
3.1.2	Fer proves amb els programes més prometedors pels interessos del treball	04/04/20	10/04/20	8
3.1.3	Fer una comparativa amb els programes seleccionats	11/04/20	12/04/20	3
3.2	**Proves i obtenció de resultats**			
3.2.1	Bateria de proves amb el programari seleccionat segons tipus 1	13/04/20	18/04/20	6
3.2.2	Bateria de proves amb el programari seleccionat segons tipus 2	19/04/20	24/04/20	6
3.3	Explicació i conclusions d'estudis rellevants per aquest treball	25/04/20	28/04/20	4
3.4	**FITA – Entrega 3 -**	**01/04/20**	**28/04/20**	**35**
4	**Millores proposades i tendències**			
4.1	**Estudiar estat de les actualització de software**			

4.1.1	Extreure conclusions de la tasca 3	29/04/20	02/05/20	2
4.1.2	Extreure conclusions de la tasca 2	03/05/20	05/05/20	2
4.2	**Estudiar sistemes actuals d'actualització de software**			
4.2.1	Extreure conclusions de la tasca 2 i tasca 3	06/05/20	08/05/20	3
4.2.2	Obtenir documentació (Web, UOC: Rec. electrònics, Revist. i llibres i BBDD)	09/05/20	12/05/20	5
4.3	Proposar una millora als sistemes actuals	13/05/20	20/05/20	8
4.4	Investigar les tendències de les actualització de software	21/05/20	25/05/20	4
5	**Memòria final**			
5.1	Elaboració de les conclusions del treball	25/05/20	26/05/20	2
5.2	Elaboració de la memòria final del *TFM*	27/05/20	02/06/20	4
5.3	**FITA – Entrega 4 - Memòria final**	**29/04/20**	**02/06/20**	**30**
6	**Presentació en vídeo**			
6.1	Elaboració d'un guió per fer un vídeo explicatiu com a síntesi del treball	03/06/20	03/06/20	2
6.2	Elaboració del vídeo de síntesi del treball	04/06/20	09/06/20	6
6.3	**FITA - Entrega 5 – Presentació en vídeo**	**03/06/20**	**09/06/20**	**8**
7	**Defensa del *TFM***			
7.1	Respondre preguntes al Fòrum del curs	15/06/20	19/06/20	3
7.2	**FITA – Defensa del *TFM***	**15/06/20**	**19/06/20**	**3**

Planificació tasques *TFM*. Taula 1

A la *Figura 1* es pot veure el diagrama de *Gantt* corresponent al desenvolupament de la *Taula 1*. S'ha fet servir el programa *ProjectLibre*™ per a fer el seguiment de la planificació del *Treball de Final de Màster*.

1.5 Breu sumari de productes obtinguts

Una vegada finalitzat el treball ha de quedar o no demostrat que *si els dispositius IoT són molt més vulnerables que els dispositius tradicionals d'Internet*, aquest seria el principal producte que ha de generar.

Entrant més en detall hi ha un llistat de productes que hi haurien de ser un cop finalitzat el treball.

- Planificació del treball, de manera opcional pot-ser un seguiment de la planificació.
- Recopilatoris que mostri una visió actual de dispositius *IoT*, dominis d'aplicació de *IoT*, protocols de comunicació de *IoT*, sistemes operatius i en el seu cas *firmware*.
- Joc de proves fets amb diversos programes i resultats otinguts.

- Proposta de millora.
- Memòria final on reflexa tot els productes anteriors.
- Vídeo de presentació.

1.6 Breu descripció dels altres capítols de la memòria

A la memòria final a més del present punt (*Introducció*), es poden trobar els següents punts:

- 2. Resultats de la investigació i recerca
- 3. Entorn de proves
- 4. Resultats obtinguts a les proves
- 5. Conclusions
- 6. Proposta de millora i bones pràctiques
- 7. Glosari
- 8. Bibliografia i webgrafia
- 9. Annexes

2. Investigació i cerca d'estudis

2.1 Taxonomia dels dispositius *IoT*

Internet of Things (*IoT*, d'ara en a davant) és un **paradigma creixent** de molta importància tècnica, social i econòmica. La *IoT* **és un concepte emergent** que abasta un **extens ecosistema de serveis i dispositius interconnectats**, com poden ser: sensors, articles de consum, aparellatge domèstic intel·ligent, cotxes, components industrials i de salut, etc. Aquestes tecnologies **recol·lecten, intercanvien i processen dades** per adaptar-se de manera dinàmica a un context específic, transformant el món i la forma de viure en el seu conjunt. *IoT* està estretament lligat als sistemes **ciberfísics** i, en aquest sentit, les implicacions de seguretat són pertinents.

2.1 Taxonomia dels dispositius *IoT*

Internet of Things (*IoT*, d'ara en a davant) és un **paradigma creixent** de molta importància tècnica, social i econòmica. La *IoT* **és un concepte emergent** que abasta un **extens ecosistema de serveis i dispositius interconnectats**, com poden ser: sensors, articles de consum, aparellatge domèstic intel·ligent, cotxes, components industrials i de salut, etc. Aquestes tecnologies **recol·lecten, intercanvien i processen dades** per adaptar-se de manera dinàmica a un context específic, transformant el món i la forma de viure en el seu conjunt. *IoT* està estretament lligat als sistemes **ciberfísics** i, en aquest sentit, les implicacions de seguretat són pertinents.

La *IoT* presenta reptes de seguretat i privacitat molt importants que cal abordar perquè aquest concepte assoleixi tot el seu potencial. Moltes consideracions de seguretat sobre *IoT* són ja conegudes per l'ús de tecnologies en xarxa. Les característiques de les **implementacions *IoT* presenten nous reptes de seguretat, amenaces i riscos múltiples que evolucionen de manera ràpida**. Aquesta protecció depèn de la protecció de tots els sistemes implicats (els dispositius mateixos, servei de *backend* del núvol i els serveis, les aplicacions, eines de manteniment i diagnòstic, etc.).

Fer front a aquests **reptes i assegurar la seguretat dels productes i serveis *IoT* és una prioritat bàsica**. Una de les principals preocupacions és l'impacte que poden tenir les diferents amenaces, ja que els atacs al desplegament de sistemes *IoT* poden suposar un perill seriós per la seguretat, la privacitat, a més, els sistemes ***IoT* es poden utilitzar com a vector d'atac contra**

altres infraestructures crítiques. Els sistemes *IoT* canvia de manera radical la forma de recollir, analitzar, utilitzar i protegir les dades personals, la qual cosa planteja **problemes de privadesa**.

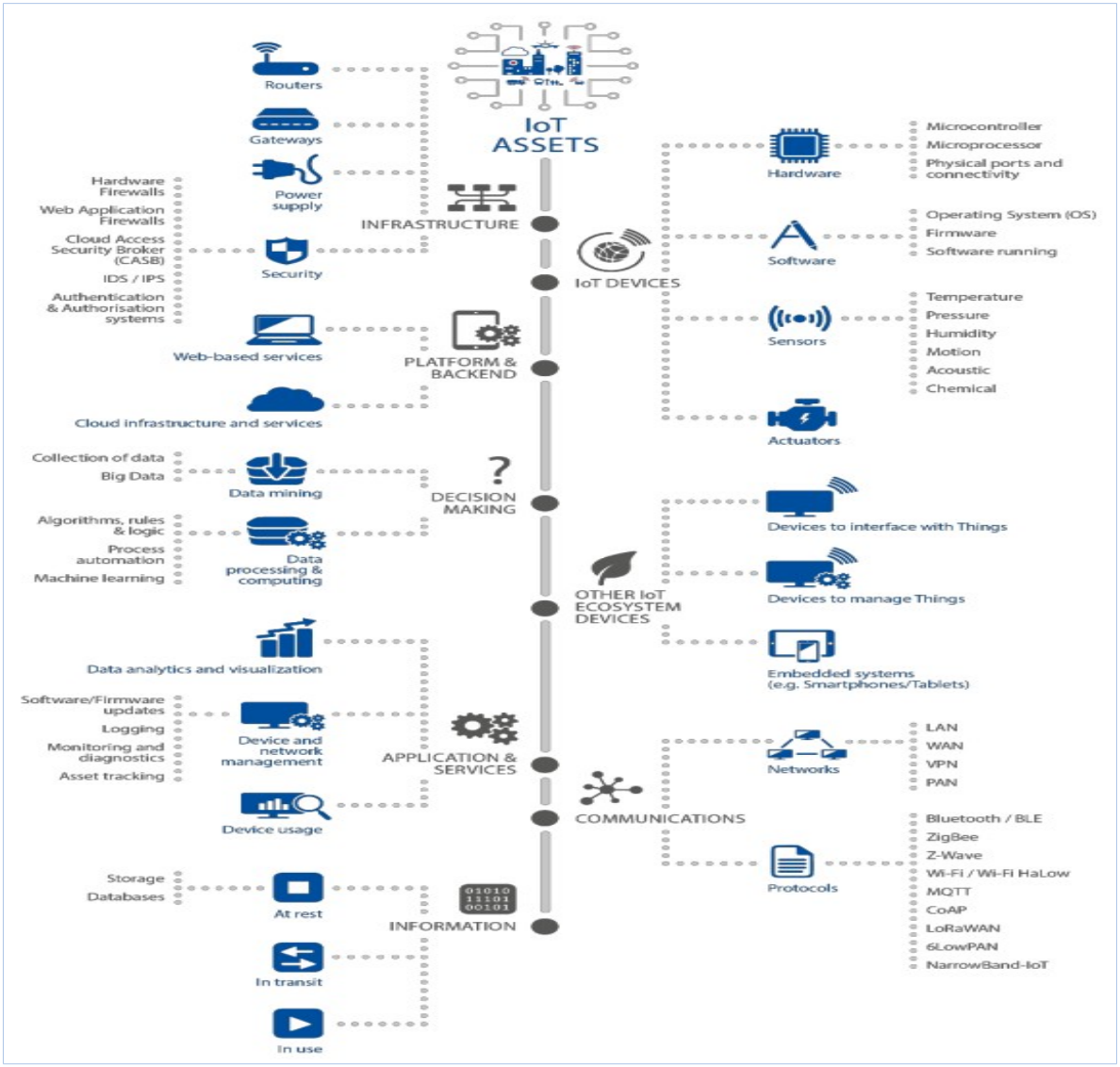

Figura 2: Taxonomia d'actius (*ENISA*, 2017).

Amb tot, a banda de mesures de seguretat tècniques, la *IoT* planteja molts **nous reptes legals, polítics i normatius, d'àmbit ampli i complex**, que són difícils de resoldre, i que amplifica algunes qüestions existents. El ràpid ritme de canvi de la tecnologia *IoT* ha superat la capacitat d'adaptació de les polítiques, legals i reguladores associades, sense deixar un marc de seguretat clar a seguir. Això ha portat a la **majoria de les empreses i fabricants a adoptar el seu propi enfocament** a l'hora de dissenyar dispositius *IoT*, provocant **problemes d'interoperabilitat entre dispositius de diferents fabricants i entre dispositius *IoT* i sistemes heretats**.

Una de les **recomanacions** de les institucions i experts responsables de desenvolupar programari de sistemes *IoT,* és de definir les **pautes de cicle de vida de desenvolupament de programari/maquinari segur** per a *IoT*. Això va destinat a desenvolupadors, operadors de plataformes, indústria, fabricants, etc.

2.1.1 Taxonomia d'actius

Per aconseguir aplicar la ciberseguretat es comença per la identificació i la descomposició d'actius. Cal aplicar una visió general dels grups i actius clau a protegir en un ecosistema IoT.

El nivell de protecció d'un determinat actiu varia en funció del cas d'ús, de l'aplicació utilitzada i de l'escenari d'ús d'aquest ecosistema *IoT*. Els diferents actius *IoT* s'han dividit en els grups d'actius definits. Aquesta taxonomia d'actius es mostra a la **figura 2**. Cal dir que el nivell més baix de la taxonomia és indicatiu i no exhaustiu, doncs per exemple, no es mostren tots els tipus de sensors, només alguns representatius, el mateix serveix per a les xarxes, als protocols, etc.

Com es pot veure aquest són molt extensos aquest actius, cal doncs **concentrar-nos en els actius que formen part de l'objectiu d'aquest *Treball Final de Màster*** els quals són:

- Programari de dispositius IoT que inclou el sistema operatiu del dispositiu IoT, el seu ***firmware*** i els programes i aplicacions instal·lats/executats.

- La gestió de dispositius IoT i xarxa mitjançant aplicacions i serveis IoT que inclou les **actualitzacions de programari del sistema operatiu, el firmware i les aplicacions**. També inclou el seguiment i el seguiment dels dispositius i xarxes, la recollida i l'emmagatzematge de registres que després poden ser utilitzats per als diagnòstics.

La **figura 3** proporciona una **visió de la criticitat dels principals actius** descrits en la taxonomia d'actius, a partir d'opinions d'experts.

2.1.1 Arquitectura *IoT*

És important no deixar que la **complexitat percebuda** del *IoT* no destorbin les possibilitats d'implementar els projectes i es comenci per establir un marc sòlid per al sistema *IoT*.

Un dels principals desafiaments que cal enfrontar, en planificar solucions *IoT*, és tractar la seva **complexitat**. En aquest sentit cal adoptar una arquitectura per nivells que ajuda a gestionar la complexitat de les solucions *IoT*. Aquesta arquitectura *IoT* basades en dades que faci l'analítica de límits, l'arquitectura de nivells que captura el flux d'informació, des dels sensors fins als serveis límits, i tot seguit als serveis en núvol. Això pot afegir capes transversals com la gestió d'identitats o la seguretat de les dades.

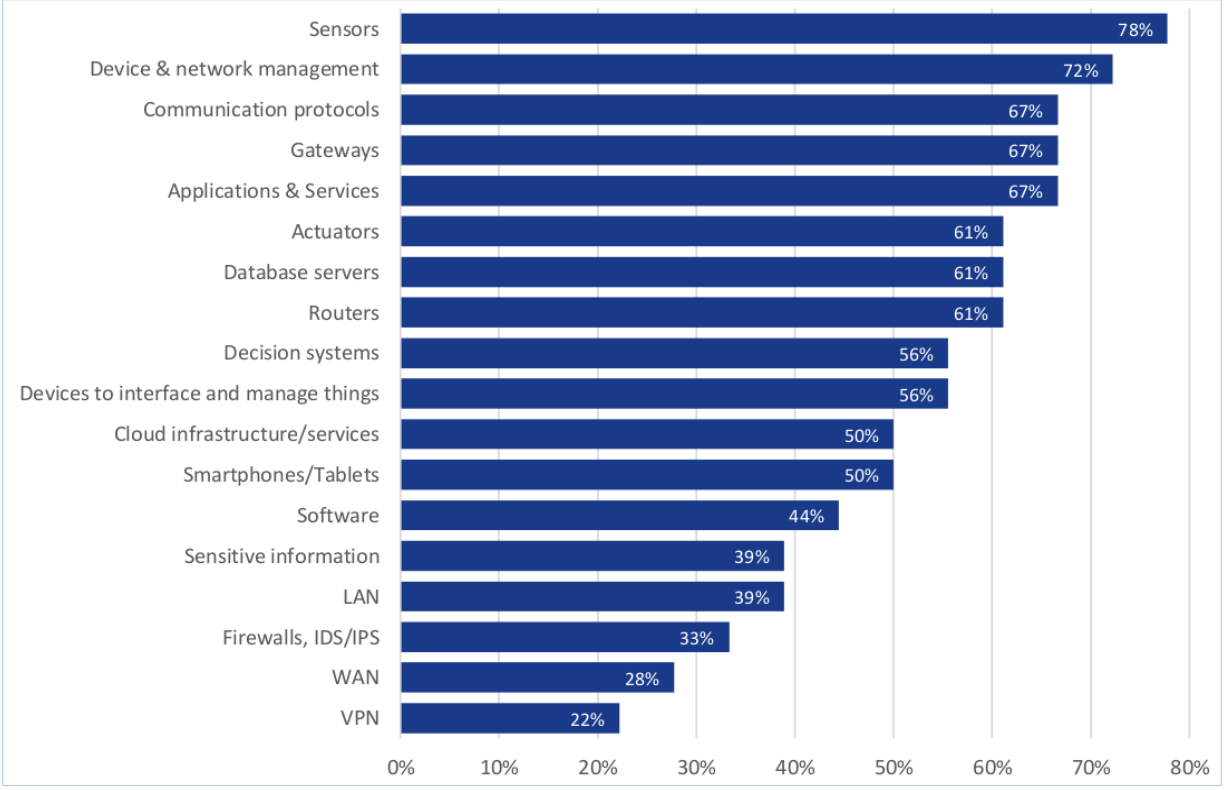

Figura 3: Criticitat d'actius (ENISA, 2017).

Caldria seguir una **arquitectura de referència** per a no tenir cap problema de desenvolupament i de posterior manteniment, escalabilitat, cicle de vida, etc. Per aquest motiu hi ha moltes iniciatives que treballen per a estandarditzar les arquitectures de *IoT* per a millorar la interoperabilitat. Les entitats involucrades en el desenvolupament de plataformes de IoT i els investigadors col·laboren per a definir **arquitectures de referència de *IoT***.

Aquestes arquitectures de referència són els fonaments arquitectònics que descriuen els blocs de construcció d'alt nivell, estableixen una terminologia compartida, etc. Algunes de les iniciatives són:

- ***IEEE 2413 Internet of Things (IoT) Architecture Working Group***: Projecte d'estandardització contínua de *IEEE* que té l'objectiu d'identificar semblances entre els dominis de *IoT*, inclosa la fabricació, els edificis intel·ligents, les ciutats intel·ligents, els sistemes de transport intel·ligents, la xarxa elèctrica intel·ligent i la cura de la salut.
- ***Industrial Internet Consortium Architecture IIRA***: Fundat per *AT&T*, *Cisco*, *General Electric*, *IBM* i *Intel*, va desenvolupar específicament el *IIRA* per a aplicacions de *IoT* industrials.

Per a desenvolupar solucions *IoT* s'ha de fer servir una arquitectura de referència com si es tractés d'una plantilla, on aquesta descriu els components de l'arquitectura de *IoT* i les seves funcions en termes d'alt nivell on s'ha de concretar requisits abstractes amb tecnologies específiques o piles de tecnologies. En aquesta línia es poden trobar arquitectures concretes desenvolupada per grans empreses com pot-ser les de *IBM*, *Intel*, *Microsoft*, *Amazon*, etc.

Les solucions de *IoT* són complexes a causa de l'escala, l'heterogeneïtat dels dispositius, la connectivitat implicada, la seguretat del sistema, l'escalabilitat, la disponibilitat i la flexibilitat.

Les 4 etapes d'una arquitectura IoT

Aquestes arquitectures de referència, sigui un model prescriptiu o una implementació concreta, acostumen ha estar definides en quatre nivells o etapes, aquestes poden ser: l'**etapa 1** formada normalment per **sensors i actuadors** sense fil. L'**etapa 2** inclou sistemes d'**agregació de dades** de sensors i **conversió** de dades **analògic-digital**. A l'**etapa 3**, els sistemes informàtics frontera que fan el **preprocessament de les dades** abans que es traslladi al ***DC***. Per últim, a l'**etapa 4**, les **dades s'analitzen, gestionen i emmagatzemen** en sistemes *DC*.

Etapa 1. Sensors / actuadors

Els **sensors recopilen dades** de l'entorn o objecte en mesurament i la converteixen en dades útils. Els **actuadors també poden intervenir per canviar les condicions físiques que generen les dades**.

L'**etapa de detecció/accionament abasta** una gran quantitat de dispositius molt heterogenis, com dispositius industrials antics, càmeres robòtiques, detectors de nivell d'aigua, sensors de qualitat

de l'aire, acceleròmetres i monitors de freqüència cardíaca, un llarg etc. On col·labora a la seva expansió les tecnologies de xarxa de **sensors sense fils de baix consum** i ***Power over Ethernet (PoE)***.

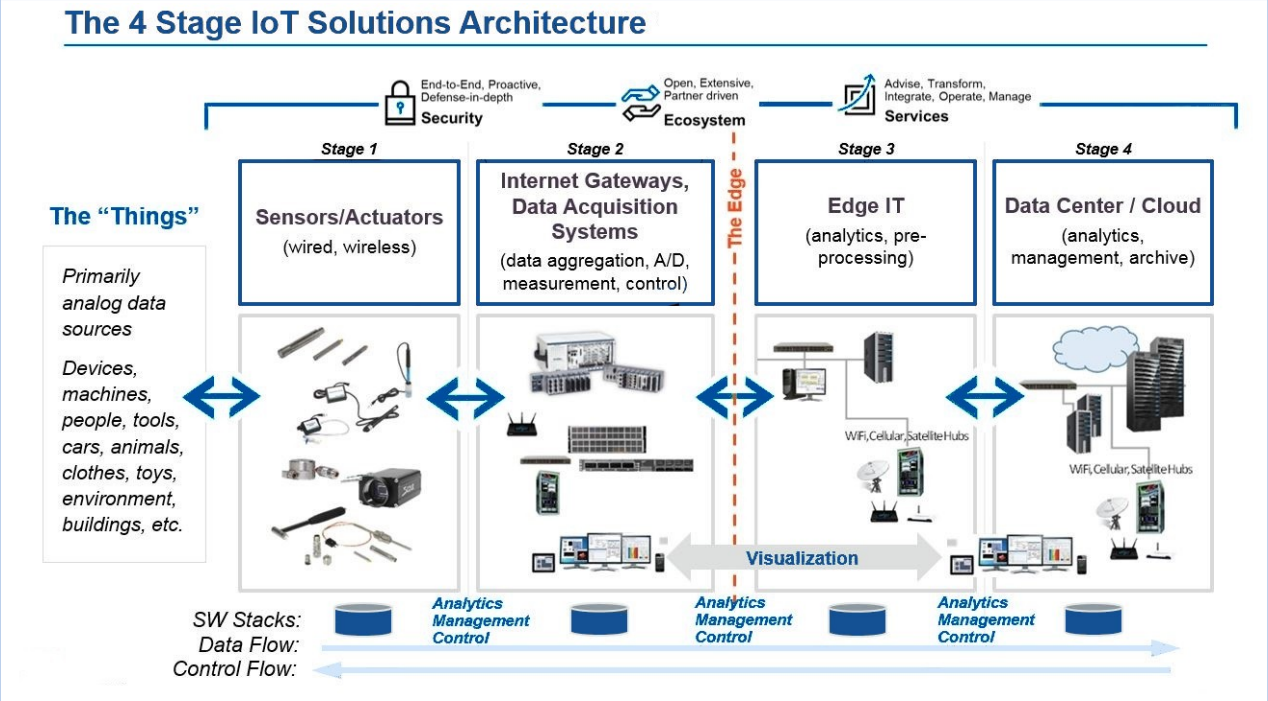

Figura 4: Les 4 etapes de l'arquitectura *IoT* (Fuller, 2016).

En una arquitectura *IoT*, es pot fer **processaments de dades en cadascuna de les quatre etapes**. Es pot processar dades al sensor però estarà **limitat per la potència** de processament del dispositiu *IoT* que acostuma a ser poca. Les **dades es troben al centre** de l'arquitectura *IoT*, s'ha de **triar** a l'hora de processar les dades entre:

- **Immediatesa**, **c**om més **immediata** sigui la necessitat d'informació**,** més s'**aproxima als dispositius finals** del sistema *IoT*.
- **Profunditat de coneixement**, per obtenir **visions més profundes que requereixen processament més extens**, s'han de traslladar les dades a un sistema **basat en un núvol** o *DC* que pugui reunir diverses fonts.

Però algunes **decisions simplement no poden esperar** a un processament profund, per un cotxe s'estavellarà? no hi ha temps per enviar aquestes dades al núvol. S'ha de **processar les dades directament al sensor**, a la mateix de la xarxa de support, per obtenir una resposta més ràpida.

Etapa 2. Passarel·les d'Internet i sistemes d'adquisició de dades (*DAS*)

Les dades dels sensors acostumen a ser de tipus **analògic**, en aquest cas fa falta que les dades s'agregin i es **converteixin en fluxos digitals** (*stream*) per poder processar-les. Els **sistemes d'adquisició de dades** (*DAS, Data acquisition systems*) fan aquestes funcions d'agregació i conversió de dades. El *DAS* es connecta a la xarxa de sensors, **agrupa les sortides i realitza la conversió analògic-digital**. La passarel·la d'Internet rep les dades agregades i digitalitzades i les dirigeix mitjançant xarxa sense fil (*Wi-Fi*, *Wi-MAX*, *Bluetooth*, etc) o cablejat, cap als sistemes de l'etapa 3 per a poder ser processades.

Els sistemes de l'etapa 2 acostumen a situar-se a prop dels sensors i actuadors, aquest dispositiu podria estar fixat físicament a un sensor per exemple. Un dispositiu o servidor de **passarel·la contigu processaria les dades i les reenviaria als sistemes etapa 3 o etapa 4**. Hi ha dues raons perquè la millor opció sigui **preprocessar-la abans d'enviar al DC**:

- Cal parar compte que els **fluxos de dades analògics** que provenen de sensors creen grans volums de dades, provenen del món físic com pot-ser el moviment, les tensions, les vibracions, etc. Això crea unes **quantitats voluminoses de dades que canvien constantment**, a més els sistemes *IoT* poden abastir un gran nombre de sensors els quals pot-ser sempre, les 24 hores del dia, estan en marxa. Per aquests motius els fluxos de dades *IoT* poden ser immensos: en alguns casos fins a *40 TB/segon,* el que suposa **una gran quantitat de dades per transportar al centre de dades.**
- A més les dades analògiques tenen característiques puntuals i estructurals específiques que requereixen el **processament de programari especialitzat**.

El millor és **convertir les dades en forma digital primer,** i això és el que passa a l'**etapa 2**. Les passarel·les intel·ligents (*gateway*), són un tipus de dispositiu frontera típic d'aquesta etapa 2, poden tenir funcionalitats addicionals com capacitat analítica de fluxos de dades en temps real, protecció contra programari maliciós i serveis de gestió de dades. La **passarel·la té el poder de càlcul per a proporcionar la informació d'una forma més comprensible** per la seva explotació.

Els dispositius ***DAS*** **i passarel·les (gateway) poden acabar en una gran varietat d'ambients**, des de la planta de fàbrica fins a les estacions de camp mòbils, de manera que aquests sistemes solen ser **dissenyats per ser portàtils**, fàcils de desplegar i prou resistents per suportar variacions de temperatura, humitat, pols, i vibració.

Etapa 3. IT frontera

Una vegada **digitalitzades i agregades les dades de *IoT*, ja està preparat per entrar a l'àmbit de les *IT* (*Information Technology*)**. Les dades poden requerir un **preprocessament** abans que entrin al centre de dades (*DC*). Aquí és on entren els sistemes de processament informàtic frontera, que poden situar-se en ubicacions remotes, tot i que generalment se situen a la instal·lació on els sensors resideixen (exemple a un armari de cablejat).

En aquesta etapa 3 acostuma a presentar-se uns **escenaris típics** com:

- Les dades en aquesta etapa, pot crear la necessitat, de més amplada de banda de la xarxa i més recursos de processament de dades. En aquesta etapa 3 el **millor és disposar de sistemes frontera capaços de realitzar analítiques (preprocessament)** per abaixar la càrrega de la infraestructura en el sentit cap a l'etapa 4, per no fer servir **un gran canal de dades cap al DC**.
- També hauríeu d'enfrontar-vos a problemes de seguretat, d'emmagatzematge i latències en el processament de dades. En aquesta etapa 3**, es pot preprocessar les dades i generar resultats significatius** per enviar-les cap a l'etapa 4.
- També es pot fer servir l'**aprenentatge automàtic frontera per cercar anomalies** que identifiquin problemes de manteniment imminents que requereixin atenció immediata (per exemple tecnologia de visualització per presentar informació). Les **infraestructures hiperconvergents, s'adapten idealment a aquestes tasques, són ràpids, fàcils de desplegar i gestionar** de forma remota.

Etapa 4. Data Center / Núvol

En aquesta etapa 4, les dades es processen en profunditat als centres de dades, les separacions entre aquestes etapes comencen a difuminar-se. En aquesta etapa es requereixen **professional TI** especialitzats en analítica de dades. La tasca important aquí seria visualitzar i gestionar el procés existent, enviar comandaments als sensors i captar la tornada.

2.2 *Dominis d'aplicació* de IoT

El terme *Internet de les coses* (*IoT*) fa referència a **qualsevol cosa de la vida diària a la qual s'accedeix o es connecta a través d'Internet**. La tecnologia IoT mostra que les característiques en diferents aplicacions necessiten la integració de la capa més alta i més generalitzada d'intel·ligència i la interfície d'usuari que ajunta l'enllaç en dispositius i serveis web utilitzant plataformes interoperables que brinden la funcionalitat necessària per als usuaris finals.

La IoT es fa servir per utilitzar els coneixements com són automatitzar, digitalitzar, optimitzar, transformar processos i models de negoci i també indústries en mutació digital. La *IoT* representa un sistema avançat d'automatització i anàlisi que engloba sensors, xarxes i intel·ligència artificial, missatges al núvol, per a formar uns sistemes complets com a productes o serveis.

Tot el procés de treball de *IoT* comença amb un dispositiu, que es comuniquen de manera segura amb la plataforma *IoT*. Les plataformes recopilen i analitzen les dades de tots els diversos dispositius i plataformes i transfereixen les dades més valuoses amb aplicacions a dispositius.

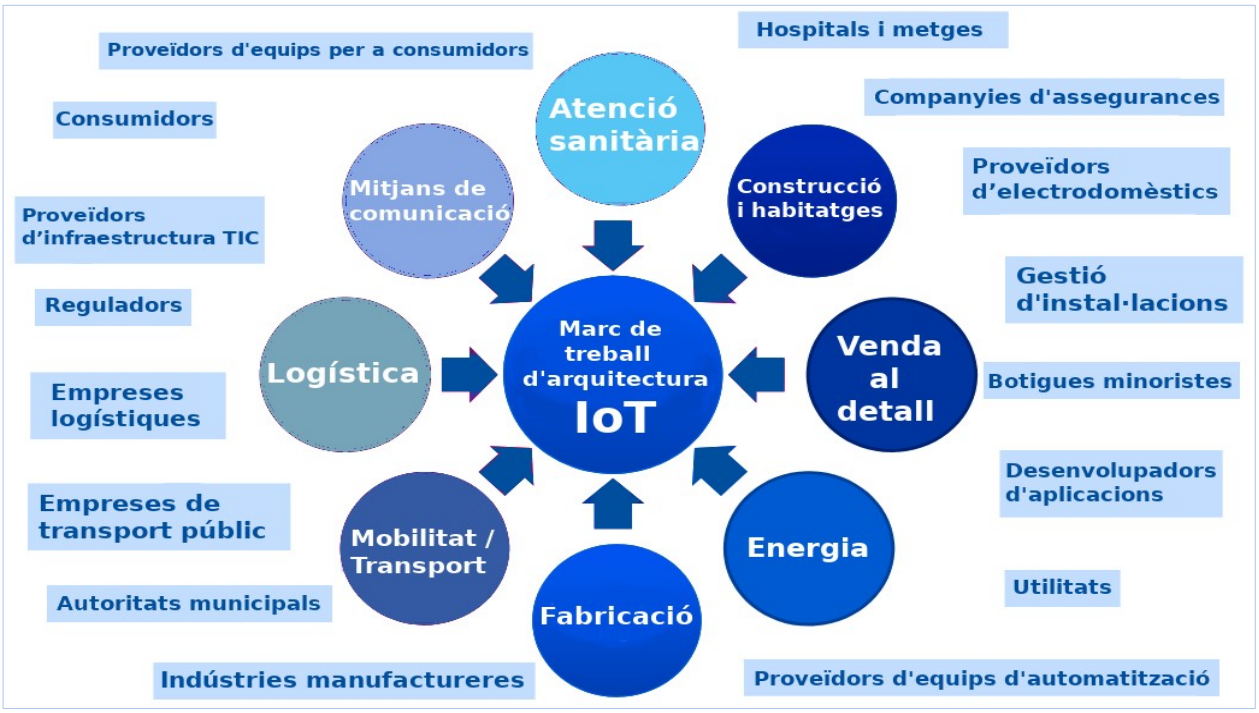

Figura 5: Dominis d'aplicació de *IoT* i parts interessades (*Nappey*, 2014).

2.2.1 Dominis i casos d'ús

Els dominis d'aplicació i els escenaris possibles de la *IoT* són quasi infinits. Tot seguit es fa un llistat de les possibilitats de dominis i casos d'estudi (*Perwej*, 2019):

- ***IoT* del domini de ciutats intel·ligents:** subministrament d'aigua eficaç, il·luminació de la ciutat, IoT en trànsit rodat, seguretat ciutadana, gestió d'escombraries, estàndard aeri, aparcament intel·ligent, *mobile crowdsensing*, edificis d'eficiència energètica, transport públic fiable i medi ambient.
- ***IoT* del domini industrial**.
- ***IoT* del domini energètic:** mesuradors intel·ligents, reparació i manteniment, recopilació de dades de consum, supervisar els serveis d'aigua en remot i vigilància del pol elèctric.
- ***IoT* del domini de la salut:** monitoratge i informes simultanis, accessibilitat i connectivitat de punt a punt, classificació i anàlisi de dades, seguiment i avís, assistència mèdica a distància, menors costos, experiència del malalt, gestió prioritzada medicament, minimitzar els errors i residus, resultats de millora dels tractaments.
- ***IoT* del domini a la casa intel·ligent:** atenció sanitària, serveis de seguretat, energia i entreteniment.
- ***IoT* del domini de l'agricultura:** monitoratge de les condicions climàtiques, tractors autònoms, agricultura de precisió, automatització d'hivernacles, drons agrícoles, gestió de cultius, control de bestiar, sistemes de gestió de finques en punt a punt.
- ***IoT* del domini de la biometria.**
- ***IoT* del domini del transport.**
- ***IoT* del domini dels negocis.**

Segur que en deixo una gran quantitat de dominis i casos d'estudi.

2.3 Comunicació, protocols, SO i firmware

La *IoT* es pot definir com ***un ecosistema ciber-físic de sensors i actuadors interconnectats, que permeten una presa de decisions intel·ligent*** (*ENISA*, 2017), es pot considerar com a un bucle continu de sensibilització, presa de decisions i accions. En entorns *IoT*, una cosa és un

objecte físic o virtual capaç de ser identificat i integrat a les xarxes de comunicació. Ja es pot veure que aquestes coses necessiten tenir unes **funcionalitats**:

- Comunicació per intercanviar dades entre una xarxa i/o els serveis del servidor (*backend*).
- Detectar, capturar dades, accionar, emmagatzemar, processar, executar aplicacions natives, aprenentatge automàtic, etc.
- Connectar-se de forma autònoma, llegir dades o controlar. Prendre una decisió intel·ligent.

Per tot aquests motius es tot seguit es mostra una aproximació senzilla de **programari i protocols** que acostumen a fer servir tot aquesta **constel·lació inabastable de dispositius** que com ja s'ha vist pot incloure un sensor, un actuador, un altaveu intel·ligent *Google Home*, un mòdem cable, un switch, un servidor, etc.

2.3.1 Comunicació

Les "coses" de IoT necessiten tant transmetre com rebre dades, tot i que no necessiten necessàriament una connexió a Internet per fer-ho, només la capacitat de transmetre les dades que recopilen/reben a altres "coses" capaces de processar-les informació o enviament mitjançant connexió a Internet. Per tant, és possible que un ecosistema IoT format per diverses "coses" funcioni sense que cap d'elles pugui connectar-se a Internet. (ENISA, 2017)

Les necessitats de comunicació varien entre els diferents tipus de xarxes *IoT*, segons la seva finalitat i les restriccions de recursos. La selecció d'un protocol determinat per a un desplegament particular de *IoT* depèn del seu cas d'ús. El fet de **combinar diferents protocols** dins d'un ecosistema *IoT* és una pràctica habitual, que fa servir passarel·les per assegurar la interoperabilitat.

Els sistemes de comunicació *IoT* es basen en la **capacitat de transmetre i rebre unitats d'informació de manera estructurada**, amb serveis localitzats a prop o en una posició llunyana, fent servir diversos tipus de xarxa diferents, però **interoperables**. Aquestes xarxes tenen diferents conjunts de propietats com *QoS*, resiliència, seguretat i gestió. Els protocols de comunicació dins dels ecosistemes IoT poden ser basats sense fil o cablejat.

Protocols de comunicació **sense fils** disponibles:

- **Protocols de ràdio de curt abast:** *ZigBee, Bluetooth/Bluetooth Low Energy (BLE), Wi-Fi/ Wi-Fi HaLow, Near Field Communication (NFC)* o *Radio Freqüència Identificació (RFID)*.
- **Xarxes mòbils i protocols de ràdio de llarg abast:** *LoRaWAN, SigFox NarrowBand-IoT (NB-IoT)* o *LTE-M*.

Cadascun d'ells es defineix en el seu propi estàndard, per exemple *ZigBee* i *ZigBee 3.0* es basen en *IEEE 802.15.4*. Els protocols i enllaços de comunicació per cable, com *Ethernet*, *USB, SPI*, *MIPI* i *I2C*, entre d'altres, també proporcionen accés als dispositius. A més, cal destacar que les comunicacions *IoT* també admeten protocols **no basats en *IP***, com *SMS*, *LiDar*, *Radar*, etc.

SESSIÓ		**AMQP, CoAP, DDS, MQTT, XMPP**	**SEGURETAT**	**GESTIÓ**
XARXA	**ENCAPSULACIÓ**	**6LowPAN, Thread, QUIC, DTLS**	**TCG, Oath 2.0, SMACK, SASL, ISASecure, ace, DTLS, Dice, ...**	**IEEE 1905, IEEE 1451, ...**
	ENCAMINAMENT	**CARP, RPL, IPv4, IPv6**		
ENLLAÇ DE DADES		**Bluetooth/BLE, Wi-Fi/Wi-Fi HaLow, LoRaWAN, Neul, SigFox, Z-Wave, ZigBee, USB**		

Llista indicativa de protocols de comunicació per a IoT (Salman, 2015). Taula 2

Les tecnologies **sense fil** tenen diferents característiques, com ara un rang de senyal específic, ample de banda, etc., es poden **classificar** com:

- Xarxes d'àrea personal sense fils (*WPAN, Wireless Personal Area Network*)
- Xarxes d'àrea local sense fils (*WLAN, Wireless Local Area Network*)
- Xarxes d'àrea ampla sense fils (*WWAN, Wireless Wide Area Network*)

La taula 2 mostra una llista indicativa de diferents protocols agrupats per la capa de comunicació. Les capes de la pila de comunicació:

- **Enllaç de dades** (*datalink*) gestiona la connexió entre dispositius *IoT* mitjançant un enllaç físic, per cable o sense fil (exemple entre un sensor i la passarel·la que connecta el connecta a Internet).

- **Xarxa** es divideix en la capa d'encaminament, que gestiona la transferència de paquets des de l'origen fins a la destinació i en la capa d'encapsulat, que crea els paquets.
- **Transport** defineix els protocols que permeten seqüenciar les dades da cada aplicació (nombre de port).
- **Sessió** defineix els protocols que permeten les capacitats de missatgeria entre els elements del subsistema de comunicació *IoT*.
- **Aplicació** on es pot executar les aplicacions finals.

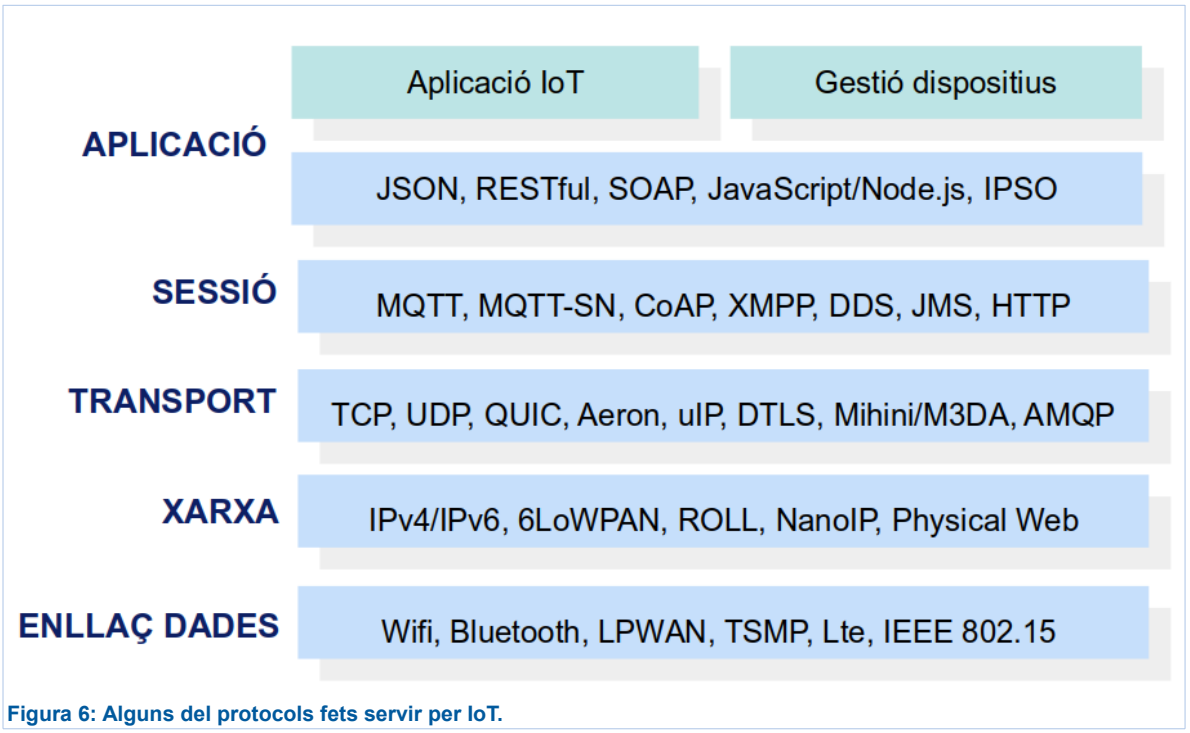

Figura 6: Alguns del protocols fets servir per IoT.

2.3.2 Programari de dispositius *IoT*

El programari associat a l'ecosistema *IoT* és avui dia immens. Associat a aquest terme es pot trobar **sistemes operatius**, **firmware**, **frameworks i eines de desenvolupament**, **plataformes**, **llenguatges**, **middlewares**, etc.

Firmware

També dins d'aquesta secció cal recordar el **firmware** que és l'objectiu d'aquest treball. Aquest tipus de programari pot-ser molt divers i variat, ja que com ja s'ha anat veient el mateix passa amb

els **dispositius IoT que són molt diversos i de naturalesa molt variada**. Cal pensar que ja s'ha explicat que aquests es poden classificar en 4 etapes:

- Etapa 1: Sensors / actuadors de molts diversos tipus i naturalesa, només cal pensar en els sensors que porta una terminal de telefonia mòbil.
- Etapa 2: Sistemes d'adquisició de dades / conversos A/D / passarel·les on aquestes últimes és un maquinari generalista en el sentit que no és d'ús exclusiu a l'ecosistema *IoT*.
- Etapa 3: IT frontera on el maquinari ja no és tan especialitzat en la IoT però si molt necessari i adient per part aquesta.
- Etapa 4: Data center / Núvol on ja es pot considerar tot el maquinari com a generalista.

A més es veu que com **més a prop de l'adquisició de dades i/o actuació, més es pot considerar un maquinari específic** per l'ecosistema IoT. Un altre idea que es pot observar és que si bé en tot el maquinari classificat per etapes vist **es fa servir firmware, és en les etapes més baixes on té major pes**, per exemple, tant un servidor com un encaminador, un switch, un punt d'accés, un balancejador, un firewall, acostuma a fer servir firmware però en aquests és una part important però és això, una part. Mentre que en els **actuadors que es faci servir firmware pot-ser és l'únic programari** del dispositiu.

Com a conclusió el **firmware és més significatiu als senzills dispositius** com a sensors, actuadors, conversos A/D, càmeres web, panys, assistents de veu, robots d'assistència, reguladors de llum, control de l'aire, temperatura, alarmes varies, monitoratge de malalts, tauletes, punt de venda mòbil, relés de control d'energia, etc.

Es pot afirmar que és possible implementar una solució d'actualització de firmware genèrica i compatible amb els estàndards en dispositius IoT **sense superar els llindars típics de 32kB de memòria RAM i 128kB de memòria flash**. (*Zandberg, K. et al.*, 2019)

Plataformes *IoT*

Hi ha diverses plataformes de núvol *IoT* al mercat actualment proporcionades per diferents proveïdors de serveis que acullen múltiples aplicacions. A més es poden estendre a serveis que fan servir algoritmes avançats d'aprenentatge per a anàlisis predictius, com pot-ser la prevenció de desastres i recuperació de la planificació mitjançant dades dels dispositius de finals.

Hi ha diversos **tipus** de plataformes *IoT* segons l'oferta del mercat:

- Plataforma de núvols *IoT* sobre de **núvols genèrics**: *Microsoft*, *Amazon*, *Google* o IBM.
- Plataforma de núvols *IoT* amb un enfocament **intensiu en connectivitat** de xarxa: *AT&T*, *Vodafone* i *Verizon*.
- Plataforma de núvols *IoT* que s'**integren de manera vertical** per a indústries específiques com pot-ser petroli, gas, la logística, el transport, etc: *GE Predix*.
- Plataforma de núvols *IoT* **oferides pels propis fabricants** de dispositius com és el cas de *Samsung* amb *ARTIK Cloud*.
- Plataforma de núvols *IoT* oferides per **grans empreses** amb recolzament borsari: *AWS IOT, Google Cloud IoT, Microsoft Azure IoT Suite, IBM Watson IoT*.
- Plataforma de núvols *IoT* amb llicències de **codi obert**: *Kaa Platform, Macchina Platform, SiteWhere Platform, ThingSpeak Platform*.
- Plataforma de núvols *IoT* amb integració amb *Arduino*, *Raspi* i altres plataformes de maquinari **fes-ho tu mateix**: *Carriots Platform, Initial State Platform, LOSANT Platform, MyDevices Cayenne Platform, Temboo Platform, Ubidots Platform*.
- Plataforma de núvols *IoT* **punta a punta** dissenyades des de la base del maquinari subministrat: *Samsara Platform, B+B SmartWorx (Acquired by Advantech), Particle Cloud*.

Les **característiques** típiques inclouen la **connectivitat i la gestió de xarxa, la gestió de dispositius, l'adquisició de dades, l'anàlisi i la visualització de processament, l'activació d'aplicacions, la integració i l'emmagatzematge**, veure taula 3.

Cal destacar que el núvol per a *IoT* té **3 maneres** de poder fer-se servir:

- **Infraestructura com a servei** (***IaaS***).
- **Plataforma com a servei** (***PaaS***): *Predix GE, Honeywell's Sentience, Siemens's MindSphere, Bosch IoT*, etc.
- **Programari com a servei** (***SaaS***): El catalitzador industrial de Siemens al núvol pot-ser un exemple.

Sistemes operatius incrustats

Molts petits dispositius *IoT* porten instal·lat un sistema operatiu incrustat. Aquest tipus de sistema operatiu està dissenyat normalment per ser **eficient i fiable en recursos**. Segons el mètode utilitzat per la multitasca, aquest tipus de sistemes operatius es considera freqüentment un sistema operatiu en **temps real**.

El maquinari que executa un sistema operatiu incrustat pot ser molt limitat en recursos com la *RAM*, *ROM* i *CPU*. A diferència d'un sistema operatiu d'escriptori, el sistema operatiu incrustat acostumen a no carregar i executa aplicacions. Això significa que el sistema només pot executar una sola aplicació. Es poden trobar disponibles uns quants: *TinyOS, Contiki, Mantis, Nano-RK, LiteOS, FreeRTOS*, etc.

Frontera	Connexió i gestió de sistemes	Informació i Acció
Gestió de dispositius / usuaris	Connectors al núvol	Taulers comandament/visualitzacions/aplicacions
Funcions i permisos	Lògica d'esdeveniments / Alertes	Constructors d'aplicacions
Porta d'accés al núvol local	Subscripcions / Facturació	Mercats de dades
Adaptadors / *SDK* biblioteques	APIs	Aplicacions verticals clau en mà
Controls de seguretat i accés	**Actualitzacions firmware/programari *OTA***	Anàlisis predictius / prescriptius
Gestió de la identitat	Emmagatzematge / Hosting d'aplicacions	Interfície de veu / Integracions AR/MR/VR

Funcions comunes de la plataforma IoT (Harwood, 2019). Taula 3

2.4 Seguretat *IoT*

Abans de passar a les conclusions caldria parar-nos a mira l'ecosistema *IoT* des d'un punt de vista de la **seguretat**, de manera més concreta **mirant els dispositius *IoT* amb implicacions sobre les vulnerabilitats d'un firmware desactualitzat**.

Hi ha una gran quantitat de **tipus d'atacs** que es poden perpetrar contra un sistema d'informació però en concret per a demostrar la hipòtesi del treball interessa els que **impliquen a dispositius *IoT*** i sent més concrets als que fans servir com a **vector d'atac el seu firmware** i encara sent més concret que estigui **desactualitzat** o afecta directament al **mecanisme d'actualització**. Tot seguit es dona un cop d'ull als escenaris més significatius.

Per exemple, és important la capacitat d'un dispositiu *IoT* de rebre actualitzacions (per exemple ***OTA***) és fonamental per resoldre **vulnerabilitats**. Aquest tipus d'actualitzacions proporcionen als fabricants de dispositius tecnològics, integradors de sistemes i operadors de solucions *IoT* els mitjans per implementar noves funcionalitats als seus productes al llarg del temps i també corregir qualsevol vulnerabilitat del dispositiu. Les actualitzacions actuen immediatament per mantenir la implementació **robusta** i garantir la **protecció de dades**.

Les actualitzacions d'*OTA* també **redueixen els costos de manteniment**. Es pot fer un desplegament d'actualització per fases i no hi ha limitacions quant a quants podeu alliberar per any. En proporcionar un servei provat i preparat per al llançament i alliberar funcions addicionals mitjançant *OTA* quan s'hagin solucionat els errors, obtindreu temps en el procés de programació.

2.4.1 Un escenari d'atac crític

Tal com es mostra a la figura 7, el primer pas és recopilar informació a la xarxa sobre els diferents dispositius IoT utilitzats a l'empresa. Un cop identificat i seleccionat un dispositiu *IoT*, l'**atacant recopila informació específica sobre les seves vulnerabilitats**. El següent pas és **explotar les diferents vulnerabilitats** que es troben en aquest dispositiu i **comprometre la xarxa**.

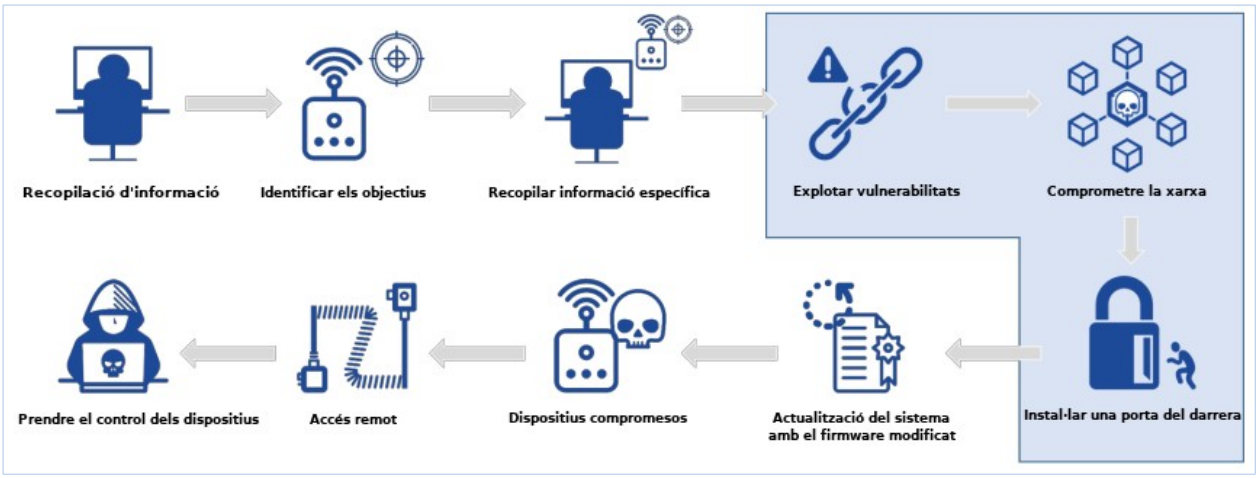

Figura 7: Atac i sistema d'administració IoT compromès (adaptat *ENISA*, 2017).

Després d'això, l'**atacant assegura la persistència de l'accés al sistema** mitjançant la configuració d'una **porta posterior**. En aquest moment, l'atacant només necessita actualitzar el

sistema (per exemple, amb un **firmware modificat**) perquè el dispositiu es vegi compromès definitivament. D'aquesta manera, l'atacant obté un **control total sobre el dispositiu**: obté la capacitat de veure totes les dades i informació que el dispositiu ha recopilat i **té accés remot** per utilitzar sempre que vulgui, etc.

PASSOS D'UN ATAC (MOSTRA BASAT EN UN ESCENARI D'ATAC D'UN CAS REAL)
1. Recopilació d'informació sobre la infraestructura
2. Identificació dels components del sistema
3. L'agredit recull més informació per identificar el sistema vulnerable. S'identifica el sistema vulnerable
4. Explotació de vulnerabilitats per comprometre primer el sistema i després a través del sistema la xarxa
5. S'instal·la una porta del darrere per tal de mantenir l'accés a aquest sistema
6. L'atacant assegura que els sistemes IoT s'actualitzen amb el firmware modificat ja sigui baixant i actualitzant l'instant el firmware o bé modificant el dipòsit de fitxers d'actualització. Això es fa per concedir a l'atacant accés exclusiu i restringir altres accessos remots
7. S'instal·la una porta del darrere per tal de mantenir l'accés a aquest sistema
8. Finalment, l'atacant pren el control sobre l'entorn IoT

Atac i compromís del sistema d'administració *IoT (ENISA, 2017)*. Taula 4

2.4.2 Atacs basats en l'actualització del firmware

Són importants els **mecanisme d'actualització de firmware segur integrat**. Tanmateix, sense aquest mecanisme, les vulnerabilitats de seguretat crítiques no poden ser solucionades i **els dispositius IoT poden convertir-se en una responsabilitat permanent**, com demostren els atacs a gran escala (*botnets*).

El botnet ***Mirai***, per exemple, va demostrar que els atacs a gran escala de *DDoS* que utilitzen **dispositius *IoT* compromesos amenacen altres infraestructures de comunicació**. És igualment alarmant que molts d'aquests dispositius *IoT* compromesos **no estiguin equipats amb un mecanisme d'actualització del firmware** i, per tant, continuen sense apedaçar fins avui dia. Això mostra la necessitat d'un mecanisme d'actualització de firmware en dispositius *IoT* en desenvolupar el producte. Si es dissenyen de forma **incorrecta**, **les actualitzacions del firmware poden convertir-se en vectors d'atac**.

Tenint en compte l'actualització de firmware com a vector d'atac, cal saber que (*Zandberg, K. et al.*, 2019):

- Les actualitzacions del firmware *IoT* d'*IETF* (*Internet Engineering Task Force*) per al grup de treball *Internet of Things* (***SUIT, Software Updates for Internet of Things***) especifiquen una arquitectura de fons senzilla per l'autenticació i la protecció de la integritat, fins i tot quan s'emmagatzemen actualitzacions en dipòsits no fiables, les especificacions del *SUIT* **permeten xifrar la imatge del firmware** per protegir-se dels atacs basats en enginyeria inversa.
- Un atacant pot intentar **actualitzar el dispositiu *IoT* amb una imatge de firmware modificada i defectuosament** de manera intencionada. Es pot prendre mesures, hi ha configuracions d'actualització que fan servir **signatures digitals per assegurar la integritat tant del firmware** com de les seves metadades. A més, el dispositiu pot verificar que un **mantenidor autoritzat va signar la imatge del firmware**.
- Un atacant pot intentar reproduir un **firmware vàlid, però antic**. Aquesta amenaça es veu mitgada mitjançant l'ús d'un **número de seqüència**.
- Un atacant pot intentar **substituir una actualització de firmware que sigui autèntica, però per a un dispositiu incompatible**.
- Un atacant pot intentar enganyar el dispositiu *IoT* per fer **flash el nou firmware a la ubicació equivocada de la memòria**.
- Un atacant pot intentar **explotar una vulnerabilitat derivada d'un desajust entre el programari prèviament instal·lat i el nou firmware**.
- Un atacant la pot **capturar la imatge del firmware en transmissió** per a l'anàlisi de la vulnerabilitat.
- En intentar **reiterades actualitzacions de firmware fraudulentes, un atacant pot esgotar la bateria del dispositiu**.
- Els atacs basats en programari, com els **atacs de desbordament de memòria intermèdia**, coneguts des del món de l'escriptori, també són molt probables que augmentin a la *IoT*. **Cal treballar més sobre l'aïllament de la memòria i la compartimentació** perquè els sistemes operatius *IoT* més populars ofereixen mecanismes d'aïllament. Els atacs basats en maquinari fa parar atenció a l'anàlisi del canal lateral, però també a components exposats, com ara la **flaix fora de xip o els ports de depuració que queden sense protecció**.

2.5 *Conclusions* rellevants per aquest treball

Aquesta secció fa un procés de documentació i maduració per intentar arribar **demostrar les hipòtesis d'aquest treball**, que cal recordar són:

- **Els dispositius *IoT* són molt més vulnerables que els dispositius tradicionals d'Internet**.
- **Els dispositius de *IoT* tenen un firmware més desactualitzat que la resta d'elements connectats a Internet.**
- **Els dispositius de IoT són molt vulnerables a ciberatacs a partir de l'anàlisi dels riscos associats a tenir software no actualitzat.**
- **Millorar la situació de vulnerabilitat de la IoT.**

2.5.1 Conclusions

Al llarg de l'exposició, feta fins ara, es pot situar-se en l'escenari que representa l'ampli ecosistema *IoT*. Aquesta **afirmació** queda recolzat per:

- El món de la *IoT* sustenta una amplia taxonomia d'actius que es tradueix en una gran diversitat de dispositius *IoT*.
- Entre els dispositius, de l'ecosistema *IoT,* més crítics segons els experts es pot trobar i per aquest ordre: sensors, dispositius de xarxa, protocols de comunicació, passarel·les, serveis, actuadors, etc. Es pot veure que els dispositius propis *IoT* són els més crítics.
- Les arquitectures *IoT* són complexes a causa de l'escala, l'heterogeneïtat dels dispositius, la connectivitat implicada, la seguretat del sistema, l'escalabilitat, la disponibilitat i la flexibilitat.
- L'arquitectura IoT normalment està definida en 4 etapes, de les quals els dispositius propis IoT es troben entre l'etapa 1 i l'etapa 2.
- Els dominis d'aplicació de la *IoT* són molt amplis, cosa que també fa molt divers el tipus de dispositius *IoT* que es poden trobar.
- Hi ha una gran quantitat de protocols de comunicacions que es poden veure involucrats els dispositius IoT: cablejats, sense fil, basats o no en IP, xarxes d'àrea ampla, local o personal, tots els nivells de la pila *OSI* estan involucrats, etc.

- El programari que es fa servir en l'ecosistema IoT és molt divers: middleware, firmware, plataformes *IoT* (núvols), sistemes operatius, etc.
- Implementar una solució d'actualització de firmware en dispositius IoT necessita de 32kB de memòria RAM i 128kB de memòria flash.
- Les vulnerabilitats del firmware *IoT* representa que és un vector d'atac tant pel mateix sistema com per la tot Internet.
- Els sistemes d'actualitzacions de firmware IoT també és objectiu d'atacs on l'atacant cerca les seves vulnerabilitats.

Es pot concloure que donat la limitada quantitat de recursos disponibles que els dispositius IoT acostumen a tenir, la gran diversitat d'aquests, l'arquitectura per nivells complexa i desplegada per una àrea extensa, la falta de mecanismes d'actualitzacions robustos amb una infraestructura per criptografia. També la diversitat de protocols de comunicacions, de programari i sistemes operatius que es fan servir. Es pot deduir que són molt més vulnerables que els dispositius tradicionals d'Internet.

Ara caldria reafirmar amb dades extretes de la realitat aquestes afirmacions.

3. Elaboració d'estadístiques

Per a l'elaboració d'estadístiques cal fer servir un seguit d'eines avui dia disponibles que permeten captar dades dels diferents dispositius connectats a Internet. L'**objectiu és poder comprovar les versions de software en general i les versions de firmware en particular** dels diferents tipus de dispositius de l'extens univers del Internet de les cosses.

Això presenta tot un seguit d'**objeccions** doncs:

- Se sap quan fas una prospecció amb una d'aquestes eines si pots arribar a tot l'univers de de la mostra que idealment seria tots els dispositius d'un tipus determinat connectats a alguna xarxa.
- En qualsevol cas es pot obtenir les dades, de la versió de firmware per exemple, d'un dispositiu que es detecti a la xarxa. Pot l'administrador del sistema emmascarar d'alguna manera aquestes dades.
- Pot-ser que la prospecció sigui objecte de «l'engany» d'un *honeypot*?
- També fa pensar sobre l'objectiu dels dispositius que es contemplen doncs dels no se sap si els detectats es troben en producció es fan servir per a entrenament formant part d'un *lab* per exemple.

A la següent secció es tornarà a fer esment d'aquest tipus de consideracions davant la prospecció de resultats.

3.1 Alternatives de software per cerca estadístiques de dispositius

Avui dia hi ha tot un seguit d'eines per a poder fer prospeccions i estadístiques del dispositius connectats a xarxa. Aquest munió d'eines que es poden trobar ara es pot fer molts tipus de classificacions, per exemple atenent a si són eines *open sources* o són propietàries, també si són tipus web o aplicacions per a instal·lar, i molts altres criteris de classificació.

Després de consultar diferents llocs web que es poden veure reflectits a la bibliografia, penso que es pot classificar en dos tipus d'eines principals atenent a les característiques de les eines que he pogut explorar, unes són del tipus ***escàner de vulnerabilitats*** i les ***web-escàner***.

Cercador	Descripció
Acunetix	Escàner de seguretat en línia d'aplicacions en línia automatitzat i totalment configurable que permet escanejar llocs web, aplicacions web i serveis web i identificar els defectes de seguretat.
Burp Suite	Cobertura de més de 100 vulnerabilitats genèriques, com ara la injecció *SQL* i *cross-site scripting (XSS)*, amb un gran rendiment contra totes les vulnerabilitats del top 10 de *OWASP*.
Censys	Plataforma que ajuda a la seguretat de la informació a descobrir, supervisar i analitzar dispositius accessibles des d'Internet.
IVRE	Framework de codi obert per a l'anàlisi de xarxa. Usa eines codi obert (Nmap, Masscan, ZGrab2, ZDNS i Zeek) per recollir dades i emmagatzemar-les en base de dades (MongoDB recomanat).
Nessus	Programa d'escaneig de vulnerabilitats per a diversos sistemes operatius. Consisteix en un dimoni, *nessusd*, que fa l'escaneig al sistema destí.
Nikto	Escàner de vulnerabilitat de la línia de comandes de programari lliure que explora els servidors web per trobar fitxers/CGI perillosos, programari de servidor desfasat i altres problemes.
OpenVAS	Escàner de vulnerabilitat, es va bifurcar des de l'última versió gratuïta de Nessus. Els plugins d'OpenVAS continuen escrits en el llenguatge NASL de Nessus.
PunkSPIDER	És un motor de cerca de vulnerabilitat web d'abast global dirigit a aplicacions web. Permet a l'usuari determinar les vulnerabilitats dels llocs web d'Internet de manera ràpida, fàcil i intuïtiva.
Shodan	És un motor de cerca que permet a l'usuari trobar, gràcies a l'especificació per filtres, diferents tipus d'equips (routers, servidors, etc.) connectats a Internet.
Skipfish	És una eina activa de reconeixement de seguretat d'aplicacions web. Prepara un mapa del lloc interactiu per al lloc objectiu mitjançant la realització de rastreig recursiu i basada en el diccionari.
W3af	És un framework popular, potent i flexible per trobar i explotar les vulnerabilitats d'aplicacions web. És fàcil d'utilitzar i ampliar i inclou desenes de plugins d'avaluació i explotació web.
Zed Attack Proxy	És un escàner de seguretat d'aplicacions web de codi obert. Està pensat per ser utilitzat tant per aquells nous a la seguretat de l'aplicació com pels provadors de penetració professionals.
ZoomEye	Motor de cerca desenvolupat per *Knownsec Inc*. Fa servir *Xmap* i *Wmap* en el seu nucli fonamental per agafar dades de dispositius i web exposats públicament i fer anàlisis *fingerprint*.

Motors de cerca i escaneig de dispositius a *Internet* (*sectools.org*, 2020). Taula 5

Els dos tipus, ***escàner de vulnerabilitats*** i ***web-escàner***, tenen el mateix fi. Uns són instal·lables i els altres són més còmodes doncs fan el rastreig des d'una web en línia.

Un característiques que s'ha de tenir en compte a l'hora de seleccionar aquestes eines és que unes estant més enfocades per exemple als sistemes operatius, altres a la inspecció de xarxes, altres tenen interfície gràfica, altres poden accedir des de línia d'ordres, altres tenen disponibles una API per a integrar amb diferents llenguatges de programació, moltes són un hibrid de totes aquestes característiques.

Després de consultar, fer algunes proves i experiència prèvia en aquest tipus d'eina m'he decidit per ***Shodan***, principalment per la seva popularitat i per que sembla que la que s'acobla més a les necessitats del treball.

3.1.1 *Shodan*

Aquest popular motor de cerca web que permet a l'usuari trobar tipus específics de hosts, com a càmeres web, routers, servidors i altres, connectats a Internet mitjançant diversos filtres. També descrit com un motor de cerca de *banners* de serveis, que són metadades que el servidor envia de tornada al client. Aquesta informació pot-ser sobre el programari del servidor, quines opcions admet el servei, missatges de benvinguda o qualsevol altra cosa que el client pugui descobrir abans d'interactuar amb el servidor.

Shodan aconsegueix dades principalment en serveis com:

- Web *HTTP/HTTPS* - ports 80, 8080, 443 i 8443
- *FTP* port 21
- *SSH* port 22
- *Telnet* port 23
- *SNMP* port 161
- *IMAP* ports 143, (xifrat) 993
- *SMTP* port 25
- *SIP* port 5060
- Reproducció en temps real, *RTSP* port 554 i molt més.

Modes de consultes *Shodan*

Permet fer consultes de 3 formes diferents:

- Consulta **web** a la mateixa adreça *www.shodan.io* com es veu a la *Figura 8*.
- Consulta per **línia d'ordes** (*CLI, Command-Line Interface*) que exposa la major part de l'*API* de manera fàcil d'utilitzar, de manera que podeu accedir a la base de dades de *Shodan* sense necessitat d'escriure els vostres propis scripts.
- Una ***API*** (*Application Programming Interface*) que inclou *Shodan Images* i *Shodan Maps*. Qualsevol cosa que es pugui fer mitjançant aquests llocs web també es pot fer directament

mitjançant l'API per a diferents llenguatges de programació: *C#, Go, Haskell, Java, Node.js, Perl, PHP, Python, PowerShell, Ruby* i *Rust*.

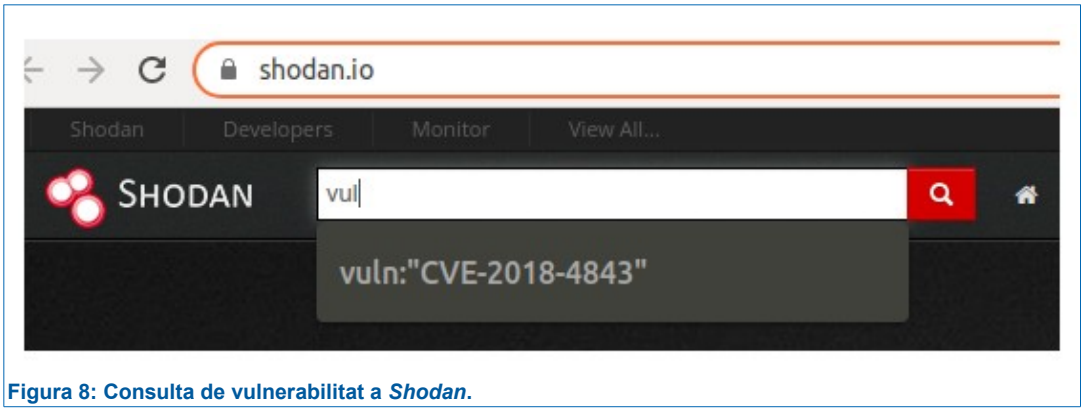

Figura 8: Consulta de vulnerabilitat a *Shodan*.

Operar amb *Shodan*

Després de fer diverses proves m'ha semblat que la millor manera d'**interactuar amb *Shodan* és fer servir la línia d'ordres**. En aquest cas el primer es **registra-se** a la web de *Shodan* per a tindre una **clau** que donen una vegada inscrit per a poder activar la *CLI* de *Shodan*.

```
X □ –  root@debian:~
root@debian: shodan -h
Usage: shodan [OPTIONS] COMMAND [ARGS]...

Options:
  -h, --help  Show this message and exit.

Commands:
  alert       Manage the network alerts for your account
  convert     Convert the given input data file into a different format.
  count       Returns the number of results for a search
  data        Bulk data access to Shodan
  domain      View all available information for a domain
  download    Download search results and save them in a compressed JSON...
  honeyscore  Check whether the IP is a honeypot or not.

      .........          .          .          .         ..........

  search      Search the Shodan database
  stats       Provide summary information about a search query
  stream      Stream data in real-time.
  version     Print version of this tool.
root@debian: shodan count  Cisco Catalyst
2246
root@debian:
```

Figura 9: Consultes *Shodan*, *help* i contar ocurrències de *Cisco Catalyst*.

Una vegada instal·lada i provada cal establir una tàctica per fer l'operativa per a poder elaborar unes estadístiques amb comoditat. Un cop he provat diverses maneres de fer la millor metodologia ha estat:

1. Baixar-se les consultes a un fitxer local.
2. Convertir el format del fitxer en un full de càlcul.
3. Consultar i filtrar les dades al mateix full de càlcul per extreure les estadístiques.
4. Reflectir les dades en fitxes per poder presentar-ho de manera clara.
5. Intentar extreure conclusions i enfrontar-ho amb la hipòtesi inicial.

```
X □ –  root@debian:~
root@debian: shodan download --limit 10000 /home/admin/resultats/scada-data scada
Search query:          scada
Total number of results:   5236
Query credits left:        0
Output file:           /home/admin/resultats/scada.json.gz
  [------------------------------------]    1%  14:59:17
Notice: fewer results were saved than requested
Saved 100 results into file /home/admin/resultats/scada-data.json.gz


root@debian: shodan convert /home/admin/resultats/scada-data.json.gz xlsx
Successfully created new file: /home/admin/resultats/scada-data.xlsx
root@debian:
```

Figura 10: Consultes *Shodan mitjançant CLI* sobre *Scada* I conversió de fitxer a full de càlcul.

scada-data.json


```
{"_shodan": {"id": "e2cb5d2c-3cd7-43ca-bf7b-4a6944267b5b", "options": {}, "ptr": true, "module":
"http", "crawler": "97b9d37f0484f45ce645307121c5c1ce0b3db578"}, "hash": 1176729728, "os": null,
"opts": {}, "ip": 1426742753, "isp": "Orange Belgium", "http": {"robots_hash": null, "redirects":
[], "securitytxt": null, "title": null, "sitemap_hash": null, "robots": null, "server":
"CirCarLife Scada v4.2.3", "host": "85.10.93.225", "html": "", "location": "/", "html_hash": 0,
"sitemap": null, "securitytxt_hash": null}, "port": 80, "hostnames": ["eu85-10-93-
225.adsl.euphonynet.be"], "location": {"city": null, "region_code": null, "area_code": null,
"longitude": 4.3447, "country_code3": null, "country_name": "Belgium", "postal_code": null,
"dma_code": null, "country_code": "BE", "latitude": 50.8509}, "timestamp": "2020-05-
24T15:40:38.824898", "domains": ["euphonynet.be"], "org": "Orange Belgium", "data": "HTTP/1.1 307
Temporary Redirect\r\nServer: CirCarLife Scada v4.2.3\r\nConnection: keep-alive\r\nDate:Sun, 24
May 2020 15:40:37 GMT\r\nContent-Length: 0\r\nLocation: html/setup.html\r\n\r\n", "asn":
"AS47377", "transport": "tcp", "ip_str": "85.10.93.225"}
{"_shodan": {"id": "85d37dce-c5ca-4ea3-ad17-b38fbf36182b", "options": {}, "ptr": true, "module":
"http-simple-new", "crawler": "65683fa99d390e0163b89adb344e9233c7422efb"}, "hash": -1560069107,
"os": null, "opts": {}, "ip": 795290299, "isp": "Hangzhou Alibaba Advertising Co.,Ltd.", "http":
{"html_hash": -568628488, "robots_hash": null, "redirects": [], "securitytxt": null, "title":
null, "sitemap_hash": null, "robots": null, "favicon": null, "host": "47.103.42.187", "html": "<!
DOCTYPE html>\n<html dir=\"ltr\" ·····························
```


Figura 11: Fitxer que proporciona les dades de *Shodan* en processador de text.

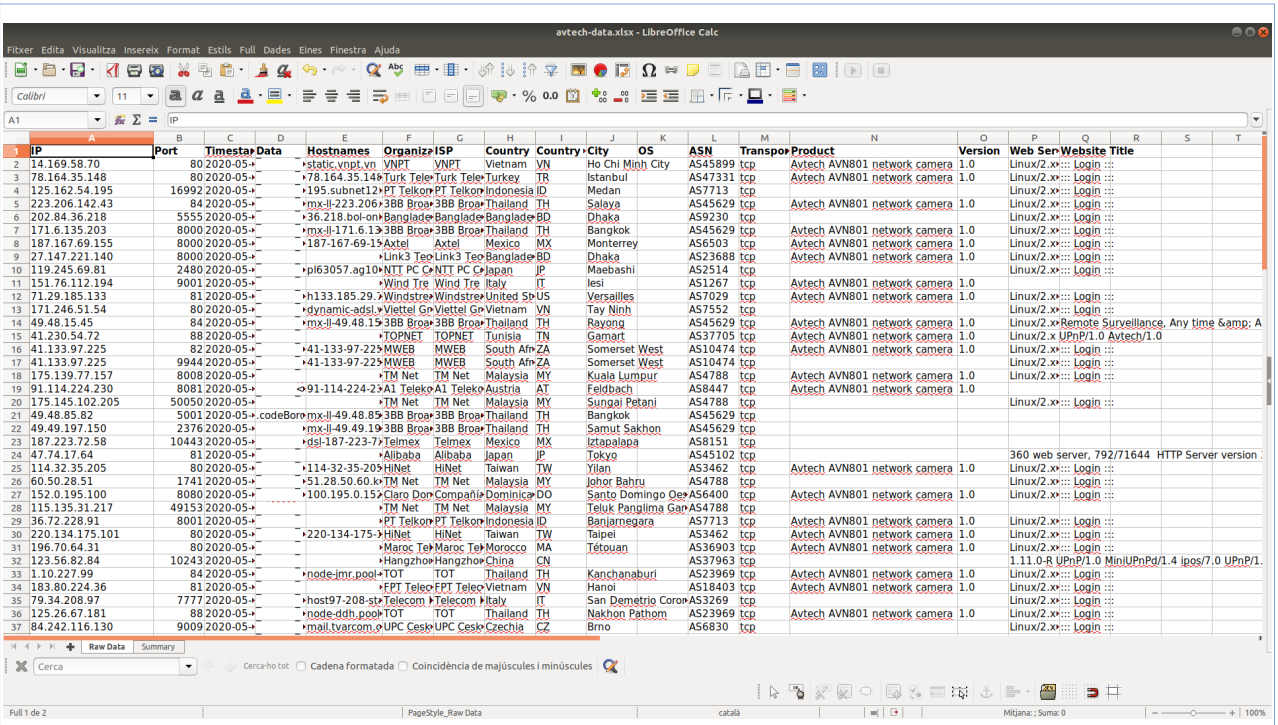

Figura 12: Full de càlcul d'una consulta *Shodan*.

A les figures 10, 11 i 12 es pot veure com s'ha dut a terme el procés de consultes de *Shodan*. Hi ha més possibilitats doncs la *CLI* té moltes més possibilitats com a un ***parse*** i/o fer servir eines externes per a tractar les dades però aquesta manera és la que per a mi va ser més àgil.

Restriccions de *Shodan*

Tot i crear un compte a *Shodan*, aquesta marca té instaurat un **sistema de crèdits** els quals donen accés a tindre un nombre més gran de resultats i a crear uns filtres més sofisticats per a fer les cerques.

Amb un perfil creat no tens cap crèdit assignat, cal pagar per a poder aconseguir crèdits. Hi ha uns plans als quals et pots acollir per a escalar crèdits que es renoven mensualment.

En cas de tindre crèdit 0 com és el meu cas reps un **màxim de 100 resultats** tot i mostrar, com es veu a la *Figura 10*, el nombre total de resultats trobats. L'altre gran restricció és que **els filtres que pots configurar són molt pobres**.

3.1.2 Altres consideracions

Hi ha dubtes dels diferents dispositius a que pot arribar *Shodan* a extreure informació. Per una banda no dona tot el llistat de dispositius trobats, si no tens crèdit, amb un màxim de 100.

Tampoc saps amb quin criteri fa les cerques, sobretot quan estàs limitat amb els filtratge que pots fer. Hi ha altres consideracions que cal tenir en compte.

Xarxes privades *Ipv4* i *Ipv6*

A l'espai d'adreçament *Ipv4* fa molt de temps que no és suficientment gran per a tenir disponibles suficients adreces públiques per a tothom. Per aquest motiu fa temps, definit a la *RFC 1918* tres rangs d'adreces privades, es pot veure a la *Figura 13*, que juntament amb el mecanisme *NAT* (*Network Address Translation*) aconsegueix resoldre aquest problema.

El que té com a conseqüència col·lateral és que aquest mecanisme aïlla i dona seguretat les xarxes per exemple d'una empresa, d'una institució o de casa doncs des de fora, la part pública d'Internet, no es pot «veure» els dispositius amb les seves adreces privades. Només aquests dispositius quan obre un port i connecten amb un client extern a la xarxa es poden accedir a ells, també pot valdre un redireccionament de ports.

Classe	Rang d'adreces reservades *RFC 1918*
A	de **10.0.0.0** a **10.255.255.255**
B	de **172.16.0.0** a **172.31.255.255**
C	de **192.168.0.0** a **192.168.255.255**

Figura 13: Rang d'adreces privades IPv4.

Un tipus de direcció de unidifusió és l'adreça de **unidifusió local única**. Les adreces *IPv6* locals úniques tenen certes similituds amb les adreces privades *RFC 1918* per *IPv4*, però hi ha grans diferències. Les adreces locals úniques s'utilitzen per l'adreçament local dins d'un lloc o entre una quantitat limitada de llocs. Aquestes adreces no haurien de poder enrutar-se a la *IPv6* global, i no haurien de traduir-se cap a adreces *IPv6* globals. Les **adreces locals úniques *Ipv6*** estan en el rang de ***FC00 :: / 7*** a ***FDFF :: / 7***.

Com a resum, els **dispositius, instal·lats en aquestes xarxes privades, si tenen contacte amb les xarxes públiques (*Internet*) però o ells prenent la iniciativa en una connexió o hi ha un redireccionament de ports fet exprofessor per l'administrador del sistema. En altre cas veig difícil que *Shodan* pugui contactar** per extreure informació.

Firewall

Una altre factor a tenir en compte és l'ús d'un tallafoc per part de l'empresa o institució on estigui localitzat el dispositiu. Aquest tallafoc acostuma a estar configurat per evitar l'entrada de **paquets mal formats** o el **rastreig de ports**. Hi ha 2 possibilitats no excloents:

- Configurar un **firewall perimetral** (de xarxa) per evitar descartar transit maliciós abans que arribi a la tarja dels servidor.
- Configurar **firewall local** al mateix servidor per a que no respongui a pings, segments i paquets mal formats.

Cal pensar que el tallafoc si té la capacitat es pot configurar amb **inspecció en profunditat**, cosa que els habilita per a veure les dades que porten els paquets i inclús ressemblar els paquets *IP* (*flag MAS*).

Altres tipus d'interferències

Altres consideracions que poden tindre afectacions amb les dades obtingudes per *Shodan* són:

- **No fer servir *Ipv4*** (substituir per *Ipv6*) per a eliminar les difusions, en particular, les **difusions *ARP*** i les adreces *MAC* d'on provenen.
- Fer servir ***VLANs*** als segments *Ethernet* de la xarxa LAN.
- Fer servir llibreries com a ***AntiSamy*** (*OWASP*) que s'encarrega de processar codi *html* i verificar si està permès o per contra és un possible intent d'intrusió.
- Fer servir **encriptació** amb *SSL/TLS*.
- Fer servir ***IDS*** *(Intrusion Detection System)*, hi ha de diversos tipus segons que controlen o quines tècniques fan servir. La col·locació de l'*IDS* és molt significativa pel seu èxit de resultats sobre tot si estan sincronitzats amb el tallafoc.

3.2 Proves i obtenció de resultats

Tot seguit es mostren en format de fitxa les dades obtingudes en la bateria de proves fetes amb *Shodan*. A les diferents cerques s'han obtingut dades principalment de software com firmware (objectiu principal), sistemes operatius (lleugers per a *IoT*), aplicacions d'explotació de dades *IoT*, protocols (tipics de *IoT*) i servidors (com a interfície de sistemes *IoT*). Les fitxes són les següents:

1 – *Siemens S7*

Descripció:

Siemens SIMATIC S7 és una sèrie de **controladors lògics programables** i sistemes d'automatització, desenvolupats per *Siemens*. Presentada el 1958, la sèrie ha passat per 4 grans generacions, l'actual és la ***Simatic* S7**, destinada a la producció i automatització industrials.

Suport producte:

https://support.industry.siemens.com/cs/products?mfn=ps&pnid=20055&lc=en-SA

Domini:

Sistemes de control industrial. Dispositius controladors lògics programables. *IoT* d'etapa 2.

Tipus software:

Es tracta del **firmware** dels dispositius tipus controlador lògic programable de *Siemens*.

Estadístiques:

Univers: *Shodan*: 997 resultats, permet 100 registres (banners) **Referències trobades:** 30 **Versió actual:** *V. 4 .4*

Versió	Núm. ocurrències	Versió	Núm. ocurrències	Versió	Núm. ocurrències
V.4.3.1	***3***	*V.4.2.0*	***3***	*V.3.0.2*	***1***
V.4.2.8	***1***	*V.4.1.3*	***3***	*V.2.6.0*	***1***
V.4.2.3	***3***	*V.4.1.1*	***1***	*V.2.2.0*	***1***
V.4.2.2	***5***	*V.4.0.0*	***2***	*V.1.5.1*	***1***
V.4.2.1	***3***	*V.3.2.14*	***2***		

Vulnerabilitats i exposicions comunes:

- CVE-2018-4843: Respondre a una sol·licitud de *PROFINET DCP* amb un paquet *PROFINET DCP* especialment dissenyat pot provocar una condició de denegació del servei del sistema sol·licitant. La vulnerabilitat de seguretat pot ser explotada per un atacant situat al mateix segment *Ethernet* (*OSI* capa 2) que el dispositiu objectiu. L'explotació amb èxit no requereix cap interacció ni privilegis dels usuaris i afecta la disponibilitat de la funcionalitat principal del dispositiu afectat.
- **CVE-2018-16561**: Les *CPU* afectades validen de forma inadequada els paquets de comunicació S7 que poden provocar una condició de denegació de la *CPU*. La *CPU* romandrà en mode *DEFECT* fins que es reinicïi manualment. L'explotació amb èxit requereix un atacant per poder enviar un paquet de comunicació S7 especialment dissenyat a una interfície de comunicació de la *CPU*.
- **CVE-2017-2680**: Es podria veure afectada per una condició de denegació de servei induïda per un paquet de transmissió *PROFINET DCP* especialment dissenyada (capa 2 - *Ethernet*).

Comentaris:

Totes les adreces subministrades són públiques *Ipv4* i com organització consten universitats.

Data prospecció: *10 / maig / 2020*

Consulta *Shodan* CLI *Siemens S7*. | Fitxa 1

2 – *SCADA*

Descripció:

El control de supervisió i adquisició de dades (*SCADA, Supervisory Control And Data Acquisition*) és una arquitectura de sistemes de control que inclou ordinadors, comunicacions de dades en xarxa i interfícies gràfiques d'usuari (*GUI*) per a la gestió de supervisió de processos d'alt nivell, alhora que inclou altres dispositius perifèrics com controladors lògics programables (*PLC*) i proporcionals discrets. La cerca concreta en el producte *CirCarLife* desenvolupat amb *Scada*.

Suport producte:

https://circontrol.com/mobility-solutions/scada-software/

Domini:

Sistemes de control industrial i domòtica. Dispositius controladors lògics programables. *IoT* d'etapa 2.

Tipus software:

Es tracta d'una **aplicació** *CirCarLife*, desenvolupat amb sistema *Scada* per a gestionar la càrrega de vehicles elèctrics.

Estadístiques:

Univers: *Shodan*: 5274 resultats, permet 100 registres (banners) **Referències trobades:** 93 **Versió actual:** *V4.3.0*

Versió	Núm. ocurrències	Versió	Núm. ocurrències	Versió	Núm. ocurrències
V4.3.0	***1***	*V4.2.4*	***4***	*V4.2.3*	***88***

Vulnerabilitats i exposicions comunes:

- **CVE-2018-12635**: *CirCarLife Scada v4.2.4* permet actualitzacions no autoritzades mitjançant sol·licituds als URIs html/upgrade.html i serveis/system/firmware.upgrade.

Comentaris:

Totes les adreces subministrades són públiques *Ipv4*. La majoria dels servidors trobats són multiservei.

Data prospecció: *11 / maig / 2020*

Consulta *Shodan* CLI *SCADA*. | Fitxa 2

3 – *Iomega*

Descripció:

Iomega ara *LenovoEMC*, és un productor de productes d'emmagatzematge extern, portàtil i en xarxa. La unitat *Zip* i *NAS* eren els productes més destacats. Per la captura del tipus de dades enfoquen el servidor de l'emmagatzematge.

Suport producte:

https://www.lenovo.com/es/es/systems/storage/nas/lenovoemc/

Domini:

Sistemes d'emmagatzematge d'informació. *IoT* d'etapa 3 i 4.

Tipus software:

Es tracta d'una **aplicació** tipus servidor de fitxer com *Samba*, *Apache* o *FTP*.

Estadístiques:

Univers: *Shodan*: 10632 resultats, 100 registres **Referències trobades:** 48 **Versió actual:** *Apache2.4.43 Samba4.10.16*

Versió	Núm. ocurrències	Versió	Núm. ocurrències	Versió	Núm. ocurrències
Apache1.3.42	***34***	*Apache2.4.12*	***5***	*Samba3.0.32*	***2***
Apache2.2.19	***23***	*Apache2.4.16*	***5***	*Samba3.5.6*	***4***

Apache2.4.7	***15***			*Samba3.5.14*	***3***

Vulnerabilitats i exposicions comunes:

- **CVE-2018-9076**: Per a alguns dispositius *Iomega*, *Lenovo*, *LenovoEMC NAS* versions 4.1.402.34662 i anteriors, quan canvia el nom d'un recurs compartit, un atacant pot crear una càrrega de injecció de comandes utilitzant caràcters "` `" enrere del paràmetre nom. Com a resultat, es poden executar ordres arbitràries com a usuari root. L'atac requereix un valor __c i un paràmetre iomega.
- **CVE-2019-6160**: Una vulnerabilitat en diverses versions dels productes *NAS Iomega* i *LenovoEMC* podria permetre a un usuari no autenticat accedir a fitxers de les accions de *NAS* mitjançant l'API.

Comentaris:

Totes les adreces subministrades són públiques *Ipv4*. La majoria dels servidors no mostren la versió.

Data prospecció: *11 / maig / 2020*

Consulta *Shodan* CLI *Iomega*. **Fitxa 3**

4 – *Avtech AVN801*

Descripció:

AVTECH avn801 HD càmera IP per a interiors de xarxa i Sensor PIR (1,3 megapíxels, Push vídeo).

Suport producte:

https://www.avtech.com.tw/EOL.aspx

Domini:

Càmera IP interior. *IoT* d'etapa 1.

Tipus software:

Es tracta de **firmware**.

Estadístiques:

Univers: *Shodan*: 146993 resultats, 100 registres **Referències trobades:** 51 **Versió actual:** ref. 3026

Versió	Núm. ocurrències	Versió	Núm. ocurrències	Versió	Núm. ocurrències
1.0	***51***				

Vulnerabilitats i exposicions comunes:

- **CVE-2013-4982**: *AVTECH AVN801 DVR* té un bypass de seguretat mitjançant el *captcha* d'inici de sessió d'administració.

Comentaris:

Totes les adreces subministrades són públiques *Ipv4*. Quasi tots utilitzen el servidor Linux/2.x UPnP/1.0 Avtech/1.0.

Data prospecció: *11 / maig / 2020*

Consulta *Shodan* CLI *Avtech*. **Fitxa 4**

5 – *Vertiv Avocent UMG-4000*

Descripció:

Vertiv Avocent UMG-4000 és un dispositiu de gestió convergent que permet la gestió remota de qualsevol dispositiu, en qualsevol ubicació, de qualsevol proveïdor, en qualsevol moment de forma segura i centralitzada.

Suport producte:

https://www.vertiv.com/es-emea/

Domini:

Sistemes d'administració remota de dispositius. *IoT* d'etapa 2.

Tipus software:

Es tracta del **firmware** dels dispositius *Vertiv Avocent UMG-4000*.

Estadístiques:

Univers: *Shodan*: 19 resultats, permet 100 registres (banners) **Referències trobades:** 12 **Versió actual:** *IS-UNITY_7.8*

Versió	Núm. ocurrències	Versió	Núm. ocurrències	Versió	Núm. ocurrències
IS-UNITY_6.6.0.0	***1***	*IS-UNITY_7.5.0.0*	***2***	*IS-UNITY_7.7.0.0*	***4***
IS-UNITY_7.3.0.0	***1***	*IS-UNITY_7.6.0.0*	***1***		

Vulnerabilitats i exposicions comunes:

- **CVE-2019-9509**: La interfície web del *Vertiv Avocent UMG-4000* versió 4.2.1.19 és vulnerable a XSS reflectida en un paràmetre HTTP POST. L'aplicació web no neutralitza l'entrada controlable per l'usuari abans de mostrar-la als usuaris en una pàgina web, cosa que podria permetre a un atacant remot autenticat amb un compte d'usuari executar codi arbitrari.
- **CVE-2019-9508**: La interfície web del *Vertiv Avocent UMG-4000* versió 4.2.1.19 és vulnerable a XSS emmagatzemats. Un atacant remot autenticat amb un compte d'administrador podria emmagatzemar un fitxer anomenat maliciosament a l'aplicació web que executaria cada vegada que un usuari navegués a la pàgina.
- **CVE-2019-9507**: La interfície web del *Vertiv Avocent UMG-4000* versió 4.2.1.19 és vulnerable a la injecció de comandaments perquè l'aplicació neutralitza de forma errònia la sintaxi de codi abans d'executar-la. Com que totes les ordres de l'aplicació web s'executen com a root, això podria permetre a un atacant remot autenticat amb un compte d'administrador executar ordres arbitràries com a root.

Comentaris:

Totes les adreces subministrades són públiques *Ipv4*.

Data prospecció: *11 / maig / 2020*

Consulta *Shodan* CLI *Vertiv Avocent UMG-4000*. | Fitxa 5

6 – *Zigbee*

Descripció:

Zigbee és un protocol de comunicacions sense cables via ràdio-freqüència (xarxa sense fil). Està dirigit al sector domèstic (domòtica), edificis terciaris (immòtica) i a ciutats (urbòtica: xarxa d'àrea metropolitana). *ZigBee* està basat en la norma *IEEE 802.15.4* i destinat a crear xarxes d'àrea personal de baixa potència i baixa velocitat de transmissió de dades.

Suport producte:

https://zigbeealliance.org/

Domini:

Domòtica. *IoT* d'etapa 1 i 2.

Tipus software:

Es tracta del **protocol** de comunicació que per exemple fan servir per exemple electrodomèstics.

Estadístiques:

Univers: *Shodan*: 41 resultats, permet 100 registres **Referències trobades:** 34 **Versió actual:** *V.1.6.8 estable*

Versió	Núm. ocurrències	Versió	Núm. ocurrències	Versió	Núm. ocurrències

V.1.4.10	***1***	*V.1.4.15*	***2***	*V.1.6.3*	***1***
V.1.4.12	***1***	*V.1.4.8*	***5***	*V.1.6.8*	***3***
V.1.4.14	***4***	*V.1.5.7*	***1***	*V.1.6.9*	***4***

Vulnerabilitats i exposicions comunes:

- **CVE-2020-7476**: Un *CWE-426*: La vulnerabilitat de la ruta de cerca no fidedigna existeix al kit d'instal·lació de ZigBee (versions anteriors a 1.0.1), que podria provocar l'execució de codi maliciós quan s'instal·la un fitxer maliciós a la ruta de cerca.
- **CVE-2019-20481**: A *MIELE XGW 3000 ZigBee Gateway* abans de 2.4.0, la funció de canvi de contrasenya no requereix el coneixement de la contrasenya antiga. Es pot aprofitar conjuntament amb *CVE-2019-20480*.

Comentaris:

Totes les adreces són públiques *Ipv4.* Moltes són *Mosquitto* una implementació del servidor *MQTT*.

Data prospecció: *12 / maig / 2020*

Consulta *Shodan* CLI *Zigbee*. **Fitxa 6**

7 – *Contiki*

Descripció:

Contiki és un sistema operatiu reduït, de codi obert publicat sota la llicència *BSD*, per a sistemes amb memòria escassa, com ara els sistemes encastats, sistemes en xarxa, etc. A més, és molt portable i està construït entorn a un kernel d'esdeveniments. Proporciona multitasca que pot ser utilitzada a nivell de processos individuals. Consumeix 2 KB de memòria *RAM* i 40 KB de memòria *ROM*.

Suport producte:

http://www.contiki-os.org/

Domini:

Dispositius amb **pocs recursos** que acostumen a estar desplegats. *IoT* d'etapa 1 i 2.

Tipus software:

Es tracta d'un **sistema operatiu** amb poques necessitats de recursos amb interfície gràfica i servidor web personal.

Estadístiques:

Univers: *Shodan*: 723 resultats, 100 registres **Referències trobades:** 81 **Versió actual:** *Contiki 3.0*

Versió	Núm. ocurrències	Versió	Núm. ocurrències	Versió	Núm. ocurrències
Contiki httpd 0.6.5	***9***	*Contiki httpd 1.14.0*	***1***	*Contiki httpd 2.4*	***71***

Vulnerabilitats i exposicions comunes:

- **CVE-2019-9183**: Es va descobrir un problema a *Contiki-NG* a 4.3 i *Contiki* a 3.0. Un desbordament de memòria intermèdia està present a causa d'un desembassament d'enters durant el processament de fragments *6LoWPAN* davant de fragments truncats a *os/net/ipv6/sicslowpan.c*. D'aquesta manera, s'accedeix a l'aplicació amb accessos de memòria no mapejada. Un atacant pot provocar una denegació del servei mitjançant un marc elaborat amb *6LoWPAN*.
- **CVE-2019-8359**: Es va descobrir un problema a *Contiki-NG* a 4.3 i *Contiki* a 3.0. Una escriptura fora de límit està present a la secció de dades durant el reassemblatge de fragments *6LoWPAN* davant de compensacions de fragments falsificats a *os/net/ipv6/sicslowpan.c*.

Comentaris:

Totes les adreces són públiques *Ipv4*. La majoria fan servir el servidor *Contiki httpd*.

Data prospecció: *12 / maig / 2020*

Consulta *Shodan* CLI *Contiki*. **Fitxa 7**

8 – *Yamaha AV Receiver*

Descripció:

Yamaha AV Receiver és un component d'electrònica de consum utilitzat en un home cinema. El seu propòsit és rebre senyals d'àudio i vídeo de diverses fonts, i processar-los i proporcionar amplificadors de potència per conduir altaveus i dirigir el vídeo a pantalles com un televisor, monitor o projector de vídeo. Les entrades poden provenir d'un receptor de satèl·lit, ràdio, reproductors de *DVD*, reproductors de discos *Blu-ray*, videoenregistrament o consoles de videojocs, entre d'altres.

Suport producte:

https://europe.yamaha.com/en/products/contents/audio_visual/downloads/firmware_software/index.html?k=&c=audio_visual

Domini:

Entreteniment llar, so professional. *IoT* d'etapa 2.

Tipus software:

Es tracta d'un **dispositiu** de lectura i reproducció de múltiples formats de música i vídeo, alguns fan servir un servidor *HTTP* com a interfície.

Estadístiques:

Univers: *Shodan*: 41 resultats, permet 100 registres **Referències trobades:** 34 **Versió actual:** *V.3.70*

Versió	Núm. ocurrències	Versió	Núm. ocurrències	Versió	Núm. ocurrències
V.3.0	***7***	*V.3.1*	***27***		

Vulnerabilitats i exposicions comunes:

- **CVE-2019-6113**: Vulnerabilitat del trànsit de directoris a *ONKYO TX-NR686 1030-5000-1040-0010* Els dispositius receptors *A/V* permet als atacants remots llegir fitxers arbitraris mitjançant un .. (punt punt) i % 2f a l'*URI* predeterminat.

Comentaris:

Totes les adreces són públiques *Ipv4*. Es troba servidors *HTTP*.

Data prospecció: *12 / maig / 2020*

Consulta *Shodan* CLI *Yamaha AV Receiver*. | Fitxa 8

9 – *Omron CJ2M-CPU33*

Descripció:

Omron CJ2M-CPU33 és un *Programmable Logic Controllers* (*PLC*), autòmat industrial dissenyat per controlar processos seqüencials. Es pot programar per l'usuari. Creat per controlar màquines, processos lògics i secundaris. Aquest dispositiu utilitza un programa lògic i pot realitzar diferents funcions -entre d'altres- com per exemple, recollir dades a través de les fonts d'entrada tant analògiques com digitals, fer càlculs matemàtics, prendre decisions a partir dels criteris preprogramats i actuar sobre dispositius externs enviant senyals analògics o digitals.

Suport producte:

https://industrial.omron.eu/en/products/CJ2M-CPU33

Domini:

Sistemes de control industrial. Dispositius controladors lògics programables. *IoT* d'etapa 2.

Tipus software:

Es tracta del **firmware** dels dispositius tipus controlador lògic programable de *Omron*.

Estadístiques:

Univers: *Shodan*: 234 resultats, permet 100 registres **Referències trobades:** 234 **Versió actual:** *02.01*

Versió	Núm. ocurrències	Versió	Núm. ocurrències	Versió	Núm. ocurrències
02.01	***132***	*02.00*	***99***	*01.20*	***3***

Vulnerabilitats i exposicions comunes:

- CVE-2020-6986: En totes les versions d'*Omron PLC CJ Series*, un atacant pot enviar una sèrie de paquets de dades específics en un curt període de temps, causant un error de servei al mòdul *Ethernet PLC*, que al seu torn fa que el servei *PLC* sigui denegat de resultats.
- CVE-2019-6556: En processar fitxers de projectes, l'aplicació (*Omron CX-Programmer v9.70* i versions anteriors i Components comuns de gener de 2019 i anteriors) no comprova si es fa referència a la memòria alliberada. Un atacant podria utilitzar un fitxer de projecte especialment elaborat per explotar i executar codi sota els privilegis de l'aplicació.
- CVE-2019-18269: A la sèrie *Omron PLC CJ*, totes les versions i a la sèrie Omron PLC CS, totes les versions, el programari comprova adequadament l'existència d'un bloqueig, però el bloqueig pot ser controlat externament o influenciat per un actor que es troba fora de l'esfera de control prevista.

Comentaris:

Totes les adreces són públiques *Ipv4*. És el *PLC* més popular de *Omron* (segons *Shodan*).

Data prospecció: *13 / maig / 2020*

Consulta *Shodan* CLI *Omron CJ2M-CPU33*. | Fitxa 9

10 – *Schneider Electric BMX P34 2020*

Descripció:

Schneider Electric BMX P34 2020 és un *Programmable Automation Controllers* (*PAC*) descriu qualsevol tipus de control d'automatització que incorpori instruccions de nivell superior. Els sistemes s'utilitzen en sistemes de control industrial (*ICS, Industrial Control Systems*) per a maquinària d'una àmplia gamma d'indústries, incloses les que participen en infraestructures crítiques. Fa servir *Modbus* és un protocol popular per als sistemes de control industrial (ICS). Proporciona un accés fàcil i cru al sistema de control sense requerir cap autenticació.

Suport producte:

https://www.se.com/ww/en/product/BMXP342020/processor-module-m340---max-1024-discrete-%2B-256-analog-i-o---modbus---ethernet/

Domini:

Sistemes de control industrial. Dispositius controladors lògics programables. *IoT* d'etapa 2.

Tipus software:

Es tracta d'un dispositiu de control i del **protocol** de comunicació ***Modbus*** que fa servir el *PAC* de *Schneider Electric*.

Estadístiques:

Univers: *Shodan*: 323 resultats, permet 100 registres **Referències trobades:** 323 **Versió actual:** *V3.20*

Versió	Núm. ocurrències	Versió	Núm. ocurrències	Versió	Núm. ocurrències
V2.9	***72***	*V2.6*	***46***	*V2.2*	***46***
V2.8	***28***	*V2.5*	***72***		

Vulnerabilitats i exposicions comunes:

- CVE-2015-6462: Cross-Site Scripting reflectit (no persistent) permet a un atacant crear un URL específic, que conté un script Java que s'executarà a *Schneider Electric Modicon BMXNOC0401, BMXNOE0100, BMXNOE0110, BMXNOE0110H, BMXNOR0200H, BMXP342020, BMXP342020, BMXP342020, BMXP342020, BMXP342020, BMXP342020, BMXP342020, BMXP342020H* o navegador de client *BMXP342030H PLC*.
- CVE-2015-6461: La inclusió de fitxers remots permet a un atacant crear un *URL* específic fent referència a *Schneider Electric Modicon BMXNOC0401, BMXNOE0100, BMXNOE0110, BMXNOE0110H, BMXNOR0200H,*

BMXP342020, BMXP342020H, BMXP342030, BMXP3420302, BMXP3420302, BMXP34H2020, BMXP34H20 el navegador redirigint a un fitxer remot mitjançant un script Java carregat amb la pàgina web.

Comentaris:

Totes les adreces són públiques *Ipv4*. Fan servir.

Data prospecció: *13 / maig / 2020*

Consulta *Shodan* CLI *Schneider Electric BMX P34 2020*.	Fitxa 10

11 – *Cisco Catalyst 4500 Series Switches*

Descripció:

Cisco Catalyst 4500 Series Switches és una família de commutadors (switch) de capa 2 més especific per a desplegar en campus tant cablejat com a suport per a sense fils..

Suport producte:

https://www.cisco.com/c/en/us/support/switches/catalyst-4500-series-switches/series.html

Domini:

Commutador de capa 2 per a comunicacions Ethernet. *IoT* d'etapa 2 i 3.

Tipus software:

Es tracta del **firmware** dels dispositius commutadors *Catalyst 4500* de *Cisco*.

Estadístiques:

Univers: *Shodan*: 2260 resultats, permet 100 registres **Referències trobades:** 39 **Versió actual:** Version 15.2

Versió	Núm. ocurrències	Versió	Núm. ocurrències	Versió	Núm. ocurrències
Version 12.2	***17***	*Version 15.0*	***7***	*Version 15.1*	***15***

Vulnerabilitats i exposicions comunes:

- **CVE-2019-1750**: Una vulnerabilitat en el sistema de commutació virtual fàcil (*VSS*) del programari *Cisco IOS XE* dels interruptors de la sèrie *Catalyst 4500* podria permetre a un atacant no autenticat i adjacent provocar la recàrrega dels interruptors. La vulnerabilitat es deu al maneig d'errors incomplet en processar els paquets del protocol *Cisco Discovery Protocol (CDP)* que s'utilitzen amb el sistema de commutació virtual fàcil. Un atacant podria explotar aquesta vulnerabilitat enviant un paquet *CDP* especialment dissenyat. Una explotació podria permetre a l'atacant provocar la recàrrega del dispositiu, donant lloc a una condició de denegació de servei (*DoS*).
- **CVE-2018-0155**: Una vulnerabilitat en la implementació de descàrrega de la detecció bidireccional de detecció bidireccional (*BFD*) dels interruptors *Cisco Catalyst 4500 Series* i *Cisco Catalyst 4500-X Switches* podria permetre a un atacant remot no autenticat causar un accident del procés iosd, provocant una denegació del servei (*DoS*) condició. La vulnerabilitat es deu a una gestió d'errors insuficient quan la capçalera BFD d'un paquet *BFD* és incompleta. Un atacant pot explotar aquesta vulnerabilitat enviant un missatge BFD elaborat a un o altre commutador afectat. Una explotació amb èxit podria permetre a l'atacant activar una recàrrega del sistema. Aquesta vulnerabilitat afecta *Catalyst 4500 Supervisor Engine 6-E (K5), Catalyst 4500 Supervisor Engine 6L-E (K10), Catalyst 4500 Supervisor Engine 7-E (K10), Catalyst 4500 Supervisor Engine 7L-E (K10), Catalyst 4500E Supervisor Motor 8-E (K10), supervisor* ···· .

Comentaris:

Totes les adreces són públiques *Ipv4*. Fan servir el port 161.

Data prospecció: *13 / maig / 2020*

Consulta *Shodan* CLI *Cisco Catalyst 4500 Series Switches*.	Fitxa 11

4. Millores proposades i tendències

En aquesta secció miro d'extreure conclusions basades sobre les prospeccions presentades al punt anterior. Cal dir que **no se'ls poden dotar de la categoria de científica** doncs ja al punt anterior ha plantejat un seguit de restriccions i consideracions que mostra que no es pot donar la categoria d'estadístiques a les dades recollides. Tot i que penso que **pot-ser una bona aproximació**.

4.1 Estat de les actualització de software

Els dispositius *IoT* ara s'utilitzen de manera vertical en molts dominis, des de la logística fins a l'agricultura de precisió, amb noves maneres d'optimitzar processos comercials i permetent nous casos d'ús. Els dispositius *IoT* també s'utilitzen en infraestructures crítiques on la seguretat juga un paper molt important. No es pot oblidar que els **dispositius *IoT* acostumen a tenir els recursos molt restringits**.

Els dispositius *IoT* tenen un impacte important en l'economia però són coneguts per la seva feble en front la seguretat. Per exemple, ***botnet Mirai***, va demostrar que els atacs a gran escala de *DDoS* que utilitzen dispositius *IoT* per a comprometre i amenaçar altres infraestructures de comunicació. Cal parar atenció en que molts d'aquests dispositius *IoT* compromesos **no estiguin equipats amb un mecanisme d'actualització del firmware** i, per tant, continuen sense apedaçar el seu programari.

Tal com s'ha vist al punt anterior, fent prospeccions a Internet sobre diferents dispositius, ha mostrat que el firmware i en general el programari dels dispositius *IoT* acostumen ha estar desactualitzats. A més tal com ja s'ha treballat moltes versions de firmware desactualitzat estan associades a vulnerabilitats conegudes i catalogades. Es pot extreure conclusions!

Conclusió:
A l'àmbit de la Internet de les Coses els dispositius IoT **acostumen ha estats desactualitzats**. Això és especialment greu doncs també s'ha vist que moltes versions antigues de programari van associats a **vulnerabilitats** i exposicions comunes què no es resolen al llarg del temps.

Això posa de manifest la necessitat de dissenyar un mecanisme d'actualització de firmware en dispositius *IoT* al començament del desenvolupament del producte. Cal pensar que la gran **majoria d'atacs** que es produeix, no només de manera específica a dispositius *IoT* també a qualsevol altre infraestructura de comunicacions, es fan servir de **vulnerabilitats ja conegudes i publicades pels diferents *CERT* fa mesos** cosa que demostra que es podia haver evitat l'atac.

Per descomptat, si es dissenyen de forma **incorrecta**, **les actualitzacions del firmware poden convertir-se en vectors d'atac**. El cuc de *Zigbee*, per exemple, va desencadenar una reacció en cadena combinant una sèrie de actualitzacions de firmware maliciosos i comunicacions inèdites promiscues. La situació es milloraria significativament si els desenvolupadors poguessin utilitzar un **mecanisme d'actualització de firmware normalitzat** en lloc d'haver de dissenyar el seu propi. En aquest article, doncs, explorem les opcions que tenen els desenvolupadors actuals i **dissenyem un prototip que permeti actualitzacions de firmware *IoT* basades en blocs de construcció estandarditzats**.

4.2 Sistemes actuals d'actualització de software i bones pràctiques

La manera tradicional per actualitzar el programari per a actius informàtics porta fer l'anàlisi, la posada en escena i la distribució de l'actualització, un procés que normalment es produeix durant les hores fora de producció. Aquestes actualitzacions acostumen a contenir controls criptogràfics (signatures digitals) aplicats per salvaguardar la integritat i l'autenticitat del programari. Aquest procés a ***Internet de les Coses*, amb el seu inabastable ecosistema de dispositius connectats desplegats en molts entorns, introdueix complexitats associades al procés d'actualització que fa obligada la necessitat de fer una reenginyeria** dels processos.

Per aquesta necessitat s'ha cercat directius o consell de parts experimentades en el tema que ens ocupa. En la cerca de directius i bones pràctiques per extreure una serie de recomanacions he decidit extreure els principals consell de publicacions de *Cloud Security Alliance* (*CSA*) que és una organització dedicada a definir i conscienciar les bones pràctiques per ajudar a assegurar un entorn de computació en núvol segur. *CSA* extreu competències en matèria professionals de la indústria, associacions, governs i membres corporatius per oferir recerca, educació i certificació, per a la seguretat del núvol.

Sobre tot s'ha fet servir el document *Recommendations for IoT Firmware Update Processes* (Khemissa et al., 2018) que és el que més s'ajusta a les necessitats del treball. Aquest treball té un decàleg de **10 recomanacions** que representen un bon resum del que s'ha de tenir en compte a l'hora de gestionar l'actualització de firmware entre els dispositius de *IoT*.

1. Back-up de configuració de treball del dispositiu abans d'actualitzar

Cal fer una còpia de seguretat de la configuració de treball actual del dispositiu IoT abans d'aplicar una actualització del firmware. Si es produeix **un problema durant el procés d'actualització, el dispositiu IoT hauria de poder tornar a carregar l'última configuració coneguda** i de confiança. Aquesta configuració es podia emmagatzemar en un repositori allotjat per una plataforma de núvol privada o pública.

La nova imatge ha de poder carregar la configuració anterior, fins i tot si aquesta configuració fa que les millores no estiguin disponibles. Aquesta característica garanteix que el dispositiu IoT **es mantingui en funcionament i es connecti per tal de fer possible la descàrrega** d'una (nova) imatge actualitzada.

2. Ha de suportar els retrocessos (*rollbacks*)

El sistema ha de permetre fer un retrocés (*rollback*) de versions de firmware tot i que les **imatges antigues del firmware no s'ha de deixar carregar sense l'autorització** del fabricant.

Un atacant pot llançar un assalt de **baixada carregant una versió antiga** i segura del firmware per explotar una vulnerabilitat coneguda. S'ha d'implementar una **funció *anti-rollback*** per evitar que es carregui una imatge antiga en un sistema. Per exemple, tots els firmware antics considerats desfasats o insegurs han de requerir una **contrasenya** proporcionada pel venedor.

3. Permetre programar actualitzacions dels dispositius

Els sistema tindria de permetre a l'administrador programar les actualitzacions per a evitar la saturació de la xarxa i limitar els temps d'inici no desitjats.
Com els dispositius *IoT* tenen un nombre de milions de milions, cal establir una estratègia intel·ligent per **evitar**:

1. Congestió de xarxa a causa d'un **augment de les transmissions** entre dispositius *IoT* i servidors d'actualització durant el desplegament d'un nou firmware.
2. Servidors d'actualització **sobrecarregats**, que poden causar problemes de denegació de servei (***DoS***).
3. **Saturació de recursos dels dispositius** *IoT*, degut a les sol·licituds d'actualització contínua dels dispositius *IoT* per actualitzar servidors durant la **congestió de la xarxa** i/o la **indisponibilitat del servidor** d'actualització.

Els dos principals models d'actualització IoT són:

- **Mode push:** els servidors d'actualització **envien** o "pressionen" la nova versió del firmware als dispositius IoT.
- **Mode pull:** periòdicament, els dispositius IoT **"tiren"** els servidors d'actualització per obtenir una nova versió del firmware.

4. Suport per opcions de configuració i actualitzacions automàtiques

Els fabricants han de donar suport a les opcions de configuracions dels administradors del sistema com pot-ser el suport a actualitzacions automàtiques. El procés d'actualització automàtica inclou dues **accions: baixar una nova actualització i després instal·lar-la**. A més, cal distingir dues categories d'actualitzacions automàtiques:

1. En el cas dels **dispositius IoT personals**, les actualitzacions es baixen **directament dels servidors d'actualització** de proveïdors IoT. Les actualitzacions automàtiques estan habilitades de tres maneres: per defecte, en configurar el dispositiu o desactivar-la mitjançant una configuració.
2. En el cas del **desplegament IoT gestionat**, els dispositius IoT són **supervisats de manera centralitzada per una organització**, una empresa privada o una empresa pública (com ara empreses o ciutats intel·ligents) i les actualitzacions **es descarreguen dels servidors d'actualització de l'organització** després de provar-los i aprovar-los. En aquest cas, les actualitzacions automàtiques haurien d'estar activades.

5. Un component gestiona les actualitzacions de tots els microcontroladors

Un **dispositiu *IoT* pot tenir un o més microcontroladors i sensors incrustats, i aquests components poden ser proporcionats per diferents fabricants**. Aquests fabricants ofereixen

contínuament actualitzacions per millorar els seus productes, resoldre errors i corregir problemes de seguretat.

Els venedors de dispositius IoT han de **gestionar les actualitzacions de tots els components dels seus dispositius**, inclús els components subministrats per tercers. Per això, **el fabricant ha de validar i proporcionar el firmware de tots els components** que constitueixen els seus productes. Això ajudarà a abordar dos **problemes** clau:

1. La **prevenció dels efectes secundaris** que afectin altres components que alteren el funcionament del dispositiu IoT.
2. La **instal·lació d'un firmware manipulat o maliciós** que comprometi el component i, a continuació, tot el dispositiu IoT.

6. Actualitzacions diferencial o completa segons l'amplada de banda

En un desplegament de baixa amplada de banda, una descàrrega a **imatge completa podria afectar el trànsit de xarxa** que bloqueja el monitoratge i la recollida de dades del dispositiu IoT. Sempre que sigui possible, es prefereixen les actualitzacions de paquets i **diferencials** que les actualitzacions completes d'imatges.

7. Actualitzacions autentificada i integritat de punta a punta

El principal repte d'un procés d'actualització segura és assegurar que una **actualització no s'hagi manipulat en el trànsit** al dispositiu *IoT* i que l'actualització tingui l'origen en els servidors d'actualització legítims. Es verifica mitjançant l'**autenticació d'origen de dades** (*DOA, Data Origin Authentication*). El proveïdor ha de **signar digitalment cada actualització** de firmware i ha de verificar la signatura digital pel dispositiu *IoT* abans de començar l'actualització.

Per ajudar en el procés, la signatura digital del **firmware es podria emmagatzemar en una cadena de blocs** per exemple.

8. Emmagatzematge de claus de signatura de verificació assegurat

Les claus de signatura utilitzada per un dispositiu *IoT* s'han d'**emmagatzemar de forma segura**. L'element segur podria ser un component especialitzat, dedicat i incrustat del dispositiu *IoT* que ofereix un emmagatzematge segur per a claus secretes.

Els **elements segurs avançats ofereixen un funcionament criptogràfic perquè les claus secretes mai no estan separades de l'element**.

9. Procediment de recuperació per possibles errors d'actualització

Si l'actualització automàtica falla i la xarxa de dispositius *IoT* està fora de línia, cal proporcionar un **procediment de recuperació manual**.

10. Suport a llarg termini per part dels fabricants

S'ha d'implementar un **acord de servei a llarg termini** (amb una durada mínima de deu anys) entre als fabricnats de dispositius *IoT* (o el proveïdor que executa la solució de suport) i els fabricants de microcontroladors, inclòs el fabricant de disseny original (*ODM, Original Design Manufacturer*) i/o el fabricant original d'equips (*OEM, Original Equipment Manufacturer*).

5. Conclusions

El que es comenta en aquesta secció ja s'ha anat comentant durant el treball i aquí es recull com a conclusió final del treball. El que s'intenta és **demostrar les hipòtesis d'aquest treball**, que cal recordar és que **els dispositius *IoT* són molt més vulnerables que els dispositius tradicionals d'Internet degut a acostumar a tenir un firmware més desactualitzat que la resta d'elements i que els converteix en més vulnerables a ciberatacs.**

El món de la *IoT* sustenta una gran diversitat de dispositius, els més crítics segons els experts es pot trobar i per aquest ordre: sensors, dispositius de xarxa, protocols de comunicació, passarel·les, serveis, actuadors, etc. Aquests ecosistemes són complexes a causa de l'escala, l'heterogeneïtat dels dispositius, la connectivitat implicada, l'escalabilitat, la disponibilitat i la flexibilitat.

Cal afegir, al ja comentat, la gran quantitat de protocols i estàndards de comunicacions que es poden veure involucrats els dispositius *IoT*, a més el programari que fan servir és molt divers.

Fixant-nos en això últim, les vulnerabilitats del firmware *IoT* representa que és un vector d'atac tant pel mateix sistema com per la tot Internet. Els sistemes d'actualitzacions de firmware IoT també és objectiu d'atacs on l'atacant cerca les seves vulnerabilitats. Se sap que per a implementar una solució d'actualització de firmware en dispositius IoT necessita de 32kB de memòria RAM i 128kB de memòria flash.

La limitada quantitat de recursos disponibles que els dispositius *IoT* acostumen a tenir, la gran diversitat d'aquests, l'arquitectura per nivells complexa i desplegada per una àrea extensa, la falta de mecanismes d'actualitzacions robustos amb una infraestructura per criptografia. També fa complexe la seva gestió, la diversitat de protocols de comunicacions, de programari i sistemes operatius que es fan servir.

A l'àmbit de la Internet de les Coses els dispositius IoT **acostumen ha estats desactualitzats**. Això és especialment greu doncs també s'ha vist que moltes versions antigues de programari van associats a **vulnerabilitats** i exposicions comunes què no es resolen al llarg del temps.

Cal pensar que la gran **majoria d'atacs** que es produeix, no només de manera específica a dispositius *IoT* també a qualsevol altre infraestructura de comunicacions, es fan servir de **vulnerabilitats ja conegudes i publicades pels diferents *CERT* fa mesos** cosa que demostra que es podia haver evitat l'atac. Per descomptat, si es dissenyen de forma **incorrecta**, **les actualitzacions del firmware poden convertir-se en vectors d'atac**.

6. Glossari

***6LoWPAN*:** (*IPv6 over Low Power Wireless Personal Area Network*) és un grup de treball conclòs a l'àrea d'Internet de l'IETF. Protocol d'Internet que es pot aplicar fins i tot als dispositius més petits, i que dispositius de baix consum.

API: (*Application Programming Interface*) és una interfície que especifica com diferents components de programes informàtics haurien d'interaccionar. Dit d'una altra manera, és un conjunt d'indicacions, quant a funcions i procediments, ofert per una biblioteca informàtica o programoteca per ser utilitzat per un altre programa per interaccionar amb el programa en qüestió.

***APT*:** (*Advanced Persistent Threat*) és un actor d'amenaça furtiu de la xarxa, normalment un grup nacional o un grup patrocinat per l'estat, que obté accés no autoritzat a una xarxa d'ordinadors i roman sense ser detectat durant un període prolongat. En els darrers temps, el terme també es pot referir a grups patrocinats no estatals que realitzin intrusions dirigides a gran escala per a objectius específics.

***AMQP*:** (*Advanced Message Queuing Protocol*) és un protocol obert de capa d'aplicació estàndard per a programari mitjà orientat a missatges. Les funcions definidores d'*AMQP* són l'orientació a missatges, ordenació en cua, encaminament (inclosos els punts-a-punt i els publicació-subscriptor), la fiabilitat i la seguretat.

***BLE*:** (*Bluetooth Low Energy*) és un estàndard que defineix una tecnologia de comunicacions sense fils per a crear xarxes d'àrea personal de baixa potència.

Botnet: (paraula formada del anglès per "robot" i "network") és un grup d'ordinadors (anomenats bots o zombies) connectats a Internet que involuntàriament, un cop han estat infectats amb un virus, un cuc o un troià, poden ser controlats remotament per realitzar tasques sense l'autorització del propietari i sense que aquest se n'adoni.

***CASB*:** (*Cloud Security Access Broker*) és un software local o basat en núvol que es troba entre els usuaris del servei de núvol i les aplicacions al núvol i supervisa tota l'activitat i fa complir les polítiques de seguretat. Un *CASB* pot oferir diversos serveis com ara la supervisió de l'activitat dels usuaris, avisar els administradors sobre accions potencialment perilloses, fer complir el compliment de les polítiques de seguretat i prevenir automàticament programari maliciós.

***CARP*:** (*Channel-Aware Routing Protocol*) protocol d'encaminament de capes transversals per a xarxes de sensors sense fils subaquàtiques. *CARP* per al protocol d'encaminament amb consciència del canal, explota informació de qualitat dels enllaços per a la determinació de relés de capa creuada. Els nodes es seleccionen com a relés si tenen un historial (recent) de transmissions amb èxit als seus veïns.

***CBOR*:** (*Concise Binary Object Representation*) és un format de serialització de dades binari basat en *JSON*.

***CERT*:** (*Computer Emergency Response Team*) Equip de Resposta davant Emergències Informàtiques és un centre de resposta a incidents de seguretat en tecnologies de la informació. Es tracta d'un grup d'experts responsable del desenvolupament de mesures preventives i reactives davant incidències de seguretat en els sistemes d'informació. Un CERT estudia l'estat de seguretat global de xarxes i ordinadors i proporciona serveis de resposta davant incidents a víctimes d'atacs en la xarxa, pública alertes relatives a amenaces i vulnerabilitats i ofereix informació que ajudi a millorar la seguretat d'aquests sistemes.

***CII*:** (Critical Information Infrastructure) és un sistema d'informació física o virtual que controla, processa, transmet, rep o emmagatzema informació electrònica en qualsevol forma inclosa dades, veu o vídeo què és vital per al funcionament de la infraestructura crítica, un atac sobre ell té un impacte debilitant sobre la seguretat nacional i pertany a una entitat de govern estatal o local.

***CIIP*:** (*Critical Information Infrastructure Protection*) totes les activitats destinades a assegurar la funcionalitat, la continuïtat i la integritat de la CII per dissuadir, mitigar i neutralitzar una amenaça, risc o vulnerabilitat o minimitzar l'impacte d'un incident.

***CISO*:** (*Chief Information Security Officer*) executiu de nivell superior en una organització responsable d'establir i mantenir la visió, l'estratègia i el programa de l'empresa per assegurar que els actius i les tecnologies de la informació estiguin adequadament protegits. El CISO orienta el personal a identificar, desenvolupar, implementar i mantenir processos a tota l'empresa per reduir els riscos de tecnologia i informació (IT). Responen a incidents, estableixen normes i controls

adequats, gestionen tecnologies de seguretat i dirigeixen l'establiment i la implementació de polítiques i procediments.

CLI: (*Command-Line Interface*) Una interfície de línia d'ordres és un mètode per manipular amb instruccions escrites el programa que subjeu sota. S'interacciona amb la informació de la manera més simple possible, sense gràfiques, només amb el text cru. Les ordres s'escriuen com a línies de text (d'aquí el nom), i, si els programes responen, generalment ho fan posant informació a les línies següents. Gairebé qualsevol programa pot dissenyar-se per oferir a l'usuari alguna classe de *CLI*.

***CoAP*:** (*Constrained Application Protocol*) Protocol de la capa d'aplicació d'Internet per a dispositius amb recursos restringits. Permet que dispositius amb pocs recursos es puguin comunicar amb qualsevol node d'Internet, és un protocol de capa d'aplicació dirigit a la IoT.

***CoMI*:** (*CoAP Management Interface*) una interfície de gestió de xarxa per a dispositius i xarxes restringides (*CoMI*). El protocol d'aplicacions restringides (*CoAP*) s'utilitza per accedir als recursos de dades i al node de dades especificats a *YANG* o *SMIv2* convertits a *YANG*. *CoMI* utilitza el mapeig YANG a *CBOR* i converteix les cadenes d'identificadors YANG a identificadors numèrics per reduir la mida de la càrrega útil. *CoMI* amplia el conjunt de protocols basats en *YANG*, *NETCONF* i *RESTCONF*, amb la capacitat de gestionar dispositius i xarxes restringides.

***COSE*:** (CBOR Object Signing and Encryption) (*RFC 8152*) descriu com crear i processar signatures, codis d'autenticació de missatges i xifratge mitjançant la representació d'objectes binaris concís (*CBOR, RFC 7049*) per a la serialització. *COSE* descriu a més una representació de claus criptogràfiques.

***CSA*:** (*Cloud Security Alliance*) és una organització sense ànim de lucre amb la missió de "promoure l'ús de les millors pràctiques per proporcionar garantia de seguretat dins del *Cloud Computing* i proporcionar formació sobre els usos de la computació en núvol per ajudar a assegurar totes les altres formes d'informàtica.

DAS: (*Data acquisition systems*) Són dispositius que fan un procés de mostreig de senyals que mesuren les condicions físiques del món real i converteixen les mostres resultants en valors numèrics digitals que poden ser manipulats per un ordinador. Els sistemes d'adquisició de dades solen convertir les formes d'ona analògiques en valors digitals per al seu processament. Aquests sistemes inclouen: sensors, circuits de condicionament de senyal i convertidors analogics a digitals.

DC**:** (Data Center) El centre de dades és una instal·lació que es fa servir per allotjar sistemes informàtics i els components associats, com són les telecomunicacions i sistemes d'emmagatzematge i on es concentren els recursos necessaris per al processament de la informació d'una organització.

DDS**:** (*Data Distribution Service*) en sistemes en temps real és un estàndard màquina-a-màquina (OMG, Object Management Group) de gestió d'objectes (de vegades anomenat middleware o framework de connectivitat) que pretén permetre intercanvis de dades fiables, d'alt rendiment, interoperables, en temps real, escalables mitjançant una publicació– patró de subscripció.

DDoS **atac:** (Distributed Denial-of-Service attack) és un atac distribuït de denegació de servei on el trànsit entrant que inunda la víctima prové de fonts diferents. Això efectivament fa impossible aturar ció-l'atac simplement bloquejant una única font.

Dispositius IoT restringits: Nodes finals amb sensors/actuadors per gestionar una aplicació específica. Accedeixen a la xarxa mitjançant altres dispositius com a passarel·la, xarxes de baixa potència i pèrdues (*Low Power and Lossy Networks, LLN*) i fent torns amb les plataformes de núvols IoT. Fa servir protocols sense fils de baix consum com *BLE*, *802.15.4* (*6LoWPAN*, *Zigbee*, *Thread*, *WirelessHART*, etc.), *LPWAN*, etc, estan alimentats per bateries i amb baixa taxa de retransmissió de dades.

DTLS**:** (*Datagram Transport Layer Security*) protocol de comunicacions de seguretat en les aplicacions basades en datagrames dins el protocol UDP. Basat en documents de recomanacions de l'IETF.

***ECC*:** (*Elliptic-curve cryptography*) variant de la criptografia asimètrica o de clau pública basada en les matemàtiques de les corbes el·líptiques. CCE pot ser més ràpida i usar claus més curtes que els mètodes com RSA i proporcionen un nivell de seguretat equivalent.

***ECDSA*:** (*Elliptic Curve Digital Signature Algorithm*) és un algoritme criptogràfic utilitzat per *Bitcoin* per assegurar que només els seus propietaris legítims poden gastar fons.

Honeypot: és un mecanisme de seguretat informàtic establert per detectar, desviar o, d'alguna manera, contrarestar els intents d'ús no autoritzat dels sistemes d'informació. Generalment, un honeypot consta de dades (per exemple, en un lloc de xarxa) que semblen ser una part legítima del lloc que sembla que conté informació o un recurs de valor per als atacants, però en realitat, es troba aïllat i controlat i que permet el bloqueig o analitzant els atacants.

IETF: (*Internet Engineering Task Force*) organització que desenvolupa i promou estàndards, cooperant estretament amb el W3C, així com l'ISO/IEC.

***IIC*:** (*Industrial Internet Consortium*) és una organització oberta que va ser formada per a accelerar el desenvolupament, adopció i expansió de l'ús de les màquines i dispositius interconnectats al sector industrial.

***ICT*:** (*Information and Communication Technology*) agrupen els elements i les tècniques utilitzades en el tractament i la transmissió de les informacions, principalment d'informàtica, internet i telecomunicacions. Per extensió, designen el sector d'activitat econòmica.

***IDS*:** (*Intrusion Detection System*) Sistema de Detecció d'Intrusos o SDI és un programa de detecció d'accessos no autoritzats a un computador o a una xarxa. El SDI sol tenir sensors virtuals (per exemple, un sniffer o analitzador de paquets de xarxa) amb els quals el nucli de l'SDI pot obtenir dades externes (generalment sobre el tràfic de xarxa).

***IoTSEC*:** (*Internet of Things SECurity*) l'àrea tecnològica dedicada a la protecció de dispositius i xarxes connectades a Internet de les coses (IoT).

***LPWAN*:** (*Low Power Wide Area Network*) són un tipus de xarxes de telecomunicacions dissenyades per tenir un llarg abast i una baixa taxa de bits per connectar objectes com sensors alimentats per bateries. Aquestes xarxes, juntament amb les ja existents, tant de curt abast (*WiFi* o *Bluetooth*) i les xarxes de telefonia mòbil habilitaran el conegut com Internet de les coses.

***MAC*:** (*Media Access Control*) la subcapa de control d'accés al medi és la capa que controla el maquinari responsable de la interacció amb el mitjà de transmissió per cable, òptic o sense fil. El subcapa MAC i el control d'enllaços lògics (LLC, Logical Link Control) formen la capa d'enllaç de dades.

Mobile crowdsensing: és una tècnica on un gran grup d'individus que disposen de dispositius mòbils capaços de detectar i computar (telèfons intel·ligents, tauletes, wearables) comparteixen col·lectivament dades i extreuen informació per mesurar, mapar, analitzar, estimar o inferir (predir) qualsevol procés d'interès comú. Recorregut multitudinari de dades de sensors des de dispositius mòbils.

NAT: (Network address translation) la traducció d'adreces de xarxa és el procés pel qual es modifiquen la informació sobre adreces a la capçalera del paquet IPv4 mentre està en trànsit per un dispositiu d'encaminament.

***NIST*:** (*National Institute of Standards and Technology*) és una agència de l'Administració de Tecnologia del Departament de Comerç dels Estats Units.

***OCF*:** (*Open Connectivity Foundation*) és una organització de la indústria que té com a missió declarada desenvolupar estàndards d'especificació, promoure un conjunt de directrius d'interoperabilitat i proporcionar un programa de certificació per a dispositius implicats a *Internet of Things (IoT)*.

OMA LWM2M: (*Open Mobil Alliance LightWeight Machine to Machine*) Protocol obert i de baixa complexitat per a la gestió de dispositius IoT o M2M. Defineix la capa d'aplicació en un model client/servidor: un servidor i un client LwM2M que està incrustat en un dispositiu LwM2M que

caracteritzen per tenir pocs recursos de maquinari obligats a comunicar-se amb protocols senzills LwM2M. Com a capa inferior acostumen a emprar el protocol CoAP.

***OTA*:** (*over-the-air programming*) Mètodes de distribució de programari i/o configuració de paràmetres que utilitzen diferents aparells com telèfons mòbils, enrutadors, receptors de televisió i perifèrics informàtics de tota mena.

PoE: (*Power over Ethernet*) és una tecnologia que permet l'alimentació elèctrica de dispositius de xarxa mitjançant el mateix cable de xarxa Ethernet UTP/STP per on reben les dades. Elimina la necessitat de preses de corrent per a alimentar el dispositiu. Regulat a *IEEE 802.3at*.

***QoS*:** (*Quality of Service*) és la descripció o la mesura del rendiment global d'un servei, com ara una xarxa de telefonia o ordinador o un servei de computació en núvol, particularment el rendiment vist pels usuaris de la xarxa. Per mesurar quantitativament la qualitat del servei, sovint es consideren diversos aspectes relacionats del servei de xarxa, com ara la pèrdua de paquets, la velocitat de bits, el rendiment, el retard de la transmissió, la disponibilitat, fluctuació de retard, etc.

***RAML*:** (*RESTful API Modeling Language*) és un llenguatge basat en *YAML* per descriure les APIs *RESTful.*

***RESTful*:** són serveis web que s'ajusten a l'estil arquitectònic *REST*, estil arquitectònic de programari que defineix un conjunt de restriccions a utilitzar per crear serveis web, i proporcionen una interoperabilitat entre sistemes informàtics d'Internet.

***RFC*:** (*Request for Comments*) Document tipus memoràndum sobre noves investigacions i metodologies relacionades amb les tecnologies d'Internet.

***RSA*:** (*Rivest–Shamir–Adleman*) és un algorisme de xifratge de clau pública.

***SNMP*:** (*Simple Network Management Protocol*) és un protocol de la capa d'aplicació que facilita l'intercanvi d'informació d'administració entre dispositius de xarxa.

SUIT: (*Software Updates for Internet of Things*) Grup d'*IETF* que se centrarà en definir una solució d'actualització de firmware (contempla aprenentatges de *RFC 4108* i altres solucions) que es pot utilitzar en dispositius de Classe 1 (definit a *RFC 7228*), és a dir, en dispositius amb ~10 KB *RAM* i ~100 KB *flaix*.

TEE: (*Trusted Execution Environment Provisioning*) és una zona segura d'un processador. Proporciona funcions de seguretat com l'execució aïllada i la integritat de les aplicacions de confiança, juntament amb disposicions per mantenir la confidencialitat dels actius. En general, *TEE* ofereix un espai d'execució que proporciona un nivell de seguretat més elevat que un sistema operatiu ordinari.

TUF**:** (*TCP ULP Framing Protocol*) Defineix un protocol de capa reduïda entre un protocol de capa superior (ULP) i TCP. Depèn d'una convenció de segmentació TCP especificada entre els punts finals dels TUF. Les convencions de reducció i segmentació permeten que un receptor TUF/TCP reconegui les unitats de dades ULP dins d'un segment TCP independentment d'altres segments TCP, això simplifica el disseny d'interfícies de xarxa.

YANG**:** (Yet Another Next Generation) Llenguatge de modelatge de dades per a la definició de dades enviades a través de protocols de gestió de xarxa com NETCONF i RESTCONF. El manté el grup de treball NETMOD d'IETF i està publicat com a RFC 6020.

7. Bibliografia

- Cisco. Networking Academy. CCNA R&S: Introduction to Networks. [Data consulta: a partir de 20 de maig de 2020] <*https://www.netacad.com*>
- Common Vulnerabilities and Exposures (CVE), Search CVE List. [Data consulta: a partir de 2 de maig de 2020] <*http://cve.mitre.org/index.html*>.
- Community.turgensec.com [Data consulta: a partir de 20 de abril de 2020] <*https://community.turgensec.com/shodan-pentesting-guide/*>.
- European Union Agency for Network and Information Security (ENISA), IoT Security Expert Group (2017). Baseline Security Recommendations for IoT. www.enisa.europa.eu/ publications: ENISA.
- Fuller, JR (2016). The 4 stages of an IoT architecture [en línia]. England: TechBeacon. [Data consulta: 30 de març de 2020] <https://techbeacon.com/enterprise-it/4-stages-iot-architecture>
- Harwood, T (2019). IoT Software Guide [en línia]. USA: Postscapes [Data consulta: 16 de abril de 2020] <https://www.postscapes.com/internet-of-things-software-guide/>
- Incibe-cert Inicio / Alerta Temprana / Vulnerabilidades. [Data consulta: a partir de 20 de abril de 2020] <*https://www.incibe-cert.es/alerta-temprana/vulnerabilidades*>.
- Khemissa S., Guzman A., Lanois L., Mehta A., Nelson T., Roza M., Russell B., i Samaniego C.(2018). Recommendations for IoT Firmware Update Processes, in IEEE Access, vol. 7, pp. 71907-71920, 2019.[Data consulta: a partir de 4 de maig de 2020] <*https://cloudsecurityalliance.org/artifacts/iot-firmware-update-processes/*>.
- Microsoft Azure: Catálogo de dispositivos Azure Certified for IoT [Data consulta: a partir de 10 de maig de 2020] <*https://catalog.azureiotsolutions.com/*>.
- Minerva R., Biru A., Rotondi D. (2015). Towards a definition of the Internet of Things (IoT) [en línia]. Italia: IEEE Internet Initiative [Data consulta: 16 de abril de 2020] <iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision 1_27MAY15.pdf>
- Nappey, P (2014). Standard for an Architectural Framework for the Internet of Things [en línia]. France: IEEE STANDARDS ASSOCIATION. [Data consulta: 10 de abril de 2020] <https://docbox.etsi.org/workshop/2014/201412_m2mworkshop/s04_standards/ ieee_p2413_nappey.pdf>
- Perwej, Dr. Yusuf & Haq, Kashiful & Parwej, Dr. Firoj & M., Mumdouh. (2019). The Internet of Things (IoT) and its Application Domains. International Journal of Computer Applications. [Data consulta: 10 de abril de 2020] <www.researchgate.net/publication/332374473>

- Saashub. The Independent Software Marketplace. [Data consulta: a partir de 2 de maig de 2020] <https://www.saashub.com/>.
- Salman, T (2015). Networking Protocols and Standards for Internet of Things [en línia]. USA: Washington University in St. Louis. [Data consulta: 12 de abril de 2020] <https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot.pdf>
- *SecTools.Org*. [Data consulta: a partir de 2 de maig de 2020] <https://sectools.org/>.
- Shodan. Explore, Developers, Monitor, etc. [Data consulta: a partir de 2 de abril de 2020] <*https://www.shodan.io/*>.
- Zandberg K., Schleiser K., Acosta F., Tschofenig H. and Baccelli E. (2019). Secure Firmware Updates for Constrained IoT Devices Using Open Standards: A Reality Check, in IEEE Access, vol. 7, pp. 71907-71920, 2019.[Data consulta: 16 de abril de 2020] <https://ieeexplore.ieee.org/document/8725488>