SEGURIDAD EN INTERNET DE LAS COSAS

Alumno: Francisco Montes Gallardo
Trabajo Fin de Grado: Grado de Ingeniería Informática
Área del trabajo final: Administración de sistemas Operativos

Consultor: Miguel Martín Mateo
Profesor responsable de la asignatura: Manuel Jesús Medonza Flores

Fecha: Junio de 2019

FICHA DEL TRABAJO FINAL

Título del trabajo:	Seguridad en el Internet de las Cosas
Nombre del autor:	Francisco Montes Gallardo
Nombre del consultor/a:	Miguel Martín Mateo
Nombre del PRA:	Manuel Jesús Medonza Flores
Fecha de entrega (mm/aaaa):	06/2019
Titulación::	Grado de Ingeniería Informática
Área del Trabajo Final:	Seguridad en el Internet de las cosas
Idioma del trabajo:	Castellano
Palabras clave	Internet of Things, vulnerabilities, security

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

El internet de las cosas o IoT está transformando la vida de las personas y al mismo tiempo se ha convertido en una verdadera revolución. Existen actualmente cientos de millones dispositivos IoT conectados a Internet y la previsión a medio plazo es que siga aumentando hasta cifras inimaginables. Sin embargo, estos dispositivos tienen, al igual que otros aparatos de uso doméstico, su propio hardware y software y en muchas ocasiones se fabrican sin tener demasiado en cuenta aspectos de seguridad. Son dispositivos que pueden estar desactualizados a las pocas semanas de su compra o incluso comprarlo con un virus de fábrica y antes de conectarlo a Internet.

Además, parece que existe una necesidad de compra casi compulsiva de este tipo de dispositivos que pone en grave peligro información confidencial, donde exponemos constantemente nuestra vida privada de una manera un tanto inquietante, información que en manos de delincuentes sería muy perjudicial ya que estos pueden hacer lo que quieran con nosotros, sin tan siquiera tener que abrir la puerta de nuestra casa.

Este TFG pretende explicar el concepto de IoT, como funcionan estos dispositivos, que les hace ser un objetivo atractivo para delincuentes. También explicaremos los ataques más típicos en dispositivos comerciales, y cuáles son las recomendaciones a seguir para poder prevenir ser atacados. Veremos que vulnerabilidades y errores de diseño por parte del fabricante podemos encontrar y se explicarán los riesgos que tenemos como consecuencia de los dispositivos que se encuentren desactualizados o sin ningún tipo de soporte.

Abstract (in English, 250 words or less):

The internet of things or IoT is transforming the lives of people and at the same time it has become a true revolution. There are currently hundreds of millions of IoT devices connected to the Internet and the medium-term forecast is to keep increasing until unimaginable figures.

However, these devices have, like other appliances for home use, their own hardware and software and are often manufactured without taking into account safety aspects. They are devices that may be out of date within a few weeks of your purchase or even buy it with a factory virus and before connecting it to the Internet.

In addition, it seems that there is an almost overwhelming need to buy this type of device that puts confidential information in serious danger, where we constantly expose our private life in a somewhat disturbing way, information that in the hands of criminals would be very harmful since they can Do what they want with us, without even having to open the door of our house.

This TFG aims to explain the concept of IoT, how these devices work, which makes them an attractive target for consumers. We will also explain the most typical attacks in commercial devices, and what are the recommendations to follow to prevent being attacked. We will see that vulnerabilities and design errors by the manufacturer can find and explain the risks we have as a result of devices that are outdated or without any support at all.

Índice de Contenidos

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

El internet de las cosas es una innovación tecnológica que nos permite transformar muchos objetos cotidianos en objetos inteligentes o Smart devices. Muchas de las cosas que nos rodean estarán conectadas a Internet en muy poco tiempo, y por lo tanto recibiendo información de manera constante, lo cual nos hará la vida más fácil en muchos sentidos, ya sea en la utilización de un uso más racional de la energía, la implementación de procesos de fabricación totalmente automatizada, Smart Cities, etc.

En la actualidad, el gran número de dispositivos conectados a internet dedicados a propósitos específicos resultan ser una amenaza real para la seguridad de los usuarios y compañías de todo el mundo. Si bien es cierto que hace unos años los creadores de virus y malwares se centraban en atacar ordenadores de uso general, en la actualidad los dispositivos IoT resultan un objetivo muy atractivo.

Podemos encontrar numerosos estudios que demuestran la creciente demanda por parte de los usuarios de tecnología con acceso a Internet, lo cual genera una mayor oferta de servicios por parte de las empresas. Estos dispositivos son fabricados por diferentes compañías y por lo tanto pueden utilizar diferentes protocolos de comunicación, diferentes softwares, sistemas operativos, arquitecturas hardware de diferentes fabricantes, en los cuales la seguridad no es el punto donde se invierta el debido tiempo.

Sin embargo, las cuestiones de seguridad se vuelven bastante relevantes en el momento que empezamos a utilizar este tipo de tecnologías y al igual que existen muchas ventajas y beneficios, también existen grandes riesgos y amenazas. En cuanto un objeto se vuelve parte del IoT, es necesario saber que estos dispositivos pueden perder la seguridad de manera inmediata, tanto física como lógica, ya que posiblemente se encontrarán localizados y serán accesibles al instante por potenciales atacantes que podrían manipular sistemas de control y modificar la funcionalidad con intenciones claramente dañinas para el dispositivo o sistema.

Con el IoT, alguien podría invadir nuestra intimidad fácilmente, encendiendo una cámara, conseguir acceder a nuestro Smart TV y poder espiarnos o controlar cualquier tipo de dispositivos que pudiera haber en una casa. Imaginen por un momento si alguien pudiera controlar un connected-car o coche conectado mientras vas conduciendo, es mejor ni pensarlo. Las posibilidades son muchas y con este documento trataremos de analizar cuáles son todos los aspectos de seguridad que la población en general tiene que tener en cuenta cuando utilizan este tipo de aparatos. Ya nadie puede escapar al uso diario de algún tipo tecnología.

Dicho lo anterior, se observa la necesidad de realizar la investigación propuesta, ya que el internet de las cosas es una de las innovaciones tecnológicas que requiere de cuidado cuando se trata de analizar las seguridades que brindará esta tendencia tecnológica a los usuarios, instituciones o empresas. Dado que todos los objetos estarán conectados a la red, cabría preguntarse ¿Quién será el responsable de asegurar nuestros dispositivos IoT? ¿Existe algún Estándar que podamos aplicar? Es difícil pronosticar la cantidad de situaciones a las cuales estaremos expuestos.

Se considera que la investigación del tema es factible porque se cuenta con los materiales y la metodología necesarios, así como para el análisis de las cuestiones a considerar en relación con la seguridad IoT. Con esta motivación se va a centrar y dirigir el TFG, hacia la investigación y

análisis de los ataques contra dispositivos IoT, en concreto dispositivos que son utilizados por usuarios finales. El resultado que se desea obtener con el desarrollo del trabajo propuesto es establecer los mecanismos de seguridad que debe tener en cuenta la innovación tecnológica del Internet de las Cosas.

1.2 Objetivos y alcance del Trabajo

El objetivo de este trabajo es analizar en profundidad todos los cambios que va a suponer la implantación de esta nueva forma de entender la tecnología en general, y con ella la sociedad y la manera de hacer las cosas tanto cotidianas como laborales. Posteriormente, se analizarán y evaluarán los riesgos que conlleva vivir inmersos en esta tecnología, donde estará al alcance de prácticamente todo el mundo y finalmente se explorarán y se propondrán diferentes soluciones para estos problemas.
En definitiva, se trata de saber si realmente estamos preparados para el cambio tecnológico que se avecina con "El internet de las cosas" y si estamos totalmente protegidos frente a esta nueva revolución.

OBJETIVOS:

General:

- Explicar el significado de IoT y dar a conocer la situación en la que se encuentra la evolución de este término y los dispositivos que podemos encontrar.
- Establecer mecanismos generales de seguridad a considerar con la innovación tecnológica del Internet de las Cosas (IoT).
- Analizar los tipos de ataques que se pueden esperar en los dispositivos IoT y cuáles son las causas y las motivaciones para realizar estos ataques.
- Entender a qué amenazas nos enfrentamos cuando utilizamos dispositivos IoT y porque somos vulnerables.
- Dar a conocer las medidas de seguridad recomendadas para proteger los dispositivos conectados a Internet y analizar la necesidad de protegerlos para garantizar la seguridad y la privacidad de los datos.

Específicos:

- Analizar la estructura y los tipos de dispositivos IoT presentes en el mercado y cuáles son los problemas de seguridad más comunes.
- Definir las debilidades y amenazas que presenta el Internet de las Cosas, en relación con la seguridad de dispositivos orientados al consumo de usuarios.
- Analizar cuáles son las recomendaciones, amenazas, y cosas a tener en cuenta.
- Determinar esquemas para diseñar objetos inteligentes con niveles de seguridad aceptables.
- Como se automatizan los ataques y creación de *Botnets.*
- Evidenciar la falta de seguridad de muchos de dispositivos que hasta hace poco tiempo no disponían de esta funcionalidad.
- Implementación de medidas para aumentar la seguridad de estos dispositivos junto con algunas recomendaciones de seguridad.

Limitaciones del alcance del proyecto

Este trabajo no considera directamente los dispositivos destinados a empresas industriales o comerciales, como sensores en aeropuertos o redes de hoteles, ciudades inteligentes, industriales de automatización, etc. ya que en este tipo de IoT normalmente las empresas y clientes tienen los

recursos e incentivos para especificar y gestionarlas características de seguridad y privacidad de los productos que compran. Además, muchos de estos dispositivos utilizan conexiones inalámbricas comerciales que no ofrecen acceso completo desde y hacia La Internet. Dicho esto, algunos de los mismos problemas tratados en este trabajo pueden estar presentes en este tipo tipologías.

El alcance de este informe también se limita a los dispositivos IoT que originan o terminan un flujo de datos. Concretamente el trabajo no se centra en los dispositivos, como un punto de acceso AP inalámbrico, routers o firewalls o en cualquier dispositivo electrónico de red por el que pasen datos.

Por último, veo le necesidad de puntualizar que este trabajo de análisis de la seguridad de las IoT no pretende ser alarmista, sino ser y hacer conscientes una realidad, así como la problemática y las recomendaciones de seguridad que se requieren para que su uso signifique un gran paso delante y no un retroceso en la seguridad, la privacidad y en definitiva de la libertad de las personas.

1.3 Enfoque y método seguido

Para la realización de este proyecto y dado de que se trata de un proyecto de investigación sobre el internet de las cosas, el método ha sido en primer lugar escoger bien los temas a tratar. Esta parte no ha sido fácil ya que hay multitud de temas que podríamos haber incluido.

Una vez seleccionando los temas, hemos ido poco a poco recopilando información de lo más variada y tratar de ajustar la información obtenida a los resultados que queremos plasmar en este proyecto de investigación.

Este es un trabajo de fondo y de constancia. Hemos seguido en la medida de lo posible los plazos marcados en la planificación inicial y esto ha sido un factor clave para la consecución del resultado final. Sin planificación hubiese resultado mucho más complicado y probablemente hubiésemos dejado cosas para el final con el potencial peligro que eso conlleva.

1.4 Planificación del Trabajo:

En cuanto a la planificación se definen por el momento 4 fechas destacables que coinciden con las fechas de entrega de cada uno de los trabajos.
En base a la temática que se ha explicado hasta ahora, se definen las tareas y subtareas que seguiremos para la realización del trabajo.

Tarea 1 - Contexto y justificación:

- Se detalla la importancia de desarrollar un trabajo que analice la seguridad de los dispositivos IOT

- Objetivos: se explica que se pretende con el desarrollo del trabajo

- Listado de tareas: Se detallan las tareas necesarias en cada fase para cubrir los objetivos descritos

- Planificación: Se estiman temporalmente las fechas de inicio y fin de cada una de las tareas descritas, mediante un diagrama de Gantt, que tiene en cuenta las fechas de entrega según la planificación del aula

- PAC 1: Plan de trabajo: Punto de control en que se entrega el plan de trabajo definido por TFG

Tarea 2 - Seguridad IoT

El objetivo de esta tarea es explicar los desafíos más destacables a los que se enfrenta el IoT, así como los ataques más habituales. Por otro lado, hablaremos de las medidas de seguridad que existen en el mercado para prevenir cierto tipo de ataques.

También veremos los tipos de dispositivos IoT y los niveles de seguridad existentes.

Esta tarea concluye con la entrega de la PEC2.

Tarea 3 - Seguridad en objetos orientados al consumidor

En esta tarea nos centraremos en la importancia de mantener la privacidad de las personas. El objetivo principal de esta tarea es continuar con el punto anterior, pero desde otra perspectiva, con el foco puesto en dispositivos IoT que cualquier usuario pueden utilizar en su día a día.

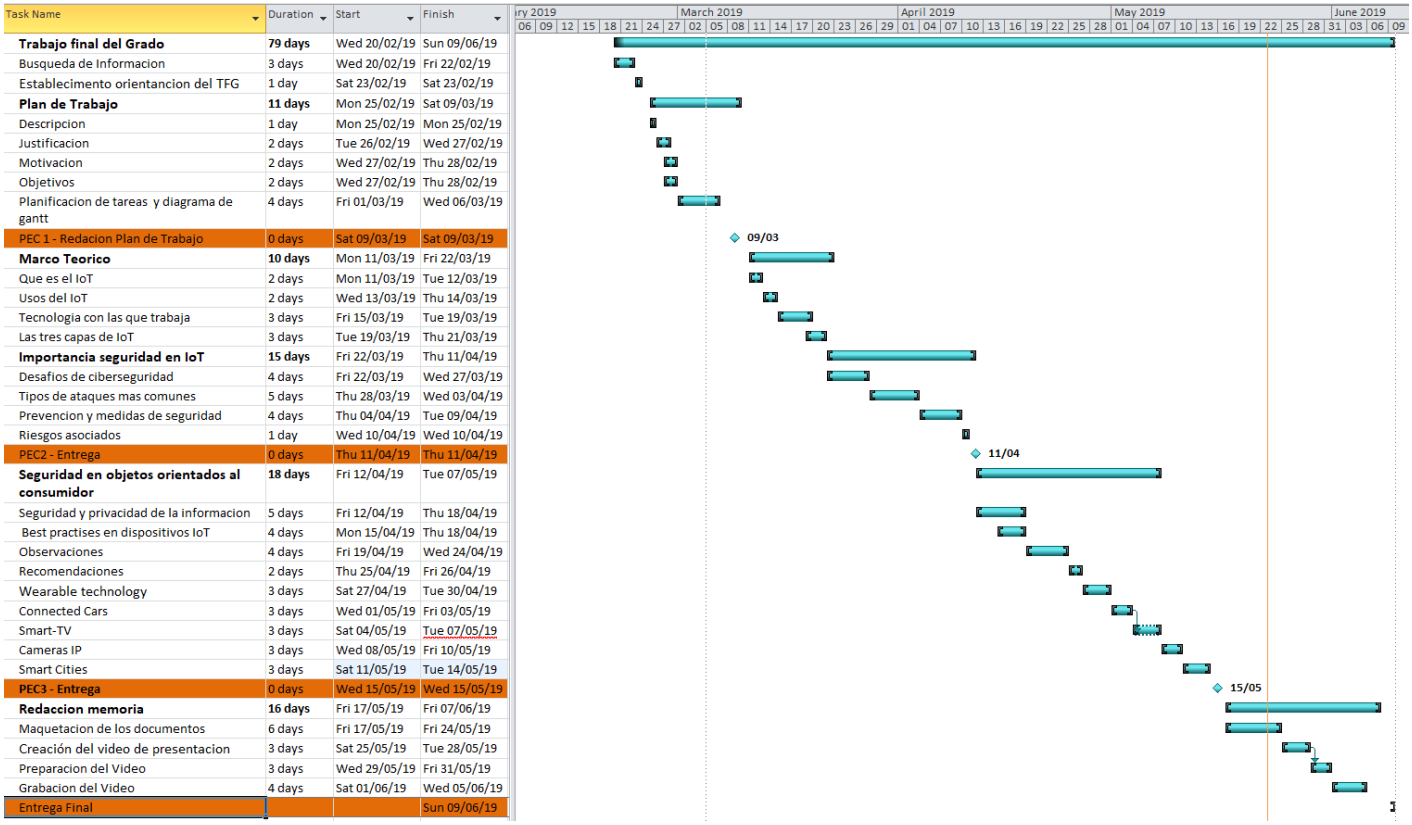
Explicaremos como este tipo de dispositivos no siguen las mejores prácticas de seguridad y explicaremos brevemente algunas recomendaciones básicas a seguir.

Esta tarea concluye con la entrega de la PEC3

Tarea 4 – Entrega final

Esta tarea consiste en la maquetación de la Memoria final y de la presentación.

A continuación, mostramos el diagrama de Gantt.



Task Name	Duration	Start	Finish
Trabajo final del Grado	**79 days**	Wed 20/02/19	Sun 09/06/19
Busqueda de Informacion	3 days	Wed 20/02/19	Fri 22/02/19
Establecimento orientancion del TFG	1 day	Sat 23/02/19	Sat 23/02/19
Plan de Trabajo	**11 days**	Mon 25/02/19	Sat 09/03/19
Descripcion	1 day	Mon 25/02/19	Mon 25/02/19
Justificacion	2 days	Tue 26/02/19	Wed 27/02/19
Motivacion	2 days	Wed 27/02/19	Thu 28/02/19
Objetivos	2 days	Wed 27/02/19	Thu 28/02/19
Planificacion de tareas y diagrama de gantt	4 days	Fri 01/03/19	Wed 06/03/19
PEC 1 - Redacion Plan de Trabajo	0 days	Sat 09/03/19	Sat 09/03/19
Marco Teorico	**10 days**	Mon 11/03/19	Fri 22/03/19
Que es el IoT	2 days	Mon 11/03/19	Tue 12/03/19
Usos del IoT	2 days	Wed 13/03/19	Thu 14/03/19
Tecnologia con las que trabaja	3 days	Fri 15/03/19	Tue 19/03/19
Las tres capas de IoT	3 days	Tue 19/03/19	Thu 21/03/19
Importancia seguridad en IoT	**15 days**	Fri 22/03/19	Thu 11/04/19
Desafios de ciberseguridad	4 days	Fri 22/03/19	Wed 27/03/19
Tipos de ataques mas comunes	5 days	Thu 28/03/19	Wed 03/04/19
Prevencion y medidas de seguridad	4 days	Thu 04/04/19	Tue 09/04/19
Riesgos asociados	1 day	Wed 10/04/19	Wed 10/04/19
PEC2 - Entrega	0 days	Thu 11/04/19	Thu 11/04/19
Seguridad en objetos orientados al consumidor	**18 days**	Fri 12/04/19	Tue 07/05/19
Seguridad y privacidad de la informacion	5 days	Fri 12/04/19	Thu 18/04/19
Best practises en dispositivos IoT	4 days	Mon 15/04/19	Thu 18/04/19
Observaciones	4 days	Fri 19/04/19	Wed 24/04/19
Recomendaciones	2 days	Thu 25/04/19	Fri 26/04/19
Wearable technology	3 days	Sat 27/04/19	Tue 30/04/19
Connected Cars	3 days	Wed 01/05/19	Fri 03/05/19
Smart-TV	3 days	Sat 04/05/19	Tue 07/05/19
Cameras IP	3 days	Wed 08/05/19	Fri 10/05/19
Smart Cities	3 days	Sat 11/05/19	Tue 14/05/19
PEC3 - Entrega	0 days	Wed 15/05/19	Wed 15/05/19
Redaccion memoria	**16 days**	Fri 17/05/19	Fri 07/06/19
Maquetacion de los documentos	6 days	Fri 17/05/19	Fri 24/05/19
Creación del video de presentacion	3 days	Sat 25/05/19	Tue 28/05/19
Preparacion del Video	3 days	Wed 29/05/19	Fri 31/05/19
Grabacion del Video	4 days	Sat 01/06/19	Wed 05/06/19
Entrega Final			Sun 09/06/19

Requisitos

Para realizar este proyecto necesitar de un ordenador personal - Laptop con procesador I5 ,8 GB de RAM y acceso a Internet.

1.5 Breve sumario de productos obtenidos

Se ha conseguido tener una pequeña visión de los problemas, amenazas, y vulnerabilidades que podemos encontrar en dispositivos IoT, así como las medidas necesarias y recomendaciones para poder prevenir este tipo de ataques.

Este trabajo está prácticamente enfocado a dispositivos de consumo, y no a dispositivos IoT industriales.

1.6 Breve descripción de los otros capítulos de la memoria

1. Introducción: Es este apartado se introduce el contexto y justificación del trabajo, objetivos, método seguido, planificación del trabajo, etc

2. Marco contextual: El fin de este capítulo es explicar el concepto IoT así como el futuro a corto plazo de los dispositivos IoT. También se hace una distinción clave para el proyecto donde podemos encontrar dispositivos basados en el consumidor por un lado y dispositivos industriales. De igual modo se explican el impacto del IoT en las personas y en los negocios y los usos del IoT en la actualidad. Por último, se repasan brevemente las tecnologías que se utilizan en el mundo IoT.

3. Importancia de la seguridad de IoT: El fin de este capítulo es explicar los desafíos y amenazas más comunes dentro del mundo del IoT. También se repasan los niveles de seguridad (datos,

hardware, software, red, y cloud) y como no, los ataques más comunes a dispositivos IoT. Finalizamos este apartando explicando las medidas de seguridad.

4. Seguridad en dispositivos orientados al consumidor: En este capítulo se estudiarán muchos de los problemas de seguridad IoT, y se explicaran cuáles son las razones que llevan a que un dispositivo IoT no sea seguro (falta de autenticación o cifrado), así como de los riesgos de conectar a Internet IoT vulnerables. Acabamos este apartado indicando una serie de recomendaciones y configuraciones para tener en cuenta cuando se utilizan estos artilugios.

5. Wearable technology: Este apartado permitirá ver muchos de los problemas a los que se enfrenta esta tecnología. Veremos los principales desafíos y ataques de privacidad, así como los problemas de autenticación más destacables.

6. Connected Cars: En este capítulo se explica el concepto de coche conectado o Smart car, de sus posibilidades, de sus beneficios, de sus ventajas y desventajas.
También hablaremos de las vulnerabilidades que presentan este tipo de vehículos y como un hacker podría manipularlo sin demasiadas complicaciones y hacer con nosotros lo que quiera. Por último, se facilitan algunos consejos de seguridad para proteger las aplicaciones móviles que gestionan los Smart cars.

7. Smart TV: Se comienza el apartado definiendo el concepto de Smart TV y todas aplicaciones que se pueden utilizar desde este tipo de televisores. Así mismo se explican las principales vulnerabilidades, sus riesgos de privacidad y las recomendaciones para prevenir ciertos tipos de ataques.

8. IP Cameras: En este apartado veremos por qué las cámaras IP son buenos objetivos para los ciberdelincuentes. Así mismo, se explicarán las mejores prácticas que deben seguir tano los fabricantes como para usuarios. Finalizaremos este apartado mostrando un caso real de ataque a una cámara IP.

9. Smart Cities: En este punto revisamos brevemente el concepto de Smart Cities, así como sus ventajas. De igual modo se explica el impacto de todos los recursos a los que afecta un ataque de este tipo, las motivaciones que llevan a los ciberdelincuentes a atacarlas. Por último, comentaremos las amenazas actuales a las que se enfrente las ciudades inteligentes.

10. Conclusiones: En este punto finalizaremos nuestro trabajo exponiendo las conclusiones del proyecto.

11. Glosario, Bibliografía, y Anexos: Como parte final de este TFG se exponen las referencias, términos, y anexos que puedan complementar este trabajo.

2. Que es el Internet de las Cosas. Teoría y puntos clave. Marco Contextual.

El internet de las cosas (en inglés, Internet of Things, abreviado IoT;) es un concepto que se refiere a una interconexión digital de objetos cotidianos con internet. También se suele conocer como internet de todas las cosas o internet en las cosas. El concepto de internet de las cosas fue propuesto en 1999, por Kevin Ashton, en el Auto-ID Center del MIT, en donde se realizaban investigaciones en el campo de la identificación por radiofrecuencia en red (RFID) y tecnologías de sensores.

La definición de IoT podría ser la agrupación e interconexión de dispositivos y objetos a través de una red ,bien sea privada o Internet, donde todos ellos podrían ser visibles e interaccionar unos con otros. Respecto al tipo de objetos o dispositivos podrían ser de cualquier tipo, desde sensores y dispositivos mecánicos hasta objetos cotidianos como pueden ser el frigorífico, una bombilla, el calzado o la ropa. Cualquier cosa que se pueda imaginar podría ser conectada a internet e interaccionar sin necesidad de la intervención humana, el objetivo por tanto es una interacción de máquina a máquina, o lo que se conoce como una interacción M2M (machine to machine) o dispositivos M2M.

Se calcula que todo ser humano está rodeado, al menos, por un total de aproximadamente 1000 a 5000 objetos. Por un lado, según la empresa Gartner, en 2020 habrá en el mundo aproximadamente 26 mil millones de dispositivos con un sistema de conexión a internet de las cosas. Abi Research, por otro lado, afirma que para el mismo año existirán 30 mil millones de dispositivos inalámbricos conectados a internet. Con la próxima generación de aplicaciones de internet (protocolo IPv6) se podrían identificar todos los objetos, algo que no se podía hacer con IPv4. Este sistema sería capaz de identificar instantáneamente por medio de un código a cualquier tipo de objeto.

El mercado de IoT ha estado en auge en los últimos años, teniendo un gran impacto tanto en consumidores como en empresas de todos los sectores del mundo. A pesar de que la tecnología ha sido ampliamente adoptada con gran entusiasmo, todavía no se ha discutido adecuadamente un patrón de seguridad para asegurar su mayor crecimiento en un panorama donde las amenazas son cada vez mayores. Después de los ataques cibernéticos a gran escala lanzados a través de redes explotadas de IoT en los últimos años, la conciencia de riesgo de IoT ha aumentado ligeramente, sin embargo, los dispositivos inteligentes siguen siendo muy vulnerables.

Una de las principales causas de las vulnerabilidades es que los fabricantes se apresuran a ofrecer dispositivos innovadores que llaman la atención del consumidor, pero ignoran por completo el cifrado de extremo a extremo. Muchos dispositivos inteligentes disponibles actualmente en el mercado son vulnerables a intrusiones de terceros. Debido a que el software de seguridad tradicional no puede defenderse de los ataques, las redes domésticas y empresariales quedan indefensas. La industria no está lejos de poner en peligro la seguridad física de los usuarios, ya que se han detectado vulnerabilidades en múltiples ocasiones en dispositivos médicos, marcapasos, cámaras de seguridad, timbres inteligentes, monitores para bebés y automóviles conectados, entre otros.

Normalmente las capacidades de esos dispositivos IoT tienen capacidades limitadas de CPU, memoria y energía, pero pueden hacer multitud de cosas dedicados su principal objetivo ; recopilar información del entorno, de fábricas e incluso ciudades.

En IoT un alto porcentaje de dispositivos son creados para el consumo, como todo lo relacionado con la automatización de los hogares, vehículos conectados, salud, aspiradoras, lavadoras, etc.…todos conectados con Wifi. Sin embargo, también se crean nuevas necesidades que se gestionan desde internet. De hecho, muchos de estos dispositivos de consumo creados por fabricantes que se han dado mucha prisa por entrar en este mundillo han recibido algunas críticas por tratarse de dispositivos bastantes cuestionables en cuanto a seguridad se refiere.

2.1.1 Tipos de dispositivos IoT en la actualidad

Los dispositivos IoT se pueden dividir en dos tipos de dispositivos; **dispositivos basados en el consumidor y dispositivos para uso industrial**, como diferentes tipos de sensores para medir la temperatura, la humedad y el movimiento. Ejemplos típicos de dispositivos basados en el

consumidor son, podrían ser: Cámaras de vigilancia, frigoríficos, televisores inteligentes, wearables y automóviles conectados.

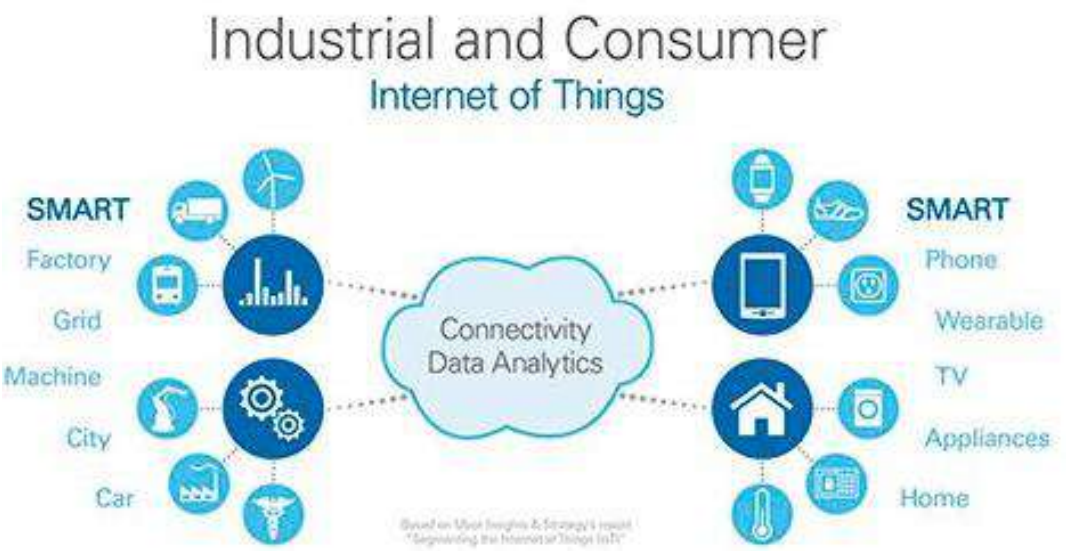


Figura 1- IoT industrial vs IoT commercial

Para la automatización del hogar, es decir, hogares inteligentes, los electrodomésticos típicos son, por ejemplo, sistemas de calefacción y ventilación, sistemas de control de iluminación y diferentes sensores para monitorear los niveles de humedad y CO2 dentro de una casa o edificio.

Cuando se habla del IoT industrial, debe mencionarse el término "Industria 4.0". La industria 4.0 cubre diferentes tipos de automatización y fabricación de tecnologías de intercambio de datos. Industria 4.0 significa que las máquinas de las fábricas y los sensores se comunican entre sí con menos o ninguna participación humana.

Por lo tanto, la automatización junto con el monitoreo intelectual proporciona una producción automatizada de mayor nivel, lo que mejora la calidad de los productos de usuario final. Basándose en el monitoreo de los resultados de los sensores, las máquinas pueden ajustar su funcionamiento de una manera más eficiente. Normalmente, las computadoras domésticas y las computadoras portátiles o incluso los teléfonos móviles no se consideran dispositivos IoT a pesar de llevar incorporadas redes inalámbricas GPS y sensores.

2.1.2 El Futuro e impacto del IoT

Según algunos estudios habrá hasta 26 mil millones de dispositivos IoT conectados en el año 2025. Sin embargo, el hecho es que la cantidad de dispositivos IoT podría ser aún mayor debido a la aparición de nuevos dispositivos IoT que vemos a diario, donde el segmento de consumidores ha aumentado considerablemente. El factor clave se encuentra en el lado del consumidor y los dispositivos de bajo costo desempeñan un papel importante. Si bien las innovaciones de IoT de hoy continúan impulsando la identificación y el establecimiento de nuevas relaciones entre objetos, sistemas y personas, el poder de la innovación crea continuamente nuevas capacidades para resolver problemas a una escala sin precedentes.

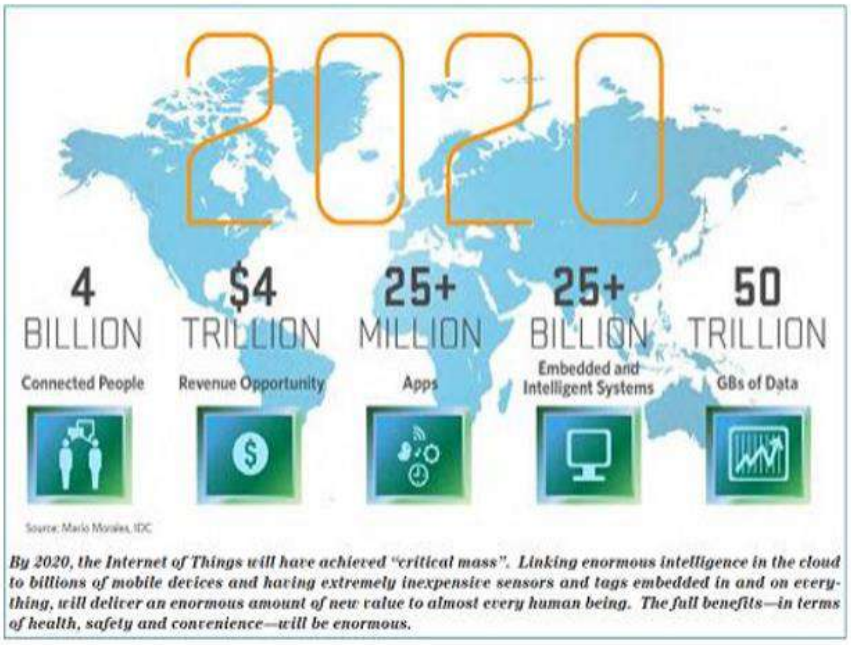


Figura 2 – Elementos conectados a IoT en 2020

Lo primero que se debe observar es el gran impacto que se producirá en todos los sectores ya que una red con tantos objetos "inteligentes" conectados entre sí necesita unas condiciones necesarias para que se pueda implantar correctamente y una de esas condiciones en las que centraremos este TFG es la seguridad y la privacidad de las personas, datos y comunicaciones.

Se estima que las aplicaciones para los consumidores, principalmente en el sector de la automoción, serán las que más difusión en los próximos años. Calculan que aproximadamente 13.000 millones de dispositivos conectados pertenecerán al sector de consumo. Tenemos un apartado dedicado a los Smart cars donde veremos los problemas y riegos que conlleva.

Seguido del sector consumo, afectará también en gran medida al sector industrial: los servicios públicos, la fabricación y el transporte serán los mercados clave de esta tecnología.
Las empresas estarán obligadas a buscar un equilibrio entre los datos recogidos y almacenados en la red por los dispositivos y sensores conectados, y el análisis de toda esa cantidad de información con el riesgo de su pérdida o mal uso. Todos los retos que plantea el IoT para la seguridad de toda esa información pondrán a las empresas en la obligación de invertir en seguridad tecnológica a unos niveles que nunca se habían pensado.

Internet de las cosas, sin duda tiene un potencial enorme y puede marcar un impacto muy significativo en el futuro de la sociedad, como hizo Internet en su día. Vamos a analizar el impacto a través de 3 puntos de vista: **Impacto en las personas, modelos de negocio que plantea, y el impacto a la hora de consumir recursos.**

<u>Impacto de IoT en las personas</u>

Interconexión de personas con personas, de personas con cosas y de cosas con otras cosas. En la misma definición de la tecnología ya se puede observar el impacto que tiene y tendrá en la sociedad IoT.

Todo estará interconectado con nosotros, basándose como referencia nuestro teléfono móvil que será la "neurona" central con la que nos conectaremos al resto del mundo. Y es que todas las aplicaciones que se están desarrollando actualmente ya dan por hecho que el usuario tiene una conexión a internet y se podrá conectar a una red sin problema. Los desarrolladores de aplicaciones y hardware solo tienen que reinventar lo que ya existe, dotándolo de conexión.

Veremos más adelante todos los peligros que esto conlleva, porque existen muchos riesgos en todo el proceso de desarrollo-comercialización-usuario.

La conexión en todo momento en una red, sin importar dónde ni cuándo, permaneciendo intercambiando datos con todos los destinos muestra de por sí el peligro que puede ocasionar.
De la resolución de esos problemas dependerá que el impacto hacia las personas sea bueno y útil, o sea un verdadero problema y una violación de todos los derechos de la sociedad.

Impacto de IoT en los negocios.

El hecho de que todo esté interconectado y las personas con ello, hace que las empresas sean capaces de adaptarse rápidamente a la nueva tecnología, sin que ello conlleve un cambio en su función principal a la que se dedique, ya que IoT cambiará la forma de trabajar y de prestar servicios a la sociedad.

No hace mucho tiempo, Con la era del 2.0 y las redes sociales, todas las empresas tuvieron que adaptarse a esta nueva forma de prestar servicios y descubrir nuevas líneas de negocio, creando nuevos puestos de trabajo orientados a nuevos expertos en la nueva tecnología. De igual forma va a ocurrir con IoT, se abrirán nuevas vías de negocio orientadas a la interconexión y aparecerán nuevas áreas de conocimiento y de trabajo.

Impacto en el consumo de recursos
La preocupación que existe hoy en día por el calentamiento global, las energías renovables, el consumo de recursos al nivel en el que lo estamos haciendo, y el aumento masivo de la población, ha hecho que los avances tecnológicos se centren en ayudar a frenar el proceso lo máximo posible.
La tecnología de Internet de las Cosas parece estar diseñada especialmente para esta tarea y es uno de los campos más prometedores. El uso de sensores puede controlar las diferentes variables necesarias para el mantenimiento de estos recursos tan necesarios y apreciados por nuestra sociedad.

2.2 Usos del IoT en la actualidad

Internet ha evolucionado rápidamente y esto ha permitido que IoT sea ya una realidad y no sólo una visión de futuro. La fama de esta tecnología radica principalmente en todas las aplicaciones y posibilidades que nos proporciona tanto para mejorar tanto la vida cotidiana de las personas como los entornos empresariales, dónde ya se está implantando desde hace algún tiempo.
Las aplicaciones son casi infinitas, pero se van a describir algunos ejemplos para dar visibilidad de alguna de ellas, tanto en la vida cotidiana como en el entorno empresarial:

Industria energética y redes inteligentes.

Podemos observar como rápidamente van desapareciendo esos días en que las empresas de servicios públicos envían trabajadores a los domicilios, para leer los medidores eléctricos y de gas instalados en el exterior de su casa. Algunas casas actualmente y otras dentro de poco tiempo,

estarán conectadas con dispositivos inteligentes que comunican la demanda eléctrica y cargan información con las empresas de servicios públicos.

Junto con la capacidad de una empresa de servicios públicos para llegar al electrodoméstico, esta tecnología apunta a hacer que nuestros sistemas de generación y distribución de energía sean mucho más eficientes y resistentes, Sin embargo, los electrodomésticos representan solo un componente de la red de área doméstica de la llamada red inteligente. Los sistemas de distribución, monitoreo y control de este sistema de energía involucran al IoT en muchas capacidades. La detección, el control y las comunicaciones que se necesitan en la producción de energía son elementos críticos de la IoT.

Si se piensa en aplicaciones industriales, IoT es usado ya en muchas plantas de producción dónde los dispositivos y sensores conectados a la red permiten analizar los datos y generar alarmas y mensajes que son enviados a los distintos usuarios para que tomen las acciones necesarias o incluso iniciar protocolos de actuación de forma automática, sin interacción humana, para corregir o tratar dichas alarmas.

Vehículos conectados y transporte

Estos vehículos aprovechan constantemente una serie de sensores a bordo que escanean la carretera y realice cálculos en tiempo real para identificar posibles problemas de seguridad que un conductor no podría ver. Además, puede incorporar otras posibilidades de comunicación adicionales de vehículo a vehículo (V2V) que permitan a otros automóviles enviar mensajes y señales a su vehículo. Los mensajes preventivos permiten tomar decisiones basadas en información que aún no está disponible para los sensores de visibilidad directa del conductor o del vehículo (por ejemplo, informes en tiempo real sobre tráfico en diferentes puntos). Con todas estas capacidades, podemos comenzar a tener confianza en las capacidades de los vehículos para conducir con seguridad y no solo informarnos sobre los riesgos.

Como comentábamos anteriormente, este sector también va a ser uno de los que más se beneficiarán de las nuevas tecnologías, y con él, los millones de usuarios que utilizan el coche, transporte público, etc. Las empresas más importantes del mundo de la automoción como General Motors van a invertir mucho dinero para desarrollar taxis inteligentes. Ford y Google siguen trabajando en coches automáticos sin conductor.

Edificios Inteligentes

El sector que más rápido ha crecido con respecto a esta tecnología y que es sin duda una realidad presente. Las casas se convertirán en un sistema inteligente capaz de adaptarse al usuario y a su forma de vida, de modo que el usuario pueda dejar de prestar atención a las tareas domésticas, hacer la comida o apagar las luces cuando vaya a dormir. Sin duda la seguridad también será un factor importante ya que la seguridad puede funcionar como no debiera y producir algún accidente doméstico.

Supongamos el frigorífico de una casa, dónde se conservan los alimentos que, a su vez, tienen una fecha de caducidad. En este escenario, se podría conectar el frigorífico a internet para que avisara al usuario a través de su teléfono móvil, por ejemplo, de cuando caducan los alimentos, si hay una bajada de temperatura por alguna avería, si algún alimento se ha está acabando o simplemente el consumo de electricidad en base al número de veces que se abre la puerta de la nevera.

Otro escenario podría ser el de la domótica, dónde ya hay numerosos dispositivos que se conectan a Internet para facilitarnos la vida , véase por ejemplo los dispositivos controlados por voz a los que se les solicita que reproduzcan una canción desde un repositorio en internet, o los dispositivos y aplicaciones que permiten controlar todos los parámetros del agua de un acuario, o incluso los sistemas de alarmas de las casas que se conectan con las centrales. Los sistemas de seguridad que se conectan a la red para avisarte cuando alguien entra en tu casa o aquellos dispositivos que permiten encender la calefacción desde un teléfono móvil.

Dispositivos médicos

Como ejemplo, los implantes incluyen cualquier sensor, controlador o dispositivo de comunicación que se inserta y opera dentro del cuerpo humano.

Si bien los dispositivos de IoT "implantables" suelen estar asociados con el campo médico (por ejemplo, marcapasos), también pueden incluir productos no médicos y casos de uso como etiquetas RFID integradas que se pueden usar en sistemas de control de acceso físico y lógico.

La industria de los implantes no es diferente a cualquier otra industria de dispositivos, ya que ha añadido nuevas interfaces de comunicación a los dispositivos implantados que permiten el acceso, control y monitoreo de los dispositivos a través de una red. Tanto los dispositivos wearables como los dispositivos IoT implantables están siendo miniaturizados en forma de sistemas mecánicos micro-eléctricos (MEMS), algunos de los cuales pueden comunicarse a través de radiofrecuencia (RF).

HeathCare

IoT tendrá muchas aplicaciones en el sector de la salud. La posibilidad de poder usar el teléfono móvil con sensores para poder medir las variables corporales y estar conectado con nuestro médico en todo momento. Poder realizar un diagnóstico rápido de un paciente, prevención de enfermedades o monitorear accidentes son las funciones principales que se esperan en este sector. Surgen campos como la realidad virtual, nanotecnología, telemedicina, etc. Todos estos dispositivos (oncología, radioterapia), estarán conectados a internet con el peligro que eso conlleva.

Agricultura y alimentación

Según la FAO (Organización de las Naciones Unidas para la alimentación y la agricultura) predice que el sector agrícola deberá enfrentarse al reto de tener que alimentar a 9,6 millones de personas que predicen para el año 2050. La producción del alimento deberá aumentar en 70% a pesar de los muchos de inconvenientes que debe de superar como la escasez de tierras de cultivo, el impacto del cambio climático en la agricultura, etc.

Aquí entra en juego la investigación de diferentes aplicaciones de IoT para este sector. Es necesario aumentar la calidad y cantidad de producción agrícola, y los sensores y la interconexión de estos producirá una agricultura inteligente. Está ocurriendo ya, aunque en menor medida.

Instituciones y corporaciones ya están recopilando grandes cantidades de información sobre cultivos, suelos, fertilizantes, información climática, maquinaria, etc. Por ejemplo, en el sector de la ganadería, ya se están utilizando sensores para monitorear y detectar las posibles enfermedades y trastornos en la salud de los animales, la temperatura corporal, el pulso, o la posición mediante GPS.

Farmacéutica

Este sector va de la mano con el sector de la salud y por lo tanto también se va a ver afectado por esta tecnología. Aunque en la industria farmacéutica la tecnología de IoT está todavía llegando, el potencial que se puede prever es enorme, sobre todo en la transmisión de datos de pacientes y seguimiento de medicamentos. Esta tecnología va a cambiar la manera de recoger los datos clínicos durante todo el proceso.

Algunos ejemplos de lo que se está empezando a desarrollar es un inhalador conectado a internet para enviar información de su uso. Así podrán monitorear cada inhalación y pueden hacer un seguimiento a sus pacientes. En el futuro veremos muchos acuerdos entre farmacéuticas y tecnológicas. La llegada del IoT a la industria farmacéutica junto con otra tecnología importante como es **Big Data**, supondrá una revolución, tanto a la hora de realizar los ensayos clínicos como la comercialización de medicamentos, hacer seguimiento a los pacientes, etc.

Transporte de personas y mercancías

IoT puede ofrecer soluciones para sistemas de peaje y tarificación, control de pasajeros, control de cargas y mercancías. También se podrá monitorear el tráfico al instante, que junto a sistemas de transporte inteligentes harán que los transportes de personas y mercancías sea más seguras. Las empresas de transporte se convertirán en más eficientes con contenedores de embalaje que puedan pesarse y escanearse por sí solos y optimizar en gran medida los flujos de transporte.

Medio ambiente

Uno de los mayores impactos y más importantes que se prevé es en el sector medioambiental, donde se estima que será el sector que más crezca en la utilización de dispositivos inalámbricos.
La integración de estos sensores y dispositivos abrirá las puertas a nuevas aplicaciones con impactos positivos sobre la sociedad como pueden ser el estado actual de los bosques, el nivel de contaminación, mediciones sobre el reciclaje, consumos de energía, etc.

El IoT en la empresa

IoT en las empresas también está avanzando con el despliegue de sistemas IoT que sirven para varios propósitos comerciales. En la industria de la energía, por ejemplo, el despliegue de infraestructuras de medición avanzadas (que incluyen medidores inteligentes con capacidades de comunicaciones inalámbricas) ha mejorado mucho el uso de energía y las capacidades de monitoreo de la empresa de servicios públicos.

La arquitectura de los sistemas empresariales de IoT es relativamente consistente en todas las industrias. Dadas las diversas capas de tecnología y los componentes físicos que comprenden un ecosistema de IoT, es bueno considerar una implementación de IoT empresarial como un sistema de sistemas. La arquitectura de estos sistemas que proporcionan valor empresarial a las organizaciones puede ser una tarea compleja, ya que los arquitectos empresariales trabajan para diseñar soluciones integradas que incluyen, puertas de enlace, aplicaciones, transportes, servicios en la nube, diversos protocolos y capacidades de análisis de datos.

Esta complejidad presenta desafíos para mantener la IoT segura y garantizar que las instancias particulares de la IoT no puedan usarse como un punto para atacar otros sistemas y aplicaciones

empresariales. Para esto, las organizaciones deben emplear los servicios de los arquitectos de seguridad empresarial que pueden ver el IoT desde una perspectiva global. Los arquitectos de seguridad deberán involucrarse de manera crítica al inicio del proceso de diseño para establecer los requisitos de seguridad que deben seguirse durante el desarrollo y la implementación del sistema IoT de la empresa.

En general, una implementación de IoT puede consistir en sensores inteligentes, sistemas de control y actuadores, servicios web y otros servicios en la nube, análisis de informes y una gran cantidad de otros componentes y servicios que satisfacen una variedad de casos de uso empresarial.

IoT amenaza con generar cantidades masivas de datos de entrada de fuentes que están distribuidas globalmente. La transferencia de la totalidad de esos datos a un solo lugar para su procesamiento no será técnica ni económicamente viable. La reciente tendencia a centralizar las aplicaciones para reducir costos y aumentar la seguridad son incompatibles con la IoT. Las organizaciones se verán obligadas a agregar datos en múltiples centros de datos distribuidos donde se puede realizar el procesamiento inicial. Los datos relevantes se enviarán a un sitio central para un procesamiento adicional.

En otras palabras, cantidades de datos sin precedentes se moverán de una manera sin precedentes. Los puntos de integración también desempeñarán un papel importante en la estrategia de adopción de IoT. La capacidad de hoy para compartir datos aumenta significativamente la superficie de ataque de una empresa; por lo tanto, deben evaluarse exhaustivamente para comprender las amenazas y como mitigarlas.

2.3. Tecnologías que se utilizan en IoT

Cuando se habla de Internet of Things, los dispositivos deben distinguirse entre dispositivos IoT comerciales e industriales, como comentamos en el apartado 2.1. Los dispositivos comerciales generalmente comprenden la automatización de casas inteligentes, cámaras de vigilancia para proporcionar más comodidad para la vida, actualmente, incluso las aspiradoras automáticas y los televisores inteligentes se pueden considerar dispositivos IoT. La cantidad de dispositivos IoT aumenta constantemente en el caso de hogares inteligentes, ciudades inteligentes o el sector de la salud.

Los dispositivos de IoT basados en la industria, Industria 4.0, suelen ser sensores o dispositivos similares que generan datos en bruto medibles procedentes de máquinas de las fábricas para proporcionar información que se basa en la toma de decisiones racional. El propósito de los dispositivos de IoT industrial es proporcionar más información sobre un proceso industrial o una máquina para guiar la producción. El objetivo de Industry 4.0 es ir hacia fábricas inteligente evitando cualquier intervención humana en los procesos de fabricación.

Los dispositivos de IoT suelen constar de las siguientes partes desde el punto de vista de la arquitectura. Los módulos básicos en el entorno de IoT, suelen ser sensores para recopilar datos medibles, la capa de transporte para entregar datos de sensores, dispositivos informáticos, aplicaciones de análisis de datos y almacenamiento para almacenar los datos. La Figura 4 muestra el punto de vista de la arquitectura del entorno IoT.

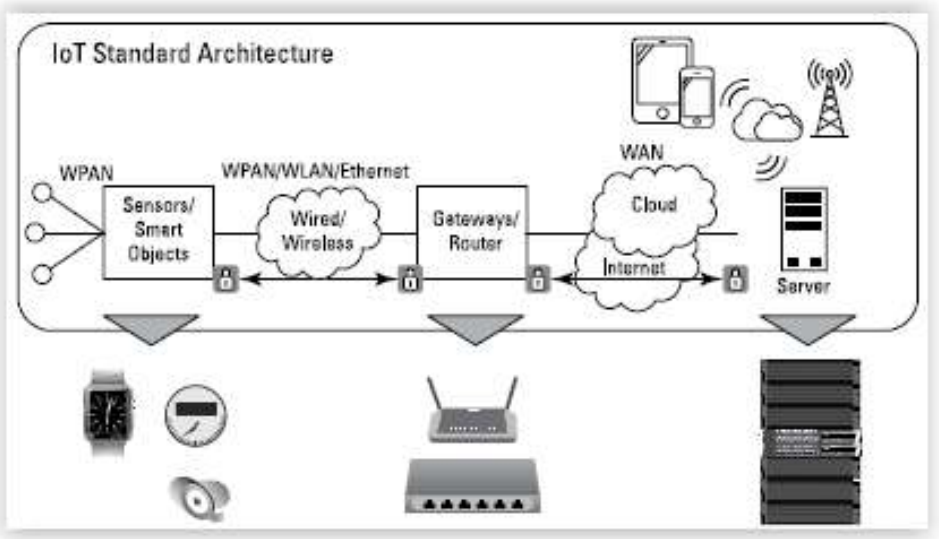


Figura 3. Arquitectura IoT (Miller 2016,6)

Como se puede ver en la figura, los componentes clave no son solo sensores u objetos inteligentes y servidores para recopilar datos, sino que la ruta de los datos, es decir la red, tiene un papel muy importante en este concepto arquitectónico. La red junto con el protocolo utilizado desempeña un papel importante dentro de los dispositivos de IoT. (Miller 2016, 32).

Los componentes básicos de la arquitectura de IoT se describen más detalladamente a continuación, pero primero mostraremos una versión reducida de lo que podría ser un dispositivo IoT sin contar con agentes externos como routers o servidores.

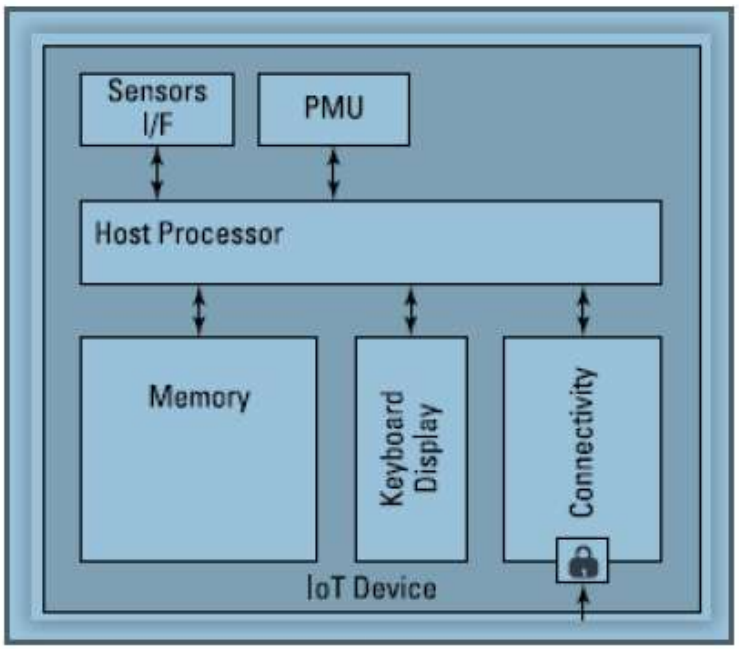


Figura 4. Dispositivo IT básico

Sensores

El propósito de los sensores es recopilar datos medibles de una máquina, dispositivo o entorno ambiental. El sensor es un componente electrónico que transforma el cambio de temperatura, la

humedad o el movimiento en formato electrónico y transmite los datos a una computadora. Los sensores se utilizan ampliamente en la industria para medir diferentes parámetros y en dispositivos domésticos de IoT.

Los sensores recogen por lo general variables físicas del entorno. Un sensor puede estar conectado a una calle, a una persona o a un automóvil, y se encargará de recoger datos característicos de lo que están conectados. Los sensores pueden actuar como desencadenantes de una acción, permitiendo la automatización de determinadas funciones. Este puede ser el caso de la activación de una alarma por la detección de una persona no autorizada o el frenado automático de un coche ante la inminente colisión con otro vehículo, en esta parte intervienen los llamados actuadores que ejecutan una acción en base a su programación y a lo que el sensor recopila.

Un sensor también podría ser un componente M2M, como un lector RFID (Radio Frecuency IDentification), o un medidor de SCADA (Supervisory Control And Data Adquisition).
A parte de estos sensores, tenemos otros dispositivos que actúan como sensores ya sean porque tienen sensores incrustados, como por ejemplo los teléfonos móviles, dispositivos del hogar, vehículos etc.

Los actuales smartphones, pueden recoger infinidad de datos precisos en tiempo real, lo que se convierten en el dispositivo número uno en la integración de IoT. Los fabricantes de dispositivos móviles deberán de comenzar a crear sensores más sofisticados para aumentar aún más la potencia y capacidad de recolección de datos. Los lectores RFID, lectores NFIC, e incluso los códigos QR pueden ser leídos por los smartphones.

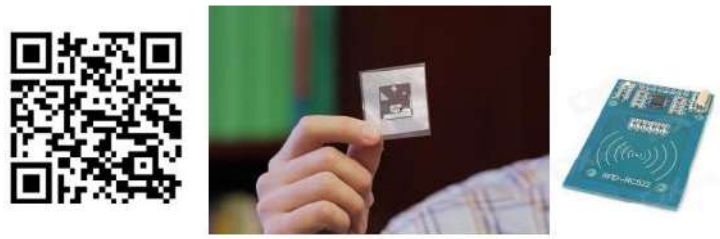


Figura 5 – Código QR, sensor NFIC y sensor RFID

Los sensores se utilizan en aparatos de uso diario para diversos fines. Por ejemplo, los sensores se utilizan en los automóviles para medir el nivel de escape de gas y, según esa información, ajustan la configuración de la gasolina y el oxígeno del motor del automóvil. Un área para los sensores son los sensores infrarrojos que se usan para las cajas de control remoto para el entretenimiento en el hogar, para la detección de movimiento y los detectores de intrusión.

Los sensores consumen energía y cuantos más pequeños, este consumo se convierte en un factor más limitador. Acorde con el tamaño del sensor, el tamaño de las fuentes de alimentación también disminuye y con ello el tiempo de funcionamiento del sensor. Por esta razón, se espera que los componentes sean capaces de generar su propia energía. De esta manera, los sensores podrán permanecer conectados a la red de forma autónoma durante más tiempo.

Capa de transporte

Igual de importante que los sensores es la infraestructura de comunicación. Todos los dispositivos necesitan una red para transferir y recibir datos para diferentes propósitos. Cuando se habla de dispositivos IoT, hay básicamente dos opciones diferentes disponibles, red cableada con conexiones de cobre o fibra, o conexiones inalámbricas con diferentes tipos de protocolos de comunicación. El

método de transferencia elegido siempre depende del tipo de dispositivo IoT y de cuáles son sus propósitos. Además, el protocolo utilizado juega un papel importante con los dispositivos de IoT.

Para las conexiones inalámbricas, hay múltiples opciones disponibles. El método de transferencia utilizado debe seleccionarse en función de la distancia de transferencia necesaria, ya que hay varias categorías para la distancia: conexiones inalámbricas de corto alcance, de medio alcance y de largo alcance. Ejemplos de corto alcance son los métodos de transferencia de **Bluetooth, Z-Wave y ZigBee**. La razón para usar el método de corto alcance es que estos dispositivos de IoT se utilizan como dispositivos de red de área personal y solo necesitan una velocidad de transferencia de datos de corto alcance y baja latencia. El rango físico suele ser desde pocos metros hasta 100 metros. Un punto clave es también el bajo consumo de energía.

Con los métodos de transferencia inalámbrica de rango medio, el bajo consumo de energía también es una característica importante. La tasa de datos también podría ser baja; sin embargo, puede haber una necesidad de comunicación de alta velocidad. Ejemplos de estos son HaLow, 802.11ah (IEEE 801.11ah 2018) y LTE Advanced, que es la versión mejorada de Long Term Evolution, LTE (LTE Advanced).

Un método de transporte muy común hoy en día es utilizar la red móvil 4G. Proporciona un método eficaz para transferir datos a alta velocidad, y la cantidad de datos también puede ser muy alto. En poco tiempo, la quinta generación de redes móviles, 5G, proporcionará una mayor velocidad y un alto rango de datos dentro de una nueva banda de frecuencia para proporcionar un medio más efectivo para futuros dispositivos de IoT.

Las redes inalámbricas permiten crear y desarrollar aplicaciones basados en la ubicuidad y la innovación. Actualmente cualquier usuario asume que en cualquier lugar a dónde va, va a disponer de una conexión a internet y va a poder utilizar todos los servicios disponibles.

Dentro de los protocolos más utilizados con dispositivos IoT son, por ejemplo, Message Queuing Telemetry Transport, MQTT, que funciona sobre el protocolo TCP / IP. El beneficio con MQTT es que es muy ligero y por lo tanto adecuado para aplicaciones IoT. Otro protocolo que hay mencionar es el Protocolo Avanzado de Message Queue Server, AMQP. Se basa en un estándar abierto y su objetivo principal es transmitir mensajes comerciales entre aplicaciones.

Servidor de aplicaciones

Desde la perspectiva de la arquitectura, los servidores en el entorno de IoT tienen múltiples roles. Los servidores son necesarios desde la ejecución del código de la aplicación hasta la administración de las aplicaciones de IoT necesarias. El dispositivo IoT puede necesitar varias aplicaciones para ejecutar lo que se pretende que haga. El servidor de aplicaciones puede ser basado en hardware o utilizando máquinas virtuales.

Como hemos comentado los servidores son necesarios para almacenar y administrar los datos en bruto generados por diferentes tipos de sensores. La cantidad de datos del sensor podría ser muy grande. El sistema de almacenamiento podría ser un almacenamiento de disco local basado en conectividad de canal de fibra, FC o almacenamiento de conexión de red, NAS o por supuesto utilizar un sistema de almacenamiento basado en la nube de un proveedor que ofrezca servidores en la nube.

Otra de las funciones clave del servidor es la autenticación del usuario para garantizar que solo los usuarios válidos que tengan privilegios para acceder a las aplicaciones de IoT. Existen varias opciones y "Best practises" para administrar las autenticaciones de los usuarios. Una posibilidad es administrar usuarios y posibles claves de seguridad localmente en el propio dispositivo de IoT o utilizar un servidor o aplicación específica de administración de usuarios dedicado para tales fines. Las posibilidades de acceso remoto y las autenticaciones de usuario también deben manejarse dentro del servidor de administración de usuarios.

Big Data y aplicaciones analíticas

Una parte importante en la arquitectura de IoT es el Big Data y aplicaciones analíticas. Actualmente hay varios proveedores que ofrecen aplicaciones para gestionar y administrar unas grandes cantidades de datos. Estas plataformas deben de permitir la gestión y el análisis de los datos en tiempo real y poder relacionar tecnologías entre sí.

La cantidad de datos generados por los dispositivos de IoT es enorme. No importa si los datos son generados por un sensor o una cámara de vigilancia o cualquier otro dispositivo de hardware IoT. Esta cantidad de datos es resulta inútil hasta que haya sido analizada y adaptada de tal manera que las personas puedan entenderla. En el peor de los casos, los datos generados del sensor son solo un texto básico de Ascii sin ningún formato.

El propósito de una aplicación de Big Data es ayudar a los analistas a comprender qué hay en los datos y, lo que es más importante, qué es lo más relevante en los datos analizados. Un papel clave con las herramientas de Big Data es también la capacidad de almacenar los datos y mantenerlos seguros. La Figura 6 representa una solución para el flujo de datos desde el sensor hasta la aplicación que realiza el análisis.

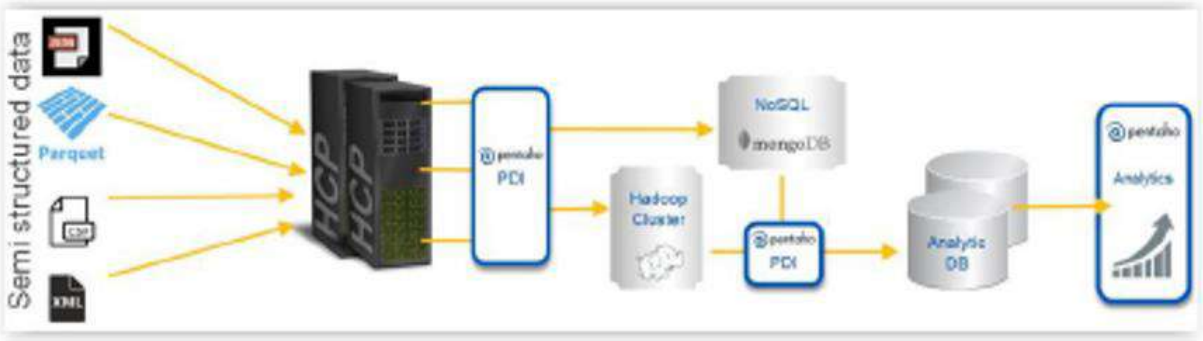


Figura 6 – Ejemplo flujo de datos sensor

El ejemplo anterior muestra el flujo de datos típico de los sensores y los módulos de aplicación necesarios para el análisis de datos. Los sensores y módulos de red están excluidos de este ejemplo.

El flujo de datos va de izquierda a derecha. Los datos sin procesar del sensor o cualquier información no estructurada o semiestructurada se recopilan desde varias ubicaciones a una ubicación principal con fines de almacenamiento. Después de la recopilación, los datos se modifican de tal manera que se pueden utilizar con las herramientas pertinentes donde se transmiten los datos a la base de datos. Las herramientas de análisis recogen los datos, los modifican y les dan el formato de tal forma que se pueden leer como tablas o gráficos.

3. Importancia de la seguridad en IoT

Uno de los mayores problemas a los que se enfrenta el IoT, es el haber avanzado en la implementación de esta tecnología en diferentes sectores sin tener en cuenta la seguridad desde un principio. Además, junto con la diversidad de tecnologías que se utilizan en todos los niveles de la arquitectura, provoca que hoy la seguridad en el ámbito IoT sea todavía uno de unos los puntos pendientes.

A pesar de esto, hay varias medidas que se pueden implementar tanto por parte de los consumidores como de los fabricantes, para garantizar una mejor protección de los datos. Hay que tener claro entonces las diferencias de estos dispositivos con respecto a los demás. Normalmente son menos complejos que un ordenador personal o Tablet ya que están diseñados para ejecutar una funcionalidad muy concreta. Esto hace que estos sistemas no sigan normas de fabricación específicas, debido a que cada fabricante habitualmente lo implementa siguiendo su propio diseño.

Esto dificulta que se pueda seguir un esquema común como ocurre con los ordenadores personales o smartphones que utilizan un sistema operativo común (MacOS, Windows, Linux, …), y los smartphones (Microsoft, Android, iOS,). De esta forma se pueden lanzar actualizaciones de seguridad comunes a cada sistema operativo porque es el fabricante de software quien las crea y despliega en los diferentes dispositivos.

En el caso de los dispositivos de IoT, es el fabricante del propio hardware el responsable de la creación y mantenimiento del software y en muchos casos puede que no se tengan los conocimientos ni la experiencia necesaria para poder proteger las posibles amenazas. A esto hay que añadirle que en muchos casos estos sistemas inicialmente no se diseñaron para estar conectados a Internet lo que conlleva que sean todavía más vulnerables y tengan un mayor riesgo de ser atacados.

Otro de los puntos a tener en cuenta en dispositivos IoT es su ubicación física, como pueden ser los sensores en semáforos, casas inteligentes, o cualquier otro tipo de sensores medioambientales, haciendo más difíciles de protegerlos, al estar accesibles por todo el mundo. Todo esto, añadido a los problemas de seguridad por defecto sobre la confidencialidad, integridad y disponibilidad, y sumado a que estos dispositivos tienen la capacidad de hacer cambios y actuar sobre el mundo real, puede ser un verdadero problema si no se consigue crear un sistema de seguridad robusto.

Desde que los ataques al IoT empezaron a hacerse cada vez más comunes, las preguntas sobre su seguridad comenzaron a centrarse en cuándo sucedería el próximo ataque, en lugar de qué medidas de seguridad se implementarían para evitarlos.

Mucha gente ya se ha dado cuenta que el IoT presenta pocas garantías en materia de seguridad que no deberían sorprendernos noticias acerca de un aumento de la inversión en soluciones de seguridad; tal como revelan algunos estudios recientes donde afirman que el gasto en seguridad para Internet de las Cosas crecerá en un 300% durante los próximos 5 años. Estos dispositivos conectados de forma insegura representan un serio problema, precisamente porque las vulnerabilidades existentes pueden aprovecharse de forma sencilla por parte de los delincuentes para crear ataques de denegación de servicio, como Mirai. Las posibilidades para los atacantes son cada vez mayores y, actualmente, y con la evolución de este tipo dispositivos no les va a faltar trabajo.

Una **botnet**, también conocida como ejército zombi, es una red constituida por un gran número de equipos informáticos que han sido "hackeados" por malware, de forma que quedan a disposición del atacante. Al tomar el control de miles de equipos, las botnets se suelen utilizar para enviar spam o virus, para robar información personal o para realizar ataques de denegación de servicio distribuido (DDoS). Actualmente, se consideran una de las mayores amenazas en Internet.

Figura 7 – Estructura de una botnet

Para que un equipo forme parte de una Botnet es necesario primero que se infecte con algún tipo de malware que se comunica con un servidor remoto o con otros equipos infectados de la red. Así, recibe instrucciones de quien controla la Botnet, normalmente ciberdelincuentes. A pesar de su gran alcance, la infección de malware Botnet no es diferente de una infección normal.

3.1 Amenazas y desafios de ciberseguridad más comunes con los sistemas de IoT

Los objetos y los sistemas con los que los usuarios interactúan como el teléfono, el coche, la llave de la puerta, la cámara de video, la Televisión, sistemas GPS, pueden ser gestionados a través de una interface vía Web. El usuario puede consultar en cualquier momento el estado de los objetos y sistemas. De igual modo, podrá recoger información acerca de los eventos que estos objetos envíen a la red pudiendo controlar en todo momento cualquier cambio, alteración o modificación de los parámetros que se estén están monitorizando o controlando.

En este apartado identificaremos los niveles de seguridad que existe en ciertos objetos que se encuentran conectados al internet, a nivel trasmisión de datos, de hardware, software, de configuración red, la Cloud y como no, la seguridad en los usuarios**.**

3.1.1 Niveles de Seguridad

Nivel transmisión de datos

Comenzaremos este bloque explicando los ataques en la transmisión de datos entre los dispositivos conectados a IoT, puesto que estos dispositivos están enfocados a estar continuamente transmitiendo información entre ellos o hacia la nube.

Como sabemos en el mundo del IoT intervienen una multitud de sistemas diferentes, o, dicho de otro modo, de sistemas distribuidos que emplean una gran cantidad de canales de distribución, ya sea inalámbricos, por cable, satélite, etc. Todas estas vías de comunicación, en particular las que son inalámbricas y en muchos casos redes públicas, son susceptibles de sufrir ataques. Por esta razón estos dispositivos necesitan garantizar un nivel de seguridad mínimo en cuanto a la ***integridad, protección y encriptación*** de sus comunicaciones ya que de lo contrario sería bastante fácil que un atacante pudiera acceder a esa información intercambiada durante la trasmisión. Esta información puede incluir datos personales o de carácter privado, o bien puede tratarse de datos técnicos que se pueden utilizar para tomar el control del dispositivo.

Es necesario por tanto un buen sistema de cifrado de datos para evitar los ataques de tipo *Man in The Middle*, en el que el atacante se encuentra en el medio de la comunicación, analizando todos los mensajes de ésta, con herramientas tipo sniffer - whireshark - sin que los participantes se den cuenta de que su comunicación está siendo interceptada. [1] Punto 4

Seguridad a nivel de hardware

Cuando se habla de seguridad a nivel de hardware estamos considerando de alguna manera, el acceso físico a los dispositivos que normalmente están conectados a Internet. Cuando un objeto se vuelve parte de un ecosistema interconectado, es necesario considerar que estos dispositivos han perdido seguridad física porque, aunque se encuentren a miles de kilómetros de distancia, podrían ser accesibles en cualquier instante por cualquier atacante. De igual modo, también podrían interceptar o modificar información, por lo tanto, podrían manipular los sistemas de control y modificar la funcionalidad con fines nada saludables.

La seguridad en el hardware para los objetos inteligentes se deberá considerar en la propia fabricación y estructura del producto de manera que permita la integridad de este y que no permita la manipulación directa en el caso de tener acceso a los mismos; por ejemplo una tarjeta de crédito inteligente deberá tener características físicas y un grado de protección suficiente de tal modo que no sea fácilmente manipulable o en el caso de un smartphone para gestionar una vivienda inteligente, se deberá considerar que en caso de pérdida o robo de dicho dispositivo las alternativas que permitan inmediatamente cambiar los accesos correspondientes para el control y monitoreo de los objetos de la vivienda. De lo contrario nos podemos imaginar que podría ocurrir. [1] Punto 4

Los ataques contra el hardware se producen especialmente cuando el dispositivo tiene una gran seguridad a nivel de software, cuando se encuentran muy bien protegidos y aislados de la red. Los ataques más habituales son los accesos a la información como memoria RAM y discos duros. Si podemos acceder a la memoria no volátil (ROM) es posible acceder a claves, información de acceso, etc.

Dos posibles medidas de protección para este tipo de ataques: La primera de ellas es garantizar que, aunque el dispositivo haya sido manipulado, se destruya de manera automática la información que contenga en caso de ataque. La segunda es un buen sistema de cifrado de información, de modo que, si finalmente acceden a los datos sea imposible descifrarlos. [1] Punto 4

Seguridad a nivel de software o lógico

A pesar de que nuestro sistema puede verse comprometido por la falta de seguridad física, resulta interesante indicar que la gran parte de los daños causados en un centro de datos no será sobre la infraestructura física sino contra información que se almacena y se procesa en el mismo. Hay que tener claro que el activo más importante que se posee en el campo de las TIC es la información, y

por lo tanto deben existir técnicas que aseguren este activo y es aquí, por lo tanto, donde entra la seguridad a nivel de software.

Parece razonable pensar que los usuarios a menudo no tienen en cuenta aspectos de seguridad cuando hacen uso de un dispositivo IoT, ya que, es habitual que se desconozcan los aspectos relacionados con la misma. De igual forma, estos aspectos a veces pueden considerarse una molestia, ya que la seguridad suele ir en contra de la comodidad y facilidad de uso. Es por esto por lo que los usuarios a veces puedan tener una imagen negativa de la seguridad, por considerarlo algo molesto y que interrumpe la capacidad de realizar un trabajo determinado.

En un entorno seguro, un usuario se encuentra con tareas que le pueden resultar incómodas como, por ejemplo, tener que cambiarlas contraseñas periódicamente, o tener que aceptar que llevar el móvil en el bolsillo para poder acceder office365, etc. y que pueden limitar las operaciones que puede realizar, así como los recursos a los que se le permite acceder. Sin embargo, la seguridad es fundamental a la hora de afrontar tareas que se realizan en sistemas informáticos ya que son las únicas medidas que pueden garantizar que éstas se realicen con una serie de garantías.

Los fallos de seguridad del software más comunes se podrían agrupar de la siguiente manera:

- Fallos debidos a errores desconocidos en el software, o conocidos sólo por entidades hostiles
- Configuración poco segura por defecto.
- Fallos debidos a una mala configuración del software, que introduce vulnerabilidades en el sistema.
- Contraseñas débiles, predecibles o dentro del código.
- Insuficiente protección a la seguridad

Los fallos descritos anteriormente pueden producir un mal funcionamiento de la aplicación, por lo que es necesario considerar lo siguiente:

- Pueden implementarse algoritmos de forma incorrecta lo que puede llevar a una pérdida de seguridad, por ejemplo, un algoritmo de generación de claves que no se base en números totalmente aleatorios.
- Pueden diseñarse servicios que, en contra de sus especificaciones, ofrezcan funcionalidades no deseadas o que puedan vulnerar la seguridad del servidor que los proporcione.
- Pueden no haberse tomado las medidas necesarias para asegurar el correcto tratamiento de los parámetros de entrada, lo que puede hacer que un atacante externo abuse de ellos para obligar al programa a realizar operaciones indeseadas.

Seguridad en la red

La seguridad de red no se basa en un método o procedimiento especifico, sino que utiliza un conjunto tecnologías y diferentes niveles de barreras que protegen y aíslan a la empresa. Incluso si falla una solución, se mantendrán otras que protegerán la red de una gran variedad de ataques.

Las tecnologías de seguridad de red protegen su red contra el robo y el uso incorrecto de información confidencial de la empresa y ofrecen protección contra ataques maliciosos de virus y gusanos. Estos pueden variar desde sistemas firewalls, detección de intrusos, routers y switches. Todos ellos pueden ofrecer algún tipo de seguridad, cada uno en un nivel diferente. Por ejemplo, los routers a nivel de la capa 3 de OSI, los switches mediante la creación de VLANS, los firewalls protegen a nivel de aplicación, etc.

Sin ningún tipo de seguridad a nivel de red, las empresas y por lo tanto los objetos conectados a la misma, se enfrenta a intrusiones no autorizadas, interrupción del servicio, periodos de inactividad de red, pérdida de información, etc. Nos ayuda a proteger la red de ataques internos y externos. Las amenazas se pueden originar tanto dentro como fuera del cortafuegos de una empresa. Un sistema de seguridad eficaz monitoriza toda la actividad de la red, detecta el comportamiento malicioso y adopta la respuesta apropiada en cada caso, como por ejemplo cerrar puertos o detener servicios.

Permite garantizar la privacidad de todas las comunicaciones. Los empleados o usuarios pueden acceder a la red desde cualquier lugar o mientras se desplazan, con la garantía de que sus comunicaciones serán privadas y estarán protegidas. Esto se lleva mediante el uso y utilización de VPNs. Una VPN (*Virtual Private Network*) es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Las empresas suelen utilizar estas redes para que sus empleados, desde sus casas, hoteles, etc., puedan acceder a recursos corporativos que, de otro modo, no podrían. [1] Punto 4

Como puede suponerse, a través de una VPN pasa información privada y confidencial que, en manos equivocadas, podría resultar perjudicial para cualquier empresa. Esto se agrava aún más si el empleado en cuestión se conecta utilizando una Wi-Fi pública sin ninguna protección. Afortunadamente, este problema puede ser mitigado cifrando los datos que se envían y reciben. Para poder lograr este objetivo, se pueden utilizar los siguientes protocolos: IPsec (*Internet Protocol Security*): permite mejorar la seguridad a través de algoritmos de cifrado robustos y un sistema de autentificación más exhaustivo o L2TP/IPsec (L2TP sobre IPsec): tecnología capaz de proveer el nivel de protección de IPsec sobre el protocolo de túnel L2TP. Al igual que PPTP, L2TP no cifra la información por sí mismo.

Por otro lado, este nivel controla el acceso a la información mediante la identificación de los usuarios y sus sistemas. Las empresas pueden establecer sus propias políticas de acceso. La denegación o la aprobación se pueden otorgar según las identidades de los usuarios, la función del trabajo u otros criterios específicos de la empresa.

En la actualidad tenemos, puntos de acceso inalámbricos en multitud de establecimientos, sucursales, oficinas domésticas, usuarios itinerantes que no paran de viajar, redes 4G de alta velocidad, servicios en la nube. Estos cambios pueden generar errores en las configuraciones que, a su vez, den lugar a problemas de seguridad. Por eso, es recomendable implementar soluciones de seguridad que se puedan poner en marcha de manera uniforme en todos los dispositivos y puntos de las infraestructuras que utilizan. También es necesario disponer de una gestión centralizada para poder monitorear cualquier actividad que ocurra en la misma. [1] Punto 4

Seguridad en la nube

Cada vez más empresas están empezando a adoptar servicios en la nube, como software como servicios (SaaS), infraestructura como servicio (IaaS) y plataforma como servicio (PaaS) por lo que a medida que aumenta el número de aplicaciones disponibles en la nube, los controles de las políticas para las aplicaciones web y los servicios en la nube deberán experimentar la evolución correspondiente.

Las tecnologías de almacenamiento en la nube en los últimos años han experimentado un crecimiento considerable en lo que respecta al número de usuarios finales y las empresas que la utilizan actualmente, hacen un alto uso de la nube; esto se debe a su gran ventaja de permitir el fácil

acceso a la información desde cualquier lugar, lo cual ha hecho de esta tecnología cada vez más popular.

Se debe realizar un análisis cuidadoso sobre, qué servicios puede utilizar cada usuario, quién debe tener permiso para publicar datos y quién puede leerlos. Aunque los servicios en la nube están desarrollando sus propios modelos de seguridad, deberán mantener cierta armonía con las estrategias de las empresas para evitar la proliferación de problemas con las contraseñas, los permisos y las infraestructuras de seguridad. La nube ofrece grandes oportunidades, pero la seguridad de las redes debe evolucionar al mismo ritmo.

Seguridad en la configuración y funcionalidad

Muchas veces, el principal problema radica principalmente en la configuración (por defecto, y posibles opciones configurables) y la funcionalidad del propio dispositivo.

Muchos fabricantes, a la hora de establecer la configuración por defecto del dispositivo, eligen unas opciones que posiblemente el usuario no va a utilizar nunca, o bien, que por estar activadas y permitir el uso de esa funcionalidad avanzada, el usuario no tenga suficientes conocimientos y la utilice incorrectamente, produciendo una brecha de seguridad y posible acceso para intrusos.

De nuevo, entra en juego el papel de fabricantes, que son los responsables directos de esta posible vía de acceso. Los distribuidores deben de ser conscientes, y adoptar una política de configuración segura, permitiendo además a los usuarios poder configurar el dispositivo acorde a sus necesidades.

Seguridad en los usuarios

Se va a terminar con una vía de acceso que no está relacionada directamente con los dispositivos IoT, sino con los usuarios. En muchos casos, si todos los puntos anteriores como el software, hardware, comunicaciones y configuraciones están perfectamente implementados y protegidos, un mal uso del usuario puede poner en serio peligro toda la información del dispositivo.

Es probablemente el principal motivo por el que se producen ataques sobre los dispositivos debido a que los usuarios son el eslabón más débil y pueden cometer errores. Uno de los principales ataques se basa en la llamada ingeniería social. Básicamente se centra en aprovechar los errores humanos para comprometer la seguridad de los dispositivos mediante la confusión y el engaño.

Debido a que la mayoría de los accesos a las plataformas privadas en internet se implementan mediante el uso de credenciales, la ingeniería social intenta acceder a ellas mediante estafas a través de correos electrónicos, sitios web falsos, o suplantación de identidad.

Es necesario crear una cultura de seguridad para los usuarios y concienciarlos sobre los problemas que pueden producir si no ponen atención a sus actividades mientras utilizan los dispositivos ya que como hemos comentado anteriormente, no sirve de nada que un dispositivo esté perfectamente protegido, si nuestra clave de seguridad la apuntamos en nuestra red social preferida. [1] Punto 4

3.1.2 Tipos más comunes de ataques en dispositivos IoT

Los ataques son acciones que se llevan a cabo de delincuentes con el fin de dañar un sistema o interrumpir las operaciones normales, explotando vulnerabilidades en los mismos utilizando

diversas técnicas y herramientas. Ataques con el fin de lograr objetivos ya sea por satisfacción personal o recompensa.

El grado de esfuerzo que un atacante debe emplear, se podría expresar en términos de su experiencia, recursos o motivación y se denomina **Vector de ataque**. Los actores son personas que son una amenaza para el mundo IoT. Pueden ser hackers, criminales, o incluso los propios gobiernos.

Los ataques más comunes podrían clasificarse en los siguientes:

• **Ataques de acceso**: En este ataque las personas no autorizadas obtienen acceso a redes o dispositivos de personas ajenas. Hay dos tipos diferentes de ataque de acceso: el primero es el acceso físico, mediante el cual el intruso puede llegar a acceder a un dispositivo físico. El segundo es el acceso remoto, que se realiza a dispositivos conectados con una dirección IP.

• **Ataques físicos**: Existen numerosos ataques que únicamente requieren de acceso físico al dispositivo IoT y a sus múltiples puertos o interfaces físicos (USB, Ethernet, consola, etc.), o incluso a sus botones. Desafortunadamente, numerosos dispositivos IoT deben estar en el **día a día al alcance del usuario**, al permitir la **interacción directa** con éste o **medir y tomar acciones en lugares concretos**, como en la vía pública, estaciones y aeropuertos, hospitales, edificios o en la habitación de un hotel.

Debe tenerse en cuenta que hay escenarios donde un atacante puede analizar las debilidades de un dispositivo IoT sin ni siquiera disponer de acceso físico al mismo, por ejemplo, obteniendo el firmware o los detalles de las actualizaciones desde la web del fabricante.

Este vector de ataque es probablemente el más prevalente ya que, sin las adecuadas protecciones a nivel físico, el dispositivo puede ser manipulado sin limitación hasta ser vulnerado.

• **Ataques de reconocimiento**: descubrimiento y mapeo no autorizados de sistemas, servicios, o vulnerabilidades. Ejemplos de ataques de reconocimiento podría ser el escaneado de puertos de red, rastreadores de paquetes, análisis de tráfico, y envío de consultas sobre información de direcciones IP.

• **Denegación de servicio DoS:** Un ataque de denegación de servicio, tiene como objetivo inhabilitar el uso de un sistema, una aplicación o una máquina, con el fin de bloquear el servicio para el que está destinado. Este ataque puede afectar, tanto a la fuente que ofrece la información como puede ser una aplicación o el canal de transmisión, como a la red informática.

• **Ataques a la privacidad**: El problema más común en dispositivos IoT. Estas amenazas afectan tanto a la privacidad del usuario como a la exposición de los elementos de red a personal no autorizado.
La protección de la privacidad en IoT se ha vuelto cada vez más difícil de proteger debido a los grandes volúmenes de información fácilmente disponibles a través de mecanismos de acceso remoto.

Desde Smart TVs a juguetes conectados, pasando por cámaras IP, dispositivos de grabación y todo tipo de dispositivos imaginables, se calcula que millones de estos dispositivos podrían ser víctima de algún ataque que se aproveche de vulnerabilidades existentes sin parchear o de a una mala política de gestión.

• **Ataque Man-In-The-Middle:** El término **Man-In-The-Middle** (hombre en el medio en inglés) denota un ataque de encriptación en una red de ordenadores. Es un tercer host que reenvía de forma transparente la información digital como una pasarela entre dos o más socios de comunicación y espías simultáneamente. El remitente y el destinatario no saben que hay un tercer host entre los dos y que en realidad no se están comunicando directamente

En un ataque de MITM, el atacante tiene control total de la información entre dos o más socios de enlace. Esto permite al atacante leer, influir y manipular la información. El atacante está reflejando la identidad del primero y del segundo interlocutor de comunicación, de modo que puede participar en el canal de comunicación. La información entre los dos hosts está cifrada, pero es descifrada por el atacante y transmitida.

• **Ataques basados en contraseñas**: A continuación, explicaremos cuales son las estrategias que usan los ciberdelicuentes para intentar robar contraseñas y de este modo ayudar a los usuarios de protegerse mejor contra este tipo de ataque o amenaza.

- Fuerza bruta: Consiste en adivinar la contraseña a base de prueba y error. Los ciberdelincuentes prueban distintas combinaciones al azar, conjugando nombres, letras, números hasta que den con el patrón correcto.

- Ataques de diccionario: Un software se encarga automáticamente de intentar obtener la contraseña. Empiezan con contraseñas simples y progresivamente van probando con palabras más complejas.

- Phishing: Una de las técnicas más utilizadas por ciberdelincuentes para robar contraseñas y nombres de usuario. Se trata de engañar a la víctima para que rellene un formulario fraudulento que suplanta a un servicio con sus credenciales de inicio de sesión.

- Ataque keklogger: La victima instala el malware en su equipo al hacer clic en un enlace o descargar un archivo de internet. Una vez instalado, el keylogger captura todas las pulsaciones del teclado, incluyendo las contraseñas y se las envía a los ciberdelincuentes.

• **Ataques de Supervisión de Control y Adquisición de Datos (SCADA**): Los sistemas SCADA (software de adquisición de datos y control de supervisión) se encargan de controlar sistemas industriales, por ejemplo, aquellos que filtran y distribuyen el agua, los que controlan el flujo en las tuberías de gas y petróleo, algunos controlan medios de transporte suburbano como el metro y otros más participan en una amplia variedad de sistemas que apoyan los procesos de manufactura. En consecuencia, esto ha provocado que desde hace no mucho se hayan vuelto el blanco de ataques informáticos.

Así pues, podríamos citar el caso de Vitek Boden en Australia, que, en el año 2000, tras ser despedido de una planta de aguas residuales, accedió de manera remota a los sistemas de su antiguo lugar de trabajo para verter lodo tóxico en ríos y parques con la idea de que por la gravedad del problema lo volverían a llamar y recuperaría su empleo.

Existen otros casos en los que la incursión de un virus informático también se ha traducido en un impacto en la disponibilidad de los sistemas SCADA. Por ejemplo, el gusano Slammer fue de las amenazas más recordadas de 2003 y entre sus efectos podemos citar el apagado de los sistemas de una central eléctrica de Ohio; ese mismo año parece que otro virus provocó una pérdida de potencia en una planta que electrificaba secciones de Nueva York, aunque el informe oficial de la Comisión Regulatoria de Energía Nuclear indica que no se tiene evidencia de tal hecho.

3.1.3 Prevención y salvaguardas

Llegados a este punto del TFG en el que ya se han repasado los ataques más comunes toca recorrer algunas de las posibles soluciones para hacer frente a las vías de ataque comentadas en puntos anteriores.

Control en las interfaces de acceso

La mayoría de los dispositivos que se conectan a la red necesitan de una serie de parámetros y opciones que pueden o deben ser configuradas según el escenario en el que convivan. Para eso las interfaces son muy importantes tanto para el usuario como para el fabricante.

El problema nace en el momento que las interfaces presentan sistemas de seguridad y autenticación obsoletos, inestables o incluso, inexistentes. La solución a este problema es realizar una interfaz capaz de poder ser controlada mediante dispositivos remotos como pueden ser tabletas, smartphones o incluso desde otro dispositivo IoT conectado. Esta interfaz debe de ser robusta y seguir una serie de "*buenas prácticas"* para que el acceso sea controlado y la seguridad, por tanto, completa.

En primer lugar, se debe de poder definir qué dispositivo o dispositivos son los que van a poder conectarse a esa interfaz si el acceso es abierto mediante internet. Si controlamos de esta forma los dispositivos, sería muy complicado que pudieran atacar nuestra interfaz de control del dispositivo y generar cualquier perjuicio.

En muchos casos, estas interfaces no **presentan ningún tipo de autenticación ni validación**, y cuando vienen implementadas, las credenciales no se han cambiado y siguen las que el fabricante suministró "out of the box".

Hay que hacer una mención especial en este apartado de autenticación la importancia de generación de las contraseñas, cuyas recomendaciones desde el Instituto Nacional de Tecnologías de la Comunicación (INTECO) se recomienda a los usuarios tener en cuenta las siguientes pautas para la creación y establecimiento de contraseñas seguras: Emplear un mínimo de **7 caracteres, mayúsculas y minúsculas, algún número y algún símbolo especia**l. Son precisamente las que hemos comentado anteriormente en el apartado de los ataques a contraseñas.

Otro de los puntos clave para el acceso a la interfaz del dispositivo se centra en el cifrado web. Cuando un sitio web implementa un sistema de cifrado hace uso del protocolo HTTPS. De este modo sería muy complicado que alguien pudiera interceptar nuestras credenciales de acceso ya que no estaríamos navegando y enviado datos en texto plano.

Otra de las opciones consistiría en utilizar un Virtual Private Network, o VPN. Esto nos permitiría crear una extensión de red segura sobre la red abierta Internet, de modo que estaríamos en una red privada con todas las funcionalidades existentes en Internet. [1] Punto 6

Actualización de dispositivos

Cuando un dispositivo aparece en el mercado, aparece con unas funcionalidades definidas y un software diseñado que aprovecha las capacidades de hardware. En muchos casos, aunque el usuario gestione correctamente el dispositivo y defina en la interfaz de control los parámetros adecuados

para una correcta seguridad, es el propio software el que presenta el problema ya que de base está mal implementado o configurado.

En este caso los esfuerzos del usuario resultan en vano ya que quien tiene que corregir este problema es el fabricante de software o hardware. La mejor solución para este tipo de problema es mantener constantemente el dispositivo **actualizado a la última versión que presente el fabricante** ya que las constantes actualizaciones presentan mejoras de seguridad, rendimiento, durabilidad, etc.

Por desgracia hay fabricantes que no presentan estas actualizaciones para solucionar los diversos problemas de seguridad. Una buena práctica consiste en analizar, a la hora de la adquisición de un dispositivo, los diferentes fabricantes para conocer quién da un mejor soporte de actualización del dispositivo y así saber que tenemos un respaldo del fabricante que resultará muy importante a largo plazo. [1] Punto 6

Configuración de red segura

Este punto no está enfocado únicamente para la seguridad en IoT, sino en general todos los dispositivos conectados a la red. Pero una de las mejores acciones que podemos poner en marcha a la hora de defendernos sobre cualquier ataque, es sin duda seguir las recomendaciones y buenas prácticas a la hora de configurar la red con la que trabajemos. En primer lugar, lo más importante es la configuración del **Firewall de la red o *Cortafuegos*.**

El cortafuegos es la primera parte de nuestro sistema de seguridad de la red que toma contacto con el exterior, y es quien va a controlar los accesos. Es por tanto una pieza clave a la hora de proteger nuestros dispositivos, aunque también puede ser el motivo por el que nuestro sistema sea totalmente vulnerable si su configuración está mal realizada.

Es por ello por lo que además entra en juego un **IDS o *Sistema de Detección de Intrusos***, que no es más que un programa que se encarga de detectar algún acceso no autorizado en nuestro sistema. En el caso de que nuestro Firewall sea defectuoso y provoque accesos no deseados, es nuestro IDS quien se encargará, gracias a los sensores virtuales, anomalías en la red que puedan ser indicio de ataques.

En el caso en el que un intruso accediera a nuestra red sin permiso y nuestro IDS lo detectase, un firewall bien configurado bloquearía los puertos y protocolos de comunicaciones para proceder a contrarrestar el ataque. [1] Punto 6

Control de aplicaciones en la nube (cloud services)

Como se ha estado comentando en todo el desarrollo de este TFG, una de las características y funcionalidades más importantes y atractivas de los dispositivos de IoT, es el acceso y suministro de datos a la nube.

El inconveniente de esta funcionalidad es su propia definición de servicio en la nube. Al estar abierta sin ningún tipo de restricción a todos los usuarios de la red, es necesario tomar una serie de medidas más estrictas. Hay que tener en cuenta que debemos de saber en todo momento como va a ser el traspaso de datos desde nuestro dispositivo al servicio, y viceversa.

Por tanto, la seguridad de este canal de comunicación es crucial, y se deben de seguir las recomendaciones de privacidad y acceso para evitar los problemas que se han expuesto en el punto de seguridad en la transmisión de datos 3.1.1.

Además, si el servicio que está en la nube es el que gestiona nuestro dispositivo, así como la gestión de los datos que proporciona, deberemos seguir las recomendaciones que hemos comentado sobre control de interfaces de acceso acerca de contraseñas y conexiones cifradas. [1] Punto 6

Uso de aplicaciones móviles

En la actualidad, en el nivel de desarrollo de la tecnología de IoT, la mayoría de las aplicaciones destinadas a IoT están orientadas a los smartphones. Esto es debido al gran auge que actualmente tienen los smartphones en nuestra vida cotidiana.

Mediante el smartphone es muy sencillo e intuitivo, debido a la cultura tecnológica que existe actualmente, poder gestionar nuestro dispositivo de IoT, acceder a nuestros datos, y monitorizar el estado actual del dispositivo. Sin embargo, para que la aplicación no se convierta en una vía de ataque, es necesario seguir una serie de requerimientos a la hora de utilizar estas aplicaciones.

Empezaremos por el primer eslabón en el proceso desde que descargamos la aplicación. Es crucial que la aplicación tenga un fabricante de confianza y una zona de descarga segura y confiable, así evitamos que desde el sitio de descarga se pueda introducir algún software malicioso. Se debe de descargar por tanto de la página oficial de aplicaciones. [1] Punto 6

El siguiente paso es instalar la aplicación. Se debe prestar mucha atención a los permisos que solicita la aplicación para poder ejecutarse. Por ejemplo, si instalamos una aplicación para poder controlar la temperatura de nuestro frigorífico, es lógico que requiera permisos de conexión a la red, pero no es que solicite permisos de lectura de nuestros mensajes.

Finalmente, debido a que nuestro smartphone lo usamos diariamente para más utilidades y no solo para el uso y control del dispositivo de IoT, debemos seguir las indicaciones que se han expuesto en el apartado de Actualización del dispositivo IoT.

4.Seguridad en dispositivos IoT orientados al consumidor

4.1 Por qué la seguridad y la privacidad de IoT son de particular interés

Los dispositivos IoT se enfrentan a los mismos tipos de desafíos de seguridad y privacidad que a los que están expuestos muchos dispositivos convencionales. Los dispositivos IoT, generalmente no ofrecen documentación clara que sirva para informar a un usuario sobre los riesgos que se presentan cuando se utilizan estos dispositivos. Además, los estudios han demostrado que confiar en el usuario final para las decisiones de seguridad no es una buena idea.

Entre las razones más relevantes podemos encontrar las siguientes:

Consumidores sin conocimientos técnicos o falta de interés.
Los usuarios finales no tienen normalmente los conocimientos técnicos necesarios para evaluar las implicaciones de privacidad y seguridad que implica la utilización de los dispositivos IoT, o pueden no tener ningún interés en hacerlo. Además, en muchas ocasiones, los dispositivos implementados

carecen de mecanismos automatizados para realizar actualizaciones seguras o hacer cumplir la política de seguridad necesaria.

Dificultad para la identificación de tanta variedad de dispositivos

Los usuarios ya tienen muchas dificultades para identificar y solucionar problemas de los dispositivos que actualmente están conectados a sus redes domésticas. Los dispositivos IoT complican esta situación aún más si cabe, ya que los consumidores conectan una cantidad cada vez más variada de dispositivos a sus redes domésticas aumentando la dificultad para comprender todo este "entramado" de cosas conectadas.

A medida que pasa el tiempo es probable que los usuarios pierdan de vista qué dispositivos están conectados, lo que hará que resulte aún más difícil protegerlos. Además, los ISP tendrán dificultades para ayudar a los consumidores a identificar el origen de los problemas de seguridad. Si bien los ISP pueden determinar que algún dispositivo en la red doméstica de un cliente ha sido atacado, es posible que no puedan identificar el dispositivo específico, debido a tecnologías como la traducción de direcciones de red (NAT) y otras tecnologías que pueden ocultar las direcciones IP actuales.

La tecnología IPV6 solucionará este problema ya que todos los dispositivos tendrán una dirección IP pública y por lo tanto visible y accesible desde cualquier punto del planeta. Tanto para la bueno como para lo malo.

Impacto en el servicio de acceso a internet

Los dispositivos IoT comprometidos con malware pueden afectar el servicio de Internet, tanto del usuario de dichos dispositivos, como de otros usuarios cuyo tráfico se realiza a través de los mismos enlaces compartidos de Internet. El malware se puede utilizar para lanzar ataques DDoS, enviar correo no deseado, atacar a otros dispositivos en la red del usuario o interferir maliciosamente con el servicio de acceso a Internet. Estos problemas aumentan los costos en los que incurre el ISP, que debe esforzarse mucho para mitigar estos ataques, ofreciendo soporte a los usuarios que no pueden entender por qué su servicio de Internet se está comportando de manera deficiente o anormal, e incluso hasta el punto de inhabilitarlo.

4.2 Muchos dispositivos no siguen las mejores prácticas de seguridad y privacidad

Es probable que se desplieguen millones de dispositivos IoT en los próximos años, lo que al mismo tiempo generará la posibilidad de convertirse en una gran plataforma para lanzar ataques y para recopilar información confidencial que se utilizara con fines maliciosos.

Además de las pérdidas que los consumidores pueden experimentar, los ISP podrían incurrir en un mayor número en las llamadas de soporte técnico, lo que aumenta el coste de las operaciones de los consumidores. Varios informes recientes han estudiado las características de seguridad y privacidad de los dispositivos IoT y han encontrado que algunos dispositivos no cumplen con las mejores prácticas de privacidad y seguridad más básicas. Los problemas potenciales que contribuyen a esta falta de privacidad y seguridad incluyen las siguientes:

Falta de incentivos para desarrollar e implementar actualizaciones después de la venta inicial

Para los dispositivos IoT de consumo vendidos a través de canales minoristas, los proveedores de dispositivos pueden tener pocos incentivos para implementar actualizaciones de software después de la venta inicial. Si los ingresos de un dispositivo provienen únicamente de la venta inicial, implica que cualquier mantenimiento del dispositivo tiene su impacto en esos ingresos iniciales, disminuyendo las ganancias. Esto al final puede fomentar la obsolescencia programada del dispositivo IoT, donde los proveedores priorizan la venta de nuevos dispositivos en lugar de dar soporte a los existentes.

Dificultad de actualizaciones seguras de software a través de Internet

Es posible que los dispositivos IoT no estén diseñados y configurados para recibir actualizaciones seguras de software a través de la red, lo que lleva a procesos de actualización complicados. Esto provoca que con el tiempo los dispositivos se vuelvan vulnerables.

Dispositivos con recursos limitados

Muchos de los dispositivos IoT que se venden en el mercado se diseñan con recursos de hardware limitados. Como resultado, ciertas medidas de seguridad básicas como el cifrado, la verificación de firmas de software y el control de acceso seguro no son factibles. Como consecuencia, los diseños que limitan el procesamiento y la capacidad de memoria de un dispositivo pueden impedir la ejecución de software de seguridad o impedir que se actualice de forma segura.

Dispositivos con interfaces restringidas

Muchos tipos de dispositivos IoT tienen interfaces de usuario limitadas o inexistentes. Incluso cuando un dispositivo implementa una interfaz de usuario a través de un dispositivo secundario (por ejemplo, una aplicación de teléfono inteligente), su funcionalidad puede ser mínima. Como resultado, las tareas como configurar un firewall local o desactivar los servicios remotos pueden resultar muy complicados. Los dispositivos también pueden carecer de la capacidad para mostrar mensajes de error o alertas a aquellos usuarios que quieran usar esta información para proteger mejor el dispositivo en cuestión.

Dispositivos con malware insertado durante la fabricación

En muchas ocasiones ocurre que los virus son insertados en los dispositivos en el momento de la fabricación, o incluso por terceros que dispongan de acceso al entorno de fabricación o empaquetado.

Un dispositivo comprometido a menudo parece funcionar normalmente, en cuyo caso la violación de la seguridad o la privacidad puede persistir hasta que se detecte el problema. Los firewalls y el aislamiento de la red no pueden defenderse contra este tipo de ataques ya que el problema viene de fábrica.

Falta de experiencia del fabricante con seguridad y privacidad

Muchos fabricantes de dispositivos IoT (y otras partes de la cadena de suministro de IoT) no tienen experiencia previa en el diseño, desarrollo o mantenimiento de dispositivos conectados a Internet. Estos fabricantes carecen de ciclos de vida de desarrollo seguros, equipos de respuesta a incidentes y experiencia con la ingeniería de seguridad y privacidad en general.

4.3 Riesgos por dispositivos vulnerables.

Los siguientes ejemplos ilustran el alcance de algunos de los problemas que pueden surgir cuando los dispositivos de IoT se vuelven vulnerables a los ataques de seguridad y privacidad. Un usuario no autorizado puede ser capaz de:

Realizar vigilancia y seguimiento no autorizados.

- Se puede saber si una persona está en el hogar, qué habitación ocupa y cuándo entra en ella.
- También se puede llegar a saber qué otros dispositivos están conectados a la red doméstica y cómo interactúan los usuarios con ellos.
- Es posible activar remotamente un micrófono o una cámara en un dispositivo para espiar a alguien.
- Y por último se puede incluso llegar a conocer si se abren o cierran puertas; la puerta de un garaje que se ha abierto y cerrado podría revelar si alguien está en casa, de tal modo que sirva para por ejemplo instalar de forma física un malware en una cámara IoT.

Obtener acceso o control no autorizado

- Sería posible apagar un termostato durante los meses de invierno para hacer que las tuberías de agua exploten dañando una vivienda.
- También es posible apagar las luces de todo el perímetro de una urbanización para ayudar en un robo físico.
- Abrir puertas para ayudar en una intrusión física o desactivar la alarma de un sensor de una puerta o ventana.
- Incluso se puede reutilizar un dispositivo para uso ilícito (por ejemplo, como minero de Bitcoin).

Provocar fallos en el dispositivo o sistema.

- Se pueden activar los sistemas de aire acondicionado residenciales para crear un aumento inesperado en una red eléctrica en un intento de crear condiciones que generen un apagón total.
- Es posible manipular los sensores de recolección de datos para modificar los parámetros relacionados con la salud, como la presión arterial, el azúcar en la sangre o información sobre el peso del paciente.
- También se podría impedir que un termostato controle la calefacción de un edificio provocando calor o frío extremos.

Todos estos escenarios crean graves riesgos de privacidad y seguridad para los usuarios finales y para Internet en general. Algunos riesgos de seguridad y privacidad para el usuario final también podrían permitir una nueva forma de acoso digital.

Los problemas de seguridad y privacidad con los dispositivos de IoT podrían, en última instancia, limitar el crecimiento futuro del sector de IoT, disminuyendo la demanda de este tipo de artilugios y por lo tanto es fundamental que estos problemas se aborden lo antes posible con el fin de respaldar el crecimiento a largo plazo del mercado de IoT.

4.4 Observaciones sobre temas de seguridad y privacidad de IoT

No es realista esperar que los fabricantes creen productos de software que estén libres de errores; cualquier software o aplicación tiene errores. Como resultado y como comentábamos anteriormente algunos dispositivos de IoT se envían "de fábrica" con un software que está desactualizado o se queda desactualizado con el tiempo.

Una de las mayores preocupaciones es que los fabricantes pueden enviar dispositivos con software obsoleto que contenga vulnerabilidades de seguridad, algunas de las cuales pueden explotarse inmediatamente cuando el dispositivo se conecta por primera vez a Internet.

Los dispositivos IoT que salen de fábrica con problemas de seguridad y privacidad no solo representan riesgos para los propietarios de los dispositivos, sino que también pueden ser explotados para abusar de todo el ecosistema IoT. Por lo tanto, la seguridad de los dispositivos de IoT es de interés no solo para los fabricantes (y otras partes de la cadena de suministro de IoT) y los clientes de dispositivos de IoT, sino también para Internet en general.

Comunicaciones inseguras en red

Los dispositivos de IoT en general pueden estar bastante limitados por los recursos, sin la potencia computacional y el ancho de banda de los dispositivos de computación más convencionales, como teléfonos móviles, ordenadores portátiles y ordenadores de sobremesa. Como resultado, muchas de las funciones de seguridad que están diseñadas para los dispositivos informáticos de uso más general son más difíciles de implementar en dispositivos IoT.

Por ejemplo, el cifrado de clave pública, que subyace en las comunicaciones seguras basadas en seguridad de la capa de transporte (TLS) y seguridad de la capa de transporte de datagramas (DTLS), puede ser difícil de implementar en ciertos dispositivos IoT con recursos limitados. Por ejemplo, los dispositivos Arduino y Raspberry Pi pueden tardar muchos segundos en realizar un cifrado asimétrico o una operación de descifrado. [5] Punto 4

Comunicaciones no autenticadas

Algunos dispositivos IoT proporcionan actualizaciones automáticas de software. Sin embargo, sin autenticación y cifrado, este enfoque es insuficiente, ya que el mecanismo de actualización podría verse comprometido o inhabilitado. El mecanismo de actualización en sí y todo el tráfico de control asociado debe ser autenticado y cifrado, y la integridad de las comunicaciones entre el dispositivo y otros puntos finales también debe poder protegerse. [5] Punto 4

Comunicaciones no cifradas

Muchos dispositivos IoT envían algunos o todos los datos sin cifrar. Esto significa que los datos pueden "filtrarse" y ser observados por otros dispositivos o por un atacante. Como resultado, algunos dispositivos de IoT filtran la información del usuario y esto puede identificar los dispositivos de IoT que se están utilizando, así como revelar la actividad y el comportamiento actual del usuario.

El envío de tráfico en texto claro no es el modelo recomendado para este tipo de implementaciones y crea problemas en los que la información personal o de otro tipo se filtra a través de una red local o de Internet. Sobre este tema, por ejemplo, la Junta de Arquitectura de Internet (IAB) sugiere e

insta a los diseñadores de protocolos a incluir por defecto el cifrado en sus implementaciones. [5] Punto 4

Falta de autenticación y autorización

Muchos ataques se originan detrás de un firewall. Como resultado, las comunicaciones detrás de un firewall no necesariamente deben considerarse confiables. Por lo tanto, un dispositivo debe establecer confianza entre los dispositivos, independientemente de si se encuentra en una red de área local o en Internet; *debe asumir que otros dispositivos no son de confianza de forma predeterminada* y deben estar autenticados y autorizados de forma explícita.

Un dispositivo que permite a una parte no autorizada cambiar su código, configuración, o acceder a sus datos, es una amenaza; el dispositivo puede revelar que su propietario está presente o ausente, facilitar la instalación u operación de malware o hacer que su función principal de IoT se vea comprometida.

Afortunadamente, a diferencia de los dispositivos informáticos de propósito general, como las computadoras portátiles, que pueden comunicarse con muchos destinos de Internet, los dispositivos IoT a menudo *se comunican con un pequeño número de destinos bien definidos.* Por ejemplo, un dispositivo puede comunicarse regularmente solo con un servidor de control o actualización que tenga un nombre DNS o una dirección IP conocidos.

Falta de aislamiento de la red

Además de los riesgos de seguridad y privacidad que presentan los dispositivos IoT fuera de la red doméstica donde está instalado, estos dispositivos también crean nuevos riesgos y son susceptibles de ataques dentro de la vivienda. Debido a que muchas redes domésticas no separan o segmentan, de manera predeterminada diferentes partes de la red entre sí, un dispositivo conectado a la red puede observar o intercambiar tráfico con otros dispositivos en la misma red doméstica, lo que hace posible que un dispositivo pueda afectar el comportamiento del resto de dispositivos conectados. Una red doméstica típica en la actualidad ofrece poco o ningún aislamiento entre dispositivos.

4.5 Fugas de datos o data leaks

La instalación de dispositivos IoT en el hogar crea la posibilidad de que estos dispositivos revelen los datos del usuario, tanto desde la nube (donde se almacenan los datos) como entre los dispositivos IoT.

Fugas de la nube

Muchos de los datos que recopilan los dispositivos de IoT se almacenan actualmente en servicios en la nube, fuera del hogar; estos servicios en la nube podrían experimentar una violación de sus datos debido a un ataque externo o una amenaza interna.

Algunos ejemplos incluyen: [5]Punto 5.2

- Una aplicación web asociada con un oso de peluche (que contiene una pequeña cámara en su nariz) contenía una vulnerabilidad de seguridad que dejaba expuestas las identidades de los niños.

• Una muñeca envío chats encriptados entre la muñeca y los servidores alojados en la nube utilizando una versión de TLS que era vulnerable a un ataque degradado, lo que hace posible escuchar las grabaciones de los niños.
• Las debilidades en la configuración del punto de acceso Wi-Fi en un vehículo motorizado hicieron que muchas ubicaciones de vehículos fueran rastreadas en sitios web que recopilan los nombres de los puntos de acceso Wi-Fi y sus ubicaciones.
• El sistema de un fabricante de automóviles envió estadísticas de ahorro de combustible, coordenadas geográficas precisas, velocidad, dirección y destino, en texto claro a un servidor central.

4.6 Recomendaciones

Esta sección del TFG presentamos algunas de las recomendaciones que se deberían de tener en cuenta para evitar los errores más comunes utilizando la tecnología existente.[5] Punto 7

1- Los dispositivos de IoT deben salir al mercado con un software razonablemente actual

Se recomienda que los dispositivos de IoT se envíen a los clientes o puntos de venta con un software actualizado que no contenga vulnerabilidades conocidas. Sin embargo, los errores de software son habituales y se dan casi por hecho, y no es raro que se descubran nuevas vulnerabilidades mientras los dispositivos están en la estantería esperando a ser comprados. Por lo tanto, es crítico que un dispositivo IoT tenga un mecanismo mediante el cual los dispositivos reciban actualizaciones automáticas y seguras durante todo el ciclo de vida del producto.

2- Los dispositivos de IoT deberían tener un mecanismo automático y seguro para actualizaciones de software

Los errores de software deben minimizarse, pero, como se señaló anteriormente, son inevitables. Por lo tanto, es fundamental que un dispositivo IoT tenga un mecanismo para actualizaciones automáticas y seguras de software. Se recomienda que los fabricantes de dispositivos IoT o proveedores de servicios de IoT diseñen sus dispositivos y sistemas basándose en el supuesto de que se descubrirán nuevos errores y vulnerabilidades con el tiempo.

Se deben diseñar sistemas y procesos para garantizar la actualización automática del software del dispositivo IoT, sin requerir o esperar ningún tipo de acción por parte del usuario. Si bien dichas actualizaciones en muchos casos deben ser automáticas y obligatorias para los usuarios finales.

3- Los dispositivos IoT deben usar autenticación robusta por defecto

Se recomienda que los dispositivos IoT estén protegidos de forma predeterminada (por ejemplo, protegidos por contraseña) y no utilicen nombres de usuario y contraseñas comunes o fáciles de adivinar (por ejemplo, "admin"). Finalmente, la autenticación para el acceso remoto debe ser segura, ya que potencialmente permite que otros que no están físicamente presente puedan monitorear y controlar aspectos dentro del hogar (por ejemplo, cambiar los controles de temperatura, monitorear la actividad del usuario). Las credenciales de autenticación deben ser únicas para cada dispositivo.

Los posibles métodos de autenticación predeterminados que satisfacen estos criterios incluyen: (1) enviar cada dispositivo con una contraseña predeterminada fija, pero exigirle al usuario que la cambie como parte del proceso de instalación (es decir, antes de que funcione el dispositivo); y (2)

enviar cada dispositivo con una contraseña única para cada unidad donde se imprima la contraseña en una etiqueta que está pegada al dispositivo.

4- Las configuraciones de dispositivos de IoT deben ser probadas y testeadas

Algunos dispositivos IoT permiten que un usuario personalice el comportamiento del dispositivo.

Se recomienda que los fabricantes prueben la seguridad de cada dispositivo con un amplio rango de configuraciones posibles, en lugar de simplemente utilizar la configuración predeterminada. La interfaz de un dispositivo debería evitar, o al menos desalentar activamente, que los usuarios configuren el dispositivo de una manera que lo haga menos seguro.

5- Los dispositivos IoT deben seguir las mejores prácticas de seguridad y criptografía

Los fabricantes de dispositivos IoT deben proteger las comunicaciones utilizando Transport Layer Security (TLS) o Lightweight Cryptography (LWC). Algunos dispositivos pueden realizar cifrado de clave simétrica en tiempo real. Además, Lightweight Cryptography (LWC) ofrece opciones adicionales para proteger el tráfico hacia y desde dispositivos con recursos limitados. Si los dispositivos dependen de una infraestructura de clave pública (PKI), una entidad autorizada debe poder revocar los certificados cuando se vean comprometidos, como lo hacen los navegadores web y los sistemas operativos de PC.

De igual modo, los proveedores que confían en el almacenamiento en la nube para dispositivos IoT deben configurar sus servidores para que sigan las mejores prácticas, y como configurar la implementación TLS/SSL para que solo acepte las últimas versiones de los protocolos utilizados.

Finalmente, los fabricantes deben evitar métodos de cifrado, protocolos y tamaños de clave con debilidades conocidas. Ejemplo WEP. Contiene varias debilidades serias que fueron identificadas por analistas criptográficos. Como consecuencia, hoy en día una protección WEP puede ser violada con software fácilmente accesible en pocos minutos.

Cifrar las comunicaciones de forma predeterminada para gestión de dispositivo
Como explicábamos anteriormente, el uso de una comunicación no autenticada o de texto sin cifrar para administrar un dispositivo representa un riesgo de seguridad significativo por lo tanto se recomienda que todas las comunicaciones para la gestión del dispositivo se realicen a través de un canal autenticado y seguro.

Comunicaciones seguras hacia y desde los controladores de IoT
Si los dispositivos IoT utilizan un controlador centralizado para facilitar la comunicación a través de Internet con un servicio en la nube, es vital que este canal de comunicaciones esté protegido en ambas direcciones.

Utilizar credenciales únicas para cada dispositivo
Se recomienda que cada dispositivo tenga credenciales únicas. Si un dispositivo utiliza criptografía de clave pública (por ejemplo, para firmar mensajes, intercambiar una clave de sesión o autenticarse), cada dispositivo debe tener un certificado único y verificable. Si un dispositivo utiliza criptografía de clave simétrica, nunca se deben compartir la clave simétrica con otras partes.

Usar credenciales que pueden ser actualizadas
Es recomendable que los fabricantes de dispositivos admitan un mecanismo seguro mediante el cual se puedan actualizar las credenciales utilizadas por un dispositivo. Sin embargo, la implementación

segura de esta recomendación requiere un cuidado especial, ya que una implementación incorrecta puede introducir un nuevo ataque.

Cerrar puertos innecesarios y deshabilitar servicios innecesarios
Es necesario que los fabricantes de dispositivos cierren puertos innecesarios, como telnet o ftp e implementen SSH en su lugar. Por otro lado, los dispositivos deben cerrar o deshabilitar las interfaces y funciones administrativas que no se están utilizando. Los dispositivos tampoco deben enviarse con controladores que el dispositivo no esté utilizando.

6- Comunicación de los dispositivos debe ser restrictiva

Es importante que los dispositivos de IoT se comuniquen solo con puntos en los que se confié. Siempre que sea posible, los dispositivos no deben ser accesibles a través de conexiones entrantes de forma predeterminada. Los dispositivos IoT no deben confiar solo en el firewall de la red para restringir la comunicación, ya que algunas comunicaciones entre dispositivos dentro de la red local pueden no necesariamente atravesar el firewall.

7- Los dispositivos IoT deberían continuar sin conectividad a Internet

Un dispositivo IoT debería poder realizar su función o funciones principales incluso si no está conectado a Internet. Esto se debe a que la conectividad a Internet se puede interrumpir debido a causas que van desde una configuración incorrecta accidental o un ataque intencional (por ejemplo, un ataque de denegación de servicio); La función del dispositivo debe ser robusta frente a estos tipos de interrupciones de conectividad.

Los dispositivos de IoT que tienen implicaciones para la seguridad del usuario deben continuar funcionando sin conexión para proteger la seguridad de los consumidores. En estos casos, el dispositivo o el sistema backend deben notificar al usuario acerca del fallo. Cuando sea posible, los fabricantes de dispositivos deberían facilitar a los usuarios la desactivación o el bloqueo del dispositivo sin obstaculizar la función principal del mismo.

8- Los dispositivos IoT deberían continuar funcionando si hay un error en la Cloud

Muchos servicios que dependen o usan un backend en la nube pueden continuar funcionando, incluso cuando la conectividad con el backend de la nube se interrumpe o el servicio falla. Por ejemplo, un termostato cuya configuración puede modificarse a través de un servicio en la nube debería, en el peor de los casos, continuar funcionando con la configuración de última hora o predeterminada. Una cámara de seguridad doméstica alojada en la nube debe ser accesible desde el hogar, incluso cuando falla la conexión a Internet.

9- Los dispositivos IoT deberían admitir las mejores prácticas de direccionamiento y asignación de nombres

Muchos dispositivos IoT pueden permanecer implementados durante muchos años después de su instalación. Como resultado, los dispositivos IoT deben admitir las mejores prácticas, para el direccionamiento IP y el uso del Sistema de nombres (DNS). La compatibilidad con los últimos protocolos garantizará que estos dispositivos sigan funcionando durante los próximos años, y que puedan admitir importantes funciones de seguridad basadas en DNS.

10- Los dispositivos de IoT deben enviarse con una política de privacidad que sea fácil de encontrar y entender

Se recomienda que los dispositivos IoT se envíen con una política de privacidad, pero esa política debe ser fácil de encontrar y comprender para un usuario común.

11- La cadena de suministro de IoT debería desempeñar su papel para abordar la seguridad de IoT

En la cadena de suministro, a menudo es difícil definir los roles que cada parte desempeña a lo largo del tiempo. Los usuarios finales de los dispositivos IoT y otros dependen de la cadena de suministro para proteger su seguridad y privacidad, y algunas o todas las partes de esa cadena de suministro desempeñan un papel fundamental durante todo el ciclo de vida del producto. Además de otras recomendaciones en esta sección, se recomienda que la cadena de suministro IoT tenga en cuenta los siguientes aspectos:

• Los dispositivos deben tener una política de privacidad que sea clara y comprensible, particularmente cuando un dispositivo se vende junto con un servicio continuo.

• Los dispositivos deben tener un mecanismo de restablecimiento que borre toda la configuración cuando un consumidor devuelve o revende el dispositivo. Los fabricantes también deben proporcionar un mecanismo para eliminar o restablecer cualquier información que el dispositivo almacene en la nube.

• Los fabricantes deben proporcionar un sistema de informe de errores con mecanismos de envío de errores bien definidos y una política de respuesta documentada.

• Deben proteger la cadena de suministro para evitar la introducción de malware durante el proceso de fabricación, así como tomar las medidas adecuadas para asegurar su cadena de suministro de software.

• Los fabricantes deben soportar y gestionar el dispositivo IoT a lo largo de su vida útil, desde el diseño hasta el momento en que se retira un dispositivo, incluida la transparencia sobre el tiempo durante el cual planean proporcionar soporte continuo para un dispositivo, y lo que el consumidor debería esperar.

• Los fabricantes deben proporcionar métodos claros para que los consumidores determinen con quién pueden ponerse en contacto para solicitar asistencia, así como facilitar la forma de comunicarse con los consumidores a fin de difundir información sobre vulnerabilidades de software u otros problemas.

• Los fabricantes deben informar sobre el descubrimiento y la remediación de las vulnerabilidades de software que presentan amenazas de seguridad o privacidad para los consumidores.

• Por último, los fabricantes deberían proporcionar un proceso de informe de vulnerabilidades fáciles de localizar en todo momento.

5. Wearable Technology

La tecnología Wearable generalmente incluye dispositivos personales como relojes inteligentes y dispositivos médicos como marcapasos inalámbricos o bombas de insulina. El principal problema de seguridad para este tipo de tecnología es la seguridad de los datos. Estos dispositivos recopilan y

transmiten grandes volúmenes de información personales sobre el propietario. En tales casos, el robo de datos y la privacidad son el principal riesgo de seguridad. Asimismo, los dispositivos médicos recopilan y transmiten información de salud privada y detallada sobre el paciente.

Al igual que en otros dispositivos IoT, la privacidad es el principal problema; un atacante que obtiene el control remoto de un dispositivo médico podría dañar o incluso matar a un paciente, por ejemplo, causando un mal funcionamiento del marcapasos o en el caso de las bombas de insulina se podría administrar al paciente exceso o insuficiente insulina.

A continuación, explicaremos las vulnerabilidades de seguridad más comunes que se pueden encontrar en este tipo de dispositivos:

1- Transmisión no segura de datos a través de Bluetooth para el almacenamiento local del dispositivo

Estos dispositivos dependen de la conexión via Bluetooth para realizar la transmisión de los datos recopilados desde los sensores hacia los teléfonos inteligente. Como resultado, el atacante puede explotar el error en el dispositivo para extraer los datos almacenados localmente, como registros relacionados con la salud. Por ejemplo, un atacante puede simplemente usar rastreadores para robar datos no autorizados detectando las señales de transmisión que emite el IoT mientras se comunica a través de Bluetooth.

2- Almacenamiento de datos inseguros en la nube

La nube utiliza un espacio público o semipúblico. El almacenamiento en la nube proporciona una mejor accesibilidad ya se puede acceder a los archivos almacenados en cualquier momento desde cualquier lugar, siempre y cuando tenga conexión a Internet.

Esta podría ser la zona más vulnerable en el mundo de los wearables debido a la cantidad de Información de identificación personal (PII) disponible. La sincronización con destino a la nube podría plantear una serie de riesgos, incluidos los ataques distribuidos de denegación de servicio (DDoS), SQL Inyección, o ataques por la puerta trasera (backdoor).

3- Falta de autenticación y autorización

La mayoría de los dispositivos wearables a menudo no vienen con un mecanismo de seguridad incorporado como las funciones de autenticación del usuario o de protección del sistema PIN y, por lo general, almacenan datos localmente sin cifrado. Además de eso, estos dispositivos requieren una mayor comunicación de seguridad en relación con el cifrado, la integridad de los datos, la confidencialidad y otros servicios de seguridad, ya que se basa en la red inalámbrica no controlada, ya sea Bluetooth o conexión Wi-Fi para transferir datos. Sin embargo, es difícil de aplicar medidas de seguridad más altas debido a su tamaño pequeño y ancho de banda limitado por lo que resulta más fácil de ser atacado. Por ejemplo, un estudio reveló que el 30 por ciento de los smartwatches que probaron durante un test eran vulnerables.

4- Falta de controles de seguridad física

Otra vulnerabilidad de seguridad para los dispositivos wearables es la posibilidad de pérdida del dispositivo. Debido a que estos dispositivos suelen ser de tamaño reducido, es más probable que podemos dejarlo olvidado en cualquier lugar. Los dispositivos perdidos o robados supondrán un riesgo para la exposición de los datos. Además, la mayoría de los dispositivos wearables a menudo

no vienen con un mecanismo de seguridad, como la autenticación del usuario o sistema de protección del sistema PIN.

Por ejemplo, Apple Watch y Google la plataforma Android Wear no tiene ninguna medida de seguridad para proteger sus costosos wearables de pérdida o robo. A continuación, se presenta un análisis sobre diversos desafíos de privacidad y aspectos de ataques a dispositivos wearables.

5.1 Desafíos y ataques de privacidad del WT

Los ataques de privacidad que plantea en WT (Wearable Technology) se pueden clasificar en privacidad de usuarios, privacidad basada en datos, privacidad basada en el tiempo y privacidad basada en la ubicación.

Identidad del usuario y privacidad de datos. Los sensores integrados, como cámaras y micrófonos, capturan datos sobre el individuo y del entorno, muchas veces sin su consentimiento. Estos datos a menudo son personales, confidenciales y sensibles, que invade la privacidad de los usuarios y plantea desafíos de privacidad como la vigilancia. Por ejemplo, Glass puede ser fácilmente pirateado ya que no tiene una implementación de autenticación fuerte. Los atacantes pueden tomar el control total y monitorear todo lo que el propietario está haciendo con la cámara y micrófono.

Privacidad basada en el tiempo y la ubicación GPS integrado en el propio dispositivo capaz de rastrear la ubicación de una persona en un momento específico. El GPS ofrece beneficios para la navegación, pero obviamente también conlleva otros riesgos. Se plantean serios problemas en la privacidad del usuario, si la ubicación de las personas puede ser rastreada. Por ejemplo, Symantec reveló que los dispositivos wearables también pueden hacer seguimiento de ubicación, aunque no hay un sensor GPS incorporado.

Esto puede ocurrir porque en el intercambio de información se puede revelar la dirección hardware del dispositivo (dirección MAC) el cual puede ser detectado con algunos rastreadores que son capaces de detectar esta dirección cuando el dispositivo se sincroniza con el teléfono móvil del usuario a través de Bluetooth.

5.2 Problemas de autenticación en dispositivos Wearables

Se supone que los dispositivos wearables deben protegerse con un mecanismo de autenticación seguro, ya que contiene una gran cantidad de información sensible. La razón de esto podría ser que los dispositivos portátiles suelen carecer de un teclado o incluso una pantalla táctil. Por lo tanto, para muchos usuarios puede resultar todo un desafío implementar una contraseña o un PIN autenticación. Por otro lado, debido al pequeño tamaño de estos dispositivos, su capacidad de procesamiento y el ancho de banda dificultan considerablemente la implementación de mecanismos de seguridad.

Sin embargo, como los wearables hacen un uso cada vez mayor de los datos personales del usuario - desde las estadísticas de fitness hasta registros de salud - la seguridad tiene que considerarse un factor crítico y darle la importancia que merece. A diferencia de los dispositivos móviles, los dispositivos wearables están siempre encendidos y están continuamente recopilando datos.

Las medidas de seguridad no solo son importantes para proteger los datos personales, sino que también son un factor crítico ya que los smartwatchs se introducen en el lugar de trabajo y también

se conectan a redes corporativas. Como consecuencia, es muy importante que se preste especial atención al mantenimiento de la confidencialidad, la integridad. y disponibilidad (tríada de la CIA).

Conclusión

A medida que avanza el mercado de IoT, WT está creciendo en popularidad por su comodidad y capacidades. WT ofrece mejores funcionalidades al proporcionar comunicación de datos en tiempo real, pero también plantea un mayor riesgo de seguridad y privacidad. Estos dos grandes retos serían los obstáculos para que WT sea adoptado ampliamente en el mercado.

Los usuarios están preocupados por la seguridad de los wearables, ya que los datos recopilados pueden consistir en información sensible sobre ellos mismos, tales como la identidad, información relacionada con la salud, o la ubicación.

Aunque esta tecnología beneficia a las personas, todavía hay algunas lagunas de seguridad y problemas de privacidad que requieren una mayor atención y esfuerzo del fabricante en el diseño de dispositivos wearables.

6. Connected Cars

El tamaño del mercado mundial de vehículos conectados alcanzó los $ 72.89 mil millones en 2017, y se espera que supere los $ 219 mil millones en 2025, según los últimos datos de ResearchAndMarkets.com . El crecimiento de la industria se debe principalmente al aumento de las posibilidades que pueden ofrecer los coches conectados, así como a los avances en la legislación relacionada. Sin embargo, hay una cosa que evita que la industria se generalice entre los consumidores, y es el hecho de que las aplicaciones de IoT se consideran un objetivo fácil para los ataques cibernéticos , lo que puede tener consecuencias graves.

Si bien ha habido varios intentos de establecer normas unificadas para la seguridad de los datos, por ejemplo, GDPR (General Data Protección, Regulación) los proveedores y fabricantes de IoT no tienen que seguir ciegamente las normas prescritas. Siempre hay espacio para mejorar, especialmente cuando se trata de seguridad de datos.
En este artículo, repasaremos algunas de las tácticas más habituales para garantizar la seguridad de los automóviles conectados y las aplicaciones de software relacionadas.

Según los últimos datos, la proporción de autos conectados a Internet entre los vehículos nuevos vendidos en todo el mundo alcanzará el 100% para 2022. Eso indica claramente la existencia de grandes oportunidades para los fabricantes y desarrolladores de aplicaciones de IoT para lanzar al mercado y fabricar a unos 190 millones de vehículos para 2021.

Los coches conectados abren una amplia gama de capacidades para controlar de forma remota un vehículo, como el seguimiento de la ubicación, la navegación, la función de bloqueo / desbloqueo, los controles de temperatura, los diagnósticos del motor, el botón de arranque del motor, etc. Por lo tanto, los beneficios de los coches conectados son bastante obvios:

- Conveniencia, optimización y una experiencia de conducción agradable
- Mayor seguridad
- Mejor control sobre el vehículo y su diagnóstico remoto
- La capacidad de automatizar tareas rutinarias (estacionamiento y asistencia de carril)
- Ahorro de costes debido a la detección oportuna de posibles problemas

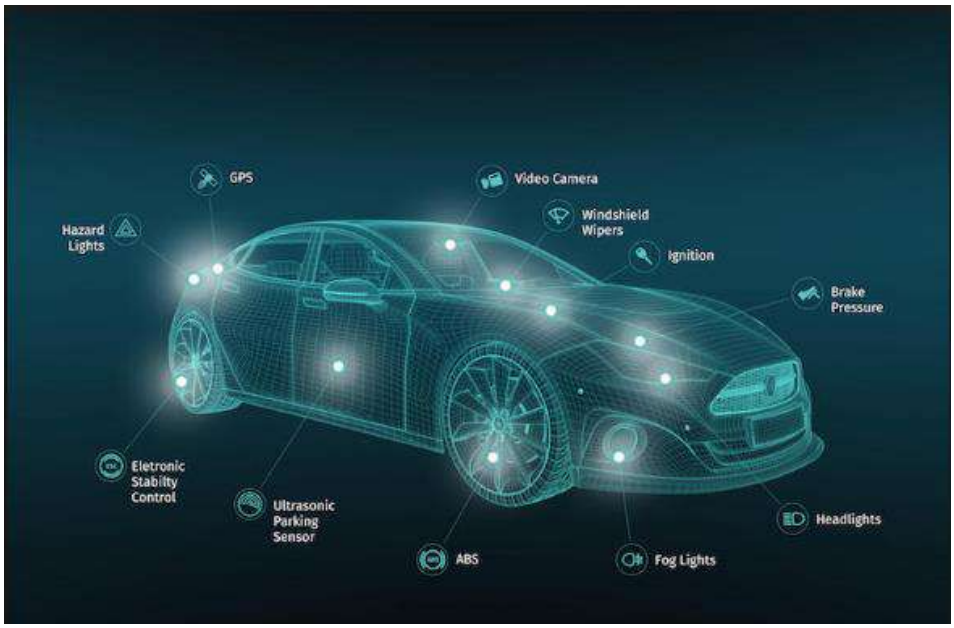


Figura 8 – Imagen de un vehículo conectado

En cuanto a las desventajas de los coches conectados, básicamente hay un solo problema que debe tenerse en cuenta: la seguridad de IoT y problemas de privacidad: ¿Cuáles son los riesgos principales?

En 2015, dos investigadores demostraron que las preocupaciones sobre la seguridad de los vehículos conectados no son infundadas. Charlie Miller y Chris Valasek encontraron una vulnerabilidad en el Jeep Chrysler: esto incluía tomar el control de sus funciones básicas, desde el control de temperatura y la radio, hasta la dirección y los frenos.

Aunque los fabricantes de automóviles desde entonces han aumentado la seguridad de sus vehículos, todavía existen ciertas amenazas relacionadas con cualquier automóvil conectado a Internet. Por ejemplo, incluso la más mínima vulnerabilidad en el sistema de un vehículo puede representar ciertas amenazas, tanto como para el conductor y los pasajeros.

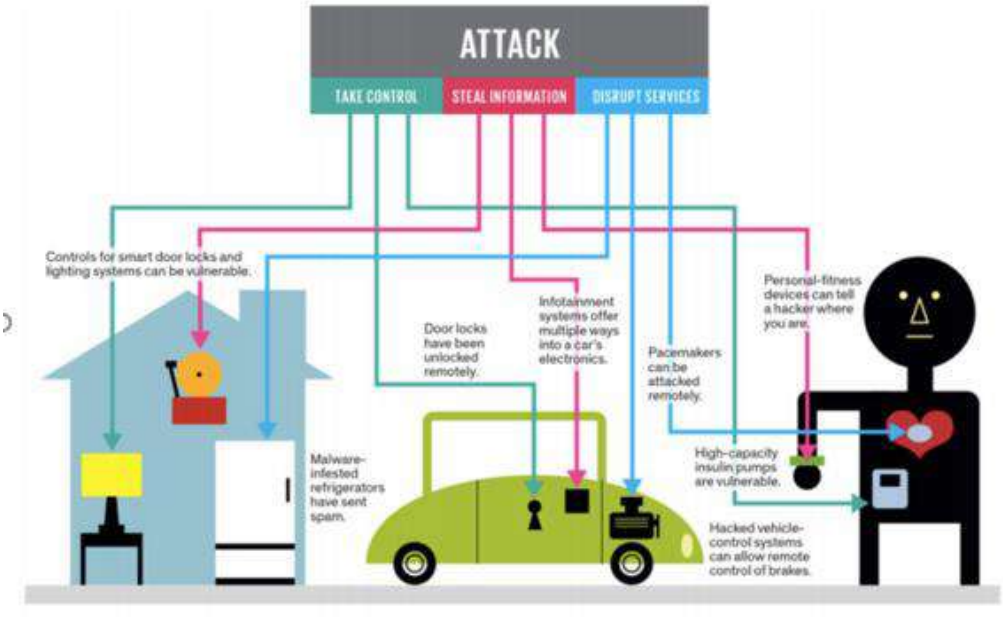


Figura 9 – Ataques a tecnología de IoT

Los ciberdelincuentes podrían realizar las siguientes acciones:

- Desbloquear y robar el coche.
- Rastrear su ubicación.
- Dañar o tomar el control de sus sistemas.
- Hacerse con el control del GPS y guiar a un conductor a una ubicación no deseada.
- Acceder a la información personal del conductor, incluido su nombre, correo electrónico, dirección del domicilio y datos bancarios (por ejemplo, número de tarjeta de crédito y fecha de caducidad)

Además, los piratas informáticos pueden rastrear el horario y los hábitos de un conductor para coordinar mejor sus acciones (por ejemplo, planificar un robo cuando un conductor está fuera de casa)

Cómo proteger las aplicaciones de los piratas informáticos: Consejos de seguridad de IoT Connected Cars

Los problemas relacionados con la seguridad de IoT y los vehículos conectados que aparecen a continuación se pueden abordar utilizando las siguientes 5 mejores prácticas:

1. Desarrollar aplicaciones teniendo en cuenta la seguridad
El principio de seguridad por defecto es especialmente importante cuando se trata de la seguridad de la Internet de las cosas. A partir de la arquitectura interna del software hasta su prueba, se debe tener siempre presente la seguridad. Se debe prestar especial atención al uso de software de código abierto e integraciones de terceros que puedan introducir fallos de seguridad adicionales.

2. Preste atención al proceso de autorización de la aplicación
Puede sonar algo obvio, pero hay que asegurarse de que sus usuarios no establezcan contraseñas que se puedan descifrar fácilmente. Establecer requisitos de contraseña segura, por ejemplo, limitar el número mínimo requerido de símbolos o implementar reglas que requieren un cierto conjunto de símbolos (letras, números, símbolos).

Otro método eficiente que añade una capa adicional de seguridad es la autenticación de dos factores (MFA o MultiFactor Autenticación).

3. Aplicar técnicas básicas de privacidad de datos.
Como cualquier dispositivo conectado gestiona datos confidenciales, las soluciones de seguridad de IoT también deben incluir las técnicas enumeradas.

Como resultado, los datos de sus usuarios serán completamente anónimos, cifrados y almacenados de forma segura en su base de datos.

4. Introducir alertas de seguridad en tiempo real.
Una de las soluciones de seguridad para vehículos conectados más populares es el llamado **sistema de detección de intrusos** en la red. Integrado en el software del automóvil, el programa realiza un seguimiento de los sistemas y controladores del vehículo, creando un perfil de sus operaciones. Gracias a eso, el sistema puede detectar la más mínima anomalía en el comportamiento del vehículo y notificar de inmediato al propietario y al fabricante.

Del mismo modo, puede aplicar técnicas de ciencia de datos y aprendizaje automático para detectar acciones sospechosas. O simplemente avisar al usuario una vez que el automóvil esté desbloqueado o se mueva cuando no debe hacerlo.

5. Hacer que las actualizaciones de seguridad sean un hábito.
Cuanto más tiempo permanezca sin actualizar los sistemas, más tiempo tendrán los hackers para descifrar su código. Hay muchas técnicas que los desarrolladores de aplicaciones pueden introducir para hacer que la conducción "conectada" sea una experiencia segura y agradable. Sin embargo, la seguridad de IoT no termina aquí.

Los consumidores también deben conocer los principios básicos de seguridad. Por ejemplo, no se recomienda conectar dispositivos o aplicaciones no autorizados al automóvil ni usar redes públicas. Los fabricantes de automóviles deberían incorporar la ciberseguridad en sus productos de forma predeterminada, adaptando las mejores prácticas de la industria, por ejemplo, encriptación de nodos, redundancia, copias de seguridad, etc.

Como hemos venido diciendo durante todo el proyecto, la seguridad en el Internet de las cosas es un tema importante pero complicado: especialmente ahora, a medida que el campo se regula cada más con la introducción de GDPR. Para asegurarse de que las aplicaciones brinden el nivel de seguridad necesario, se debe hacer de la protección de datos un elemento clave la estrategia.

La contratación de profesionales en Protección de Datos dedicado se está convirtiendo en una práctica común entre las empresas de IoT. Alternativamente, es habitual asociarse con un proveedor de tecnología de confianza con la experiencia necesaria en la construcción de soluciones de IoT escalables y seguras que puedan ofrecer la orientación necesaria y sirva de guía ante los desafíos de seguridad de IoT.

7. Smart-TV

Comenzamos este apartado definiendo el concepto de Smart TV: Un Smart TV es un televisor que puede conectarse a Internet y ejecutar diferentes aplicaciones como si de uno de esos avanzados Smartphones con Android se tratase. Estas aplicaciones permiten hacer cosas más complejas que las Televisiones tradicionales, como ver programas y películas bajo demanda, ver vídeos de YouTube desde una interfaz fácil de usar, revisar Facebook o comunicarse por Skype, todo desde el TV.

Estos dispositivos tienen, como no iba ser de otra manera, vulnerabilidades de seguridad que permitirán a los piratas informáticos, por ejemplo, cambiar remotamente los canales, el nivel de volumen o robo de datos confidenciales. Por otro lado, los fabricantes de estos dispositivos pueden monitorear y recopilar mucha información, probablemente más de lo que cualquier usuario desearía.

Figura 11 – Servicios Smart TV

¿Por qué los televisores inteligentes son vulnerables?

Entre los diversos televisores inteligentes que fueron examinados por Consumer Reports, se encontró que los televisores fabricados por Samsung y TCL y los dispositivos que utilizan la plataforma de televisores inteligentes de Roku tienen fallos de seguridad.

En el caso de los dispositivos TCL, los fallos se encontraron en las interfaces de programación de aplicaciones (API) de la plataforma Roku TV subyacente, que también se usa en dispositivos creados por otras compañías como Sharp, Hisense, LG y los propios dispositivos de transmisión de Roku. Las API son un conjunto de funciones que permiten interacciones entre diferentes software y hardware. Las empresas y los desarrolladores utilizan la API de Roku para crear aplicaciones para sus dispositivos.

Para explotar una vulnerabilidad, un pirata informático necesitaría acceso a los televisores Wi-Fi de destino. Esto puede suceder si el usuario de una computadora portátil o teléfono inteligente en la misma red es engañado para que instale una aplicación infectada con malware o visite una página web con código malicioso.
El exploit de Samsung es un poco más complicado y solo funcionaría en un dispositivo que haya interactuado previamente y haya obtenido acceso al televisor objetivo del ataque.

Casi todos los televisores inteligentes tienen navegadores integrados y, a diferencia de las computadoras portátiles y teléfonos inteligentes, las restricciones de hardware y software en los electrodomésticos inteligentes les impiden ejecutar antivirus y otras herramientas de seguridad.

Los riesgos de privacidad de los televisores inteligentes

La mayoría de los televisores inteligentes utilizan el reconocimiento automático de contenido (ACR), una tecnología que permite a los fabricantes identificar y clasificar el contenido que está viendo. Esto incluye servicios por cable, DVD y discos Blu-ray. ACR recopila muestras de audio, video y metadatos de los televisores y las envía al fabricante, que luego analiza los datos para comprender las preferencias del usuario y recomendar otros programas que le puedan interesar. Pero lógicamente también utiliza esta información con fines publicitarios y de marketing.

Algunos de los televisores permiten a los usuarios desactivar el ACR mientras siguen aceptando un acuerdo de privacidad básico. Sin embargo, incluso esos acuerdos de privacidad básicos pueden requerir que se renuncie a servicios de localización y el hecho de no aceptar las condiciones podría privar de las funciones "inteligentes" del televisor; por ejemplo, no se podría transmitir nada desde Amazon, Netflix u otros servicios basados en la web.

Cómo proteger tu televisión inteligente

Para alguien sin conocimientos de informática es muy difícil saber si su dispositivo se ha visto comprometido, Sin embargo, hay algunas medidas que pueden minimizar la superficie de ataque de los usuarios,

- Actualizar constantemente el firmware de la Smart TV y las aplicaciones que se ejecutan en el mismo (la mayoría de los televisores inteligentes tienen una opción de actualización automática).

- Prefiere las conexiones por cable a las inalámbricas porque son más difíciles de comprometer.
- Adquirir televisores inteligentes de proveedores acreditados que tienen un historial de corregir errores regularmente y lanzar actualizaciones de seguridad.
- Evite conectar memorias USB al televisor porque pueden contener malware.

Se recomienda asegurarse de que se entienden claramente los términos y condiciones y las políticas de privacidad antes de activar cualquier servicio.

El próximo Reglamento general de protección de datos de la UE (GDPR) hará que los proveedores proporcionen declaraciones de política de privacidad más detalladas y claras que permitan a los consumidores comprender qué datos se recopilarán y cómo se utilizarán.

También se recomienda no utilizar navegadores genéricos en televisores inteligentes porque no tienen controles de seguridad incorporados para protegerse contra ataques web maliciosos.
Los consumidores pueden instalar un dispositivo de protección inteligente para el hogar , como CUJO, Dojo o F-Secure Sense. Estos dispositivos utilizan un conjunto de técnicas como la supervisión del comportamiento de los dispositivos y la inspección de paquetes para detectar y bloquear la actividad maliciosa en la red doméstica.

La capa adicional de seguridad que proporcionan los dispositivos de seguridad para el hogar inteligente puede compensar las vulnerabilidades inherentes que existen en los dispositivos de IoT.

8. Cameras IP

El número de estos dispositivos ha superado los 100 millones en todo el mundo por lo que es importante comprender qué hace que las cámaras IP sean objetivos tan fáciles de atacar, cómo funcionan los ataques y cómo protegerlas mejor y de manera más eficiente.

Uno de los primeros ataques contra cámaras IP surgió a finales de 2013 en la forma del gusano Darlloz Linux. Al explotar una vulnerabilidad de PHP en dispositivos conectados a Internet que podría propagarse a través de dispositivos IoT, incluidos routers domésticos, decodificadores y cámaras IP.

Figura 12 – Imagen de una cámara IP

¿Por qué las cámaras IP hacen buenos objetivos?

Las cámaras IP se han convertido en un objetivo común para los atacantes por las siguientes razones:

• *Conectividad constante*. Tener una conexión continua a Internet hace que las cámaras IP sean fáciles de localizar. Una vez hackeadas, permanecen disponibles para satisfacer las necesidades de los piratas informáticos.

• *Bajo coste de ataque*. Una vez que los atacantes encuentran una manera de hackear una cámara IP, puede usar el mismo enfoque contra otros modelos similares, lo que hace que el costo por ataque sea muy bajo.

• *Falta de supervisión*. Incluso el personal experto en ciberseguridad no está dispuesto a gestionar cámaras IP como harían con otros dispositivos conectados a internet. La falta generalizada de software de seguridad incorporado también deja a las cámaras IP vulnerables a todo tipo de explotación.

• *Alto rendimiento*. La mayoría de las cámaras IP tienen suficiente capacidad de computación para realizar tareas, como la minería de criptomonedas, sin que los usuarios finales se den cuenta.

• *Gran ancho de banda.* Diseñado para la comunicación de video, el ancho de banda de las cámaras IP es adecuado para facilitar los ataques DDoS.

Tanto los vendedores de cámaras IP como los usuarios deben seguir las mejores prácticas de seguridad para minimizar las vulnerabilidades.

Mejores prácticas para fabricantes de cámaras IP

• Como ocurre con todos los dispositivos IoT hay que considerar la seguridad en cada dispositivo desde el inicio por la tanto hay que asegúrese de que los desarrolladores escriben código de forma segura e incorporen siempre la última versión de software para reducir la posibilidad de vulnerabilidades.

• Actualizaciones de seguridad. Asumir la responsabilidad de hacer que los dispositivos sean seguros y mantenerlos actualizados vía parches o actualizaciones de firmware inmediatamente después de descubrir nuevas vulnerabilidades.

• Asociarse con proveedores profesionales de ciberseguridad.

Expertos altamente especializados hacen esfuerzos continuos para mantenerse al día con las últimas amenazas, por lo que colaborar con proveedores de seguridad cibernética de renombre tiene mucho sentido.

Mejores prácticas para usuarios de cámaras IP

•A la hora de comprar una cámara hay que asegurarse que se trata de una cámara IP segura. La mayoría de los usuarios encuentran el nivel de seguridad de las cámaras IP casi imposible de mejorar. Los usuarios deben contar con proveedores de confianza.

• Cambiar la contraseña predeterminada de cualquier dispositivo antes de usarla. Muchos ataques implican el uso de contraseñas de dispositivos predeterminadas. Por lo tanto, los usuarios deben cambiar la contraseña predeterminada de cualquier dispositivo.

• Deshabilitar puertos o protocolos de red innecesarios. El ataque Persirai mostró que tener una contraseña segura no garantiza la seguridad del dispositivo. Los usuarios de cámaras IP también deben desactivar UPnP en sus routers.

• Aplicar nuevos parches de seguridad o actualizaciones de firmware inmediatamente. El uso del firmware más actualizado puede ayudar a minimizar la posibilidad de vulnerabilidades. Se deberían escoger cámaras IP con capacidades de autoprotección o que implementen soluciones de seguridad de red con una función de parcheo virtual.

• Implementar medidas de seguridad de red para descubrir o detener las comunicaciones sospechosas. Los usuarios deben habilitar las funciones de seguridad, como los cortafuegos y la prevención de intrusiones en sus routers domésticos.

Ataque típico de ataque a Cámaras IP. A continuación, mostraremos en pocos pasos como podríamos comprometer una cámara IP **y a través de la siguiente figura.**

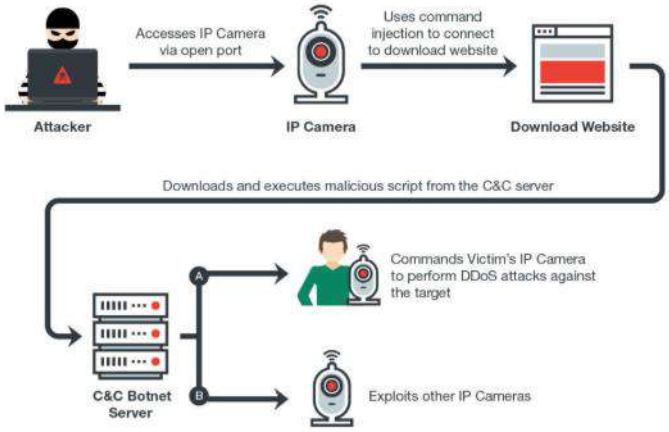


Figura 12 – Ataque a una cámara IP

El primer paso sería localizar cámaras IP y esto resulta una tarea bastante sencilla si contamos con el llamado «buscador de los hacker», **Shodan** es un motor de búsqueda parecido a Google, con la diferencia que, en vez de indexar el contenido, almacena los dispositivos conectados a Internet (routers, servidores, cámaras, etc).[20]

Por ejemplo, vamos a buscar cámaras IP, de la marca Honeywell y que se encuentren en Madrid, para ellos accedemos a Shodan y buscamos con el siguiente filtro:[20]

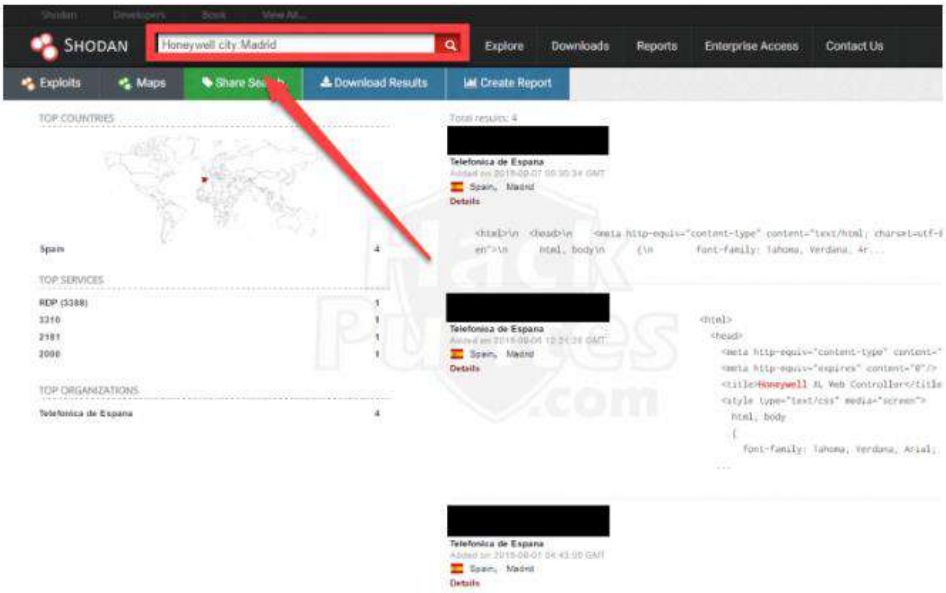


Figura 13 – Resultado de una búsqueda con Shodan

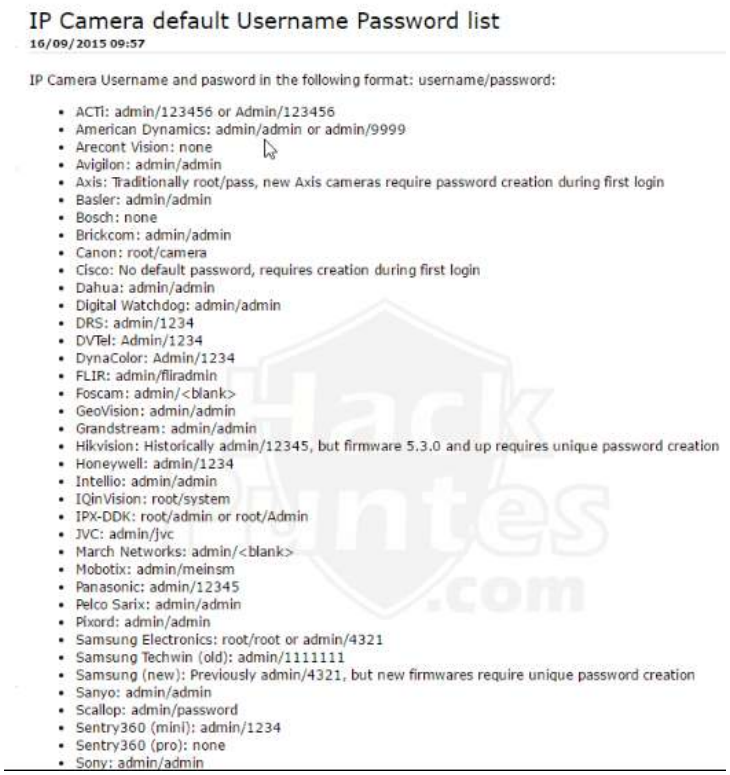
En este caso el buscador ha encontrado cuatro IPs que tiene cámaras de la marca Honeywell en Madrid, puede parecer que hemos encontrado pocas cámaras, pero debemos de tener en cuenta que Shodan es un buscador, y es posible que no haya registrado todas las cámaras accesibles, por lo tanto, hay que hacer uso de la utilizad Nmap para rastrear dentro del rango de IPs.

Nmap es un escáner de puertos, y permite rastrear IPs que dispongan de servicios a la escucha filtrando por puerto, por lo tanto, supongamos que hemos obtenido la IP 172.26.100.50. Lo siguiente es buscar si dentro de su rango hay más cámaras, buscaremos en el rango 172.26.0.0 al 172.26.255.255, y filtraremos por los puertos 3310, 2181 y 2000, esto lo podemos hacer con el siguiente comando:

nmap 172.26.0.0/16 -p 3310, 2181, 2000

El segundo paso es intentar acceder a la cámara con las credenciales por defecto. Aunque parezca extraño, es increíble que aún haya gente que no cambie las credenciales por defecto de los dispositivos, existe muchísimas cámaras IPs que las tienen, y no solo cámaras IPs, sino cualquier tipo de dispositivo.

Si consultamos en Internet por las claves por defecto podemos fácilmente encontrar listados como el que mostramos en la siguiente figura.



IP Camera default Username Password list

16/09/2015 09:57

IP Camera Username and pasword in the following format: username/password:

- ACTi: admin/123456 or Admin/123456
- American Dynamics: admin/admin or admin/9999
- Arecont Vision: none
- Avigilon: admin/admin
- Axis: Traditionally root/pass, new Axis cameras require password creation during first login
- Basler: admin/admin
- Bosch: none
- Brickcom: admin/admin
- Canon: root/camera
- Cisco: No default password, requires creation during first login
- Dahua: admin/admin
- Digital Watchdog: admin/admin
- DRS: admin/1234
- DVTel: Admin/1234
- DynaColor: Admin/1234
- FLIR: admin/fliradmin
- Foscam: admin/<blank>
- GeoVision: admin/admin
- Grandstream: admin/admin
- Hikvision: Historically admin/12345, but firmware 5.3.0 and up requires unique password creation
- Honeywell: admin/1234
- Intellio: admin/admin
- IQinVision: root/system
- IPX-DDK: root/admin or root/Admin
- JVC: admin/jvc
- March Networks: admin/<blank>
- Mobotix: admin/meinsm
- Panasonic: admin/12345
- Pelco Sarix: admin/admin
- Pixord: admin/admin
- Samsung Electronics: root/root or admin/4321
- Samsung Techwin (old): admin/1111111
- Samsung (new): Previously admin/4321, but new firmwares require unique password creation
- Sanyo: admin/admin
- Scallop: admin/password
- Sentry360 (mini): admin/1234
- Sentry360 (pro): none
- Sony: admin/admin

Figura 14 – Listado de usuarios y contraseñas por defecto

Una vez que ya **sabemos la IP y la contraseña por defecto**, abrimos Mozilla Firefox, escribimos la IP y cumplimentamos el formulario con las credenciales por defecto.[20]

Figura 15– Página de inicio para gestión de una cámara IP

Si hay suerte nos aparece la siguiente pantalla la cual nos indica que ya estamos dentro

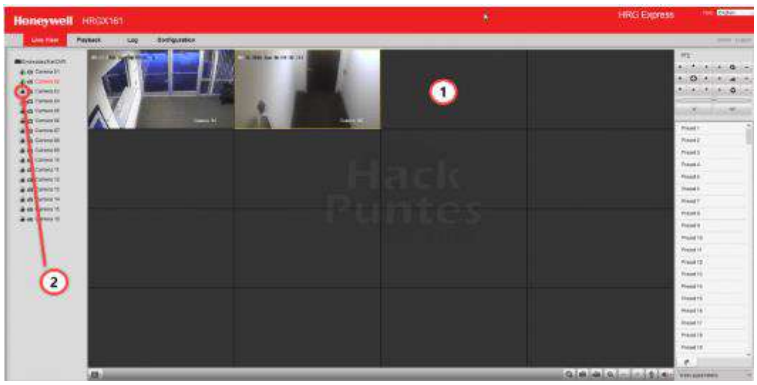


Figura 16 – Contenido que reproducción cámara IP

Vamos a ir añadiendo cámaras**,** también podemos moverlas desde el panel derecho [20]

Figura 17 – Panel de control de Honeywell

Preservando el acceso.

En este momento, tenemos acceso a las cámaras, pero es posible que el administrador cambie las contraseñas por defecto y ya no tengamos acceso a ellas. Una vez dentro, podemos crear un segundo (o tercero y cuarto) usuario con permisos de administrador

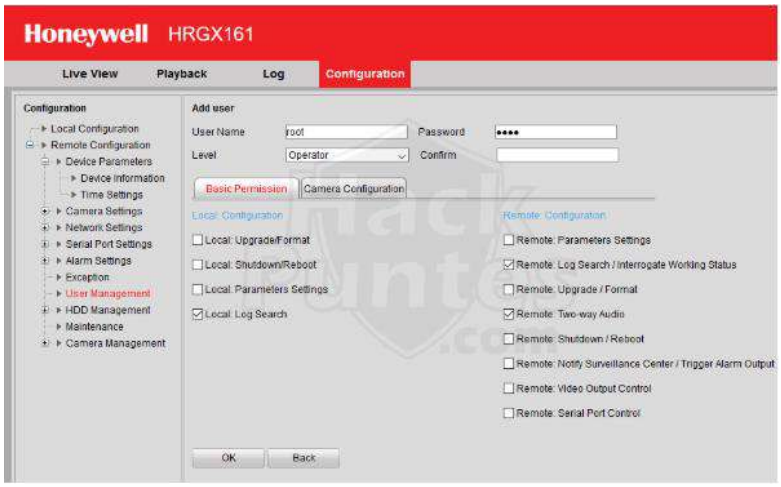


Figura 18 - Panel para la administración de usuarios

9. Smart Cities

Las ciudades inteligentes (smart cities) son aquellas que utilizan todas las ventajas e innovación de la tecnología que junto al resto de recursos hace de ellos un uso más eficaz, promoviendo el desarrollo sostenible y, en definitiva, mejorando la calidad de vida de sus ciudadanos. En definitiva, es la combinación de personas, tecnología y creatividad para hacer más sostenible y eficiente a cualquier ciudad del mundo.

Ventajas de las ciudades inteligentes

El internet de las cosas (IoT), el big data, aplicaciones móviles, y la industria 4.0 está consiguiendo mejorar la eficiencia de las ciudades. En este sentido, una ciudad puede gestionar la tecnología para mejorar la vida de las personas y más concretamente, para conseguir beneficios como:

- Eficiencia energética.
- Ahorrar costes a sus ciudadanos.
- Seguridad.
- Optimizar los servicios públicos.
- Mejorar la transparencia en la gestión de las administraciones.
- Conseguir retener empresas y atraer talento.
- Mejorar la comunicación con los ciudadanos.

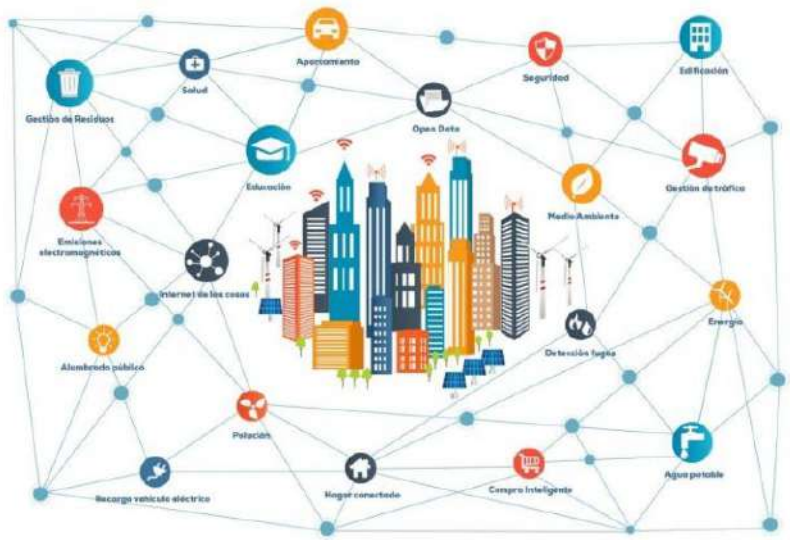


Figura 19 - Diagrama de una Smart City

Las ciudades inteligentes están cambiando y transformando la manera en que vivimos y trabajamos. Aplicando tecnologías IoT de vanguardia con virtualización, Big Data, Cloud, inteligencia artificial, machine Learning y demás, representan un intento continuo de superar los desafíos asociados al rápido crecimiento de las ciudades inteligentes. El único problema es que los sistemas tecnológicos también plantean graves preocupaciones de privacidad y seguridad.

A medida que el ritmo de desarrollo en tecnología continúa acelerándose, es de vital importancia considerar dónde se originan las principales amenazas que giran en torno a las Smart Cities. La ciberseguridad se ha convertido en un asunto de máxima importancia en nuestra sociedad. De los ciberataques sufridos hasta ahora pueden extraerse valiosas conclusiones que permitan anticiparse a los riesgos para el futuro de las ciudades inteligentes.

El último ciberataque lo tenemos en los efectos a nivel mundial que ha causado el **ransomware Wannacry**, que afectó a muchos países en los que paralizó organizaciones y sistemas de información de miles de empresas, un toque de atención importante que obliga a estar preparados ante los efectos de estas amenazas.

Impacto por un ciberataque a una Smart City

En relación con los sectores y servicios afectados ante un posible ciberataque en la Smart City actuando contra dispositivos conectados (IoT) se pueden resumir en la siguiente figura:[22]

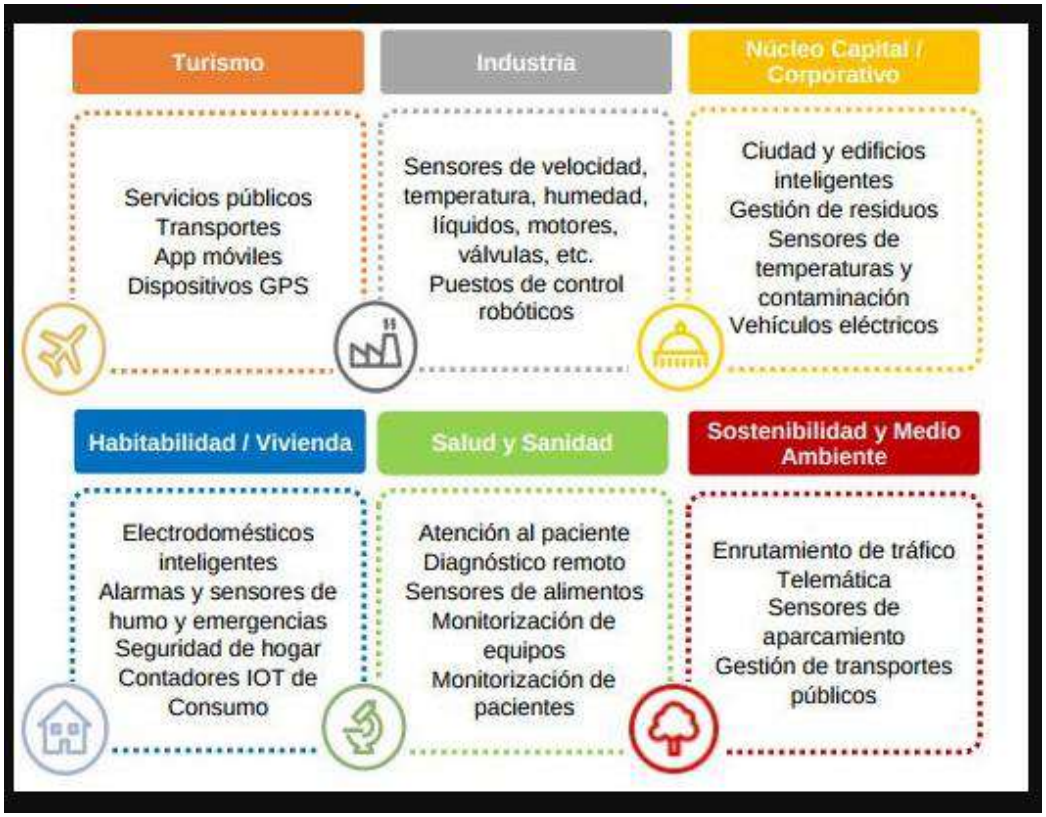


Figura 20 – Servicios afectados por un ciberataque a Smart city

Por otro lado las motivaciones de los ciberdelincuentes podrían ir dirigidas a:[22]

- Obtención de información confidencial que genere ventaja competitiva.
- Imposibilitar el suministro de los servicios, por el agua, el gas, la luz, etc..
- Sustracción de datos de carácter confidencial, recopilación de información para elaborar perfiles y comportamientos de personas o entidades para, posteriormente, ser vendida a terceros.
- Creación de nuevas vías de intercambio de información, de nuevos métodos de pago (por ejemplo, Bitcoin).

La característica principal en un entorno de Smart City es la interoperabilidad de todos los sistemas y servicios, y por esta razón se han analizado e identificado las mínimas áreas de ciberseguridad que deben ser tenidas en cuenta por cualquier compañía o usuario, con el fin de salvaguardar los pilares fundamentales en los que se basa la seguridad:

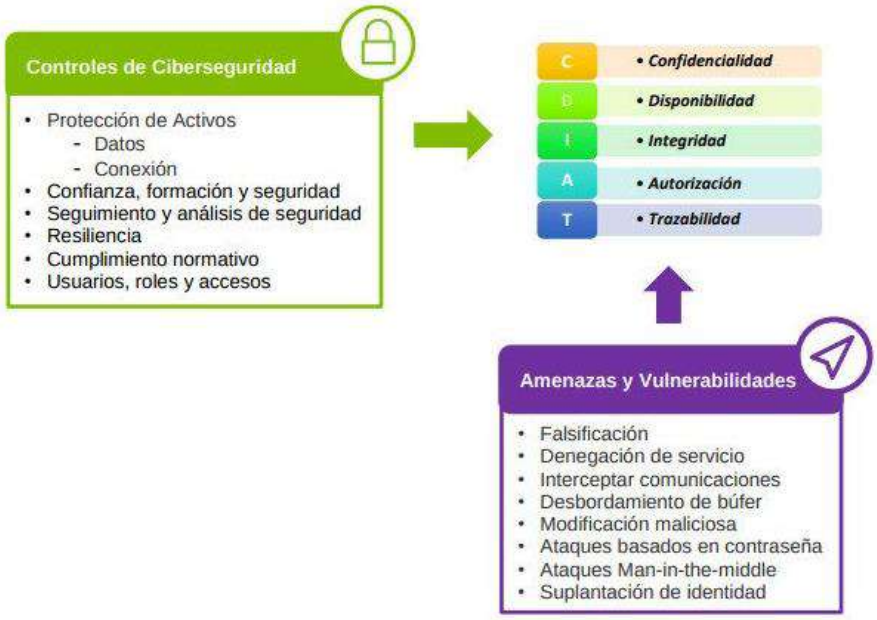


Figura 21– Áreas de ciberseguridad que deben ser cubiertas

Amenazas contra la Smart City: Vectores de Ataque [22]

Un ciberataque puede utilizar múltiples vectores de ataque para intentar conseguir sus objetivos, lo que incrementa la dificultad para su prevención. Los ciberataques se han incrementado en todos los países del mundo lo que refuerza la hipótesis de que el número de incidentes se incrementará de forma significativa en el corto plazo, lo que obliga a todas las organizaciones a buscar y adoptar las medidas necesarias para mejorar su ciberseguridad para hacer frente a escenarios cada vez más complejos.

Principales riesgos y amenazas contra la Smart City. Estos son los principales vectores de ataque dirigidos a la Smart City:

1- Malware. El malware es software malicioso instalado sin autorización. Suele ser el vector de ataque más utilizado en la actualidad, junto con los Exploit Kits, sirviendo en muchos casos como mecanismo de entrada de otros tipos de ataques ya que una vez instalado normalmente se convierte en la puerta trasera para intentar tomar el control de sistemas y entornos de forma silenciosa.

Puede infectar sistemas y aplicaciones, realizar modificaciones ilegítimas, extraer o destruir información, etc. Cada vez en mayor medida se destina a infectar ordenadores y dispositivos para crear Botnets.

La **gran amenaza para la Smart City** en este ámbito se basa en la capacidad de los dispositivos IoT de ser utilizados como vía de infiltración para alterar la ciudad y su gestión, al sector empresarial y a la ciudadanía en general.

En estos momentos, la principal amenaza desde el punto de vista de malware viene por la incidencia del **Ransomware** que secuestra los equipos y pide un rescate para su liberación. Se estima que en la actualidad existen 60.000 variantes siendo las más conocidas siendo las más conocidas CryptoWall y TorrentLocker.

2- Exploit kits. Paquetes de software que incluyen un conjunto de utilidades ya desarrolladas, con el objetivo de explotar diferentes vulnerabilidades afectando a la disponibilidad, integridad y/o confidencialidad del objetivo. Actualmente se trata de uno de los vectores de ataque más utilizados para comprometer los sistemas por su facilidad de uso, lo que los convierte en muchos casos en un arma al alcance de gran número de posibles atacantes.

3- Phishing. Ataque que utiliza la suplantación de servicios y webs, engañando al usuario para, entre otros fines, robar información confidencial, así como inyectar software malicioso. La gran amenaza para la Smart City se centra en el robo de credenciales, que servirán de pasarela para acceder a dispositivos IoT a los que los usuarios cuyos datos se han obtenido de forma fraudulenta, tengan permiso. En el caso de infraestructuras y edificios públicos críticos, la amenaza es aún mayor.

4- Ataque de denegación de servicio (DDoS). Un ataque de denegación de servicio (Distributed Denial of Service) provoca la saturación del objetivo, en la red y/o en los sistemas (servidor, sitio web, etc.) impidiendo el acceso a los usuarios; normalmente, de forma temporal, hasta que se consigue restablecer el servicio. Ejemplos recientes indican una tendencia mucho más peligrosa para el entorno de las Smart City, que ha llegado para quedarse: Los ataques DDoS que aprovechan la vulnerabilidad de los sistemas IoT.

5- Interceptación, robo o sabotaje de datos
En el ecosistema Smart City, la toma de decisiones se convierte en crítica para gobiernos, corporaciones, investigadores, ciudadanos y será inviable si no se confía en la autenticidad e integridad de la información. En este vector de ataque, los ciberdelincuentes explotan las vulnerabilidades de protocolos inseguros de comunicación y de transmisión de información entre dos dispositivos o sistemas de información.

El sector sanitario es actualmente uno de los puntos de máxima atención ante las posibles amenazas contra la Smart City. Tomando como ejemplo un hospital, podríamos encontrarnos desde no disponer temporalmente de los datos clínicos, pasando por la alteración de los resultados de maquinaria de análisis, hasta la pérdida de vidas humanas por la modificación de elementos de radioterapia o incluso de marcapasos.

6- Pérdida de control en el acceso a datos Cloud
El número de ataques destinados a proveedores de este tipo de servicios se incrementa a medida que su uso se extiende, siendo el malware y las botnets las mayores amenazas. Si tomamos en consideración el aumento del acceso a los datos desde dispositivos inteligentes, escritorios virtualizados, etc., el escenario se complica bastante.

Mediante ataques “Man in the Cloud”, en el caso de repositorios compartidos por múltiples usuarios, cualquier infección se propagará con mayor rapidez, comprometiendo mayor número de recursos.

Medidas de prevención

Ante este panorama de amenazas contra la Smart City, es necesario poner encima de la mesa las posibles soluciones para contrarrestar estos vectores de ataque, cuya solución pasa por fijar medidas de prevención como:

- **Establecer procedimientos**, así como medir, analizar y definir los umbrales normales de respuesta y operación de los elementos involucrados, para detectar anomalías que puedan incidir en la seguridad.
- **Establecer un marco de seguridad** con políticas, normas y procedimientos de seguridad, aplicables tanto de forma individual a los elementos de la infraestructura, como al conjunto de procesos que soportan los servicios ofrecidos por la Smart City.
- **Exigir a fabricantes e integradores** que incorporen la ciberseguridad como uno de los pilares básicos de actuación. La industria de la ciberseguridad deberá enfrentarse al reto que supone asumir el coste de unos recursos que deben ser proporcionales a la infraestructura del atacante.
- **Dotarse de pólizas de Ciberseguros**, ya que, a diferencia de los países más avanzados en este sentido, la mayoría de las organizaciones españolas no disponen de ciberseguros que cubran los daños reputacionales y económicos asociados a un ciberataque.[22]

10. Conclusiones

Como se ha venido explicando durante todo este TFG, se ha querido dar a conocer el concepto de "el Internet de las cosas". IoT es una realidad que ya está en la vida de cada uno de nosotros. Esta manera de pensar no es nueva y se viene dando desde las primeras interconexiones con computadores, pero que cada vez más se han ido añadiendo más y más dispositivos a Internet donde era impensable que se pudieran intercambiar datos e información unos con otros.

Este TFG se ha ido centrando en la importancia en la seguridad del IoT, tanto a nivel de fabricación o producción como a nivel de usuario. La seguridad y privacidad de nuestros datos e información es uno de los aspectos que más preocupan a la población. En términos generales, la seguridad debe de estar centrada tanto en los dispositivos (configuración, acceso, información cifrada) y seguridad de la red. A nivel empresarial, esta evolución de la tecnología también supone un importante desafío ya que el nivel de aportación en los distintos ámbitos de trabajo es de un valor incalculable, pero el gran reto consiste en controlar todas amenazas a la seguridad que conlleva y ayudar a prevenirlas.

Hay sectores en los que esta tecnología ya está suponiendo una transformación y se está afianzando sin ningún tipo de dudas. Con la realización de este TFG he llegado a la conclusión de que para que esta tecnología tenga éxito y siga creciendo debe de ser totalmente segura para el consumidor final. Hemos repasado los problemas de seguridad más habituales en dispositivos comerciales. Esta tecnología debe de suponer un avance no solo en el acceso y rapidez de datos, sino también un avance en la seguridad.

Dicho lo anterior trataré de aportar una serie de conclusiones:

1. La sociedad interconectada no solo conllevará un cambio a nivel tecnológico sino a nivel personal, donde la mentalidad y forma de vida cambiará totalmente para adaptarse a la nueva forma de pensar, trabajar, y realizar tareas cotidianas. Tras investigar y recopilar todo tipo de información para la elaboración de este proyecto, mi opinión es que todavía no estamos preparados.

2. Los riesgos y problemas que surgen en la seguridad relacionados con el uso y expansión de IoT no son nuevos, sino que existen desde las primeras interconexiones con computadoras. Lo que cambia es la dimensión en la que estos problemas y amenazas ocurren en la actualidad.

3. El hecho de que la interconexión de dispositivos aumente exponencialmente, generará un gran tráfico de internet que afectará en gran medida a las infraestructuras que existen actualmente.

Será un reto conseguir que esta tecnología se pueda afianzar en todo el mundo, incluso en países en los que aún las estructuras de acceso a internet son precarias y poco avanzadas.

Ahora entendemos mejor lo que se puede llegar a alcanzar en el mundo del IoT. Por último, como hemos visto a lo largo de todo el proyecto, IoT es una realidad, pero que avanza poco a poco y despacio, y no parece que vayan a frenarle las preocupaciones por la seguridad, limitaciones tecnológicas o costes. Actualmente tal vez no sea necesario comprar un dispositivo con sensores para que abra las puertas de la casa cada vez que lleguemos, pero se trata de un proceso que empieza por este tipo de aplicaciones hasta llegar a dispositivos y funciones inimaginables.

11. Glosario

IoT: Es un sistema de dispositivos informáticos interrelacionados, máquinas digitales y mecánicas, objetos, animales o personas que cuenten con identificadores únicos(UID) y la capacidad de transferir datos a través de una red sin necesidad de interacción de persona apersona o de persona a computadora.

Malware: Es cualquier programa o archivo que es perjudicial para el usuario. El Malware incluye virus informáticos, gusanos, caballos de Troya y spyware.

NAT o Network Address Transalation: En un router de internet donde varios equipos de una red local salen a internet bajo una misma IP pública, el NAT cuando llega la respuesta de Internet a una petición interna sabe quién la realizo y la redirige al equipo adecuado, es decir, se encarga de esas traducciones.

Firewall: Programa informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad.

Login: Es el acto de introducir las credenciales (Usuario y contraseña) en un sistema informatico

Ciberdelicuente: Persona que utiliza el ordenador y las redes de comunicaciones para cometer delitos.

Exploit: Es una palabra inglesa que significa explotar o aprovechar, y que en el ámbito de la informática es un fragmento de software, fragmento de datos o secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

SSL: SSL es el acrónimo de Secure Sockets Layer (capa de sockets seguros), la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas e impedir que los delincuentes lean y modifiquen cualquier dato que se transfiera, incluida información que pudiera considerarse personal.

DDoS: Se trata de una ataque de denegacion de servicios realizado de manera distribuida

Botnet: Se trata de una red de ordenadores controlados por un tercer actor y con la capacidad de obedecer las ordenes de este.

DNS: E sistema de nombres de dominio es un sistema jerárquico de nombres descentralizados para computadores, servicios u otros recursos conectados a Internet o una red privada.

Nmap: herramienta para el rastreo de puertos sobre una IP. Actualmente incluye una gran flexibilidad

Shodan: es un motor de búsqueda que nos permite encontrar dispositivos expuestos en Internet. Este buscador se dedica a recorrer Ips y buscar puertos abiertos almacenando el banner de dicho servicio

Zigbee: redes inlambricas PAN de bajo consumo, baja velocidad y bajo coste basado en el estandar IEE 802.15.4

12. Bibliografía

[1] Seguridad en Internet de las cosas: Estado del arte
http://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRT-CV%5D%20Informe-Internet_de_las_Cosas.pdf

[2] Cuzme Rodriguez Fabian, Internet de las cosas y cuestiones de seguridad, Geovanny abril 2015
http://repositorio.puce.edu.ec/bitstream/handle/22000/8492/INTERNET%20DE%20LAS%20COSAS%20TESIS%20Y%20CONSIDERACIONES%20DE%20SEGURIDAD%20-%20FINAL.pdf?sequence=1&isAllowed=y

[3] Ville Sulkamo - IoT from cyber security perspective Case study JYVSECTEC, June 2018 School of Technology, Communication and Transport, master's thesis
https://www.theseus.fi/bitstream/handle/10024/151498/IoT%20from%20cyber%20security%20perspective.pdf?sequence=1&isAllowed=y

[4] Mohamed Abomhara and Geir M. Køien, Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks

[5] Bitag Report - Internet of Things (IoT) Security and Privacy Recommendations
https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

[6] IoT Security for Surveillance Cameras Whitepaper- Ensuring IoT Security for IP Cameras – TrendMicro
https://www.trendmicro.com/us/iot-security/Solutions/IoT-Security-for-Surveillance-Cameras

[7] IOT Security for Dummies – Lawrence Miller
https://www.insidesecure.com/index.php/cn/.../IoT-for-dummies

[8]Trabajo de Fin de Grado - Internet de las cosas- seguridad - Alumno: Miguel Castro Sola - Septiembre, 2016
https://sinbad2.ujaen.es/sites/default/files/publications/Memoria_0.pdf

[9] International Journal of Network Security & Its Applications (IJNSA) Vol.8, No.3, May 2016 Ke Wan Ching and Manmeet Mahinderjit Singh

[10]https://economipedia.com/definiciones/ciudad-inteligente-smart-city.html

[11]http://www.magazcitum.com.mx/?p=1605#.XOpNGo77SaE -- Fuente para SCADA

[12] Brian Russell, Drew Van Duren**,** Practical Internet of Things Security – June 2016

[13] Fundación de la Innovación Bankinter - El Internet de las Cosas En un mundo conectado de objetos inteligentes

[14] Christian Dancke Tuen - Security in Internet of Things Systems, June 2015

[15] Smith, S. 2017. The Internet of Risky Things. Trusting the Devices That Surround Us. O'Reilly Media Inc

[16] Steven Hsu - IoT Security Guidelines - Device Life Cycle Overview

[17] Farzad Kamrani, Mikael Wedlin, Ioana Rodhe , Internet of Things: Security and Privacy Issues

[18] Wikipedia - https://en.wikipedia.org/wiki/Internet_of_Things

[19] Rodrigo Roman, Pablo Najera, Javier Lopez, "Securing the Internet of Things", Computer Societ 58, Sep. 2011, https://www.nics.uma.es/sites/default/files/papers/1633.pdf

[20] https://hackpuntes.com/hacking-camaras-ip-montandome-propio-gran-hermano/ 10/05/2019

[21] https://www.fracttal.com/blog/2018/10/10/9-aplicaciones-importantes-iot 25/04/2019

[22] https://www.blog.andaluciaesdigital.es/ciberataques-y-amenazas-contra-la-smart-city/ 25/05/2019