Escuela Politécnica Superior de Jaén

Grado en Ingeniería Informática

UNIVERSIDAD DE JAÉN

Escuela Politécnica Superior de Jaén

INTERNET DE LAS COSAS. PRIVACIDAD Y SEGURIDAD

Alumno: Lorenzo Gómez Padilla

Tutora: Macarena Espinilla Estévez

Dpto: Informática

Junio 2016

Universidad de Jaén

Escuela Politécnica Superior de Jaén
Departamento de Informática

Macarena Espinilla Estévez , tutora del Trabajo Fin de Grado titulado: Internet de las cosas. Privacidad y Seguridad, que presenta Lorenzo Gómez Padilla, autoriza su presentación para defensa y evaluación en la Escuela Politécnica Superior de Jaén.

Jaén, Junio 2016

El alumno: La tutora:

Lorenzo Gómez Padilla Macarena Espinilla Estévez

Índice

1. Introducción

1.1 Motivación

El término Internet de las cosas (Internet of things o IoT) hace referencia a todos los objeto comunes que con los avances tecnológicos se pueden conectar a internet. El internet de las cosas se implantó cuando el número de dispositivos supero al número de personas conectadas a internet (entre 2008 y 2009). A día de hoy es normal que la mayoría de usuarios no solo se conecten a través de un ordenador o un portátil sí que también dispongan de smartphones o tablets, con ello el acceso a internet es prácticamente permanente sin importar donde se encuentre el usuario. Según el informe ONTSI en el tercer trimestre de 2015 en España el 78,2% de personas usa internet en alguna ocasión. Según también este informe en el tercer trimestre de 2015 los dispositivos más usados para conectarse a internet son los smartphones con un 76%, el 54.3% usa un ordenador portátil y en tercer lugar el ordenador de sobremesa el 48.8% [1].

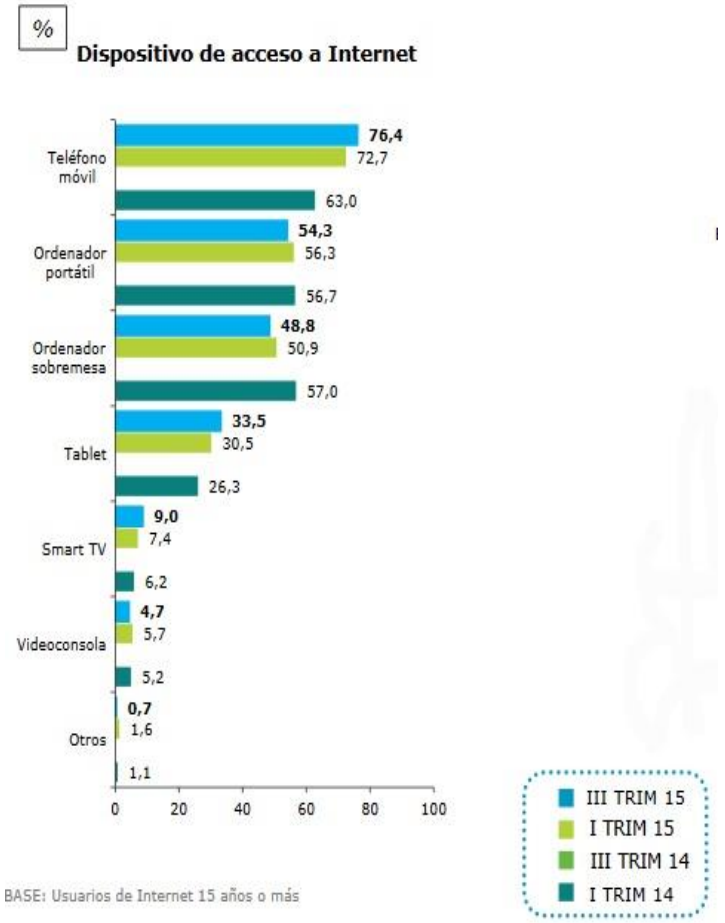

Ilustración 1. Dispositivos de acceso a internet ONTSI

Cada vez hay más usuarios usan internet y cada vez más con más dispositivos por eso el término internet de las cosas engloba objetos comunes que hasta el momento no disponían de conexión a internet como por ejemplo neveras, lavadoras, coches, televisiones, relojes,… pero que ya disponen de ella.

Como se ha comentado, el término internet de las cosas engloba a una gran cantidad de objetos comunes que normalmente no se conectaban a internet pero

ahora si lo están. Con dicha evolución algunos objetos como los que hemos nombrado anteriormente disponen de conexión a internet. La conectividad de estos aparatos permite multitud de opciones como puede ser controlar estos objetos de forma remota a través de otros dispositivos o a través la propia aplicación web de la que dispongan. Además puedes recibir información externa al dispositivo como por ejemplo cualquier aparato que pueda recibir la climatología de una ciudad, poder consultar el correo electrónico en la pantalla que lleve incorporada que tenga el dispositivo o leer las noticias. Todas estas funciones dependerán del dispositivo y los servicios que tenga implementados, además claro está de las propias funciones de las que consta el dispositivo. Internet mediante esta nueva forma de interacción será una parte fundamental en las tareas comunes y cotidianas del día a día. Incluso el término internet de las cosas también se está denominando en algunas ocasiones el internet del todo (Internet of Everything). Esto es debido a que la tendencia de estos tipos de dispositivo va evolucionando y en aumento exponencialmente.

Esto hace que vivamos en una sociedad ubicua, en la cual los dispositivos hablan con nosotros e incluso entre ellos mismos. Los expertos del Future Trends Forum considera que el internet de las cosas llegara a las diferentes industrias en pocos años, en la siguiente ilustración podemos ver las diferentes industrias y cuáles son las predicciones sobre ellas (Ilustración 2).

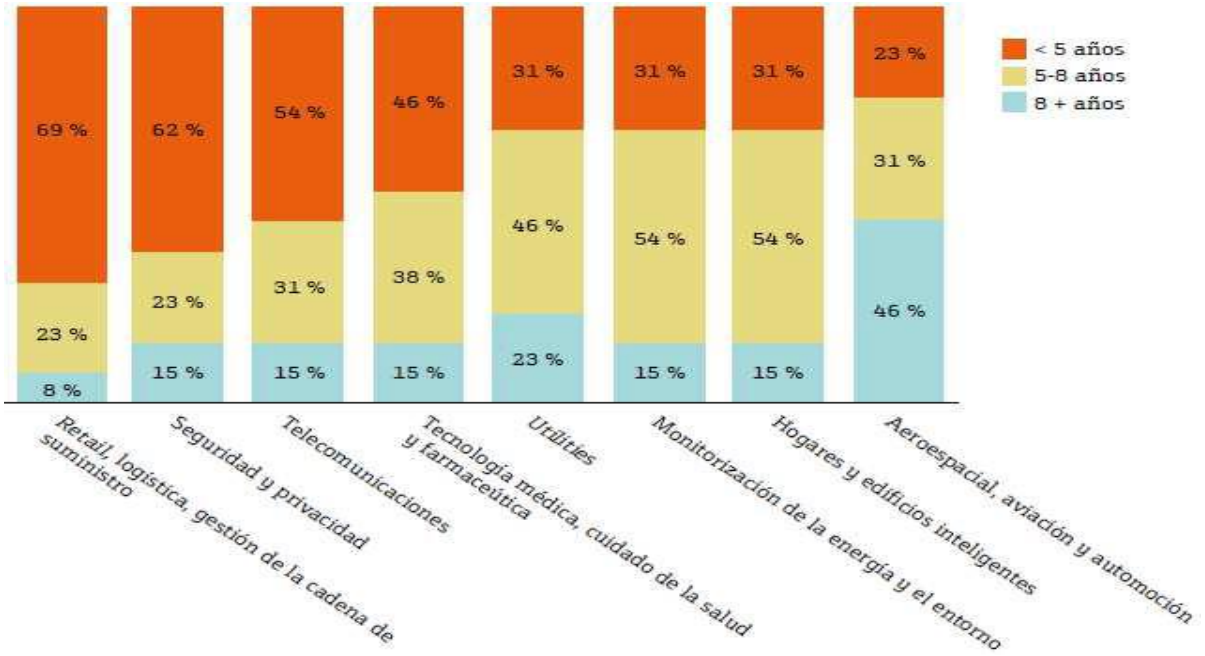

Ilustración 2 Velocidad de adopción del Internet de las Cosas en las distintas industrias

Algunos dispositivos como ejemplo del internet de las cosas que están llegando a nuestras vidas son los llamados wearables. Son pequeños y son dispositivos que se llevan “puestos” es decir se los pone y ellos son capaces de captar información de ciertas actividades que realiza el usuario. Además proporcionan algunos servicios dependiendo del dispositivo, normalmente estos dispositivos van conectados a otros dispositivos entre los cuales hay un tráfico de datos entre ellos. Varios ejemplos de dispositivos wearable son los smartwacth, google glass, sensores incorporados en la ropa o zapatillas como son las Nike+ o incluso biosensores médicos para controlar la glucosa o el colesterol por ejemplo.

Otro ejemplo de la evolución de esta tecnología en la vida real es la domótica. Muchas de las nuevas casas construidas disponen de este tipo de sistema. Con ello se permite a los usuarios que realicen de formo remota y/o automática acciones dentro de la casa, como puede ser el control de las persianas, de las luces, la calefacción e innumerables acciones. Todos estos sistemas están interconectados a través de internet y va en aumento como todos los elementos del internet de las cosas.

1.2 Alcance y objetivos

En el siguiente proyecto se va estudiar y analizar la seguridad en que se encuentran los dispositivos que están dentro del internet de las cosas.

Pero antes de comentar los aspectos de seguridad de dichos dispositivos vamos a ver qué es exactamente el internet de las cosas y vamos a ver la evolución que puede sufrir. Vamos a ver ejemplos de cómo el internet de las cosas puede evolucionar en multitud de ámbitos. De este modo podemos hacernos una idea de lo importante que es la seguridad en estos dispositivos debido al amplio abanico de ámbitos en los cuales se puede aplicar.

La seguridad es un aspecto muy importante a tener en cuenta debido a que cada vez más hay más dispositivos conectados a internet, lo que supone que hay mayor exposición de datos a la red. Aunque pueda parecer que muchos de los dispositivos dentro de la categoría del internet de las cosas no son relativamente críticos, pueden llegar a serlo si no son usados de forma adecuada. Muchos de estos dispositivos tienen vulnerabilidades que software malicioso puede aprovecharse de ellos. El problema viene cuando cada vez, más dispositivos se están conectando a internet y

no se está teniendo tan en cuenta la seguridad de dichos dispositivos. La seguridad tendría que ser de las cosas más importantes a tener en consideración desde el diseño de los dispositivos.

En el siguiente proyecto se va a realizar un análisis del estado de los dispositivos que son catalogados como el internet de las cosas. Además vamos a poner un poco en contexto el marco legal de la unión europea respecto al tratamiento de la información

La seguridad de la información es un aspecto clave y que preocupa debido a que el número de dispositivos que se conectan a internet va en aumento, esto conlleva un crecimiento de datos expuestos en la red. Aunque en principio se puede considerar que los dispositivos del internet de las cosas no son críticos, son dispositivos que pueden a llegar serlo debido a la información que manejan y al mal uso que se le s puede dar. Muchos de estos dispositivos no cuentan con la suficiente seguridad y muchos de ellos tienen fallos de autenticación, sus interfaces son vulnerables, la transmisión de datos no es segura,…. Es nos lleva a que se está evolucionando sobre la funcionalidad y la tecnología que usan estos dispositivos pero no tanto en la seguridad que es un aspecto que debería ser considerado de gran importancia, como ya analizaremos, el tema de la seguridad debería se primordial desde el diseño del dispositivo.

En este proyecto también daremos algunos consejos o recomendaciones para la prevención y salvaguardar la información y hacer que nuestros dispositivos sean lo más seguros posibles.

También vamos a comentar algunos casos reales en los cuales algunas vulnerabilidades han sido explotadas por algún atacante y que pueden provocar grandes pérdidas y provocar riesgos a los usuarios. Casos en los cuales objetos comunes que estén conectados a internet y que algún tercero se pudiese hacerse con el control de tal objeto y manejar a su voluntad, como ejemplo de esto imaginemos una nevera que esté conectada a internet, si algún tercero se hiciera con su control podría por ejemplo modificar la temperatura o incluso desconectarla los que afectaría a la calidad de los alimentos, pudiendo afectar ya no solo económicamente a las personas por la pérdida de dichos alimentos sino también a su salud porque si los alimentos sufren bajadas y subidas de temperatura pueden

ponerse malos y si las personas no se han percatado de este ataque y los consumen pueden ponerse enfermos. Por tanto la seguridad como vemos es un punto clave y si no disponemos de dispositivos seguros pueden provocar grandes perjuicios.

Hasta ahora se han puesto ejemplo de un entorno doméstico pero el internet de las cosas abarca mucho más, estos dispositivos por ejemplo también son usados en un entorno industrial y empresarial. En estos casos una falta de seguridad en dispositivos del internet de las cosas puede provocar a la empresa grandes pérdidas económicas y sociales. Como ejemplo lo que podría ocasionar a una empresa que un tercero tomara el control del aire acondicionado de su centro de datos, esto podría ocasionar una pérdida de información y paralizar la empresa con lo que supone una pérdida económica importante dependiendo del volumen de trabajo de la empresa. Otro ejemplo puede ser que algún atacante pudiera acceder a los servicios en la nube que una empresa ofrece a sus usuarios, en la cual están todos sus datos, si este hecho se da a conocer la gente no confiara en esta empresa y no contratarían sus servicios con lo cual la empresa perdería la confianza de sus usuarios.

Con todo esto no se intenta que los usuarios no confíen en estos dispositivos pero si es cierto que hay que tener ciertos cuidados, los usuarios tienen que ser conscientes de que el internet de las cosas en una realidad y que puede conllevar algunos riesgos y que se tienen que seguir unas recomendaciones para hacer de uso más seguro, confiable y libre. Para todo esto en este informe vamos a ver los posibles vectores de ataque para estos dispositivos y algunas medidas de prevención.

Además de todo esto, también vamos a centrarnos en uno de los dispositivos del internet de la cosas, los wearables. Vamos a definir exactamente en qué consisten, vamos a describir algunos ejemplos de ellos y vamos a ver qué problemas de seguridad pueden tener y algunas recomendaciones para hacer que nuestro dispositivo se lo más seguro posible y evitar que los usuarios se vean afectados por algún ataque indeseado.

Los objetivos de este proyecto son los siguientes:

- Descubrir que es el internet de las cosas, así como su situación y su evolución. También dar a conocer la gran cantidad de dispositivos distintos que entran dentro de esta categoría.
- Ver los riesgos que pueden surgir si no se tiene en cuenta la seguridad de estos dispositivos y ver cómo puede afectar a los usuarios y a las empresas. Daremos a conocer los riesgos que ha dado a conocer los expertos de la comisión europea y ver en qué ámbitos puede afectar
- Conocer el marco legal que la Unión Europea exige para las empresas que se ubiquen dentro de la Unión Europea.
- Evidenciar la falta de seguridad de muchos de los dispositivos del internet de las cosas que están interconectados entre sí y a internet.
- Ver en detalle cuales son las posibles vías de ataque que pueden utilizar los atacantes para poner en riesgo la seguridad de estos dispositivos.
- Conocer algunas medidas de protección recomendadas para estos dispositivos que están conectados entre sí
- Concienciar a los usuarios de los posibles ataques y engaños que pueden sufrir a través de estos dispositivos para minimizarlos.
- Dar a conocer algunas amenazas reales sobre dispositivos que conocemos
- Conocer en qué consisten los dispositivos llamadas wearables, así como algunos ejemplos
- Ver los riesgos de seguridad que se pueden producir en los dispositivos wearables.
- Algunas recomendaciones para que nuestro dispositivos wearable se los más seguro posible.

2. Internet de las cosas. Aplicaciones

Antes de empezar a ver cuáles son los riesgos y vulnerabilidades de seguridad y privacidad del internet de las cosas vamos a ver qué es exactamente y veremos algunos ejemplos que se pueden dar gracias a esta tecnología. Bien es cierto que esta tecnología ahora mismo está en auge por lo que varios ejemplos que veremos a lo largo de este capítulo está todavía en estudio o en desarrollo pero que un breve espacio de tiempo estará a la orden del día

Ya hemos visto que el internet de las cosas son todos los objetos que hasta ahora no tenían internet pero en los que se está empezando a incorporar, la idea de todo esto es que estén en nuestra vida cotidiana y que pasen desapercibidos, ayudándonos en nuestras tareas y en nuestros servicios. El principal objetivo del internet de las cosas es crear entornos y dispositivos inteligentes (“Smart”) y conscientes para multitud de aplicaciones, estas pueden variar desde aplicaciones relacionadas con la energía, el transporte, la salud,… es decir, infinidad de áreas [2]. El internet de las cosas consiste en objetos conectados a internet e interconectados entre sí mismo, estos dispositivos pueden compartir la información que han captado para su procesamiento por otros dispositivos o bien para almacenarla en internet para su posterior procesamiento.

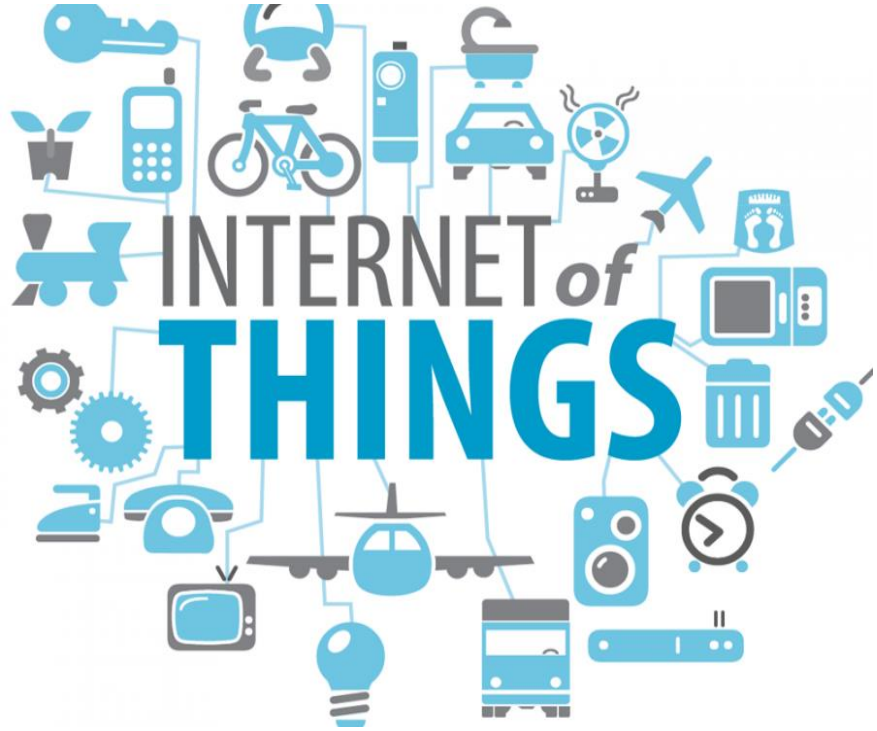

Ilustración 3 Multitud de áreas del internet de las cosas

Hay múltiples aplicaciones para el internet de las cosas y muy diversas, puede estar presente en prácticamente todos los ámbitos de la vida cotidiana de las personas y de las empresas. En los siguientes apartados vamos a ver una muestra de las aplicaciones concretas dentro de múltiples áreas como ejemplos, estos ejemplos son dispositivos que ya se están implantando o que podrían convertirse así en un futuro no muy lejano con la evolución de la tecnología [3].

3.1 Smart Cities

Las SmartCities o ciudades inteligentes también llamadas ciudades eficientes son aquellas que tienen un desarrollo urbano que está basado en la sostenibilidad capaz de responder al momento y adecuadamente a las necesidades básicas de instituciones, empresas y de las personas, en los diferentes aspectos, como pueden ser el económico, operativos, sociales y ambientales [4].

Ilustración 4 Ejemplo de SmartCity

- Parking inteligentes: capaces de monitorizar las plazas de aparcamiento disponibles en la ciudad.

- Salud Estructural: capaces de monitorizar las vibraciones y estado de los materiales de los edificios, monumentos, puentes,….
- Mapas de ruido: Los cuales monitorizan el nivel de ruido de las zonas de bares o pub y las zonas céntricas en tiempo real.
- Congestión de tráfico: monitorización de los vehículos que circulan y los peatones para optimizar su circulación.
- Iluminación inteligente: la iluminación será de manera adaptativa en función del tiempo
- Gestión de residuos: se monitorizan los niveles de basura de los contenedores para optimizar las rutas.
- Sistemas de transporte inteligente: las carreteras y autovías son inteligentes lo que significan que pueden dar mensajes de advertencia y desviar la circulación dependiendo de las condiciones meteorológicas y los eventos que se produzca como pueden ser los atascos o accidentes.

3.2 Smart Environment

Un entorno inteligente en el cual el mundo físico que está integrado e invisible con sensores, actuadores, visualizadores y elementos computacionales, integrados de manera completa en los objetos cotidianos de nuestras vidas y conectados a la red ininterrumpidamente[5].

Ilustración 5 Ejemplo de SmartEnvironment

Los entornos inteligentes intentan satisfacer la experiencia de las personas en todos los ambientes, sustituyendo trabajos peligrosos o físicos y tareas repetitivas por ejemplo.

- Detección de incendios forestales: se monitorizan los gases y previene de incendios.
- Contaminación del aire: monitoriza la emisiones de CO2 y las controla en las fábricas, coches,….
- Prevención de deslizamientos y avalanchas: controlan la humedad del suelo, vibraciones y la densidad de dicho suelo, para poder así detectar condiciones peligrosas.
- Detección temprana de terremotos: controlan las zonas en los lugares específicos de temblores.

3.3 Smart Water

Se encargan de la gestión del agua en las ciudades y de que todo esté en orden en este ámbito. El agua es el recurso más preciado en la ciudad y su gestión inteligente es uno de los principales retos a los que se enfrentan las Smart Cities [6].

- Calidad del agua: analiza la aptitud del agua en los ríos y mares para la fauna y la elección para su uso potable.
- Fugas de agua: monitoriza los tanques y las tuberías de agua para comprobar la presión del agua y si presencia de ésta fuera de ellos.
- Inundaciones: monitoriza las variaciones del nivel del agua en ríos, embalses,….

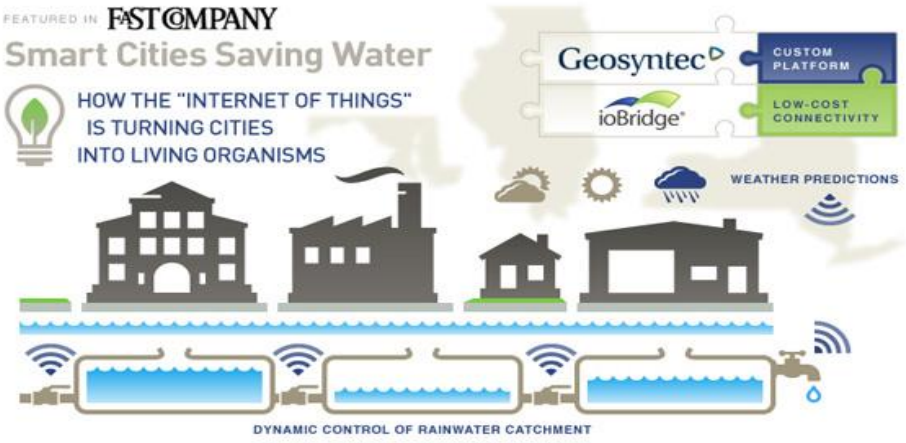

Ilustración 6. Ejemplo de Smartwater

3.4 Smart Metering (Contadores Inteligentes)

Son medidores inteligentes que calcula el consumo de una forma más detalla que los controladores convencionales. Con estos dispositivos se puede ofrecer la posibilidad de comunicar esta información a través de la red a un centro de control [7].

- Smart Grid: controla y gestiona el consumo de energía.
- Nivel del depósito: controla los niveles de agua, gas, petróleo,…
- Instalaciones fotovoltaicas: Optimizan y gestionan el rendimiento en las instalaciones de energía solar.
- Flujo de agua: monitoriza la presión del agua en su transporte.
- Cálculo de almacenamiento en silos: controla y mide el nivel de vacío y peso de las mercancías

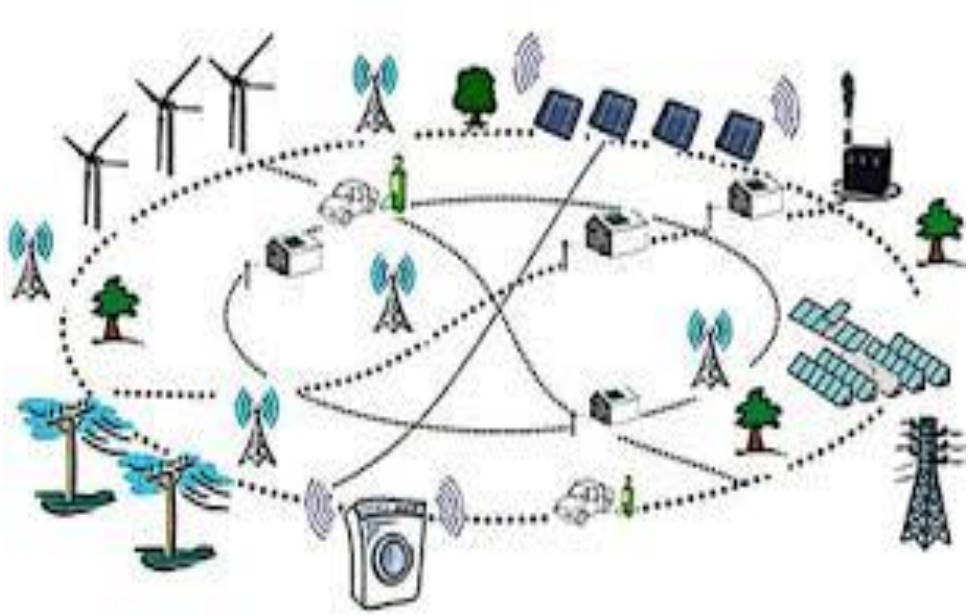

Ilustración 7 Ejemplo de Smart Metering

3.5 Seguridad y Emergencias

Con el internet de las cosas incluyendo sensores y detectores en ambos ámbitos se puede controlar las emergencias y la seguridad de ciudades, campos,… como por ejemplo:

- Control de acceso perimetral: Controla el acceso a las áreas restringidas y detecta personas en zonas no autorizadas.
- Presencia de líquidos: controla y detecta líquidos en centros de datos, almacenes,… para prevenir averías y corrosión.
- Niveles de radiación: mide los niveles de radiación en los entornos de las centrales nucleares para alertar en casos de fuga
- Gases nocivos y explosivos: detecta los niveles de gases y fugas en los entornos industriales y empresas de riesgo de este nivel.

3.6 Retail (venta al por menor)

Es el sector económico que engloba a empresas que se dedican a la comercialización masiva de productos o servicios uniformes a un gran volumen de clientes. Es el sector industrial que suministra productos al consumidor final

- Control de la cadena de suministro: monitorización de condiciones que está almacenado un suministro a lo largo de toda su trayectoria y hace el seguimiento de los productos
- Pagos mediante NFC: procesa los pagos que están basados en la ubicación o duración de una determinada actividad.
- Aplicaciones para compras inteligentes: se obtiene asesoramiento en el mismo punto de venta de acuerdo a los hábitos o costumbres de los clientes, preferencias,….
- Gestión inteligente del producto: controla la reposición de los productos en los estantes de los mercados.

3.7 Logística

La logística es el conjunto de medios y métodos necesarios para llevar a cabo la organización de una empresa o llevar a cabo un servicio, normalmente de distribución.

- Calidad de las condiciones de envío: monitorizan el envío de suministros, como puede ser las vibraciones, golpes, aperturas, ruptura de cadena de frío,….
- Ubicación del artículo: busca elementos en las grandes superficies para agilizar el proceso de búsqueda.

- Detección de incompatibilidad de almacenamiento: detecta y genera advertencias en los contenedores de almacenamiento de productos inflamables juntos a productos que pueden llegar a ser explosivos.
- Rastreo de flotas: controla la rutas seguidas por los productos delicados como productos médicos, joyas,….

Ilustración 8 Logística

3.8 Control Industrial

En este ámbito se trata de aplicar el internet de las cosas para utilizarlas en el campo de la automatización y el control automático para mejorar la eficacia y la eficiencia de la industria mediante el uso de esta tecnología.

- Aplicaciones M2M: diagnostica automáticamente y controla los activos de la empresa
- Calidad del aire interior: controla los niveles de oxígeno y de gases nocivos para la salud del interior de las plantas químicas para garantizar la seguridad de los trabajadores.
- Monitorización de la temperatura: controla la temperatura del interior de los refrigeradores industriales o médicos que contengan mercancía sensible a cambios de temperatura.
- Presencia de ozono: controla los niveles de ozono en el proceso de secado de la carne en fábricas de alimentos.

- Ubicación interna: ubicación interna de los bienes de una empresa usando etiquetas. Estas etiquetas pueden ser de dos tipos, activas (ZigBee) o pasivas (RFID/NFC).

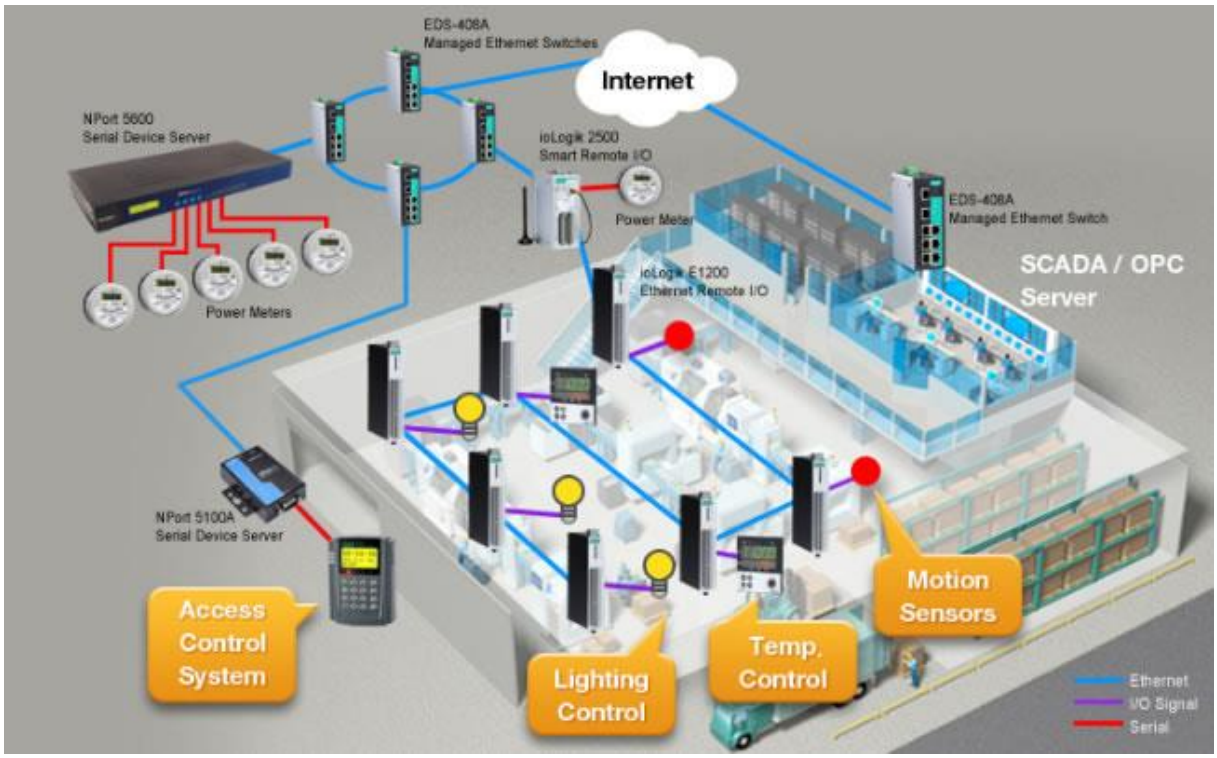

Ilustración 9 Control Industrial

3.9 Agricultura inteligente

En la agricultura inteligente se usan la tecnología del internet de las cosas para mejorar la agricultura. Con esta nueva tecnología se puede modernizar el campo y las explotaciones, gracias a esto se consiguen mayores beneficios y reducción de costes [8].

- Mejora de la calidad del vino: monitorización de la humedad del suelo y el diámetro de los troncos de las cepas que controlan la cantidad de azúcar en las uvas y la salud de la vid
- Casas Verdes: controlan las condiciones micro-climáticas para elevar la producción de las frutas y hortalizas de calidad.
- Campos de golf: se riega selectivamente, buscando las zonas más secas y reduciendo así el agua necesaria para mantenerlo

- Red de estaciones meteorológicas: analizan las condiciones meteorológicas en los campos, de esta manera se puede pronosticar la formación de hielo, aparición de lluvia, sequía,….
- Compost: monitoriza los niveles de humedad y temperatura de la paja, alfalfa,….

Ilustración 10 Ejemplo de dispositivo para la mejora del vino

3.10 Domótica y Automatización del hogar

La domótica es el conjunto de sistemas que automatizan una vivienda, aportando servicios de gestión energética, seguridad, bienestar y comunicación. Estos sistemas pueden estar integrados por medios interiores y exteriores de comunicación, cableados o inalámbricos. Este control se puede realizar desde dentro o fuera del hogar [9].

- Uso de energía y agua: monitorización y seguimiento del consumo de energía y agua y recomendaciones para ahorrar costes y recursos.

- Aparatos de control remoto: conexión y desconexión, y control remoto de diferentes electrodomésticos del hogar.

Ilustración 11 Casa con un sistema de domótica

- Sistemas de detección de intrusos: detección de aperturas de puertas y ventanas de la vivienda para prevenir intrusos.
- Conservación de bienes: monitorización de las condiciones para preservar nuestros bienes.

3.11 eHealth (Salud)

Este término hace referencia a la práctica de cuidados sanitarios que son apoyados en tecnologías de la información y las comunicaciones [10].

- Detección de caídas: asistencia a personas mayores o discapacitadas en viven solas.
- Neveras sanitarias: controlan las condiciones de almacenamiento y de temperatura de los medicamentos, vacunas,….
- Cuidado de deportistas: monitorizan las constantes vitales de los deportistas en los centros de alto rendimiento o en la práctica del deporte.
- Vigilancia de pacientes: vigila las condiciones de los pacientes en los hospitales y en los hogares de ancianos

- Radiación ultravioleta: mide los rayos UV del sol y advierte a las personas cuando es perjudicial para ellos.

Ilustración 12 eHealth

3.12 Wearebles

Los dispositivos wearebles son dispositivos que los usuarios llevan “puestos”. Estos dispositivos pueden cumplir multitud de funciones dependiendo del dispositivo.

- Smartwatch: son dispositivos que sincronizan su información con smartphones o tablets, además los últimos modelos también pueden usar usados independientemente y tiene multitud de aplicaciones o y widgets. Además pueden realizar llamadas, sacar fotos o capturar videos.
- Textil: dispositivos que se incluyen en la propia ropa y proporciona información al usuario, como por ejemplo ropa que detecta los rayos uva y nos avisa si puede ser perjudicial para nuestra salud o por ejemplo marcas como Nike o Adidas que incorporan chips en sus zapatillas y se puede medir el rendimiento en los entrenamientos.
- Pulseras fitness: estas pulseras comprueban nuestro estado de salud y mide nuestras pulsaciones, calculan los pasos que damos, la velocidad, horas de sueño,…. De este modo podemos llevar un control total de nuestro cuerpo

3. Marco legal

En este capítulo vamos a ver la normativa que se aplica al internet de las cosas. En principio vamos a ver la normativa que aplica la Unión Europea a la protección de datos. Veremos que normativa deben seguir las empresas y los dispositivos que tratan con la información de los usuarios aunque como veremos a continuación estas normativas son algo antiguas (del año 1995 y 2002) y son las que están en vigor ahora mismo y las que se deben aplicar.

El tratamiento de los datos personales y la circulación de los mismos en la Unión Europea deben atenerse a lo dispuesto en la Directiva 95/46/CE [12] y en la Directiva 2002/58/CE [13]. Los responsables del tratamiento de estos datos que tengan su sede en Europa deben cumplir con esta normativa. Pero muchos de estos responsables de dispositivos o servicios no provienen de Europa, en la mayoría de casos de China o USA por ejemplo, y en ocasiones estos prescinden de cumplir estas normativas para que se ajusten a los requisitos de confidencialidad previstos en la normativa Europea.

Estas previsiones afectan a multitud de agentes en el mercado, como son fabricantes, gestores de redes sociales, desarrolladores de aplicaciones,… en mayor o menor medida todos ellos actúan sobre los datos de los usuarios y participan de algún modo en alguna de las fases por la que pasa la información, por lo tanto son responsables de dicha información [14].

- Confidencialidad en las comunicaciones
  El almacenamiento de la información o el acceso a ella en los terminales de los usuarios a través de la red solo se permitirá, en el sentido del artículo 5 de la Directiva 2002/58/CE, cuando se facilite toda la información referente a la finalidad del tratamiento de los datos de forma clara y completa al usuario y siempre que el responsable de tal tratamiento ofrezca al usuario el derecho a oponerse. Se entiende que el almacenamiento de información permitido se realiza cuando es estrictamente necesario para proporcionar un servicio que el propio usuario solicita.
- Legitimidad del tratamiento de datos

El tratamiento de los datos estará legitimado cuando se cumplan los requisitos previstos en el artículo 7 de la Directiva 95/46/CE. En el ejercicio de tal artículo son esenciales tres de ellos:

- Consentimiento: cuando el usuario de su consentimiento de forma inequívoca
- Ejecución de un contrato en el que el usuario sea parte: la aplicación de este motivo está delimitada por la necesidad, es decir, que requiere una conexión directa y objetiva entre el tratamiento de datos y la finalidad de la ejecución contractual esperada por el interesado
- Satisfacción del interés legítimo perseguido por el responsable del tratamiento o por los terceros a quienes se comuniquen los datos: siempre y cuando no prevalezca el interés o los derechos y libertades fundamentales de los usuarios.

- Calidad de los datos

  Aquí se centra en las previsiones contenidas en el artículo 6 de la Directiva 95/46/CE. Lo primero es que los datos deben de ser tratados de manera leal y lícita. El principio de lealtad requiere que los datos personales nunca sean tratados sin el consentimiento del individuo. Los agentes que estén implicados en el tratamiento de dicha información deben informar a los usuarios cuando se recopile dicha información, bien sea propia del usuario o de su entorno. El otro requisito es que los datos sean recopilados por un fin concreto, explícito y legítimo. Todo esto es para conseguir el objetivo de que el usuario pueda saber cómo y con qué finalidad se usaran sus datos y con esa información el propio usuario decida puede confiar en tratamiento de los mismos.

  El tratamiento de los datos debe ser adecuado, pertinente y no excesivo con la relación a los fines para los que se recogen. El principio de minimización de datos implica que los datos innecesarios para dicha finalidad que se buscaba por el agente no podrán ser recogidos y almacenados solo por el simple hecho de que a posteriori puedan resultar útiles.

- Tratamiento de datos especiales o sensibles.

  Las aplicaciones que están diseñadas para instalarse en los dispositivos inteligentes pueden tener acceso y procesar los datos personales que revelen el origen étnico o racial del individuo, opiniones políticas, credenciales religiosas o filosóficas, pertenencia a sindicatos, salud o vida sexual; datos

que son calificados como sensibles y que requieren una protección especial prevista en el artículo 8 de la Directiva 95/46/CE. Para el tratamiento legítimo de estos datos es necesario obtener el consentimiento explícito del usuario, a no ser que el tratamiento se refiera a datos que el propio usuario ya haya hecho públicos voluntariamente.

- Seguridad del tratamiento

  En el artículo 17 de la Directiva 95/46/CE obliga al responsable del tratamiento de datos a "*aplicar las medidas técnicas y de organización adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados […]".* Se requiere además, que el responsable del tratamiento de los datos seleccione un encargado que cumpla las garantías suficientes en relación con las medidas de seguridad técnica y organización de los tratamientos que deben realizarse.

  Las medidas de seguridad deben cumplirse teniendo en cuenta las restricciones operativas específicas de cada dispositivo. A día de hoy la mayor parte de los sensores no son capaces de establecer una conexión encriptada como consecuencia de la prioridad otorgada a la autonomía física del dispositivo. Por lo tanto sus componentes se sirven de comunicaciones WiFi normalmente y se caracterizan por tener unos recursos limitados en cuanto a energía e informática, estos dispositivos son vulnerables a los ataques físicos , espionaje o ataques proxy. El internet de las cosas cuenta con una compleja cadena de suministros con multitud de agentes que tienen diferentes grados de responsabilidad, pudiendo la falta de seguridad provenir de cualquiera de estos dispositivos.

- Derechos del interesado en el tratamiento: derecho de acceso y oposición

  Los usuarios que tienen derecho a conocer los datos objeto de tratamiento, la finalidad y los destinatarios a quienes se comunican. Tienen derecho a la rectificación de los mismos, la supresión o bloqueo de estos cuyo tratamiento no proceda y a que se informe a terceros que tengan estos datos en su poder de las modificaciones pertinentes.

  Los usuarios también tienen la posibilidad de revocar cualquier consentimiento prestado previamente y oponerse al tratamiento de datos que esté relacionados con el mismo. Estos derechos se deben poder ejercer sin

ninguna restricción ni obstáculo y las herramientas para ejercer dicha oposición deben estar accesibles y ser eficaces.

Como conclusión de este tema, como vemos el gran problema es que las muchas de las empresas que suministran dispositivos en nuestro país o en la unión europea no tiene sus sedes en Europa y los dispositivos provienen de otros continentes con lo cual no se aplica esta normativa y por lo tanto estos dispositivos pueden tener vulnerabilidades e incumplir el tratamiento de datos personales.

Otro gran problema de esta normativa es que debido a su antigüedad no se contemplan casos que se pueden dar con tecnologías actuales como es el internet de las cosas. En los cuales hay una amplia variedad de dispositivos, con sus propias características y diferentes tipos de comunicación.

Ahora veremos en España que normativa usamos, en principio se rige por la normativa de la Unión Europea y por ley orgánica de protección de datos (LOPD), la cual tiene unas bases parecidas a las que ya hemos nombrado con las normativas de la Unión Europea. Actualmente en España a través de la Agencia Española de Protección de Datos se ha aprobado un plan estratégico que nombra por primera vez el internet de las cosas. El Plan Estratégico 2015-2019 se lleva a cabo con el di de cumplir con el artículo 37 de la Ley Orgánica 15/1999, de 13 de diciembre, en el cual se señala entre sus funciones *proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal* e incluye *velar por el cumplimiento de la legislación sobre la protección de datos y controlar su aplicación* [30].

El Plan Estratégico 2015-2019 está compuesto por 5 ejes de actuación y un apartado se contempla el caso que estamos estudiando. En el cual se muestra que hay diversos estudios que señalan que la interconexión de objetos y personas y el internet de las cosas va a sufrir un crecimiento exponencial en los próximos años con lo que puede provocar un gran impacto en la privacidad, por consiguiente la AEPD (Agencia Española de Protección de Datos) debe estar preparada para toda esta evolución. Lo que propone este plan estratégico es realizar estudios sobre el internet de las cosas y lo llamado sociedad conectada que abordara temas como el big data, internet de las cosas, Smart cities, y todos los ejemplos puestos en el capítulo anterior.

El gran problema de estas normativas que se aplican en nuestro país y en la Unión Europea es que son normas que se crearon hace tiempo y que aunque se trata sobre la protección de datos de carácter personal no se contemplan nuevas situaciones que se pueden dar con las nuevas tecnologías. Aunque si es cierto que por ejemplo se están tratando la Directiva 95/46/CE y se prevé una reforma adaptándola a los nuevos tiempos o por ejemplo el plan estratégico de 2015-2019 de la AEPD, pero sigue existiendo el problema porque todavía no se han aplicado estas reformas o no se contemplan hasta que pase un tiempo o se hagan estudios pero mientras tanto en la actualidad hay multitud de dispositivos que procesan datos de carácter personal y que se están transmitiendo y procesando.

Otro problema relacionado con todo esto es quien es el titular o de quien son propiedad los datos recogidos por el internet de las cosas. La normativa de privacidad establece el principio del consentimiento informado en el cual se da los derechos de acceso, rectificación, cancelación y oposición de los datos a las personas pero no se establece en ningún momento quien es el titular o propietario de dichos datos. Otro caso diferente es que la empresa por su propia voluntad quiera dar a las personas el control total de sus datos o "vida digital" [31].

Un ejemplo de esto puede ser en las Smart cities o ciudades inteligentes que se están empezando a implantar, estos sistemas procesan una gran cantidad de datos que recogen de diferentes suministros de servicios como puede ser el tráfico de vehículos, consumo eléctrico o de agua,… todos estos datos son gestionados normalmente terceros, es decir, los ayuntamientos no tienen capacidad para recolectar o gestionar estos datos y se contratan a terceros. Todos estos datos tienen que ser propiedad de alguien pero por ley no viene definido o incluso las ganancias que se puedan obtener del tratamiento de esos datos. El problema es que nuestra legislación no contempla estos casos y lo único que deja claro es que la empresa que pone los medios para recolectar y procesar los datos o la base de datos tiene derechos sobre la misma pero solo sobre la base de datos no sobre los datos en sí, pero en cambio sobre los datos no hay ninguna legislación explicita que regularice la propiedad de los mismos.

3.1 Ejemplo de política de privacidad: Runtastic

Esta aplicación es una aplicación del tipo de entrenador personal que ayuda al usuario en diferentes tipos de deportes o actividades. Con su plataforma se pueden

realizar seguimientos y analizar los entrenamientos. Como ejemplo esta aplicación se puede usar cuando el usuario sale o correr y dependiendo de los dispositivos que lleve puede ver la ruta que ha seguido, la velocidad que ha llevado, el tiempo que tardado, las pulsaciones,…. Esta aplicación tiene acceso a los datos del usuario a su estado de salud, a su geolocalización,… por los tanto esta aplicación tiene acceso a datos personales del usuario por lo que es muy importante las política de privacidad de estos datos [32].

Si revisamos la política de privacidad vemos que Runtastic cumple con la normativa de protección de datos y garantiza los derechos sobre los datos a sus usuarios. La política de privacidad también nos informa de que el usuario puede elegir con quien compartir su información, aunque avisa que algunas funciones implican que su activación el usuario acepta que sus datos sean compartidos con terceros. Además cada usuario puede cambiar la política de privacidad accediendo a la configuración de su cuenta.

También nos informa de que la información personal de cada usuario solo será utilizada por la propia aplicación para su uso y poder mejorar la aplicación y servicios que ofrecen y no será compartida con terceros a no ser que sea requerido legalmente o por el consentimiento del propio usuario. Aunque también nos dice que los usuarios consienten expresamente el almacenamiento y el uso de la información de identificación no personal con fines de publicidad en la propia aplicación o por sus socios, lo que quiere decir, que los datos sin que se identifiquen con el usuario pueden ser usados por Runtastic para sus propios fines.

Un problema de privacidad que se comenta también es que la aplicación cuenta con complementos de medios sociales, es decir cuanta con complementos que enlaza la aplicación y los datos que maneja con las redes sociales como puede ser Facebook o Twitter por ejemplo. En estos casos Runtastic no se hace responsable de la información que se comparta en estos medios y el uso que le den. El usuario se hace responsable de usar estos complementos y lo que quieren compartir.

Para finalizar en la política de privacidad se informa que solo con el uso de la aplicación el usuario está aceptando dicha política.

Una vez vista la policita de privacidad y sus principales puntos observamos que los datos son propiedad de Runtastic y aunque cumplan con la normativa pueden compartir los datos siempre y cuando no se identifiquen con los usuarios. Además si los usuarios aceptan o usan los complementos de las redes sociales los datos personales pueden ser compartidos y usados por terceros y Runtastic no se responsabiliza de dicho uso. Por lo tanto el usuario pierde el control de sus datos.

Para finalizar el usuario tiene que tener muy clara la configuración de la aplicación y ver que permisos y a que áreas accede de dicha aplicación, porque como hemos visto según la configuración los datos pueden ser compartidos con terceros y lo mismo ocurre si se accede a determinadas áreas o se activas determinadas funciones que solo por hacerlo el usuario está aceptando (la mayoría de veces sin ser consciente de ello) compartir sus datos personales con terceros.

Por lo tanto hay que tener mucho cuidado con la configuración de esta aplicación y dejando solo los permisos que creamos convenientes y teniendo cuidado a las áreas o funciones que accedemos. Además los usuarios deben ser conscientes de que si acceden a las redes sociales a través de la aplicación pierden el control de sus datos.

3.2 Ejemplo de política de privacidad: Facebook

Facebook como ya sabemos es una red social que cuanta con millones de personas registradas. Esta red social sirve para compartir fotos, videos, comentarios,… y toda esta información personal debemos saber cómo es tratada y que responsabilidades tenemos y tiene las propia red social.

Si leemos la Declaración de derechos y responsabilidades [33] que nos proporciona Facebook observamos que somos los propietarios de todo el contenido y la información que publiquemos en la red social y podemos contralar como se comparte accediendo a la configuración.

Cuando publicamos algún contenido otorgamos que Facebook sujeto a nuestra configuración de privacidad una licencia no exclusiva, tranferible, con posibilidad de ser subotorgada, libre de regalías y aplicable globalmente para utilizar cualquier contenido IP que publiques. Es licencia finaliza cuando eliminamos en contenido o la

propia cuenta del usuario, a menos que ese contenido se haya compartido por terceros y estos no lo hayan eliminado.

Cuando se elimina algún contenido Facebook puede hacer que permanezca en las copias de seguridad durante algún plazo de tiempo razonable aunque no estará disponible para terceros.

Al usar alguna aplicación, esta aplicación podrá solicitar permiso para acceder a nuestro contenido e información. Si aceptamos el acuerdo de la aplicación será esta la que procesara nuestros datos y utilizara, almacenara y transferirá.

Cuando en nuestra configuración de privacidad hacemos publico nuestro contenido aceptamos que cualquier persona que use Facebook o incluso ajenas a Facebook puedan acceder y usen nuestra información.

Como vemos en Facebook nosotros somos los propietarios de nuestra información pero con la salvedad de que si algún otro usuario la comparte o alguna aplicación a la que le demos permiso la use perdemos el control de dicha información. Incluso si nosotros borramos ese contenido si otro usuario o aplicación la compartido esta información sigue estado disponible en dicho usuario o aplicación. Por lo tanto cualquier contenido que publiquemos debemos ser conscientes de que podemos perder el control de esta información y nos arriesgamos a que sea usado por cualquier usuario. Por lo tanto hay que tener una buena configuración de privacidad para controlar todo lo posible el acceso a nuestros contenidos e información y debemos ser conscientes y responsables del contenido que publicamos.

4. Riesgo del internet de las cosas

Como hemos visto en el capítulo anterior el internet de las cosas está presente en muchos ámbitos, tanto desde el punto de vista de los usuarios hasta el punto de vista industrial y empresarial. Viendo tantos ejemplos y viendo todos los ámbitos en los que puede estar presente el internet de la cosas se ve la importancia de analizar los riesgos y como veremos en los siguientes capítulos cuales son las amenazas y veremos cómo poder evitarlos o al menos minimizarlos lo máximo posible.

Vamos a estudiar los riesgos asociados a la evolución del internet de las cosas. Estos riesgos dependen de la información que manejen los dispositivos, de la función que realicen y la dependencia que se tenga del propio dispositivo. Vamos a ver cuáles son los riesgos más comunes y las áreas que se pueden ver afectadas ante algún ataque realizado con éxito.

Un ataque realizado con éxito puede afectar a la integridad de la información que dispone el dispositivo, a la accesibilidad y la identidad del propio usuario provocando una suplantación de la identidad. Una de las cosas más importantes a tener en cuenta es la disponibilidad del dispositivo, es uno de los aspectos que mayor problema nos puede generar, sobre todo si hablamos por ejemplo de una industria, en la cual una parada del servicio provocada por un ataque de denegación de mismo puede provocar pérdidas bastante cuantiosas. Otro factor importante es el tema de la confidencialidad de los datos, la cual debe estar garantizada tanto la que esta almacenada en el propio dispositivo como a la transmitida por el dispositivo, bien entre dispositivos o bien a la red.

Los expertos de la Comisión Europea [11], a partir de múltiples estudios realizados que identifican los principales riesgos en entornos altamente conectados, señalan como problemas importantes a tener en consideración, en cuanto a privacidad y protección de datos y la seguridad de la información en los dispositivos del internet de las cosas, los siguientes:

- Asegurar la continuidad y la disponibilidad en la provisión de servicios basados en el internet de las cosas, intentando evitar posibles fallos y cortes en el funcionamiento. Todo esto está muy relacionado con el modelo de arquitectura que se utilice en la prestación de servicios basados en el internet de las cosas, modelo centralizado contra modelo descentralizado.

- Consideraciones en el diseño de tecnologías del internet de las cosas. Es adecuado tener en cuenta las cuestiones de seguridad y privacidad en la fase de diseño, aunque por regla general esto no se hace así y todas estas cuestiones normalmente se tienen en cuenta en la fase de funcionamiento, cosa que limita la efectividad de las medidas de seguridad y es menos eficiente en lo referente a los costes. Este conveniente tener en cuenta las cuestiones de seguridad en la fase de diseño en los dispositivos del internet de las cosas debido a que dichos dispositivos no cuentan con la suficiente memoria y procesamiento como para poder implementar las protecciones necesarias de seguridad a posteriori, o por lo menos aplicar las medida tradicionales de seguridad.
- Los riesgos son sensibles al contexto y aplicación. Dependiendo del ámbito de aplicación o en el contexto en el que se encuentre, los riesgos varían dependiendo de que se requiera de los dispositivos del internet de las cosas. La amplia gama de dispositivos con los que cuenta el internet de las cosas supone un gran problema a la hora de crear soluciones de tipo más general.
- Trazabilidad, análisis del rendimiento, tratamiento ilícito. La gran cantidad de datos que recopilan estos dispositivos plantea un gran problema de autentificación y confianza en dichos dispositivos
- Reutilización de datos. Debido al aumento de la cantidad de datos que manejan los dispositivos del internet de las cosas, es posible que dichos datos puedan utilizarse para otros propósitos que no sean los originales, este es un tema que preocupa bastante y que es necesario controlar.
- Posicionamiento GPS. Los wearables son dispositivos que los usuarios llevan consigo mismos. Normalmente, dichos dispositivos están conectados a internet por lo que se pueden geo posicionar fácilmente en cualquier momento, de hecho algunos dispositivos disponen de un módulo GPS para este fin. Esto hace que los usuarios estén localizados y esa localización que registrada en la red, dependiendo de la configuración de privacidad con la que cuente esta información puede estar al alcance de cualquiera. Estas situaciones además de con los wearable también se puede producir con los propios smartphones en los cuales hay aplicaciones que no sabemos que tienen acceso a la localización pudiendo producir el mismo problema.

- Ejercicio de los derechos de protección de datos para las personas y el cumplimiento de la legislación para las organizaciones. Con las aplicaciones en los dispositivos del internet de las cosas que normalmente funcionan en “background”, los usuarios no son conscientes de la información que recopilan o el procesamiento que se le da a dicha información. Hay que tener muy en cuenta el acceso y control de los datos, así como el permiso para recopilarlos y con qué frecuencia optima se pueden capturar.
- Pérdida o violación de la privacidad y protección de datos de los usuarios. Como ejemplo de este riesgo vamos a poner las nuevas tarjetas de crédito contactless, dichas tarjetas pueden leerse sin necesidad de autenticar nada, esto conlleva el riesgo que cualquier atacante se haga con los datos del cliente y pueda realizar compras sin consentimiento del usuario.
- Pérdida o violación de la privacidad y protección de datos de los usuarios. Como ejemplo de este riesgo vamos a poner las nuevas tarjetas de crédito contactless, dichas tarjetas pueden leerse sin necesidad de autenticar nada, esto conlleva el riesgo que cualquier atacante se haga con los datos del cliente y pueda realizar compras sin consentimiento del usuario. Los dispositivos del internet de las cosas cada vez almacenan más información, en muchos casos esta información se almacena en la nube y los usuarios pueden acceder a ella desde multitud de dispositivos y en cualquier sitio mediante un usuario y contraseña. En estos casos, cuando un atacante pudiera acceder a esta información puede vulnerar la privacidad de los usuarios. En cualquier caso, el robo de información ya no solo puede producirse por una vulnerabilidad del dispositivo del internet de las cosas, si no debido a que cada vez estos dispositivos como por ejemplo los wearable, cada vez son más pequeños, lo que hace que resulte relativamente fácil que cualquier usuario pueda perderlo y cualquiera pueda acceder a toda la información que contenga, este aspecto hay que tenerlo también en cuenta en este punto
- Realización de ataques maliciosos contra los dispositivos y sistemas del internet de las cosas. Si no se aplican controles de seguridad adecuados puede producirse problemas graves que produzca otros problemas o riesgos como los mencionados anteriormente. Lo complicado de esta tarea es identificar cuáles son los controles adecuados para los sistemas del internet

de las cosas, debido a que todavía es un campo innovador y se desconoce su evolución futura. El problema de esto reside en la heterogeneidad de los dispositivos del internet de las cosas lo que hace más que probable que se tenga que definir un control de seguridad para cada sistema o arquitectura

- Lock-in del usuario, se refiere a que los usuarios se queden en un estado "bloqueado" en un proveedor específico de servicios de internet de las cosas y les sea complicado migrar a otros proveedores, cosa que viene provocada por la no homogenización.
- Implicaciones relacionadas con la salud. Existen riesgos referente a la identificación y fiabilidad de la información obtenida del o hacia el paciente. Las soluciones de sanidad electrónicas actuales que se basan en el internet de las cosas están dirigidas a entornos abiertos, entornos en los cuales al estar interconectados recogen e intercambian datos sensibles de los pacientes muy rápidamente, situación que es difícil de controlar y que genera un riesgo en la salud de los pacientes. Por la importancia de este ámbito ya se han realizado algunos avances, como puede ser el diseño de un protocolo de autenticación para la comunicación entre los dispositivos médicos mediante la tecnología RFID que garantiza la seguridad y privacidad de los datos de los pacientes.

5. Seguridad y privacidad del internet de las cosas

El incremento del internet de las cosas está cambiando nuestra visión de ver internet, está cambiándolo de la forma tradicional, como lo conocemos hasta ahora, a una visión más integrada de objetos “inteligentes” que interactúan entre sí. Esto está llevando a que cada vez haya mayor número y diversidad de sensores y dispositivos. Esto conlleva que haya ámbitos en los cuales se manejen datos sensibles y la perdida de información o acceso sin control pueda afectar gravemente la privacidad de los usuarios, por lo tanto la seguridad debe ser un punto clave en el desarrollo y expansión de estos dispositivos. Ha día de hoy no se dispone de ninguna pauta bien definida para la seguridad del internet de las cosas y esto debe ser un factor clave.

Como hemos visto en los anteriores capítulos el internet de las cosas esta en multitud de ámbitos y viendo los riesgos es muy importante ver la seguridad de estos dispositivos debido a que manejan una gran cantidad de datos que a veces los propios usuarios no son conscientes de tal volumen.

Los expertos sugieren que uno de los principales inconvenientes para la implantación es la seguridad y privacidad. El motivo son las restricciones que imponen los propios dispositivos y redes del internet de las cosas que imposibilita la aplicación inmediata de soluciones tradicionales de seguridad. Debido a las características que por lo general caracterizan a los dispositivos de IoT como son pocos recursos de memoria y procesamiento, hacen que usar los protocolos tradicionales de seguridad y criptografía sea casi inviable. Por lo tanto se presenta un panorama nuevo que supone un gran desafío.

El internet de las cosas esta compuestos por objetos “inteligentes” interconectados entre si y a internet, es conlleva la presencia de internet en cualquier cosas, en cualquier lugar y en cualquier momento, lo que eleva que haya más entradas y salidas de información, y por lo tanto mayor riesgo. La heterogeneidad de los objetos conectados hace que sea difícil encontrar una solución genérica y que haya distintos niveles de riesgo con diferentes soluciones.

La seguridad de los sistemas depende de la capacidad que tengan para responder a ataques externos como para evitar daños al entorno o a los usuarios. La seguridad debe ser confidencialidad, integridad y disponibilidad. Estos son los principios que

tenemos que conseguir con el internet de las cosas adaptándolas a cada objeto y sus necesidades.

Para identificar las vulnerabilidades de seguridad para los dispositivos del internet de las cosas es imprescindible tener en cuenta las particularidades de cada dispositivo. Por regla general, son dispositivos empotrados con menos recursos y menos complejos que un ordenador personal, debido a que están diseñados para cumplir unas funciones particulares y no con un propósito general. Como hemos comentado anteriormente esto hace que sean sistemas heterogéneos y cada fabricante implementa sus propias soluciones. Al contrario que sucede con los PCs o los Smartphone que usan un sistema común o global. En estos casos usan un sistema como como suele ser Windows, Android, Linux,.. que son más sencillos de mantener y aplicar actualizaciones de seguridad debido a que el propio proveedor software es que los mantiene. Pero por el contrario los sistemas del internet de las cosas es el propio

En bastantes casos, el problema no está relacionado con las capacidades del dispositivo si no en las configuraciones por defecto de dichos dispositivos. Por lo general, los dispositivos del internet de las cosas no establecen unos métodos de entrada y salida de datos compatibles con los de los ordenadores personales y en la mayoría de casos tienen que facilitar el acceso a través de sus interfaces de administración mediante medios más complejos y menos familiares para el usuario normal. Con este problema surge el concepto de Security by Default (seguridad por defecto) lo que se interpreta en la necesidad de implantar una configuración por defecto lo más segura posible para un dispositivo desde su fabricación. Aunque en la mayoría de casos no es así. Este hecho se produce porque los fabricantes de dichos dispositivos establecen de fábrica una configuración de seguridad entre media y baja, que no requiere de grandes conocimientos por parte del usuario para configurar dicho dispositivo para su uso. Gracias a esto se intenta conseguir una buena impresión para el usuario y dar una buena imagen de marca y producto, debido a que los usuarios casi sin configurar ninguna opción ya disponen del dispositivo para su uso. Esto conlleva que los usuarios medios que usan este dispositivo, no tengan grandes conocimientos de las posibilidades de configuración de seguridad de sus dispositivos y en la mayoría de los casos la configuración de tal elemento sea la de fábrica que puede ser potencialmente insegura.

Otro de los principales problemas de seguridad es la ubicación física de estos dispositivos, la gran variedad de dispositivos como televisores, wearebles, sistemas domóticos,… hacen que sea muy complicado de proteger, ya que permite un acceso sencillo físico a ellos. Lo que hace que se produzcan riesgos bastantes graves de seguridad.

Los dispositivos del internet de las cosas además de los peligros de seguridad habituales sobre la disponibilidad, confidencialidad e integridad de la información también añaden riesgos a la seguridad y salud de las personas debido a que la mayoría de los dispositivos constan de actuadores o componentes que realizan cambios en el mundo real, de ahí la importancia de la seguridad en dichos dispositivos.

En los siguientes apartados veremos las deficiencias de seguridad de diferentes tipos, analizando cada una de ellas [15].

5.1 Deficiencias de seguridad en la transmisión de datos

En esta sección vamos a ver las deficiencias que se pueden dar en un ataque en la transmisión de datos, debido a que los dispositivos del internet de las cosas están orientados al envío de información entre los distintos dispositivos o directamente a internet. Lo fundamental para estos casos es la protección de la información en el tránsito de la misma.

Ilustración 13 Comunicación entre diferentes dispositivos

Es normal la importancia que tiene la seguridad en las comunicaciones para estos dispositivos. En la mayoría de dispositivos del internet de las cosas se forman sistemas distribuidos que requieren de gran cantidad de canales de comunicación de

distintos tipos como puede ser inalámbrica, cablead o cualquier otro medio de transmisión. Todas estas comunicaciones, prestando especial atención a las que usan medios inalámbricos o redes públicas son propensas a sufrir ataques a la confidencialidad en las comunicaciones.

Cuando no se asegura un nivel idóneo de seguridad en la identificación, privacidad e integridad en las comunicaciones de los dispositivos del internet de las cosas, es posible que estas deficiencias puedan ser aprovechadas por un atacante remoto para comprometer la información transmitida. Esta información puede incorporar datos de carácter personal o privados, o datos sensibles que puedan ser usados para pertrechar algún ataque mayor.

Si no se asegura el canal de comunicación con un cifrado de datos, puede resultar relativamente fácil para cualquier atacante realizar ataques del tipo Man in The Middle (intermediario en español). Este ataque consiste en que el atacante captura la información, la lee, la procesa y la modifica y la envía al dispositivo destinatario haciéndose pasar por el dispositivo emisor, de este modo está en un punto intermedio en la comunicación, sin hacerse notar ni para el emisor ni para el receptor. De este modo el atacante puede obtener toda la información que desee y si lo desea modificarla para conseguir sus fines tanto en el emisor como en el receptor.

Una situación para ejemplificar esta situación de falta de seguridad podría ser en el sistema de domótica de una vivienda nueva, una vivienda en lo que todo estuviese automatizado por un sistema en la nube mantenida por el fabricante, en la cual podemos controlar las persianas, la iluminación, las puertas, el agua,…. Imaginemos que existe este problema de seguridad comentado en este apartado y las transmisiones de datos no son seguras entre la vivienda e internet, un atacante podría interceptar las comunicaciones y ver la información enviada y mandarla al servidor o podría modificarla y enviarla. Esto supone que el atacante podría saber en todo momento cuando hay gente en el domicilio, saber que puertas o ventanas están abiertas o cerradas, es decir, saber el estado por completo de la casa, eso solamente interceptando la información. En el caso de que también la modifique la información podría ser capaz de dar las mismas instrucciones que el propio usuario, con lo cual podría hacer lo que quisiera, desde apagar o encender las luces, cortar el

agua,… incluso hasta abrir y cerrar las puertas o ventanas a su antojo con todos los riesgos que eso conlleva.

5.2 Deficiencias de seguridad provocadas por el software

Uno de los ataques más usuales tanto en el internet de las cosas como en el ámbito general es el aprovechar las vulnerabilidades del software. Lo primero que tenemos que considerar es el sistema operativo en sí. Muchos de los dispositivos del internet de la cosas usan versiones adaptadas de sistemas operativos comunes (Windows, Linux, Android,..) de forma que se disminuyen los costes de fabricación. Esto conlleva un riesgo de seguridad, debido a que cuando se detectan vulnerabilidades en los sistemas operativos comunes son aprovechables en todos los dispositivos en los que son instalados, posibilitando a los potenciales atacantes una puerta de entrada a una inmensidad de dispositivos.

Ilustración 14 Diferentes sistemas operativos

Otra línea de ataque incluso más común que la anterior son las interfaces web, que son muy frecuentes de usar en dispositivos del internet de las cosas, debido a que estos dispositivos por regla general son de tamaño reducido y no disponen de pantalla, teclado o dispositivos apuntadores, lo que hace que se acabe permitiendo su administración desde otro dispositivo. Es bastante común que estas interfaces web se publiquen directamente a internet para facilitar a los usuarios la administración del dispositivo desde la red. Al igual que pasaba con los sistemas operativos, con las interfaces web al detectarles alguna vulnerabilidad de seguridad afectará a todos los dispositivos que la tengan implementada, por lo que afecta a multitud de dispositivos.

Otra propiedad común a multitud de dispositivos del internet de las cosas es el uso de servicios en la nube. Al igual que en los casos anteriores si existen deficiencias en la gestión o actualización de estas plataformas se puede crear un riesgo para la seguridad que permita acceder a la información almacenada en la nube y dependiendo de los servicios que implementen incluso se tomar el control del dispositivo. Pudiendo afectar a todos los dispositivos conectados a la nube.

Algunos dispositivos del internet de las cosas como son los smartphones, smartv, smartwatch,.. se pueden descargar e instalar aplicaciones de terceros en los propios dispositivos que aumentan su funcionalidad. En estos casos existe riesgo en la seguridad porque se puede usar esas aplicaciones como puerta de entrada a los dispositivos y tomar el control de ellos y obtener la información. Estos ataque se pueden ejecutar de dos formas, una seria explotando la vulnerabilidad identificada del software y la otra descargando aplicaciones maliciosas que permitan obtener toda la información del dispositivo e incluso poder controlarlo.

Para finalizar este apartado, está muy extendido el uso de aplicaciones móviles que se instalan en nuestros Smartphone para controlar la gestión de algún dispositivo. Estas aplicaciones móviles pueden ser usadas para realizar ataques, ya sea mediante las vulnerabilidades o deficiencias de la implementación de las propias aplicaciones o mediante aplicaciones maliciosas que asemejen la conducta y la apariencia de las aplicaciones originales para conseguir el acceso a los dispositivos del internet de las cosas.

Para ejemplificar estas vulnerabilidades, imaginemos que tenemos un sistema de vigilancia en nuestro domicilio compuesto de varias cámaras que manejamos desde múltiples dispositivos digitales (smartphones, tablets,..). Tienen la funcionalidad de ver a tiempo real que está sucediendo, de apagar y encender las cámaras e incluso dirigirlas donde queramos. En estos casos en nuestros dispositivos tenemos instalada una aplicación para poder controlarlas o incluso contamos con un servicio en la nube para poder usarlas. Cualquier vulnerabilidad en el software de los dispositivos, como la aplicación, como el servicio en la nube puede comprometer la información e incluso permitir a algún atacante utilizarlas a su gusto. Esto podría permitir al atacante ver los que se está viendo en las cámaras a tiempo real, apagar y encenderlas, moverlas a puntos concretos,...

5.3 Deficiencias de seguridad provocadas por la funcionalidad y la configuración

Otro asunto a tener en cuenta en la seguridad de cualquier sistema es su propia funcionalidad. En muchas ocasiones, la configuración por defecto o los propios usuarios no conservan un criterio acorde con la seguridad con la que se implementó o la configuración de la funcionalidad del servicio. En el internet de las cosas ocurre este problema debido a que la mayor parte de los dispositivos no tiene una adecuada política de seguridad de fábrica.

En la mayoría de ocasiones los dispositivos del internet de las cosas tiene de fábrica habilitados muchas más funcionalidades por defecto que las que normalmente el usuario usa. Esto es debido a que los fabricantes configuran los dispositivos de esta manera para que los usuarios sin tener que tener grandes conocimientos sobre el dispositivo y sus configuraciones puedan usarlo al momento, dando a la empresa mejor imagen de marca y de producto. Como resultado los dispositivos tienen funcionalidades activas que pueden suponer agujeros de seguridad en la actualidad o en el futuro si no se actualiza o se gestionan adecuadamente.

Para ejemplificar esta deficiencia de seguridad vamos a hablar de los router que tenemos en las viviendas para conectarnos a internet. Estos router vienen en muchas ocasiones configurados de fábrica con un cifrado, unos años atrás algunos proveedores de internet suministraban routers con un cifrado WEP, de los cuales se descubrió que se podía obtener la clave de acceso a la red con el nombre y codificación del SSID del punto de acceso wifi. En este caso la configuración de fábrica que traían estos routers provocaban una brecha de seguridad porque cualquier atacante podía acceder a nuestra red y dependiendo de la protección con la que contaran los servicios de los que dispongamos podían ser objetivos de ataques al poder ser posibles vulnerabilidades.

5.4 Deficiencias de seguridad del hardware

Otro punto bastante importante a tratar son las posibles vulnerabilidades en la implementación hardware. Por regla general son las vulnerabilidades menos frecuentes aunque si es cierto que cuando se produce una vulnerabilidad de este tipo suelen ser bastante peligrosas y bastante difíciles de solucionar.

Es cierto que estas vulnerabilidades ya existían antes de considerar el internet de las cosas y en muchas ocasiones no hace falta que el dispositivo esté conectado a internet. Sin embargo es un punto muy importante debido a que es una de las vías de entrada más habituales.

Muchos de los dispositivos para recopilar datos del internet de las cosas están dispersos en grandes áreas, esto hace bastante complicado aplicar controles de seguridad físicos. En estos casos es más simple el acceso físico a los dispositivos que en los sistemas herméticos que están en los centros para el procesamiento de datos.

Estos ataques se basan en comprender la estructura y realizar un análisis de comportamiento del dispositivo. Estos ataques se emplean cuando el software es seguro o en sistemas en los que no se tiene acceso mediante la red, bien sea porque están localizados en redes aisladas o bien protegidas del acceso público.

Hay que recalcar que estos ataques para efectuarlos se necesitan o requiere del uso de equipamiento especial. Dependiendo del equipamiento con el que cuente el atacante se puede realizar diferentes tipos de ataques, como pueden ser monitorizar la interfaz del dispositivo, hasta ingeniería inversa o la manipulación de componentes internos del dispositivo

Dependiendo de la importancia de los dispositivos y de los datos que manejen se aplicaran mayor o menor medidas de seguridad en estos dispositivos. En tipos de dispositivos wearable que solo gestionen algunas notificaciones del Smartphone con el que estén asociados no tendrá tantas medidas de seguridad como por ejemplo un sistema industrial que gestione los datos de una fábrica.

Uno de los ataques más comunes en estos casos suele ser el acceso directo a los componentes de almacenamiento, tanto volátil (memoria) como la no volátil (disco duro). Según sea el dispositivo puede ser más o menos complejo el acceso a la memoria y de ahí poder extraer los datos, otro tema ya es que esos datos estén bien protegidos y no sea fácil acceder a la información almacenada.

Como hemos visto se puede acceder a la memoria volátil y no volátil, en el caso de la memoria volátil supone un gran riesgo que puedan acceder a ella, debido a que se

puede acceder fácilmente a ella en caliente y obtener las claves criptográficas, credenciales o cualquier información almacenada en ella.

Por otra parte la memoria no volátil es algo más compleja en este sentido, si es cierto que se puede desmontar el dispositivo para acceder a él y extraer la información que contengan pero puede haber medidas de seguridad para que esto no sucede. Una solución sería poner una protección física para evitar que se pueda manipular este dispositivo o que una vez se acceda a él se destruya su soporte en el caso de que lo manipulen o bien la otra opción es que los datos que contengan estén cifrados para que no tenga acceso cualquier atacante.

Uno de los grandes problemas de estos dispositivos es que borrado de la información. En la mayoría de ocasiones cuando el usuario piensa que ya se ha borrado la información nos encontramos con que no ha sido así y eso es debido a las características de estos dispositivos y las estructuras de archivos que usan. Normalmente para borrar archivos se modifican las tablas de asignación de archivos, cambiando de ocupada a disponible, es decir, no se borra la información que contenía ese espacio de archivos sino que se marca como disponible para poder guardar otra información en su lugar. Además aunque se haya sobrescrito en el espacio liberado hay herramientas que pueden reconstruir la información que ahí se almacenaba sino se ha borrado esa información un número determinado de veces. Hay políticas de seguridad que según el grado de importancia de los datos, estipula que se deben sobrescribir los datos entre 7 y 32 veces para casos donde los datos sean sensibles.

Un ejemplo de esto es cuando se quiere vender o reutilizar algún dispositivo como por ejemplo un Smartphone, una eliminación de datos que no sea segura 100% puede facilitar que el nuevo propietario del dispositivo pueda acceder a los datos del antiguo

Para ejemplificar esta situación vamos fijarnos en los sistemas de control y asistencia del tráfico. En las carreteras hay montones de panel informativos, paneles para el uso de carriles, de túneles, redes de semáforos,…. Todos ellos están distribuidos por todas las carreteras por lo que tienen un alto rango de distribución, por lo que cuentan con subestaciones para controlarlas que son fácilmente accesibles físicamente (la mayoría solamente están protegidas por cajetines que

pueden ser forzados). El atacante podría acceder a dichas subestaciones y aprovechar las vulnerabilidades del hardware, de este modo podría controlar lo que se muestra en los paneles de información, gestionar a su antojo la red de semáforos,… con el peligro que conlleva eso.

5.5 Deficiencias de seguridad provocadas por los propios usuarios

Para finalizar con este tema, vamos a hablar de los ataques que se pueden sufrir por el propio usuario y su experiencia. En muchas ocasiones, a pesar de que los dispositivos del internet de las cosas sean seguros, un mal uso o negligencia por parte del usuario puede llegar a complicar el servicio.

Sobre este tema se ha hablado en multitud de ocasiones pero es uno de los principales problemas que los atacantes aprovechan para conseguir el acceso al sistema y esto esta propiciado porque todos estos dispositivos en mayor o menor medida esta para ser usados por personas.

Estos ataques vienen provocados en la mayor parte porque los atacantes aprovechan el desconocimiento o la ignorancia para conseguir la información necesaria para lograr sus propios objetivos. Esto es lo denominado Ingeniería Social, basada en la manipulación psicológica de los usuarios, utilizándolos para acceder a los sistemas mediante estafas o engaños.

La mayoría de sistemas o servicios en la red para proteger sus datos usan un sistema de autentificación, normalmente basado en usuario y contraseña, este es el principal objetivo de los atacantes, obtener el usuario y contraseña para poder acceder, normalmente lo hacen mediante estafas como puede ser los casos de phishing, que consiste en un envío masivo de correos centrados en obtener los credenciales de acceso a servicios de los clientes o acceso a la banca online, por ejemplo. También se puede realizar ataques más elaborados en los cuales el atacante puede realizar una investigación del usuario en internet, consultando su actividad en la red, así como sus perfiles sociales,…, cuanto más descuidado sea el usuario en cuestión o inconsciente al publicar o suministrar su información en la red, más sencillo resultara para los atacantes realizar sus ataques y con ello mayor posibilidad de éxito

Para ilustrar esta situación vamos a poner como ejemplo un sistema de banca online, en la cual se puede acceder desde multitud de dispositivos y en la cual se puede acceder con el DNI del titular y una clave. Los atacantes podrían ponerse en contacto con el cliente haciéndose pasar por un responsable de dicho banco en los cuales están haciendo unas labores de mantenimiento o de verificación de identidades. Mediante este engaño los atacantes podrían obtener las claves de acceso a la banca online del cliente. De confirmarse el ataque el cliente correría el riesgo de poder perder su dinero o gran parte de él. El atacante podría tener acceso a la banco haciéndose pasar por el propio cliente y podría comprobar todos los movimientos, saldo actual y realizar transacciones. De ahí la importancia de que los propios usuarios verifiquen la identidad de las personas que contactan con ellos y tengan conocimiento de los riesgos que pueden correr.

Estos ataques de Ingeniería Social pueden ser desde simples ataques hasta ataques muchos más complejos. Normalmente, se elaboran ataques bastantes complejos si el beneficio que pueden obtener los atacantes es mayor por lo que por regla general estos ataques son destinados a empresas o administraciones públicas.

6. Prevención

Una vez visto todos los problemas de seguridad que se pueden dar en el internet de las cosas vamos a ver también de manera detallada las prevenciones. Lo que vamos a ver ahora es dentro de nuestras posibilidades, tener un uso lo más seguro posible. Para minimizar al máximo posible los riesgos de seguridad y privacidad de estos dispositivos se pueden aplicar una serie de medidas.

Como hemos visto las deficiencias de seguridad vamos a ver los controles y recomendaciones para evitar o minimizar los riesgos de seguridad [16]

6.1 Control de interfaces de acceso

Los dispositivos del internet de las cosas incluyen funciones de red para su gestión, control o transmisión de datos, pero por regla general no disponen de interfaces de usuario, como teclados o pantallas para poder administrarlas. En la mayoría de estos casos la solución suele ser la implementación de una interfaz web que permita el acceso al dispositivo para configurar los parámetros o funciones del dispositivo del internet de las cosas desde cualquier otro dispositivo remoto como puede ser un ordenador, smartphone, tablet,....

En todos los dispositivos de debe poder controlar el acceso al mismo, y con más importancia si su interfaz es pública en internet. En la mayoría de los casos las interfaces suelen carecer de autenticación o en el caso de que la tenga vienen configuradas con los parámetros por defecto, que el fabricante hace públicas.

En las interfaces que usan autenticación es imprescindible que se cambien lo antes posible las credenciales para acceder por defecto por unas creadas por nosotros mismo y con más seguridad. Con esto lo que conseguimos es que los atacantes tengan mayores dificultades a la hora de hacerse con el control de nuestros dispositivos.

Las contraseñas que pongan los usuarios deberían seguir unas directrices para complicar lo máximo posible a los atacantes, estas directrices son:

-Tener como mínimo una longitud de 7 caracteres

-Usar mayúsculas y minúsculas

-Usar números

-Usar algún símbolo especial

Si la interfaz de nuestro dispositivo no usa autenticación y no hay manera de habilitarla, no deberíamos acceder a través de la red sin que se aplique ninguna medida de control adicional.

Otro aspecto importante en el uso de este tipo de interfaces es el cifrado... Las interfaces web implementa un cifrado cuando se usa el protocolo HTTPS (este protocolo se usa cuando en la barra de direcciones de nuestro navegador antes de la ruta pone https:// o con un candado en la conexión). En los casos en los que veamos que no se emplea ningún tipo de cifrado se desaconseja hacer pública la interfaz de administración o conexión directamente a internet. Como ejemplo de esto, imaginemos que en nuestro router domestico no tiene contraseña y dejamos la red abierta. Al no ir cifrada la conexión cualquier persona podría conectarse a ella y podría capturar nuestras claves de autenticación para el servicio al cual nos queremos conectar debido a que los datos no van cifrados.

Si fuese necesario el acceso al dispositivo desde fuera de la seguridad de la conexión de nuestra vivienda, la mejor recomendación es la implementación de un acceso alternativo al mismo, como puede ser el uso de un servicio de VPN (Virtual Prívate Network), con esto tendríamos acceso a nuestra red local y tendríamos un acceso con total seguridad, debido a que usa un cifrado de datos y autenticación en la comunicación.

De esta manera podemos evitar o minimizar los riesgos de la transmisión de datos entre los dispositivos mediante una contraseña y de software evitando estos programas o páginas que no son seguros o actúan en ambientes seguros.

6.2 Actualización del dispositivo

En la mayoría de ocasiones, a parte de la configuración que los propios usuarios puedan hacer de sus dispositivos, la correspondiente implementación del dispositivo del internet de las cosas puede provocar diversas vulnerabilidades de seguridad que pueden comprometer la seguridad del dispositivo.

Para paliar este riesgo, lo recomendado seria que el dispositivo se mantuviese en la medida de lo posible actualizado con la última versión de software o firmware que suministre el fabricante. Para ello podemos configurar nuestro dispositivo, siempre que esta opción esté disponible, para que se actualice de manera automática siempre que el fabricante ponga a nuestra disposición una nueva actualización, en el caso de no ser posible instalar que nos avise el dispositivo de que hay una nueva

actualización y que sea el propio usuario el que la instale. En el caso de que el dispositivo no cuenta con ninguna opción de poder actualizar el dispositivo automáticamente o al menos nos avise de si hay alguna actualización disponible, debe el ser el propio usuario el que debe encargarse de realizar periódicamente una serie de comprobaciones y ver si existe alguna actualización y actualizarlo.

Bien es cierto que existen algunos fabricantes que no permiten esta opción porque no disponen de actualizaciones con relativa frecuencia o incluso que no faciliten ninguna actualización a sus dispositivos. Por eso es importante que antes de adquirir algún dispositivo conozcamos la marca y que servicio de post-venta tienen, porque hay muchos fabricantes que no actualizan sus dispositivos o bien pasado relativamente poco tiempo dejan de actualizar sus dispositivos o que por el contrario si actualizan sus dispositivos pero con relativa tardanza, lo que supone que ya se ha detectado la vulnerabilidad y los atacantes ya se pueden haber aprovechado de estas antes de que actualicemos nuestros dispositivos.

La recomendación para estos casos que hemos comentado es adquirir productos de fabricantes internacionales que suelen dar un buen servicio de post-venta o asegurarnos de que el fabricante se preocupa por mantener sus dispositivos actualizados.

Si ya disponemos del dispositivo y no está actualizado, bien sea porque no se disponga de actualizaciones o bien porque la que tengamos sea de hace bastante tiempo y se hubiesen hallado nuevas vulnerabilidades, la recomendación es conectarlo a redes seguras y conocidas, como puede ser nuestra red doméstica con un buen cifrado o bien usar como se ha dicho anteriormente una conexión segura como una VPN.

De esta manera evitamos los riesgos derivados del software, bien sea con las actualizaciones que solucionan las vulnerabilidades o bien conectándolo en redes seguras para correr los mínimos riesgos.

6.3 Configuración segura de la red local

Lo primero que vamos a tratar en este punto no es específico o propio de los dispositivos del internet de las cosas, es útil para cualquier dispositivo conectado a internet. Se trata de la seguridad de nuestra red usando un cortafuegos, con esto podemos rechazar por defecto las conexiones entrantes provenientes de internet y sol permite conectar dispositivos que estén dentro de nuestra propia red.

Dependiendo de nuestras conexiones o necesidades podremos habilitar los accesos externos que nos sean necesarios, teniendo en cuenta el riesgo que pueda conllevar.

Los siguiente puntos que vamos a tratar sí que tienen están relacionados con el tema que estamos tratando en este proyecto, el internet de la cosas.

Por regla general, los fabricantes de dispositivos del internet de las cosas por defecto habilitan multitud de puertos de acceso o gestión, para las diferentes funcionalidades que dispongan sus dispositivos. Cuando los usuarios configuran sus dispositivos para tener acceso a internet, deben tener en cuenta que lo más aconsejable es controlar que solo se permita el acceso a los puertos que sean estrictamente necesarios para su funcionamiento o el uso que le vayan a dar al dispositivo, de esta manera disminuimos los riesgos que pueden sufrir. Es esencial que los usuarios tengan esto claro, la mayoría de veces estos dispositivos no disponen de ningún método para especificar los puertos que deben tenar acceso por lo que se facilita el acceso al dispositivo al completo, lo que permite el acceso remoto a todos los puertos del dispositivo. Por este motivo, dependiendo del router con el que contemos o sus características se recomienda tener una configuración adecuada como puede ser emplear reglas de NAT o de Port Forwarding (redirección de puertos). Dicha configuración es prácticamente soportada por la mayoría de routers que se encuentran hoy día en el mercado.

En los routers hay un método simplificado para conectarse a una red wifi que es el uso de Wifi Protected Setup (WPS). Este protocolo fue implementado en 2007 por la Wi-fi Alliance, lo que hace es facilitar a los usuarios una implementación sencilla de una red inalámbrica sencilla. El protocolo WPS no es un mecanismo de seguridad en sí, es un proceso asistente para implementar una red inalámbrica con WPA2, que sirve para minimizar la actuación de los usuarios en entornos domésticos o redes profesionales de pequeñas dimensiones. El problema viene cuando hace pocos años se ha averiguado que este protocolo tiene una vulnerabilidad y que puede permitir el acceso a la res por un atacante en unas pocas horas y para ello existen unas herramientas que lo realizan automáticamente. En gran cantidad de dispositivos este servicio viene activo por defecto y aunque no sepamos si nuestro router puede ser vulnerable o no, se recomienda desactivar este protocolo en los routers. Para poder desactivarlo lo que tenemos que hacer es acceder dentro de nuestro router y buscar la configuración de seguridad y desactivar la opción de WPS.

Últimamente se ha comenzado a emplear el protocolo UPnP (Universal Plug and Play) para facilitar a los usuarios la administración de su red local. Este protocolo se diseñó para facilitar a los usuarios la interconexión automática de dispositivos en la red. Lo más destacado de este protocolo es que automatiza la apertura de puertos a internet que los dispositivos conectados a la red local puedan necesitar. Si es cierto que es bastante cómodo para los usuarios no tener que preocuparse de que puertos necesitan sus dispositivos y tener que abrirlos manualmente, pero puede suponer un riesgo usar este protocolo. Por defecto, muchos dispositivos pueden solicitar la apertura de puertos de acceso remoto que no consideremos adecuados u oportunos o incluso que puedan supones un riesgo bastante grave para la seguridad. Para solucionar esto lo recomendado es deshabilitar en la medida de lo posible este protocolo dentro de las características de nuestro router.

En esta sección se pueden solucionar o minimizar los riesgos derivados de la transmisión de datos y de la funcionalidad o la configuración de los dispositivos.

6.4 Identificación y control del uso de servicios en la nube

Como se ha comentado ya, muchos dispositivos del internet de las cosas usan servicios en la nube o cloud services, por lo que nuestros datos pueden acabar allí.

Con estos servicios no es necesario abrir ningún puerto, solamente con un acceso a internet el dispositivo manda la información a internet. Muchos de los dispositivos del internet de las cosas están creados con esta finalidad, sin embargo, es esencial que tengamos constancia de las medidas de seguridad que aplica el propio dispositivo y el sitio en internet que recibe los datos que mandan los dispositivos, también es importante saber que política de privacidad se aplican a dichos datos.

También es bastante común que los dispositivos se gestionen externamente sirviéndose de un servicio web que el propio fabricante facilita. En estos casos el usuario debe acceder al servicio en la nube y este será el encargado de conectarse y de gestionar nuestro dispositivo, o también nos permitirá acceder a la información del mismo, como pueden ser los datos que el propio dispositivo capture. Para asegurar la seguridad el usuario debe seguir las normas para el uso de contraseñas a la hora de elegir una para conectarse a través de la nube y también se debe requerir que se use una conexión cifrada con el servicio mediante el protocolo HTTPS anteriormente comentado

En esta sección evitamos o minimizamos los riesgos provenientes de la transmisión de datos entre los dispositivos e internet.

6.5 Uso de aplicaciones móviles para dispositivos del internet de las cosas

Últimamente, los dispositivos del internet de las cosas se controlan mediante aplicaciones para los smartphones. Por regla general para los usuarios es más fácil y más común usar una app móvil para manejar sus dispositivos y además se facilita el acceso, es más práctico y nos permite monitorizar nuestro dispositivo. Para realizar esto debemos tener en cuenta los requerimientos de seguridad cuando usemos las aplicaciones de este tipo.

Con las aplicaciones móviles hay que tener en consideración, la procedencia de la app, es decir, hay que tener cuidado de donde descargamos las aplicaciones y hacerlo siempre desde un sitio de confianza. Si descargamos la app desde cualquier página o sitio no oficial corremos el riesgo de que esa aplicación pueda estar modificada e incluya funcionalidades maliciosas que pueden poner en riesgo la seguridad de nuestro dispositivo y comprometer la información personal o incluso el propio dispositivo en sí, dependiendo de la capacidad de disco software.

En el momento que instalamos una aplicación de este estilo, hay que tener en cuenta los permisos que nos solicita la propia aplicación para funcionar. Es lógico pensar que si instalamos una aplicación para controlar nuestra smarttv nos solicite permisos para acceder a nuestra red para poder conectarse a la smarttv pero no es normal que nos solicite permisos para acceder a nuestros contactos o mensajes. En estos casos lo que debemos hacer es denegar los permisos que nos pida para la información que no consideremos que sea estrictamente necesario y una vez hecho esto comprobar que verdaderamente la fuente de la que hemos obtenido la aplicación es fiable

De esta manera evitamos las posibles deficiencias software asegurándonos de que las apps sean fiables.

6.6 Buenas prácticas y cultura de seguridad

Todos estos sistemas están preparados y diseñados para interactuar o dar algún servicio a los usuarios. Esto provoca que no solo los sistemas sean objetivos de ataque sino que las personas también puedan serlo con el fin de acceder a un sistema informático.

Por regla general se suele asociar con el entorno del usuario la parte más débil de la seguridad, por lo que es un objetivo potencial de ataque y de los que más usados son en la actualidad.

Por ello, es necesario que los usuarios sean conscientes de que pueden ser atacados y que puedas reconocer las estafas o phishing, para que no sea fácil para los atacantes engañarlos. En general, se debería desconfiar de cualquier información que nos comuniquen desde una fuente que no conozcamos, y sea por el medio que sea (como puede ser por teléfono, email, en persona,...). Para evitar riesgos, lo primero que deberían hacer es solicitar algún tipo de identificación y constatar por otro medio por el cual ha sido contactado, la veracidad de la información.

Normalmente, un proveedor de un servicio no pedirá a los usuarios ningún tipo de credencial o autenticación de acceso y mucho menos lo harán por medios como pueden ser los correos web o formularios web que no están cifrados (como hemos comentado en un punto anterior ninguna página que no use HTTPS). Los proveedores o administradores de algún servicio cuentan con un listado de los usuarios y pueden gestionarlos. De modo que si recibimos alguna solicitud dudosa por parte de estos administradores o proveedores debemos desconfiar y validar todos los datos de la misma.

Para reducir al mínimo los daños que nos puede causar ser objeto de una estafa o engaño, se recomienda a los usuarios que dispongan de credenciales diferentes para cada uno de los servicios que disponga. Esta medida se recomienda porque si algún atacante se hace con dicha información es muy fácil buscar los servicios que usa el usuario y poder acceder a ellos y obtener toda la información que quiera. Otra recomendación para estos casos es siempre que los servicios los permitan es la autenticación por dos factores, de esta manera aunque los atacantes puedan autenticarse como el usuario, no podría conseguir nada más debido a que necesitarían pasar el segundo factor de autenticación, que puede ser por ejemplo un SMS al móvil como usan la mayoría de bancos para realizar algunas gestiones.

Aparte de la desconfianza y la verificación de la información es importante la formación y la concienciación de los usuarios para que los usuarios sean capaces de identificar las estafas y sepan cómo reaccionar adecuadamente ante ellas. El problema es que cada vez se usan técnicas más complejas y elaboradas para engañar a los usuarios y a veces es difícil identificarlas.

En esta última sección de este capítulo prevenimos los riesgos generados por los propios usuarios, haciendo que tengan mayor concienciación y conocimiento de estos dispositivos.

7. Ejemplos reales de amenazas de seguridad y privacidad

A continuación vamos a ver algunos ejemplos de ataques reales que han atentado contra la seguridad y privacidad del internet de las cosas, una vez visto el capítulo de seguridad y privacidad y viendo las deficiencias vamos a poner unos ejemplos de estos casos y viendo cómo puede afectar a los datos y las personas.

7.1 Google Glass y Samsung Galaxy Gear 2

Los expertos de seguridad de Kaspersky Lab [17] han analizado dos dispositivos wearables para ver sus las vulnerabilidades, estos dispositivos son las Google Glass y el reloj Samsung Galaxy Gear 2.

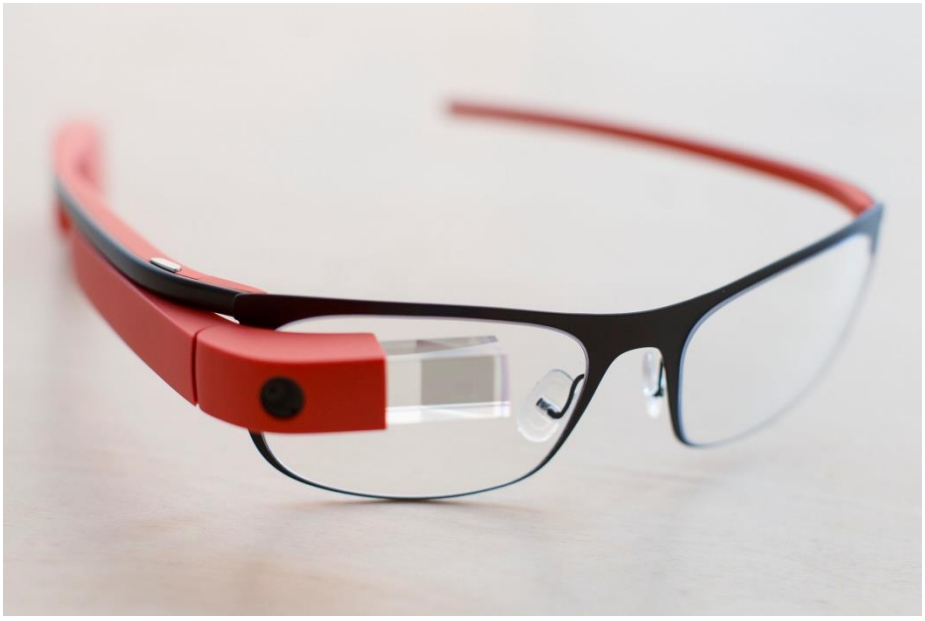

Ilustración 15 Google Glass

Los expertos de la empresa de seguridad Kaspersky Lab encargos de realizar estos análisis han sido los analistas Roberto Martínez y Juan Andrés Guerrero

Respecto al primer dispositivo, las Google Glass, los analistas nos comentan que hay dos formas de poder conectar las gafas a la red, un de ellas es mediante bluetooth con el dispositivo móvil con el que comparte su conexión o la otra que es directamente por wifi. Esta última opción es la que más libertad ofrece al usuario pero según nos indica Roberto Martínez, esta funcionalidad hace que las gafas estén expuestas a ataques vectoriales de red, especialmente del tipo Man in the Middle, debido a que la comunicación entre los dos sistemas puede ser interceptada.

En las pruebas que realizaron con este dispositivo vincularon éste a una red de seguimiento y control de los datos que transmite. Analizando los datos que recogieron mostraron que no todo el tráfico que se intercambia entre el dispositivo y el hotspot estaba cifrado. Con las pruebas que hicieron pudieron averiguar que el usuario había estado buscando hoteles, compañías aéreas y destinos turísticos, lo que provoca que se pueda vigilar al usuario de una forma sencilla. “En realidad no es una vulnerabilidad muy grave, pero aun así, a través de perfiles de metadatos de intercambio de tráfico web podría convertirse en el primer paso hacia un ataque más complejo contra el usuario del dispositivo”, afirma Roberto Martínez

Respecto al otro dispositivo el Galaxy Gear 2, este dispositivo está diseñado para que cuando se haga una foto emita un ruido fuerte para advertir de que se está haciendo una foto. Analizando el dispositivo, según Guerrero, el software de este dispositivo mostraba que tras el rooting y utilizando ODIN, una herramienta de software de Samsung, es posible habilitar el Galaxy Gear 2 para que cuando haga las fotos no se emitiera ningún ruido. Según nos indican los analistas esto abre una puerta a posibles escenarios en los que se podría violar la privacidad de las personas.

Aparte del tema de la cámara, algunas aplicaciones de este dispositivo se cargan en el dispositivo mediante la ayuda del Gear Manager, una aplicación encargada de trasmitir una app del Smartphone al smartwatch. Cuando la app se instala en el sistema operativo del smartwacth, éste no muestra ninguna notificación en la pantalla, lo que provoca que los ataques estén dirigidos a la instalación de aplicaciones sin que se me muestre nada en el reloj

Juan Andrés afirma que en este momento la empresa no tiene evidencias de que los wearables sean objetivo de ataques por parte de los creadores de amenazas APT “es probable que en el futuro se conviertan en objetivo si llegan a ser son adoptadas ampliamente por los consumidores. En el futuro los datos recogidos por estos dispositivos atraerán nuevos jugadores a la escena el ciberespionaje**”**

7.2 Correos SPAM

Otro caso es un investigador de la empresa Proofpoint [18], el cual deteco entre diciembre de 2013 y enero de 2014 el envío de una campaña de correo malicioso,

como se ve en su propio articulo empezaron a investigar para conocer desde que dispositivos se mandaban los correos de SPAM, para averiguar que tipo de dispositivos formaban las botnet. Cuando empezaron el analisis descubrieron que alrededor del 25% del correo malicioso no habia sido enviado desde un dispositivo convencional, como un pc u ordenadores portatiles, si no que eran dispositivos catalogados dentro del internet de las cosas. Entre los dispositivos que mandaron los correos se pueden encontrar desde routers domésticos, smartTV e incluso alguna nevera. En la realización de este analisis se determino que gran parte de los dispositivos compartian software común , como por ejemplo el uso de sistema empotrados basados en Linux o servidores web ligeros basados en Apache. Esto evidencia las deficiencias en la gestión de segutidad de esto dispositivos.

7.3 SmartWatch Pebble

Otro ejemplo se produjo en agosto de 2014 en el que se dio a conocer una vulnerabilidad en un dispositivo wearable que tiene un uso muy difundido, el reloj Pebble. Es un smartwatch que se puede enlazar con el smartphone, y este muestra las notificacion recibidas por su pantalla. La vulnerabilidad era capaz de provocar la denegación del servicio y en algunos casos era capaz de borrar la memoria del dispositivo. Para llevarlo a cabo solamente era necesario enviar 1500 mensajes de whatsapp al dispositivo en un periodo de 5 segundos [19].

7.4 Viking Jump

Esta app llamada Viking Jump [20] se trata en una app disponible en Play Store, se trata de un juego el cual cuenta con un número elevado de descargas (más de 100.000 descargas hasta la fecha de su retirada)que está infectado con el el malware “Viking Horde”. Este malware está atacando a los dispositivos Android a través de varias app, una de ellas es la ya comentada Viking Jump. El equipo de investigación de Check Point notificó a google el 5 de mayo de 2016 de la existencia de este malware en esta app y a día de hoy ya no está disponible esta app en play store.

Este malware consiste en que una vez instalada la app en el dispositivo se une a una botnet que es una red de dispositivos que son controlados por el atacante, sin que el usuario que tiene el malware instalado sea consciente de ello. Los dispositivos infectados o bots son usados por el atacante para sus propios fines,

como puede ser para hacer clics en publicidad para que el atacante reciba los ingresos o para realizar ataques DDoS para inutilizar sitios web.

Este malware afecta tanto a dispositivos con root como sin él, pero en el caso de los dispositivos root aparte de instalar el malware también se instala un código que el atacante puede ejecutar remotamente, de esta manera se puede ver afectada la información que el dispositivo tiene almacenada. En los dispositivos root además este malware aprovechando los privilegios con los que cuenta hace bastante difícil eliminarlo.

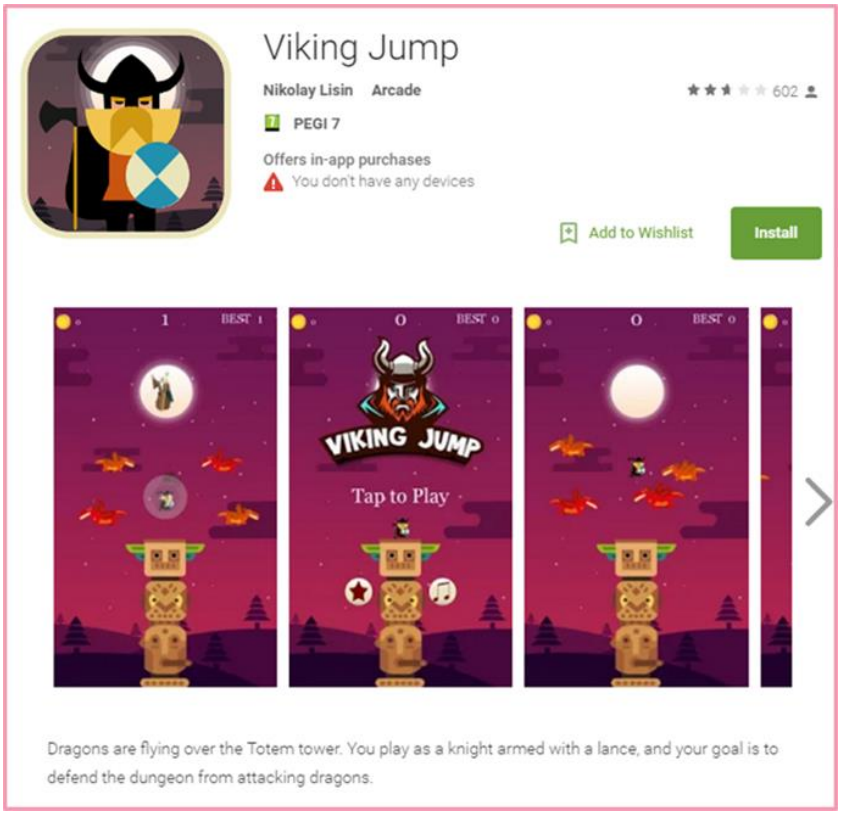

Ilustración 16 Google Play Viking Jump

7.5 Interrupción de una operación

En un hospital de Estados Unidos hubo un problema mientras se realizaba una operación de cateterismo [21] , es decir, una operación de corazón. El problema vino cuando los equipos que se usan para estas operaciones que están automatizados y permite ver imágenes a tiempo real de la operación y hacer un seguimiento en este caso de la operación de cateterismo cardiaco se la señal con el monitor.

Este incidente se produjo por una mala o inapropiada configuración de los equipos, en concreto del antivirus del que este equipo disponía, estaba programado que se realizase un análisis del equipo cada hora, sabiendo que estas operaciones son largas y que son de gran importancia debido al órgano que están interviniendo. Lo que provoco esta mala configuración fue que se perdió la señal con el monitor y el dispositivo reiniciándose, el equipo médico que estaba realizando la operación tuvo que detener si intervención durando 5 minutos en los cuales en este caso no sucedió

nada grave pero podría haber puesto en juego la vida del paciente si hubiese surgido cualquier imprevisto. Finalmente la operación se reanudo cuando el dispositivo se inició de nuevo y se completó la intervención con éxito.

Este incidente se produjo en febrero de 2016 y puso de manifiesto que hay que comprobar la configuración de los equipos para que se adecue al uso que queremos darle.

7.6 Chrysler

Algunos modelos de la marca Chrysler como son los Jeep Cherokees, Chrysler 200s y el Dogde Rams se ha descubierto que pueden ser hackeados y los atacantes pueden hacerse con el control remoto de dichos vehículos. Esta vulnerabilidad viene a través del servicio Uconnect del que disponen [22].

Ilustración 17 Jeep Gran Cherokee

La seguridad de estos coches se vio comprometida por una vulnerabilidad del tipo zero day que fue descubierta por un grupo de investigadores y que vieron que podían hacerse con el control total del vehículo a través de internet.

Este grupo de investigadores invitaron al redactor de un medio de comunicación del sector para que probaran el vehículo en la autovía. En la prueba el redactor pudo comprobar que el aire acondicionado y los parabrisas se activaban sin que él los hubiese tocado. Después de controlar eso sistemas que no repercuten en la seguridad procedieron a cortar la transmisión y emitir sonidos por el sistema de altavoces que provocaron un gran susto en el redactor. En otra prueba que realizaron cortaron también el sistema de frenos y acabo con el coche en la cuneta.

Con esto vemos la importancia de la seguridad en estos dispositivos en este caso en los coches debido a que se pueden producir accidentes y poner en riesgo la vida de las personas. Chrysler ya soluciono esta vulnerabilidad con un parche e informando a sus usuarios de la importancia de actualizar el sistema de sus coches para evitar cualquier tipo de ataque.

7.7 Ransomware en los hospitales

A principios de 2016 se ha descubierto un ataque mediante el malware ransomware a varios hospitales, uno en Los Ángeles, dos en Alemania y recientemente otro en Wichita. Según los expertos de Kaspersky Lab [23] estos ataques no son una sorpresa, con el internet de las cosas en auge, en el campo de la medicina han aumentado los dispositivos médicos que son básicamente ordenadores que usan un sistema operativo y que por regla general están conectados a internet, redes externas o servicios en la nube todo ello para tratar de mejor manera a los pacientes.

Con malware de este tipo los atacantes son capaces de acceder a los datos de los dispositivos y hacerse con el control de ellos, pudiendo restringirlos, modificarlos o incluso borrarlos. En los ataques que se han registrado se limitó el acceso al dosificador de un paciente y en algunos se restringe los datos hasta que el hospital pague un rescate. El FBI emitió un comunicado informando que lo mejor era no pagar nada porque no se asegura que devuelvan el acceso y los datos pero en algunos hospitales como el de Wichita hicieron el primer pago pero no tuvieron el acceso a todos sus servicios hasta que no hicieran un segundo pago. No se tienen más datos de este último ataque porque todavía está bajo investigación pero como vemos la seguridad de estos dispositivos debe ser prioritaria debido a que se pone n juego la vida de los pacientes que estén en los hospitales [24].

7.8 AceDeceiver, malware en IOS

Son muchos los tipos de malware que afectan a los dispositivos Android pero el sistema IOS tampoco se libra de estos ataques. Con este malware llamado AceDeceiver los dispositivos que tengan el sistema IOS y no se les ha hecho jailbreak también se ven afectados [25].

El equipo de investigadores de Palo Alto Networks descubrieron este malware y vieron que se instala de forma que el usuario no es consciente de este software en su dispositivo y realiza un ataque del tipo man in the middle, este malware aprovecha un fallo de diseño en el sistema Apple llamado FairPlay. Este malware hace un ataque man in the middle entre el usuario de iTunes y el App Store de Apple.

Según indica el equipo de investigación de Palo Alto Networks el atacante primero tiene que adquirir una app de la App Store para interceptar el código de autorización. De esta manera el atacante simula en el comportamiento de cliente de iTunes y asi puede acceder al software del usuario.

Por el momento solamente se han detectado casos de este tipo solamente en China pero según avisa estos ataques se puede dar en cualquier parte del mundo.

7.9 SmartTv

Los investigadores de Kaspersky ya han dado con uno de los primeros malware en las SmartTv Con las nuevas televisiones SmartTv podemos conectarnos a internet y disponer de multitud de apps directamente en nuestro televisor [26].

Ilustración 18 SmartTv

Se ha detectado un tipo de malware que afecta a estos dispositivos, este malware lo que hace es bloquear el acceso al navegador y aparece una ventana emergente indicando que se contacte con el servicio técnico y aparece un número de contacto. Este malware está basado en JavaScript que unen malware del tipo ransonware que bloquea el sistema y otro de tipo scareware que proporciona un servicio técnico falso.

El código fuente de este malware según los investigadores de Kaspersky Lab parece redirigir a una serie de dominios para acceder a otros malware, según informa los investigadores este malware parece creado por profesionales con experiencia en estos ámbitos. Aunque según el estudio de este malware parece que aún se encuentra inacabado y puede tratarse de un prototipo.

8. Wearables

En este apartado vamos a centrarnos en uno de los dispositivos del internet de las cosas, los wearables. Ya hemos analizado en general la seguridad y privacidad de los dispositivos del internet de las cosas y ahora vamos a poner el caso en concreto de uno de ellos.

Weareable hace alusión al conjunto de dispositivos electrónicos que el propio usuario lleva consigo mismo en alguna parte del cuerpo y que interactúan constantemente con el usuario y con otros dispositivos para conseguir el fin por el cual fueron creados. Algunos ejemplos como los relojes inteligentes o smartwatch, zapatillas de deporte con gps incorporado, pulseras que monitorizan nuestro estado de salud, botones con bluetooth que abrochas en tu ropa y controlar la exposición a los rayos UV nocivos (Ilustración 2), e infinidad de dispositivos que hoy en día va en aumento.

Ilustración 19 Botón bluetooth

La palabra wearable tiene la raíz inglesa que significa “llevable” o “vestible”, en este ámbito tecnológico hace alusión a “ordenadores corporales” o dispositivo informático o sensor digital que se lleva puesto el propio usuario de esta manera es un elemento que se incorpora e interactúa constantemente con el usuario debido a que lo lleva en todo momento consigo mismo [27]

Como hemos dicho los wearables son todos los dispositivos que incorporan un microprocesador y que se utiliza diariamente formando parte de nuestras vidas, dentro de esta definición no entra en esta categoría las smarttv, ebooks,… que aunque contenga un microprocesador y los usemos prácticamente a diario no son dispositivos que podamos decir que son “llevables” o “vestibles” como pueden ser las pulseras, relojes,…que son usados como dispositivos wearable.

Muchas grandes empresas están apostando por estos dispositivos, empresas como Intel, Adidas, Nike, Sony entre otras cada vez más están incorporando estos dispositivos y cada vez están más a la orden del día y mucha gente dispone de dichos dispositivos.

Todos estos dispositivos como son las pulseras, relojes, camisetas, gafas,… son capaces de recoger y transmitir datos, interactuar con otros dispositivos y facilitar algunas tareas a los usuarios. Todos estos dispositivos nos acompañan en todo momento, lo que representan el punto de unión de los datos y las personas, esto hace que se generen grandes cantidades de información de identificación personal. Los wearables captan, procesan y transmiten datos sobre el usuario, como puede ser tu ubicación, actividad, movimientos, estado de salud,…. Incluso estos dispositivos son utilizados en medicina, dispositivos que se pueden adquirir sin receta hasta aparatos que si la requieren. Además se prevé un gran crecimiento de estos estos dispositivos en los próximos años. Por lo tanto, hay que ver cuáles son los riesgos de seguridad de estos dispositivos para poder evitar ataques que puedan poner en peligro datos sensibles sobre el propio usuario.

8.1 Riesgos de seguridad

El mayor riesgo de seguridad tanto para los propios usuarios de estos estos dispositivos como para las empresas que los suministran, es la exposición no autorizada de datos sensibles, de información de identificación personal. Como ejemplo de esto vamos a hablar de la empresa VTech [28].

Esta empresa vende dispositivos infantiles, los primeros dispositivos eran herramientas para el aprendizaje con aspectos similares a los equipos portátiles, pero con el tiempo la empresa creó un portal online para ayudar a las familias a sacar el mayor provecho de sus compras. En este portal tenían que registrar sus datos y los datos de los niños que usarían lo dispositivos. Cuando empezaron a añadir conexión a los dispositivos, gracias a este portal se podían descargar actualizaciones, intercambiar mensajes,….La empresa fue una de las primeras en meterse en el sector de los wearables y creo un smartwatch para niños. El problema vino cuando un investigador analizo los dispositivos y publicó que los sistemas de VTech utilizados para captar y almacenar los datos de los cliente no eran seguros, lo

que quiere decir que una gran cantidad de datos sensibles de los padres y de los hijos que estaban registrados habían sido expuestos durante bastante tiempo a personas no autorizadas. Lo que provoco una gran pérdida de valor en las acciones de la empresa.

Esto provoco que varios investigadores analizaran los dispositivos de VTech y que descubrieran varias vulnerabilidades entre las que se hallaban el cifrado débil en una aplicación móvil de VTech y que se encontrara un chip vulnerable en algunos dispositivos de esta empresa.

Este gran riesgo de seguridad hay que tenerlo en cuenta desde el momento que se empieza a desarrollar un dispositivo hasta el seguimiento de la información de los usuarios finales con dicho dispositivo. Todo ello requiere un gran esfuerzo y una inversión que si no se realiza puede poner en riesgo todo desde el primer momento en la seguridad de los datos.

El riesgo es que algún atacante que se dedique sacar provecho personal pueda tener acceso a los datos personales de los usuarios y pueda vender esa información, pedir un pago a modo de rescate de dicha información,…. Toda esta industria del crimen de datos crece conforme crece o aumenta la información personal que se maneja. Y en este caso los wearables son dispositivos que son una gran fuente de información personal. Estos atacante pueden atacar directamente estos dispositivos (endpoints) o directamente los servidores que almacenan dicha información. Los wearable son endpoints que suministran información a los servidores para poder ofrecer todos los servicios que ofrecen. Lo que hace que los atacantes vean estos dispositivos como una fuente de ganancias si pueden sacar provecho de la información. Como mostramos en la siguiente imagen cualquiera de estos puntos puede ser un vector de ataque.

Ilustración 20 Vectores de ataque de los wearables

Otro motivo para tener en cuenta la seguridad de los datos que manejan estos dispositivos son las agencias del estado que se encargan de la protección del consumidor como en España puede ser la AGPD, la Agencia Española de Protección de Datos, o por ejemplo en EEUU es la FTC, Comision Federal de Comercio. Estas agencias son las encargadas de velar por la privacidad de los datos del consumidor. Estas agencias recomiendan una serie de prácticas y de normas tanto a las empresas como a los usuarios para velar al máximo por la privacidad y la seguridad de la información que manejan.

Por ejemplo la FTC ya ha actuado para resolver un casos de este ámbito que estamos tratando del internet de las cosas y fue para resolver los cargos contra unas cámaras de seguridad SecurView en de empresa TRENDnet. Por lo que este tipo de agencias se están preparando para estos nuevos ámbitos que antes no existían. De hecho la FTC ha publicado un documento titulado “Careful Connections: Building Security in the Internet of Things” (Conexiones seguras: Como crear seguridad en el internet de las cosas), del cual sus principales puntos son los siguientes

- Empieza por lo fundamental.
- Aprovecha las conclusiones a las que llegaron los expertos en materia de seguridad.
- Diseña tu producto teniendo siempre en cuenta la autenticación.
- Protege las interfaces entre tu producto y los demás dispositivos o servicios.
- Considera cómo limitar los permisos de acceso.
- Aprovecha las herramientas de seguridad que ya están disponibles.
- Evalúa las medidas de seguridad antes de lanzar el producto.
- Establece la configuración segura como opción predeterminada.
- Utiliza las comunicaciones iniciales con tus clientes para educarlos sobre la forma más segura de usar el producto.
- Establece un enfoque eficaz para actualizar tus procedimientos de seguridad.
- Mantente siempre atento.
- Innova en la forma de comunicarte.
- Hazles saber a tus clientes potenciales las medidas que estás tomando para proteger la información del consumidor.

Para algunos investigadores el punto débil de la seguridad de los wearables no es tanto el dispositivo en sí, sino más bien en su conectividad. Algunos investigadores aseguran que la vulnerabilidad de estos dispositivos es sobre todo es la conectividad con el Smartphone al que normalmente están asociados. Normalmente estos dispositivos se vinculan a través de una conexión Wireless de corto alcance como puede ser el Bluetooth. A través de este medio se mandan y reciben datos entre el wearable y el Smartphone, lo que provoca que los atacantes vean este último dispositivo como su objetivo para acceder a la información.

Por regla general los atacantes suelen acceder a la información de los Smartphone a través de software malicioso, en estos casos se usan aplicaciones con malware, en muchas ocasiones estas aplicaciones tiene un aspecto familiar para el usuario y suelen parecerse a aplicaciones populares, pero con algunas diferencias que producen dudas de la autenticidad de estas aplicaciones.

Estas aplicaciones maliciosas se pueden usar para usar para muchas cosas dependiendo el objetivo del atacante, se puede usar para realizar llamadas, enviar y recibir información, conocer la ubicación a través de GPS o ver cualquier problema

de salud dependiendo del dispositivo wearable que el usuario tenga conectado, todo ello sin que el usuario tenga constancia de lo que está sucediendo. El problema es que una vez que el atacante tenga acceso al dispositivo móvil, los atacantes tendrán todo el control y todos los recursos de los que dispone el usuario a su alcance para conseguir sus objetivos.

Ilustración 21 Dispositivo wearable conectado vía Bluetooth con un Smartphone

8.2 Prevención de riesgos en dispositivos wearables

Para prevenir estos riesgos y ataques de seguridad los usuarios deben seguir una serie de recomendaciones para minimizar todo lo posible los riesgos de un ataque [29]. Unas recomendaciones son las siguientes:

- Cuando usemos un wearable para hacer ejercicios, deshabilitemos el Bluetooth (siempre claro está que no sea necesario), de este modo reducimos la posibilidad de que pueda ser atacado.
- Si no hay manera de deshabilitar el Bluetooth, intentaremos asignar solo un ordenador portátil para usar esta información, de esta manera reducimos los equipos en los cuales tenemos nuestra información almacenada.
- También debemos restringir o controlar que información compartimos en las redes sociales o en sitios web. Debemos tener cuidado a la hora de compartir dicha información que puede ser visible por usuarios no deseados.

- Siempre que podamos intentar pasar la información del wearable directamente al dispositivo que deseemos, es decir siempre que podamos usar un método lo más seguro posible para transferir dicha información
- Cuando realicemos una transferencia de datos, borrar la información del weareble, de este modo evitamos que si perdemos este dispositivo la persona que lo encuentre tenga acceso a toda nuestra información.
- Antes de adquirir algún dispositivo wearable y usar la aplicaciones relacionadas, investigar sobre la marca de ese dispositivo y ver si tiene alguna vulnerabilidad de seguridad. Intentar en la medida de lo posible adquirir dispositivos de marcas conocidas o que bastantes usuarios usan, de este modo nos será más fácil enterarnos de algún fallo de seguridad, además si es una empresa grande normalmente suelen responder si sucede algún problema.
- Además de investigar sobre la empresa que proporciona el dispositivo es recomendable informarnos sobre que tecnología usa, que medidas de seguridad tiene implementadas, que datos recoge y como se gestionan dichos datos. Con estos podemos evitar grandes riesgos innecesarios.
- Usar siempre que el dispositivo lo permita un PIN, aunque no es un método infalible en la seguridad, puede hacer complicado el acceso a los atacantes y disuadirlos de realizar un ataque contra nuestros dispositivos.
- Limitar la información a la que tienen acceso los wearables. Estos dispositivos no necesariamente tiene que tener acceso a toda la información de los usuarios. Se pueden establecer los permisos para salvaguardar la privacidad del usuario. Estableciendo los permisos adecuados que el dispositivo necesite para cumplir su función evitamos bastantes riesgos.
- Utilizar sistemas de seguridad total que protejan también nuestros ordenadores, de este modo si realizamos una copia de seguridad del Smartphone evitamos que puedan tener acceso a esos datos a través de este dispositivo.

9. Conclusión

En este proyecto se ha presentado el estado del internet de las cosas y de todo lo referente a él. El internet de las cosas es un término que se aplica a todos los objetos que hasta eran objetos cotidianos sin conexión a internet y que con la evolución de la tecnología y de la sociedad recientemente se han convertido en objetos que están conectados a internet. Como se ha visto en este proyecto, el número de dispositivos que se conectan a internet supero hace algunos años al número de personas que se conectan a internet, y esto solo es el principio porque según la evolución este dato va en aumento y se prevé que en los próximos años este datos eleve exponencialmente. Esto hace que los usuarios dispongan de mayor número de dispositivos.

Ilustración 21. Imagen que hace referencia al aumento de dispositivos conectados a internet

A lo largo de este proyecto se ha evidenciado la importancia de que todos estos dispositivos cuenten con unas medidas de seguridad adecuadas, que tiene que aplicarse tanto en el producto como a nivel de los usuarios. Como hemos visto estos dispositivos pueden ser a atacados y pueden provocar grandes riesgos, puede amenazar la seguridad, la privacidad de nuestros datos en incluso puede atentar contra la integridad de las personas. Se debe tener en cuenta la protección de nuestros dispositivos, tanto el acceso a él, como la configuración del dispositivo, información a la que tiene acceso o que transmite, el cifrado de datos que usa,... y además de nuestra propia red, teniendo en cuenta su cifrado y su configuración teniendo en cuentas los puertos que pueden estar abiertos y teniendo especial cuidado con los protocolos que usamos o que están habilitados, bien porque los hayamos habilitado nosotros mismos o porque venga así por defecto.

La seguridad de los dispositivos del internet de las cosas depende tanto de los fabricantes que tienen que ajustarse al marco legal y procurar hacer todos sus dispositivos lo más seguros posibles, minimizando al máximo las vulnerabilidades que puedan tener, así como el mantenimiento de dichos dispositivos creando actualizaciones para mantener a los dispositivos siempre seguros. Como los propios usuarios que deben hacer un uso adecuado de dichos dispositivos y preocuparse y concienciarse de que la configuración de estos se la más segura posible, intentar siempre conectarlos de manera segura sin que haya perdida o ataques en la transmisión de datos y procurando que sus dispositivos se mantengan siempre actualizados.

Como hemos visto existen múltiples vías o deficiencias por la cuales los dispositivos son vulnerables a ataques, como pueden ser por software, hardware, transmisión de datos,.... Pero también se pueden llevar a cabo muchos normas o recomendaciones por la cual todos estos riesgos minimizados.

Hemos comprobado también algunos ataques reales que se han llevado a cabo y han mostrado las deficiencias de los dispositivos y de la importancia que tiene la seguridad en todos los ámbitos en los que esté presente el internet de las cosas. Como puede ser en el ámbito personal, los propios usuarios no sean conscientes de un robo de información personal o de sus actividades, en el ámbito industrial en el cual una pérdida del control de los dispositivos puede provocar grandes pérdidas económicas o una pérdida de información sensible de sus usurarios, e incluso en el ámbito medico en la cual cada vez está más presente y en la que se manejan datos sensibles de los pacientes, los cuales pueden ser monitorizados a través de dispositivos, aunque bien es cierto que en este ámbito debido a la delicada información que se maneja hay algunos avances de seguridad que evitan en la medida de lo posible posibles ataques.

Y por último hemos conocido un poco más que son los dispositivos wearable, los cuales están en auge en la actualidad y que se espera que su producción y venta se ve incrementado en los próximos años, como vemos dentro de esta categoría están dispositivos como los smartwatch, pulseras que controlan nuestra actividad física y monitorizan nuestra salud, incluso ropa con sensores que grandes marcas deportivas están incorporando para mejorar nuestro rendimiento físico y deportivo.

Con estos dispositivos la gran vulnerabilidad que puede producirse no está tanto el dispositivo en sí, que en ningún momento hay que descuidar su seguridad, como en la trasferencia de datos entre este dispositivo y cualquier otro, hay que tener especial cuidado a la hora de transmitir estos datos, para ello debemos usar un canal seguro, comprobar a que datos tienen acceso el wearable y en la medida de lo posible cifrar la transferencia de datos o los datos en sí.

Para prevenir ataque de seguridad se dan una serie de recomendaciones que son útiles para que los usuarios lleven a cabo y así poder disfrutar de sus dispositivos sin riesgo alguno.

Todas estas nuevas tecnologías se están incorporando en nuestras vidas y el internet de las cosas está presente en el día a día de cada individuo, cada vez su uso se hace más cotidiano y con la evolución de los dispositivos y los servicios que ofrecen hacen a los usuarios la vida un poco más fácil, el cual es el principio de estos dispositivos. Bien es cierto que hay que tener cuidado a la hora de usarlos pero con las medidas necesarias se minimizan los riesgos y son un gran aporte para la sociedad.

Finalmente vamos corroborar que todos los objetivos marcados al principio de este proyecto se hayan cumplido a lo largo del mismo.

- Hemos descubierto que es el internet de las cosas y hemos visto varios ejemplos y en multitud de ámbitos donde se puede aplicar el internet de las cosas en el capítulo 2.
- En el capítulo 4 hemos visto los riesgos del internet de la cosas y hemos visto en que ámbitos puede afectar el internet de las cosas, esto último se evidencia en el capítulo de ejemplos reales y en el capítulo 2 viendo la gran cantidad de ámbitos en los que puede afectar.
- En el capítulo 3 hemos visto las normativas que la Unión Europea tiene sobre la protección de datos que manejan estos dispositivos.
- Se ha evidenciado los problemas de seguridad y de privacidad de los diferentes dispositivos en el capítulo 4, en el capítulo de ejemplos hemos visto varios dispositivos que tienen deficiencias de seguridad y por último hemos analizado un poco más en profundidad la seguridad de los wearables.

- Para ver las posibles vías de ataque hemos visto en el capítulo 4 todas las subsecciones son posibles ataque o vías de ataque a los dispositivos del internet de las cosas.
- En el capítulo 6 hemos visto las medidas de prevención y unas recomendaciones para evitar problemas de seguridad y privacidad del internet de las cosas.
- En el capítulo 6 en la última sección se trata el tema de las personas para concienciarlas sobre los riesgos de estos dispositivos y a tomar las medidas necesarias para no tener ningún riesgo
- En el capítulo 8 hemos visto varios ejemplo de ataques que se han materializado y los daños o riesgos que han causado
- En el capítulo 9 hemos analizado más a fondo los dispositivos wearable viendo los riesgos de seguridad y viendo que prevenciones o recomendaciones tenemos que tener con dichos dispositivos

10. Bibliografía

[1]Observatorio Nacional de las telecomunicaciones de la SI. Enlace: http://www.ontsi.red.es/ontsi/es/estudios-informes/perfil-sociodemogr%C3%A1fico-de-los-internautas-datos-ine-2015

[2]Clúster ICT-AUDIOVISUAL de Madrid (2013). Internet de las cosas: Objetos interconectados y dispositivos inteligentes

[3] Internet de las cosas. Objetos interconectados y dispositivos inteligentes (Marzo 2013). Posibles Aplicaciones.

[4] Smart Cities. Enlace: http://www.creatingsmartcities.es/

[5] Smart Metering Enlace: https://en.wikipedia.org/wiki/Smart_meter

[6] Smart Enviroment. Enlace: http://web.ua.es/es/smart/smart-environment-un-entorno-de-calidad-de-vida.html

[7] Smart Water. Enlace: http://www.creatingsmartcities.es/ambitossmart-water.php

[8]Agricultura inteligente. Enlace: http://smartrural.net/agricultura-inteligente/

[9] Domotica. Enlace: http://www.cedom.es/sobre-domotica/que-es-domotica

[10] eHealth. Enlace: http://www.abc.es/tecnologia/informatica/software/abci-ehealth-planes-tecnologia-para-unir-medicina-y-smartphones-201511112203_noticia.html

[11]Politécnica de Madrid. Seguridad en el internet de las cosas

[12]Agencia española de protección de datos Directiva 95/46/CE. Enlace: https://www.agpd.es/portalwebAGPD/internacional/textosynormas/textos_union_europea/textos_directivas/common/pdfs/B.4_Directiva_95-46-CE.pdf

[13]Agencia española de protección de datos Directiva 2002/58/CE. Enlace: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/B.6-cp--Directiva-2002-58-CE-protecci-oo-n-e-intimidad-en-comunicaciones-electronicas.pdf

[14]Wearables: ¿cuál es el riesgo de seguridad? Enlace: http://www.welivesecurity.com/la-es/2015/12/14/wearables-riesgo-seguridad/

[15]CSRIT-CV. Seguridad en el internet de las cosas. Estado del arte

[16]IOT Simple. Enlace: http://www.iotsimple.com/seguridad-en-iot

[17] Google Glass y Samsung Galaxy Gear2. Enlace: http://www.baquia.com/emprendedores/kaspersky-lab-advierte-de-los-riesgos-de-seguridad-de-los-dispositivos-wearables

[18] CSRIT-CV. Seguridad en el internet de las cosas. Estado del arte. Recopilación de incidentes.

[19] Pebble. Enlace: http://wearabledevices.es/2014/08/pebble-smartwatch-esta-afectado-por-una-vulnerabilidad-con-la-que-un-atacante-remoto-puede-borrar-todo-su-contenido/

[20]Amenaza de seguridad Viking Jump. Enlace: http://muyseguridad.net/2016/05/11/viking-jump-malware-android/

[21]Interrupción de una operación de cateterismo cardiaco. Enlace: http://muyseguridad.net/2016/05/10/antimalware-interrumpe-operacion-cateterismo-cardiaco/

[22]Vulnerabilidad en coches Chrysler. Enlace: http://muyseguridad.net/2015/07/23/coches-chrysler-hack/

[23]Malware ransomware. Enlace: http://muyseguridad.net/2016/06/01/ransomware-hospitales/

[24]Amenazas en los hospitales. Enlace: http://muyseguridad.net/2016/04/25/hospitales-hackers/

[25]Vulnerabilidad en el sistema iOS. Enlace: http://muyseguridad.net/2016/03/22/acedeceiver-malware-dispositivos-ios-sin-jailbreak-silenciosa/

[26]Amenazas en las SmartTV. Enlace: http://muyseguridad.net/2016/01/18/smarttv-malware/

[27]Lourdes García Montoro (2015). Wearables: qué son, cómo funcionan y que peligros entrañan para nuestra privacidad

[28]Los riesgos de seguridad de los ‘wearables. Enlace:
http://www.ticbeat.com/seguridad/riesgos-seguridad-wearables/

[29]Consejos de seguridad para el uso de wearables. Enlace:
http://guateanuncia.com/tech/consejos-de-seguridad-para-el-uso-de-wearables/

[30] Agencia Española de Protección de Datos (2015) Resolución 20 de noviembre 2015. Plan Estratégico 2015-2019.

[31] ¿De quién son los datos del big data e internet de las cosas? Enlace: http://blogs.elconfidencial.com/espana/blog-fide/2016-04-21/de-quien-son-los-datos-del-big-data-e-internet-de-las-cosas_1168423/

[32] Runtastic. Política de Privacidad. Enlace: https://www.runtastic.com/es/politica-de-privacidad

[33] Facebook. Política de datos. Enlace: https://es-es.facebook.com/legal/terms/update