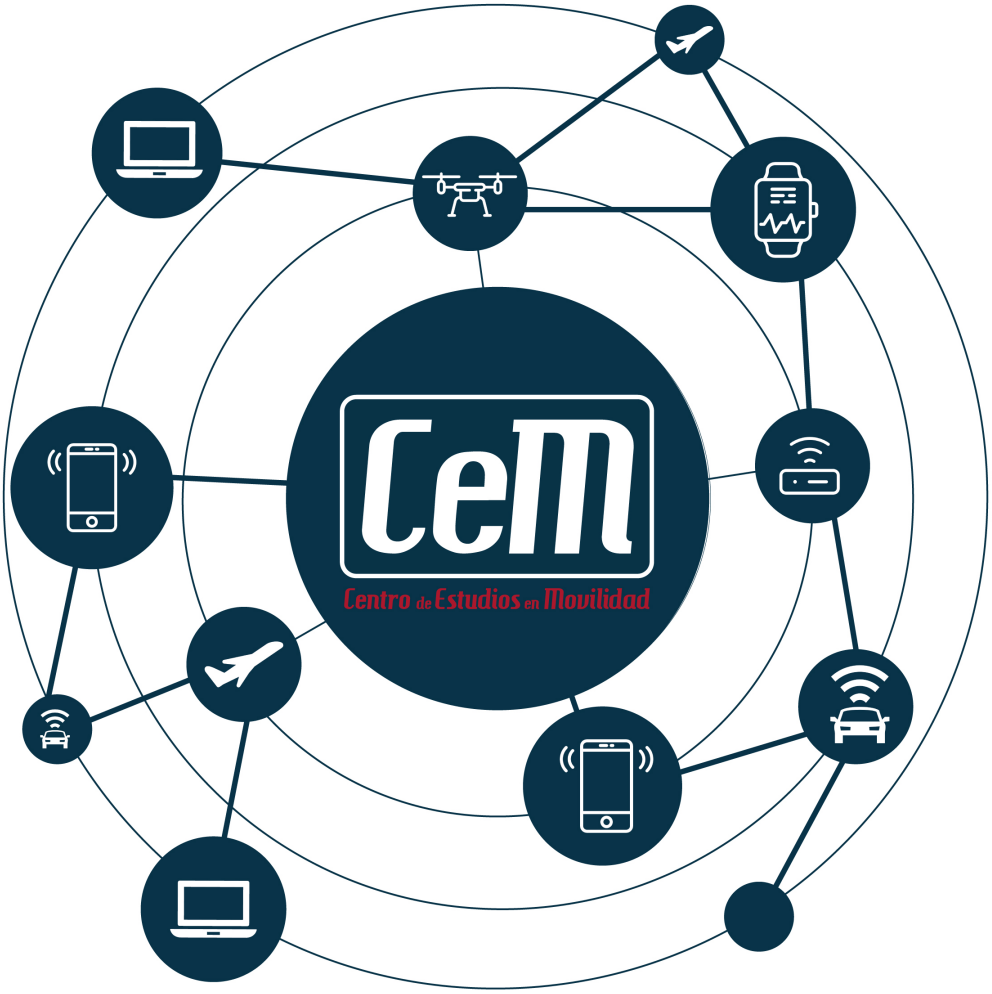


Una iniciativa de

isms forum spain

ESTADO DEL ARTE E IMPLICACIONES DE SEGURIDAD Y PRIVACIDAD EN EL INTERNET DE LAS COSAS

VERSIÓN 1.0. 17 de octubre de 2017

COLABORADORES

Coordinador general:
Francisco Lázaro

ESTADO DEL ARTE DEL INTERNET DE LAS COSAS (IOT)

Coordinador:
Juan Manuel Zarzuelo

Grupo de trabajo:
Espejo, Beatriz
Grande, Elías
Venganzones, José María

ANÁLISIS DE LOS VECTORES DE ATAQUE DEL INTERNET DE LAS COSAS (IOT)

Coordinador:
Raúl Siles

Grupo de trabajo:
Cabrera, Pedro
García, Raúl
Labiaga, Ricardo
Pérez, Alberto
Riego, Javier del

IMPACTO DE LAS TECNOLOGÍAS IOT Y DISPOSITIVOS MÓVILES EN LA PRIVACIDAD DE LAS PERSONAS

Coordinadora:
Paloma Llaneza

Grupo de trabajo:
Benéitez, Helena
Díaz, Rosa
González Calero, Francisco
Palomo, Alicia
Velázquez, Rafael

BUENAS PRÁCTICAS EN DISPOSITIVOS IOT y MARCA DE GARANTÍA

Coordinadores del manual de buenas prácticas:
Jorge Hurtado y Antonio Fontiveros

Coordinadora del Reglamento de Uso de la Marca de Garantía:
Paloma Llaneza

Grupo de trabajo:

Álamo, José María del
Bardallo, Josep
Benéitez, Helena
Carbayo, Javier
Carmona, Javier García
Galán, Ana Belén
Iparraguirre, Ana
Pascual, Juan Carlos
Rey, Noemí
Santos, Rafael
Tejero, Alberto

DIRECCIÓN Y SOPORTE

García, Daniel
Campo, Laura do

ÍNDICE

BLOQUE I:
ESTADO DEL ARTE DEL INTERNET DE LAS COSAS (IOT)

1. INTRODUCCIÓN

1.1 DEFINICIÓN DE SISTEMA IOT

Llamado a ser la próxima revolución industrial, debido al impacto que tendrá en negocios, gobiernos y consumidores por los cambios que implica en la forma de interactuar con el mundo físico, Internet of Things es una realidad a día de hoy, presente en dispositivos cotidianos como juguetes, cámaras o alarmas de vigilancia casera.

Por otro lado, y mirando al futuro, las estadísticas auguran que el crecimiento de dispositivos conectados a Internet pase de algo más de 6.000 millones en 2016 a más de 20.000 millones en el año 2020. (Gartner, Febrero 2017).

Categoría	2016	2017	2018	2020
Consumidores	3,963.0	5,244.3	7,036.3	12,863.0
Ámbito Empresarial General	1,102.1	1,501.0	2,132.6	4,381.4
Ámbito Empresarial Específico	1,316.6	1,635.4	2,027.7	3,171.0
Grand Total	**6,381.8**	**8,380.6**	**11,196.6**	**20,415.4**

Tabla1.- Número de Dispositivos IoT instalados. Fuente: Gartner (Enero 2017)

El término Internet of Things, fue utilizado por primera vez en 1999 por Kevin Ashton, cofundador y director ejecutivo de AutoID, refiriéndose en este caso a los dispositivos conectados en la red RFID en la que estaba trabajando:

”I could be wrong, but I’m fairly sure the phrase “Internet of Things” started life as the title of a presentation I made at Procter & Gamble (P&G) in 1999. Linking the new idea of RFID in P&G’s supply chain to the then redhot topic of the Internet was more than just a good way to get executive attention. It summed up an important insight which is still often misunderstood.”

Y sin embargo, más de 18 años después de su concepción, con la integración actual en la sociedad y los múltiples ámbitos donde se está desarrollando, a día de hoy carece de una definición oficial.

Para el propósito de este documento, podemos determinar que un Sistema IoT estará compuesto por todos aquellos elementos que en conjunto hacen posible el funcionamiento del dispositivo de IoT, pero también que lo hacen vulnerable. Es decir, además del propio dispositivo físico, ya se trate de un Smartwatch, pulsera, etc., también serán elementos necesarios a considerar el software, las redes de comunicaciones, sensores, transmisores, almacenamiento de la información, etc.

A continuación se muestra un “sistema de IoT” de ejemplo.

Ilustración 1. Ejemplo de sistema de IoT para dispositivos de tipo Smartwatch. Fuente: Elaboración propia.

Una primera aproximación de lo que entendemos por Internet de las cosas o IoT (por sus siglas en inglés de Internet of Things), podrían ser los objetos cotidianos conectados a Internet. Objetos cotidianos tales como: juguetes, lavadoras, neveras, televisores, estanterías de comercio, marcapasos, bombas de insulina, ascensores e incluso la agrupación y trabajo coordinado de éstos (casas, edificios, coches, trenes, ciudades, etc.).

Estos dispositivos suelen contener al menos uno de los siguientes elementos:

- Sensores, encargados de obtener el estado de uno o varios dispositivos y sus caracterís ticas y/o propiedades.
- Actuadores, encargados de tomar acciones y modificar el estado de uno o varios dispositivos y sus características y/o propiedades.
- Comunicaciones locales.
- Comunicaciones fuera del entorno local.
- Hubs (o controladores), encargados de centralizar las tareas de gestión, monitorización y control del resto de objetos o dispositivos IoT.

Por tanto en el presente estudio, se considera un dispositivo asociado al Internet de las Cosas o IoT (Internet of Things) a todo objeto físico o dispositivo inteligente (denominado comúnmente smart), con capacidades de computación, es decir, que dispone de electrónica y/o de un ordenador embebido (habitualmente de reducido tamaño), y con capacidades de interconexión con redes de datos, ya sean internas (por ejemplo, en el hogar, empresa o en un entorno industrial o de movilidad, como los vehículos) o externas (conectado a Internet).

Dentro de los dispositivos IoT se encuentran tanto sensores (encargados de obtener el estado de unos o varios dispositivos, así como sus características y/o propiedades) y actuadores (encargados de tomar acciones y modificar el estado de uno o varios dispositivos y sus características y/o propiedades), como los controladores (o hubs), encargados de centralizar las tareas de gestión, monitorización y control del resto de objetos o dispositivos IoT.

Estos objetos tienen capacidades de proceso de información que funcionan como “pequeños ordenadores” que se incorporan a nuestras prendas e incluso para mejorar nuestra salud, se adhieren, se implantan, se inyectan, se tragan, etc.

Su potencia aumenta cuando el IoT se une a otras tecnologías y/o prácticas tales como el tratamiento masivo de datos y la búsqueda de relaciones (Big Data), la capacidad de la nube para el procesamiento o almacenamiento, la inteligencia artificial, el machine learning (que las máquinas aprendan solas) o la inteligencia cognoscitiva aplicada a los sistemas, llegando hasta los robots e incluso a conectar objetos a nuestro cerebro u otros órganos.

Esta nueva inmersión en la tecnología supone igualmente una inmersión de la tecnología en nosotros. Nuestra vida va a cambiar en todos los sentidos. Ser más dependientes de la tecnología, no sólo al hacernos la vida más cómoda al mejorar nuestro ocio y cultura, sino también al mejorar nuestra salud, prolongando nuestra vida y la calidad de la misma.

Pero también afectará a nuestra vida laboral; esta tecnología forma parte de la industria conectada 4.0, la cual no sólo aportará mayor control, eficacia y eficiencia del proceso productivo, sino que dará paso al trabajo con robots (primero de forma colaborativa y en unos años competitiva).

El uso del IoT será omnipresente. Diferentes estudios cifran entre 20 y 50 mil millones de estos dispositivos en el 2020.

Con estos dispositivos podemos ir a escenarios sencillos, donde un sensor de temperatura del interior de la casa dispare un aviso indicando que no ha entrado en funcionamiento la calefacción de la comunidad y actúe sobre la bomba de calor de nuestro equipo individual de aire acondicionado; o por el contrario, sin ser ni mucho menos el más complejo, sí que nos da una idea de la posible interacción de dispositivos en virtud de la temperatura, de la situación del destino del puesto de trabajo, del tráfico actual y de la previsión basada en el histórico, así como del estado del vehículo autónomo. Puede que el despertador suene diez minutos más tarde y conforme a nuestros hábitos el desayuno esté listo, tengamos nuestros medicamentos genómicos (específicos para nosotros) preparados y la ducha esté a la temperatura adecuada, junto con la recomendación de la ropa más adecuada. En este escenario, junto con nuestra agenda, los dispositivos portables nos indicarán el ejercicio necesario y las opciones de la dieta para mantenernos en estado óptimo.

2. COMPONENTES TECNOLÓGICOS

La tecnología es fundamental en Internet de las Cosas (IoT) y, en este sentido, las mejoras en los sistemas y la integración de las distintas tecnologías ha producido un entorno ideal para esta revolución.

A continuación detallamos las principales áreas que componen el ecosistema de Internet of Things: Hardware, Software y Comunicaciones.

2. 1. HARDWARE

Uno de los principales canalizadores del crecimiento de IoT ha sido la evolución del hardware. Los avances en este campo han generado hardware de mejor calidad, tamaño reducido y un precio muy asequible, que pone al alcance de todos los usuarios la tecnología y, por tanto, la posibilidad de realizar proyectos de mayor o menor calado de manera autónoma.

Existen multitud de dispositivos con capacidad de proceso, almacenamiento, sensores y emisores desde 15 a 200 dólares, que, sumado a la documentación existente en la red, facilitan la creciente tendencia del DIY ("Do It Yourself" o "Hazlo tú mismo").

2. 2. SOFTWARE/FIRMWARE

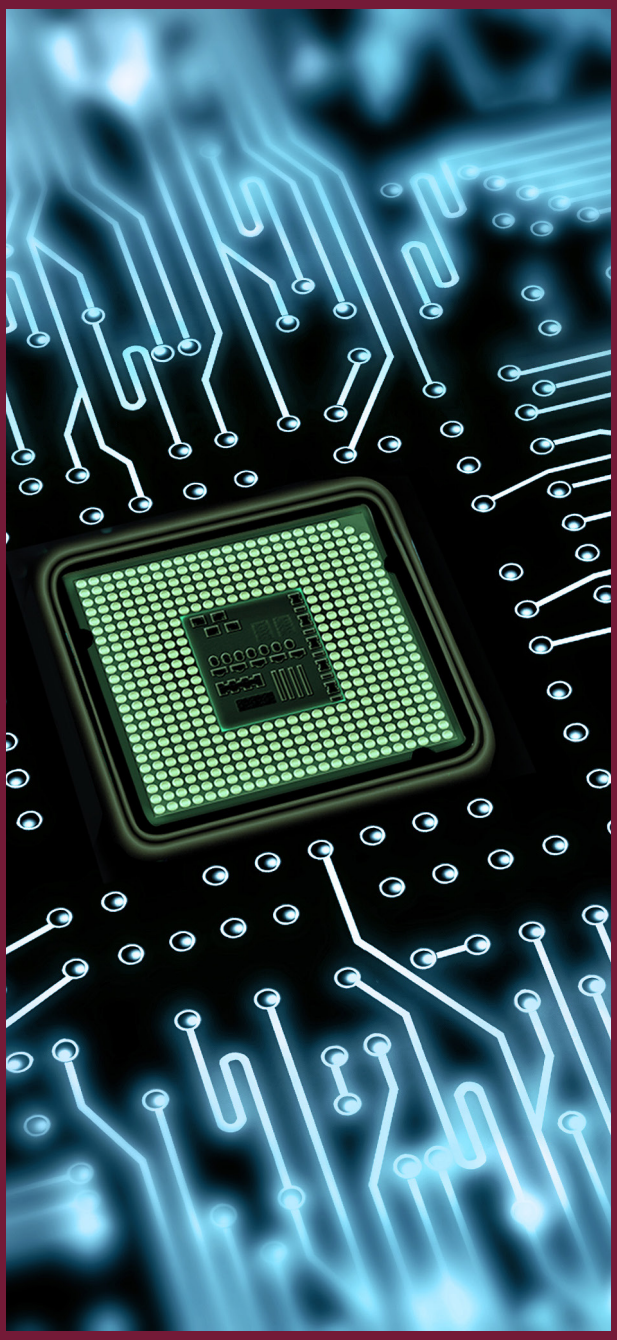
Existen diferentes aspectos en los que el software tiene un impacto importante en IoT:

- Firmware o sistemas embebidos: El fundamento de los "smart devices" parte de tener un sistema operativo embebido que utilice las capacidades de cómputo, almacenamiento y comunicación necesarias para aportar un valor añadido.

- Software/aplicaciones de canal: Cuando se comparte información entre dispositivos IoT, se hace a través de aplicaciones destinadas a generar beneficio a los usuarios.

Un ejemplo práctico podría ser una aplicación en un móvil recibiendo notificaciones desde dispositivos BLE (Bluetooth Low Energy) como los beacons. Esta aplicación a su vez, utilizaría esa información para comunicarse con un servidor que aportaría valor al usuario a través de servicios.

- Big Data y software analítico (back-end): Uno de los grandes beneficios económicos de Internet of Things está en las posibilidades que ofrece la cantidad de información que se genera a diario y el valor que tiene explotarlo a través de software analítico.



2. 3. COMUNICACIONES

La transferencia de información es fundamental para que los dispositivos IoT funcionen. Existen multitud de redes de comunicación que habilitan distintos canales de trasmisión, desde las más conocidas (WiFi, Bluetooth, 2G/3G/4G) a redes de amplio espectro como LoRaWAN o comunicaciones de frecuencia en cercanía como el NFC.

Nombramos a continuación las más significativas y una breve descripción de las mismas:

● WiFi: Tecnología inalámbrica por excelencia, definida por la Wi-Fi Alliance como “wireless local area network (WLAN)”, tiene un radio de acción que permite establecer redes de comunicaciones de tamaño medio (viviendas, oficinas, etc). Debido a su enorme implantación en dispositivos (prioritariamente ordenadores portátiles, tablets y móviles), hace que sea una de las tecnologías más utilizadas por los desarrolladores de proyectos/productos IoT.

● Bluetooth: El Bluetooth es una tecnología inalámbrica de corto alcance muy importante. Su asociación al mercado de la telefonía le atribuye un gran calado social, posicionándolo como una de las tecnologías prioritarias. Existe otra tecnología similar llamada Zigbee, más focalizada en el sector industrial.

● 2G/3G/4G: Las redes de telefonía son unas de las más longevas y que se mantienen con un nivel más alto de desarrollo. La evolución de estas tecnologías está experimentando mejoras en la velocidad de transmisión de datos y la seguridad de los canales. Actualmente se trabaja en la próxima versión, el 5G.

● NFC: Protocolo de comunicación de proximidad muy utilizado por dispositivos móviles y de manera más o menos reciente por tarjetas de crédito, para facilitar métodos de pago ágiles.

● LoRaWAN: Una de las más significativas en el mundo del IoT, pues combina su gran radio de acción con los dispositivos de bajo consumo. Aunque habitualmente se utiliza de manera unidireccional o bidireccional, permite la multidifusión, lo que ofrece muchas posibilidades. Existen otras redes con características similares como Sigfox o Neul.

● Z-Wave: Muy utilizada para la comunicación de los dispositivos de baja energía del sector de la domótica. Entre sus características más interesantes está la fácil escalabilidad, con capacidad de control de hasta aproximadamente 250 dispositivos.

3. ÁMBITOS DE APLICACIÓN

Desde el punto de vista del mercado, es necesario tener en cuenta los diferentes sectores donde actualmente la tecnología tiene una aplicación más importante y, a su vez, describir la aportación que tiene la tecnología sobre los posibles usuarios receptores y la madurez e implicación de los mismos.

La reciente eclosión del Internet of Things, se ha desarrollado de una manera diferente dependiendo del sector. En algunos de ellos, la implantación está en un grado muy avanzado, como puede ser en los consumibles (smartphones, wearables, etc.), pero quedan muchos nuevos sectores donde la aplicación de estas tecnologías aportará un claro beneficio y progreso.

Gracias al IoT todo pasa a ser inteligente y así encontramos su uso en sectores tales como: el hogar inteligente (smart home), la energía inteligente (smart energy), las ciudades inteligentes (smart cities), el transporte inteligente (smart transport), las salud inteligente (smart health) o la Industria 4.0.

3.1. HOGAR (Smart Homes)

La domótica es un concepto bien asentado en el mercado desde hace años. Utilidades como el control electrónico (programado u on-line) de elementos como la calefacción o los sistemas de riego, son utilizadas de manera habitual.

Con las tecnologías IoT, se adquiere la capacidad de que los propios elementos existentes en la vivienda sean capaces de realizar acciones en base a unas directrices específicas.

Siguiendo con el ejemplo del sistema de riego, sería posible dotar a este de sensores de temperatura, humedad y presión atmosférica, para modificar la periodicidad o el flujo de riego, además de emitir una notificación al móvil del dueño de la vivienda.

De tal modo, la interconexión entre los diferentes dispositivos electrónicos puede facilitar y automatizar ciertas tareas que se realizan en el hogar, por lo que este mercado va a generar un importante cambio en la vida de las personas y también en los mercados, debido a la adaptación de todos los dispositivos a estas nuevas funcionalidades.

3.2. ENERGÍA (Smart Grids)

La distribución de energía también ha querido hacerse un hueco en el mundo de las tecnologías, convirtiendo las redes energéticas en canales de distribución bidireccional, de modo que los usuarios no solo consumen energía, sino que también pueden producirla, por ejemplo, mediante placas solares, beneficiando así tanto al usuario por la reducción de consumo como a las empresas distribuidoras.

Para permitir dicha bidireccionalidad, así como para incrementar la eficiencia en la operación de redes energéticas, se están empezando a cambiar los contadores tradicionales por contadores de lectura telemática, siendo estos mucho más precisos y permitiendo la lectura a distancia, de modo que se evitan las visitas del técnico (abaratando el servicio), así como las lecturas estimadas de algunos meses.

Además, al tratarse de dispositivos que incorporan lógica programable, facilita la detección de averías, se agiliza su recuperación y permite a los usuarios consultar el consumo que realizan y el precio de la energía por horas, ayudando optimizar el consumo.

A finales de 2018 todas las viviendas y comercios en España, contarán con estos nuevos contadores.

3.3. SMART CITIES

A raíz de nuestra búsqueda de la sostenibilidad, la idea de las ciudades inteligentes se ha desarrollado más rápidamente, dando soluciones a las necesidades básicas de habitantes, instituciones y empresas.

Son ya varios los ámbitos en los que se empiezan a pronunciar este nuevo concepto de ciudades, como la señalización de estacionamientos libres, la conexión de elementos como el transporte público o los vehículos particulares.

- La señalización de estacionamientos libres, que pueden disminuir el tráfico de vehículos al localizar fácilmente las plazas disponibles.

- La conexión a Internet de elementos como el transporte público, permitiendo al ciudadano conocer el tiempo de espera o a la empresa correspondiente si alguno de los vehículos ha sufrido una avería.

- "Movilidad inteligente" promovida por la DGT, que pretende mejorar la circulación disminuyendo también los accidentes. Una de las premisas es que la información se realizará de forma anónima, permitiendo la privacidad de los usuarios. El hecho de que los usuarios o vehículos estén conectados permitirá que se les informe de la aproximación de otros vehículos, peatones o ciclistas, comunicar el estado técnico del vehículo, nivel de consumo, emisiones y demás, o comunicar a las autoridades y otros usuarios la localización del vehículo en caso de avería entre otros servicios.

Uno de los requisitos fundamentales para que este tipo de ciudades se lleven a cabo, es la participación y educación de los ciudadanos en este nuevo sistema.

Otros aspectos relacionados con el entorno de las ciudades inteligentes son:

- De la parte de automoción, los vehículos eléctricos, ya presentes en transporte público y en vehículos privados, así como la creación de carriles bici que impiden utilizar vehículos de motor, reduciendo las emisiones de CO_2.

- Las fuentes de energía renovables, como por ejemplo, las placas solares en viviendas y edificios o en alumbrado público y señalización luminosa.

- Las anteriormente mencionadas Smart Grids.

Se trata del sector más lento en adopción del IoT, sólo el 42% de los municipios han desplegado dispositivos IoT y sensores.

Las ciudades contarán con sensores de luz que no sólo responderán a las mediciones de luz ambiental, sino que en virtud del nivel de seguridad de la zona iluminarán con mayor o menor grado. Se instalarán sensores de limpieza en contendores y camiones, de luz, de ruido, de tráfico inteligente, entre otros muchos.

3.4. SANIDAD

En sanidad, la adopción de estas tecnologías supone un gran avance tanto para médicos como para pacientes, permitiendo, por ejemplo, la monitorización a distancia. De este modo se podrán salvar vidas gracias a la recepción de alertas que permitan detectar alguna anomalía en los datos del paciente.

Esta interacción tecnológica hace años que se está usando en aparatos como los marcapasos, conectados inalámbricamente a internet y que mediante un "router" específico envían información diariamente al médico, permitiendo detectar cualquier anomalía en el corazón del paciente, así como el ajuste de parámetros del propio marcapasos.

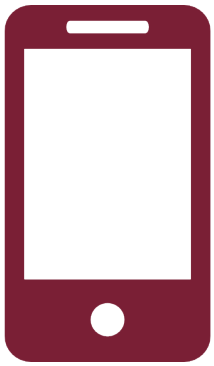
El 60% de las organizaciones sanitarias de todo el mundo han introducido dispositivos IoT en sus instalaciones, convirtiéndose así en el tercer sector más avanzado en la implementación de IoT.

Desde el 2015 hay píldoras inteligentes que se ingieren para conocer el asentamiento de los medicamentos en nuestro organismo mientras que también están homologados implantes inteligentes.

Para construir un marco de colaboración en este ámbito, la FDA (U.S. Food & Drugs Administration) ha publicado diversos estudios donde trata de exponer recomendaciones para el tratamiento de los dispositivos por parte de los fabricantes:

- Postmarket Management of Cybersecurity in Medical Devices Guidance.
- Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices.
- Guidance to Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shell Software.

Con esta guía, la administración pretende fomentar la colaboración de las partes interesadas y la comunicación, crear conciencia sobre el marco de la ciberseguridad voluntaria y animar a todas las partes intervinientes en la salud pública a desarrollar estrategias innovadoras para evaluar y mitigar las vulnerabilidades existentes.



3.5. CONSUMIBLES

El inicio de Internet de las cosas (IoT) llegó a nosotros casi sin avisar, y hoy en día está presente en casi todas las casas de mano de los smartphones. Fue en 1999 cuando DocoMo, una operadora, permitió visualizar páginas web adaptadas en el teléfono móvil.

A raíz de los móviles con conexión a Internet, a principios del siglo XXI de la mano de Microsoft, surgieron las tablets, aunque empezaron a tener éxito en 2010 con la aparición del iPad.

Ligado a dispositivos conectados a smartphones, encontramos que se está empezando a trabajar en ropa con sensores capaces de informar: si la prenda detecta niveles de rayos solares dañinos para la piel, si la persona que lleva la prenda se está alejando, o enviar la actividad cardíaca, la frecuencia respiratoria, o la actividad muscular de la persona.

El inicio de Internet of Things llegó a nosotros casi sin avisar, y hoy en día está presente en casi todas las casas españolas de mano de los teléfonos móviles de última generación. Fue en 1999 cuando DocoMo, una operadora, permitió visualizar páginas web adaptadas en el teléfono móvil.

A raíz de los móviles con conexión a Internet, a principios del siglo XXI de la mano de Microsoft, surgieron las tablets, aunque empezaron a tener éxito en 2010 con la aparición del iPad. Las tablets tienen una funcionalidad similar a los móviles, pero dando acceso a una pantalla más grande y fácil de leer y, además son completamente táctiles.

El primer smartwatch de la historia, tuvo su aparición en 1977 de la mano de HP, que fabricó un reloj que incorporaba calculadora. A raíz de este prototipo, y a lo largo de los años, estos relojes han ido evolucionando e incluyendo distintas funcionalidades como sistemas operativos, cámara digital, puerto infrarrojos, reproductor de mp3, agenda electrónica. Y no fue hasta 2004 cuando Microsoft creó un smartwatch con funcionalidades compartidas con los móviles, como la recepción de mensajes de texto, de noticias y previsión meteorológica entre otros. Finalmente en 2010 Sony lanzó un smartwatch capaz de conectarse por bluetooth a un smartphone de modo que se puedan consultar mensajes del móvil, contestar llamadas, etc. La tendencia del mercado es que estos relojes dejen de ser dependientes de los smartphones y sean capaces de realizar las mismas funciones que tienen ahora sin depender de ellos.

Ligado a dispositivos conectados a smartphones, encontramos con que se está empezando a trabajar en ropa con sensores capaces de informar si la prenda detecta niveles de rayos solares dañinos para la piel, si la persona que lleva la prenda se está alejando, útil para niños, o enviar la actividad cardíaca, la frecuencia respiratoria, o la actividad muscular de la persona.

3.6. INDUSTRIA

Más de siete de cada diez (72%) empresas han introducido dispositivos IoT en el lugar de trabajo, pero todavía queda un largo camino. Se calcula que en el 2018 más de cuatro millones de personas en el mundo, estarán supervisadas directamente por una máquina.

3.7. AUTOMOCIÓN

El concepto de coche equipado con acceso a Internet ya no es exclusivo de los sistemas multimedia (música, mapas y películas están disponibles a bordo en los coches de lujo modernos), sino que también cuenta con tecnología IoT los sistemas de llaves de coches en sentido literal y figurativo. Mediante el uso de aplicaciones móviles propietarias, es posible obtener las coordenadas GPS de un coche, seguir su ruta, abrir sus puertas, poner en marcha su motor y encender sus dispositivos auxiliares. La tendencia de la automoción está orientada a los vehículos conectados a Internet con diversidad de funcionalidades derivadas.

La tendencia de la automoción está orientada a los vehículos conectados a Internet con diversidad de funcionalidades derivadas.

La mayoría de los modelos nuevos en el mercado, ya incluyen una red WiFi propia (la mayoría a través de tarjetas de telefonía) que permiten al propietario del coche y sus acompañantes conectar sus dispositivos a la red del vehículo. Con este tipo de redes se pueden cubrir servicios de posicionamiento, mapas de carreteras o servicios de información y emergencia (reportar el volumen de tráfico o un accidente).

Que los automóviles integren sensores y emisores, pueden permitir a otros ámbitos (como las SmartCities) aprovechar la información para integrar otros tipos de servicios, como podría ser el caso de los semáforos inteligentes, que regulan su actividad según el tráfico.

Del mismo modo, se está avanzando en los vehículos autónomos, es decir, sin necesidad de conductor, guiados por los sensores externos y la información que la centralita recibe de los servidores centrales.En la actualidad, ya disponemos de estos vehículos conectados a un ordenador central capaces de controlar todas las funciones del vehículo, e incluso, se comercializan vehículos con tecnología parkassist (aparcamiento automático mediante sensores).

En mayo de 2015, Google sacó a las calles de Mountain View, California, sus primeros vehículos autónomos. Y otras marcas como Tesla se están esforzando en realizar avances en este ámbito. Aunque debemos remontarnos a los años 80 para conocer las primeras apariciones de vehículos autónomos, los avances tecnológicos actuales han favorecido que estos comiencen a tomar protagonismo.

Recientemente, un estudio de seguridad de 7 aplicaciones móviles que cuentan con más de 6 millones de descargas, para el uso en coches conectados, ha dado a conocer que estas aplicaciones disponen de características potencialmente peligrosas que permitirían robar el vehículo o incapacitar funcionalidades importantes del vehículo.

Y si el concepto de vehículo conectado lo llevamos al máximo nivel (que nuestra actual imaginación nos permite) llegaríamos al mundo del vehículo autónomo, el cual conducirá por nosotros y literalmente nos pondremos en sus manos. En dicha confianza de seguridad en la circulación es donde surge la desconfianza de los expertos de seguridad de la información.

Los usuarios que tomarán parte en esta actual tendencia, son los ciudadanos de a pie, de todos los rangos de edad, expertos o no en el mundo de la tecnologías.

Cierto es que, gran parte de la aceptación social sobre la tecnología en la actualidad, ha sido apoyada por las nuevas generaciones, desde los denominados Millenials o Generación Y (nacidos entre los años 80 y 90) que han formado parte de los últimos avances tecnológicos y los han ido adaptando a sus vidas, hasta la Generación Z (del 2000 en adelante) que han utilizado la tecnología desde una fase muy temprana de su vida. Ambos forman parte de los llamados Digital Natives/Born Digital o nativos/nacidos digitales.

La edad del público es cada vez más corta, por lo que se deben tener en cuenta una serie de medidas, tanto referentes a la formación y educación de los usuarios, como a la seguridad de los propios dispositivos y comunicaciones. Encontramos que incluso los bebés forman parte, pues existen juguetes con conexión a internet, cámaras de fotos que capturan a los niños e interactúan con ellos o simplemente, las cámaras de vigilancia utilizadas por los cuidadores.Por otro lado, nuestros mayores también hacen uso de estas tecnologías, por ejemplo, en la tele-asistencia o en los dispositivos de localización para casos de emergencia.

4. ASPECTOS DE SEGURIDAD

Una vez tratados los componentes tecnológicos y sectoriales de Internet de las Cosas (IoT), es necesario definir los aspectos de seguridad implicados.

Como toda tecnología, su uso acarrea unos riesgos que pueden ser atenuados por intereses económicos y de otras índoles como pueden ser el terrorismo, las ciber-mafias y/o delincuentes. Estos últimos bucan hacer dinero con los dispositivos ya sea secuestrándolos virtualmente (haciendo que no funcionen) y exigiendo un rescate para que vuelvan a funcionar, o bien exprimiendo información sacada de nuestra privacidad o utilizando la capacidad de nuestros equipos para atacar a terceros como hace pocos meses ocurrió con cientos de miles de dispositivos IoT como cámaras y otros elementos, que desde ellos dejaron mudas a compañías tan relevantes como twitter, Spotify, Amazon o la CNN, entre otras.

Pensemos el impacto negativo que podría causar el ciber-terroristas en infraestructuras críticas para el país, modificando por ejemplo el tratamiento del agua; o si un pirata informático lograse controlar el desfibrilador cardioversor implantable (DCI) inalámbrico que se encuentra dentro del cuerpo de un paciente.

Ya han aparecido informaciones de ataques al IoT, en las que detallan como la CIA utiliza televisores para extender la "escucha" y el espionaje al interior de las casas, utilizando el micrófono del televisor, o como los delincuentes han bloqueado clientes en sus habitaciones e inutilizado televisores para chantajear y pedir dinero a cambio de liberarles de ese secuestro tecnológico (RoT).

En la seguridad del IoT (lo que algunos llaman SoT) nos encontramos con una serie de desafíos tales como la seguridad en todo el ciclo de vida (desde los trabajos de diseño, hasta el difícil mantenimiento de actualizaciones / parches de seguridad) sumando a la forma a la que podremos proteger la red doméstica sin prácticamente conocimiento de tecnología y seguridad por parte de sus dueños y usuarios.

Si como ciudadanos/consumidores no nos preocupamos por la seguridad y la demandamos, los fabricantes no invertirán en algo que, ahora, no está regulado ni interesa al cliente. Y si eso es así, y si llegamos al 2020 sin seguridad, lo que será cierto es que 20.000 millones de dispositivos tendrá un importante impacto en la vida de las personas.

4.1. SEGURIDAD DE LA INFORMACIÓN EN SISTEMAS IOT

Según la International Standard Organization (ISO), la definición de activo sería: "Algo que tiene valor para la organización". ISO/IEC 13335-1:2004. Cambiando de enfoque, si en lugar de una organización se tiene en cuenta al usuario del dispositivo de IoT, la definición de activo en nuestra metodología sería: "Algo que tiene valor para el usuario".

Según la definición de activo como "algo que tiene valor para el usuario", dentro de este sistema se puede identificar como principal activo a la información. La información generada a partir de la actividad del usuario, pero también la información aportada directamente por éste, ya sea a través de sus datos personales, bancarios o de cualquier otra índole.

Así, disponemos de un "Sistema de IoT" que pertenece a un usuario y cuyo principal activo es la información. Por tanto, si entendemos este sistema como un sistema de información, en términos de activos del sistema de información es posible distinguir:

- Al usuario.
- La información.
- El software (sistema operativo y aplicaciones).
- Hardware.
- Comunicaciones.

Además, hay que tener en cuenta que todo sistema de información debe:

- Salvaguardar la propiedad de la información.
- Mantener la integridad de la información.
- Asegurar la confidencialidad de la información.
- Garantizar la disponibilidad de la información.
- Llevar a cabo los fines del usuario, es decir, ser eficiente en el sentido de que debe cumplir los objetivos del usuario.

Precisamente, la gestión de la seguridad de la información se centra en preservar las tres dimensiones de seguridad principales asociadas a la información, que son según AENOR:

- Disponibilidad. Asegurar que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.
- Confidencialidad. Asegurar que la información es accesible solo para aquellos autorizados a tener acceso.
- Integridad. Garantizar la exactitud y completitud de la información y los métodos de su proceso.

La información se encuentra expuesta a riesgos, entendiendo riesgo como la probabilidad de amenazas a los activos que utilicen las vulnerabilidades (debilidades) y se produzcan impactos negativos. El análisis del riesgo y la implantación de controles son la herramienta primordial para mitigar el riesgo. Y aunque el riesgo siempre existe, éste se puede mitigar, siendo su mitigación el objetivo de aplicar controles de seguridad.

Una de las prioridades desde el punto de vista de negocio es el Time to Market, pues lo deseado es que el usuario que compra un producto, pueda usarlo desde el minuto 1 sin necesidad de conocimientos específicos o configuraciones, lo que muchas veces implica que este efecto Plug&Play, vaya en detrimento de la seguridad a través de configuraciones estándar "débiles".

En gran parte de los casos, los dispositivos se fabrican sin tener en cuenta la seguridad y a medida que se ha añaden funcionalidades, inteligencia y conexión a Internet, se van adaptando, cuando lo ideal sería que se tuviera en cuenta durante la fabricación de estos, desde el inicio del diseño.

4.2. DIFICULTADES DE NEGOCIO

Una de las prioridades desde el negocio es el "Time to Market", pues se desea que el usuario que compra un producto, pueda usarlo desde el primer minuto sin necesidad de conocimientos específicos o configuraciones, lo que muchas veces implica que este efecto Plug&Play vaya en detrimento de la seguridad a través de configuraciones estándar "débiles".

En gran parte de los casos, los dispositivos se fabrican sin tener en cuenta la seguridad, y a medida que se añaden funcionalidades se van adaptando, cuando lo ideal sería que se tuviera en cuenta durante la fabricación de éstos, desde el inicio del diseño.

4.3 CONCIENCIACIÓN

Además de las medidas a tomar por parte de los fabricantes, también es necesario que los usuarios se preocupen por las cuestiones de seguridad y privacidad de los productos que adquieren; antes , durante y después de la compra.

Debemos como consumidores conocer sobre qué preguntar (riesgos, facilidades,..), interesarnos por las respuestas, decidir responsablemente si lo adquirimos y, una vez adquirido debemos ser conscientes que debemos instalarlo y mantenerlo de tal forma que sea seguro para nosotros. Cuanto más exijamos con conocimiento, los fabricantes más invertirán en seguridad y usabilidad de la misma.

Finalmente, debemos usar los dispositivos de una forma segura y que nos garantice preservar la privacidad de la información ya sea en los propios dispositivos, en nuestra red doméstica, en servicios en la nube o en redes sociales.

Es muy importante que se realice una concienciación social, que todos y cada uno de los usuarios tengan el conocimiento suficiente para realizar sus actividades del modo más seguro.

4.4 ESTÁNDARES DE CALIDAD

Es muy importante que los posibles problemas, las buenas prácticas y controles asociados a las vulnerabilidades mencionadas, se traten de manera general siguiendo las recomendaciones de seguridad.

Los estándares de calidad o sellos de confianza son un mecanismo muy adecuado de establecer un marco de referencia donde confluyen usuarios, fabricantes y desarrolladores. De este modo, todos los productos quedan bajo unos estándares que aseguran unos parámetros mínimos de calidad y seguridad.

El Centro de estudios de Movilidad e Internet de las cosas (CemIoT), de ISMS Forum, con sus expertos de los grupos de Privacidad y Legalidad, Sensibilización y Amenazas (Hacking), Buenas prácticas y Marca de Garantía, a lo largo de los próximos capítulos desgranan los principales hitos a tener en cuenta.

BLOQUE II:
ANÁLISIS DE LOS VECTORES DE ATAQUE DEL INTERNET DE LAS COSAS (IOT)

1. VECTORES DE ATAQUE

El presente documento tiene como objeto identificar y definir las áreas de análisis asociadas a la superficie de exposición y a los vectores de ataque propios de los dispositivos IoT, con el propósito de poder evaluar las potenciales debilidades y vulnerabilidades de seguridad y/o privacidad que afectan a este tipo de dispositivos y a sus servicios o plataformas asociadas.

El conjunto de áreas de análisis identificadas en los siguientes apartados permitiría evaluar de manera global la seguridad de cualquier dispositivo o solución IoT, pudiendo existir vulnerabilidades de seguridad comunes entre diferentes áreas, como por ejemplo debilidades en los mecanismos de autentificación, autorización, cifrado (en reposo y en tránsito), tanto en el interfaz web de gestión del dispositivo IoT, como en su comunicación con "la nube" o con aplicaciones móviles, en otros servicios de red que éste proporciona, etc.

Los distintos vectores de ataque asociados a un dispositivo IoT se pueden agrupar en las siguientes categorías, según su naturaleza. Asimismo, estos reflejan la posible aproximación que podría tomar un potencial atacante a la hora de intentar vulnerar la seguridad de los mismos, y la privacidad de su propietario o de sus usuarios, o a la hora de encontrar debilidades en sus mecanismos de seguridad, en caso de disponer de alguno:

• VECTOR DE ATAQUE FÍSICO

Aquellos ataques que requieren de acceso físico al dispositivo: puertos o interfaces USB, Ethernet, HDMI, serie, consola, depuración, JTAG, etc., o botones que cambian el comportamiento del dispositivo (por ejemplo, activación de WPS). Estos ataques suelen tener como fin obtener información almacenada localmente en el dispositivo, como pueda ser el firmware o las claves de cifrado de las comunicaciones almacenadas en una memoria flash, o disponer de acceso privilegiado al mismo.

Este vector de ataque se describe en detalle en los apartados 2.1 y 2.2, asociados al análisis de los puertos de conexión y del firmare del dispositivo IoT, respectivamente. Debe tenerse en cuenta que el firmware del dispositivo IoT puede ser analizado sin disponer de acceso físico al mismo, por ejemplo, obteniendo una copia desde la web de soporte del fabricante, empleada para distribuir imágenes o actualizaciones de firmware.

• VECTOR DE ATAQUE SOBRE LAS COMUNICACIONES

Aquellos ataques cuyo objetivo es uno o varios protocolos o tecnologías de comunicación del dispositivo con un tercero (otro dispositivo IoT, un controlador o hub, un dispositivo o aplicación móvil, servicios remotos en redes internas o en "la nube", etc.). Los ataques a las comunicaciones suelen tener como fin la interceptación para poder analizar los datos intercambiados (eavesdropping), así como la manipulación de los datos y de las capacidades de señalización (para cometer fraude, denegación de servicio (DoS), suplantación, etc.).

Como la variedad de protocolos de comunicación empleados en el mundo IoT es muy amplia, a su vez se clasificarán las comunicaciones según el medio de transmisión: ondas que viajan por el aire libre (radio frecuencia o RF) o mediante una conexión física empleando un cable. Dentro de las comunicaciones inalámbricas o de radio, se volverá a distinguir entre aquellas que utilizan bandas de frecuencias libres (o no licenciadas) y para las que no es necesario por tanto disponer de una licencia para transmitir y recibir datos, de aquellas comunicaciones comerciales (o reguladas) que sí requieren disponer de una licencia para poder transmitir y recibir datos.

1. Comunicaciones cableadas
Si el dispositivo está conectado por una conexión mediante un cable físico (USB, Ethernet, HDMI, serie, etc.).

2.Comunicaciones inalámbricas
En función de la tecnología de radio frecuencia empleada. A su vez se pueden clasificar en:

2.1 No licenciadas
Bluetooth, Bluetooth Low Energy (BLE), Wi-Fi, Z-Wave, LoRa, LoRaWan, SigFox, etc., y otros mecanismos de comunicación propietarios (ej. habitualmente empleando las frecuencias de 433 y 868 MHz en Europa).

2.2 Licenciadas
Comunicaciones móviles (2/3/4G), LPWA, WiMax, etc. Este vector de ataque se describe en detalle en los apartados 2.3, 2.4 y 2.5, correspondientes a las comunicaciones entre el dispositivo IoT y servidores remotos en "la nube", comunicaciones con dispositivos y aplicaciones móviles, y comunicaciones inalámbricas, respectivamente.

• VECTOR DE ATAQUE SOBRE LAS CAPACIDADES DE GESTIÓN

Aquellos ataques cuyo objetivo son los mecanismos de gestión locales de los propios dispositivos IoT. En determinadas circunstancias los ataques pueden ser también lanzados contra la pla-

taforma y/o capacidades de gestión remota de los dispositivos, escenario que tiene asociado un mayor impacto, ya que podría dejar a todos los dispositivos de un mismo tipo o entorno desconectados de su servicio de gestión central e incomunicados entre sí, y sin posibilidad de ser reconfigurados y monitorizados.

Este vector de ataque se describe en detalle en el apartado 1.6, asociado al interfaz web y otros interfaces de gestión del dispositivo IoT.

• VECTOR DE ATAQUE SOBRE LOS SERVICIOS Y/O DATOS

Aquellos ataques dirigidos hacia los datos que recoge el dispositivo o la plataforma IoT asociada, caracterizados por estar almacenados en el propio dispositivo o en servidores centrales, y sus servicios asociados. En determinadas circunstancias, como las pulseras inteligentes (de salud o deportivas) que recogen información sobre la salud y/o estado físico de sus usuarios, el objetivo del ataque se centra en obtener los datos e información privada recolectada previamente.

Este vector de ataque se describe en detalle en los apartados 1.7 y 1.8, asociados al análisis de otros servicios de red y de las capacidades de almacenamiento local de datos e información del dispositivo IoT, respectivamente.

La clasificación planteada pretende ofrecer una visión general de las áreas de exposición de los dispositivos IoT. Debido a las relaciones existentes entre sus diferentes componentes, debe tenerse en cuenta que hay solapamientos y relaciones intrínsecas entre las diferentes áreas, ya que, por ejemplo, hay funcionalidades de gestión tanto en el acceso físico al dispositivo (ej. un interfaz de consola o debug) como en sus comunicaciones (ej. un interfaz de gestión web).

pamientos y relaciones intrínsecas entre las diferentes áreas, ya que, por ejemplo, hay funcionalidades de gestión tanto en el acceso físico al dispositivo (ej. un interfaz de consola o debug) como en sus comunicaciones (ej. un interfaz de gestión web).

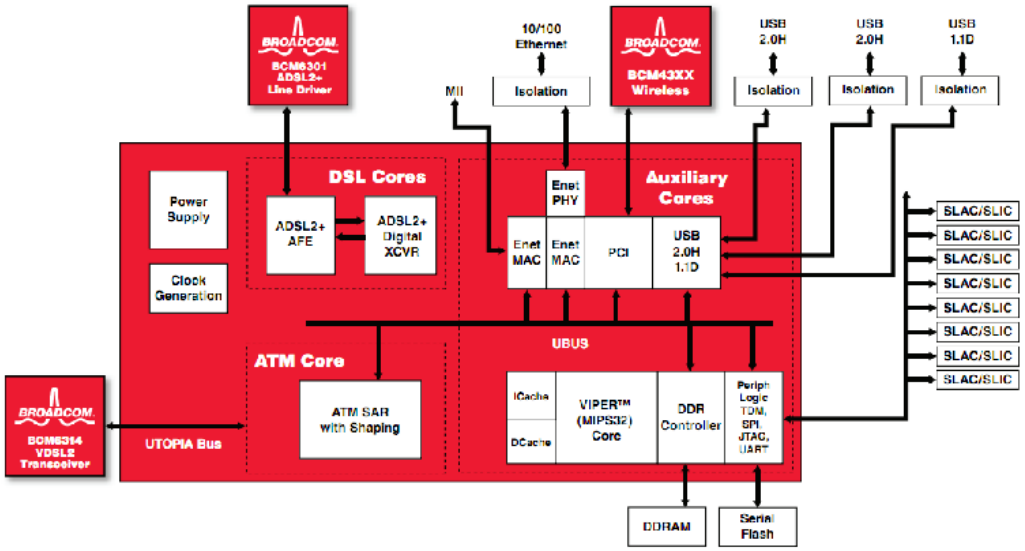
Por tanto, los vectores de ataque se han englobado dentro de una categoría según su objetivo principal (ej. ataque sobre las capacidades de gestión del dispositivo), siendo conscientes de que existen otras posibilidades y criterios para la clasificación de los mismos.

Los siguientes apartados detallan los vectores de ataque para cada una de las categorías definidas anteriormente.

1.1 PUERTOS DE CONEXIÓN DEL DISPOSITIVO IOT

1.1.1 DESCRIPCIÓN Y OBJETIVOS DEL VECTOR DE ATAQUE

Como punto de inicio en el estudio de un dispositivo IoT, se debe proceder a reconocer los elementos físicos y componentes que forman parte del dispositivo, en lo que se conoce como obtención de información (information gathering). En esta fase del ataque el objetivo es reunir toda la información posible acerca del dispositivo bajo estudio; memorias instaladas en la placa base (FLASH, ROM, SSD, etc.), microcontroladores, chips de los interfaces de comunicación, antenas y, por supuesto, cualquier tipo de interfaz que aporte comunicación con el dispositivo, como puede ser un interfaz de depuración JTAG, consola, puerto serie, Ethernet, USB o micro USB, etc. Suele ser muy común en este tipo de ataques comenzar realizando un esquema de los componentes del dispositivo lo más exacto posible que permita reconocer el funcionamiento del mismo y su arquitectura, a partir del cual se identificarán los siguientes elementos que pueden ser atacados, en busca de más información detallada sobre estos. A modo de ejemplo se puede ver a continuación el esquema de un router doméstico de líneas xDSL generado tras una revisión exhaustiva del dispositivo:



Fuente: http://www.redeszone.net/huawei/hg556a/

Dependiendo del tipo de dispositivo que se analice, se puede establecer una primera gran diferenciación en dos tipos de dispositivos: aquellos que tienen algún tipo de protección física o lógica más avanzada contra potenciales atacantes que accedan al dispositivo sin el conocimiento o herramientas adecuadas (en inglés anti-tampering o sabotage detection) y aquellos otros dispositivos que no presentan estas contramedidas. Por otro lado, se pueden encontrar dispositivos que almacenan datos totalmente o parcialmente cifrados en las memorias de almacenamiento como una posible contramedida adicional contra el acceso no autorizado a los datos críticos que maneja el dispositivo.

Una medida empleada en los primeros terminales móviles era el uso de tornillos distintos y de un tamaño muy reducido respecto a los habituales, como medida disuasoria para evitar que el usuario pudiera abrir el dispositivo con el objetivo de identificar la composición interna del mismo o manipularlo, lo que se considera como una medida más contra acceso inapropiados al dispositivo.

A día de hoy, los terminales de punto de venta (TPV) o alarmas para el hogar son claros ejemplos de dispositivos que incorporan contramedidas similares, borrando el contenido de las memorias al abrir el dispositivo físicamente, para evitar así fugas de información confidencial.

En este vector de ataque también se englobaría cualquier botón del dispositivo IoT que permita o facilite cambiar el comportamiento o funcionamiento del dispositivo, y que pueda permitir disponer de acceso privilegiado al mismo. Por ejemplo, el botón de activación de WPS asociado a las capacidades Wi-Fi del dispositivo puede permitir el acceso Wi-Fi al mismo, o un botón de reset que puede permitir que se haga uso de una configuración insegura o que se arranque en un modo especial privilegiado desde el gestor de arranque del dispositivo.

Una medida empleada en los primeros terminales móviles era el uso de tornillos distintos y de un tamaño muy reducido respecto a los habituales, como medida disuasoria para evitar que el usuario pudiera abrir el dispositivo con el objetivo de identificar la composición interna del mismo o manipularlo, lo que se considera como una medida más contra acceso inapropiados al dispositivo.

A día de hoy, los terminales de punto de venta (TPV) o alarmas para el hogar son claros ejemplos de dispositivos que incorporan contramedidas similares, borrando el contenido de las memorias al abrir el dispositivo físicamente, para evitar así fugas de información confidencial.

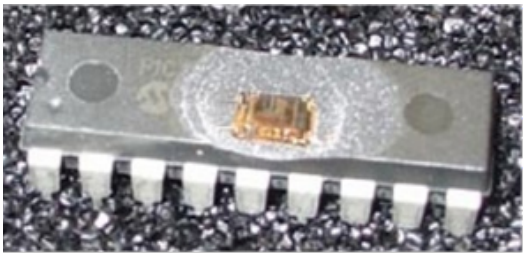
En este vector de ataque también se englobaría cualquier botón del dispositivo IoT que permita o facilite cambiar el comportamiento o funcionamiento del dispositivo, y que pueda permitir disponer de acceso privilegiado al mismo. Por ejemplo, el botón de activación de WPS asociado a las capacidades Wi-Fi del dispositivo puede permitir el acceso Wi-Fi al mismo, o un botón de reset que puede permitir que se haga uso de una configuración insegura o que se arranque en un modo especial privilegiado desde el gestor de arranque del dispositivo.

1.1.2 TÉCNICAS Y HERRAMIENTAS DE ATAQUE

Una vez se obtiene acceso físico al dispositivo IoT, se puede proceder con las siguientes fases de análisis que forman parte de un proceso habitual de ataque de hardware hacking:

1. Análisis de los componentes mediante hardware teardown (desmontando el hardware).
2. Análisis de los puertos e interfaces de conexión, tanto internos como externos.
3. Ingeniería inversa del firmware (ver apartado 2.2).
4. Silicon die analysis (desmontar el silicio).

Como se puede ver, en los casos de análisis más avanzados se podría incluso llegar a desoldar componentes y atacar, química o físicamente, sus circuitos para poder analizar las pistas y entender así como la información es intercambiada entre los distintos componentes:



Fuente: http://www.grandideastudio.com

El estudio de los puertos e interfaces de conexión internos y externos se centra en el reconocimiento de elementos que permitan interactuar con partes o con todo el dispositivo: JTAG, consola, serie, Ethernet, USB o micro USB, I2C, SPI, CAN, smartcard, etc. Para todos aquellos puertos o interfaces no estándar de depuración, es muy habitual el estudio de las señales mediante osciloscopios, analizadores lógicos o sniffers dedicados.

Por otro lado, exponer un puerto USB sin las medidas de seguridad apropiadas puede permitir, no sólo el arranque de otros sistemas operativos desde dispositivos de almacenamiento externos, como puede ocurrir en un ordenador, sino también el uso de binarios o ficheros creados especialmente para encontrar o explotar fallos de programación en el firmware del dispositivo.

En el estudio realizado por Collin Mulliner y Benjamin Micheleen del año 2012 sobre ataques basados en emulación de dispositivos de almacenamiento a televisores inteligentes (Smart TV), se demostró que aprovechando estos fallos de seguridad se podía ejecutar código con privilegios en los televisores. Estos ataques también son ampliamente explotados en las videoconsolas, donde el código malicioso se almacena en tarjetas de almacenamiento externas para explotarlo con el uso de determinados videojuegos vulnerables a dicho código.

Los puertos serie de consola accesibles pueden permitir acceso inmediato al dispositivo con un usuario privilegiado. En algunos modelos de drones recientes, el puerto micro USB puede ser utilizado no sólo para recargar la batería, sino también para acceder a un modo consola conectándolo mediante un adaptador específico a un puerto serie de un ordenador, conocido como “USB to Serial FTDI conversion board”.

En otros dispositivos, los puertos de consola pueden encontrarse tras un puerto serie común, mediante conectores RS-232 o RJ-45.

Ataques más sofisticados pueden combinar varios de estos puertos, como por ejemplo el ataque al frigorífico "LG Smart Refrigerator" mostrado en la conferencia DefCon 22, donde se mostró como conectándose en primer lugar al pinout UART se podía abrir una sesión con permisos privilegiados, para posteriormente introducir una unidad USB y cargar desde ésta nuevo código, desde el cual se podía abrir una nueva sesión con acceso total al sistema operativo y a las aplicaciones de desarrollo.

Por último, los interfaces de red Ethernet o Wi-Fi, pueden dejar accesibles portales web de administración del equipo. Dichos interfaces web pueden presentar vulnerabilidades web comunes (XSS, CSRF, inyecciones SQL, etc.) que al ser explotadas podrían permitir ejecutar código en el dispositivo con privilegios o acceder a información de una base de datos (ver apartado 2.6).

En mayo del año 2015 un grupo de investigadores españoles publicaron un extenso listado de vulnerabilidades que afectaban a 22 modelos de routers domésticos (SOHO). Casi al mismo tiempo, aparecía en varias webs públicas código malicioso que intentaba explotar vulnerabilidades parecidas sobre distintos routers, para finalmente efectuar un ataque de envenenamiento DNS.

Este mismo tipo de errores también está muy presente en cámaras de vigilancia de todo tipo (monitores para bebes, cámaras web, cámaras de video vigilancia, etc.), donde para algunas smartcams, como la "Samsung SmartCam", se han publicado bugs en ciertas versiones que permiten cambiar la contraseña de administración sin conocer la contraseña anterior, pudiendo así ganar acceso privilegiado a la cámara.

1.1.3 EJEMPLOS DE VULNERABILIDADES Y/O INCIDENTES IOT EMPLEANDO ESTE VECTOR DE ATAQUE

A continuación, se listan ejemplos de estos ataques que han permitido aplicar técnicas de ingeniería inversa sobre (referencias):

"Read It Twice! A mass-storage-based TOCTTOU attack", Collin Mulliner y Benjamin Michele, USA Agosto 2012:
http://www.mulliner.org/collin/

Estudio de múltiples dispositivos IoT, incluido el refrigerador LG: "Hack All The Things: 20 Devices in 45 Minutes", CJ Heres, Amir Etemadieh, Mike Baker, Hans Nielsen, USA Agosto 2014:
https://www.defcon.org/html/defcon-22/dc-22-speakers.html#Heres

Estudio de femtocelda realizado por el grupo THC en 2009. Apartado "4" dedicado al estudio del hardware que compone el dispositivo:
https://wiki.thc.org/vodafone

Algoritmos propietarios como el CRYPTO1, perteneciente a las tarjetas NFC Mifare Classic, hasta desvelar dicho algoritmo a la perfección:
https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf

Estudio del algoritmo CRYPTO1 por Karsten Nohl y Henryk Plötz publicado en 2007, para el cual se realizó la ingeniería inversa del algoritmo mediante análisis hardware, llegando a reconstruir las pistas de los circuitos identificando puertas lógicas, etc.:
https://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html

Estudio de alarma de uso doméstico, para el cual se recurre al análisis hardware del dispositivo en varias ocasiones:
https://funoverip.net/2014/11/reverse-engineer-a-verisure-wireless-alarm-part-1-radio-communications/

Estudio de diversos dispositivos IoT y sus vulnerabilidades, así como pinouts y diagramas, fruto de la conferencia "Hack All The Things: 20 Devices in 45 minutes" de la DefCon 22:
https://www.exploitee.rs/index.php/Main_Page

1.2 FIRMWARE DEL DISPOSITIVO IOT

1.2.1 DESCRIPCIÓN Y OBJETIVOS DEL VECTOR DE ATAQUE

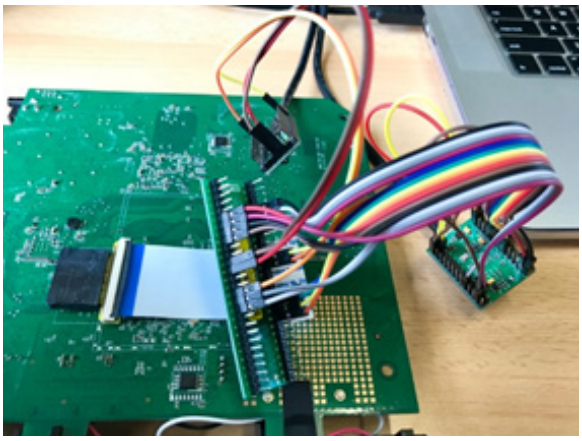
Se podría definir el firmware del dispositivo IoT como la capa software de más bajo nivel que interactúa directamente con el hardware y que puede incluir una o varias capas superiores que amplían las funcionalidades del hardware. En el caso concreto de los dispositivos IoT, actualmente hay bastante heterogeneidad en el conjunto de firmware y sistemas operativos disponibles, adaptándose a las capacidades del dispositivo sobre el que se encuentra instalado. Mayoritariamente están basados en versiones ligeras del kernel de Linux con las funcionalidades básicas, según el tipo de dispositivo IoT.

Mediante el estudio del firmware es posible encontrar diferentes vectores de ataque con los que se puede permitir, desde encontrar credenciales por defecto para alguno de los servicios disponibles en el dispositivo IoT, hasta descubrir puertas traseras creadas por el fabricante para poder llevar a cabo tareas de depuración o disponer de un acceso privilegiado, y que se han olvidado de eliminar en la versión de producción.

1.2.2 TÉCNICAS Y HERRAMIENTAS DE ATAQUE

Para obtener el firmware de un dispositivo IoT, existen varios métodos. Por un lado, se puede extraer directamente del dispositivo IoT mediante acceso físico al mismo empleando algún método de conexión cableada (habitualmente puertos USB, serie, consola, depuración, JTAG, etc.) o inalámbrica (menos habitual, Wi-Fi, Bluetooth, etc.). Por otro lado, se puede conseguir directamente desde la propia web de soporte del fabricante, donde en ocasiones se permite su descarga para la actualización/reinstalación del mismo.

Una vez obtenido el firmware se puede comprobar que tipo de sistema de ficheros utiliza (Squashfs, Cramfs, YAFFS2, etc.). Para obtener una lista completa de los sistemas de ficheros más comunes en dispositivos embebidos basados en Linux se recomienda consultar “http://elinux.org/File_Systems”. Una vez se identifica el tipo de sistema de ficheros, se puede usar la aplicación Binwalk con el objetivo de saber la dirección exacta donde se encuentra el sistema de ficheros dentro del firmware, para posteriormente montar una copia del mismo y tener acceso completo al sistema de ficheros utilizado por el dispositivo IoT.



Fuente: https://www.mdsec.co.uk

El firmware también suele estar comprimido para ahorrar espacio. Los métodos de compresión más usados comúnmente son LZMA, GZIP, Zlib, Zip, ARJ, etc. En este caso, se debe de buscar la dirección de memoria donde se encuentra el “número mágico” donde comienza el sistema de ficheros, para posteriormente copiarlo usando el comando de Linux dd. Otra opción, si se conoce el sistema de ficheros, sería utilizar herramientas creadas específicamente para extraerlo en ese formato. Por ejemplo, para el sistema de ficheros squashfs, se puede utilizar la herramienta unsquashfs. Una vez extraído el sistema de ficheros, se podrían buscar contraseñas escritas en texto claro, así como fallos de seguridad realizando un análisis estático de código de los ficheros binarios utilizados por el sistema embebido, o un análisis detallado de sus ficheros de configuración.

Otro componente crítico del dispositivo IoT es el gestor de arranque o bootloader, que se inicia en primer lugar al arrancar el dispositivo y que ejecuta posteriormente el firmware.Los bootloaders más conocidos son Das uboot, Redboot y CFE.

Para obtener más información acerca de los bootloaders en dispositivos embebidos basados en Linux se recomienda consultar “http://www.informit.com/articles/article.aspx?p=1647051”.

En caso de que el firmware se encuentre cifrado, habría que obtener las claves con las que ha sido cifrado y descifrarlo, antes de poder realizar los pasos descritos anteriormente.

Si el firmware se encuentra firmado criptográficamente, sólo va a ser posible instalar un firmware en el dispositivo IoT que haya sido firmado previamente por el fabricante, lo que a priori dificultaría bastante la posibilidad de instalar un firmware modificado, salvo que se identifiquen vulnerabilidades en el proceso de generación o verificación de la firma.

Si fuera posible realizar una actualización del firmware de forma online (es decir, descargándola directamente de la web del fabricante desde el dispositivo IoT), se debe comprobar si la conexión se realiza de forma segura (cifrada, mediante HTTPS) o insegura (en claro), y qué parámetros se tienen en cuenta tanto en el dispositivo IoT como en el servidor para permitir la actualización. Como ya se ha comentado anteriormente, también habría que verificar si el firmware está firmado o no, ya que se podría suplantar el firmware mientras es descargado al dispositivo IoT. También se debe de comprobar si modificando la fecha del dispositivo, o las referencias de fecha del tráfico intercambiado, es posible instalar una versión de firmware anterior (y posiblemente vulnerable), para luego explotar alguna vulnerabilidad conocida y obtener acceso sobre el dispositivo IoT.

Complementariamente al análisis del firmware, algunos dispositivos IoT permiten guardar una copia de seguridad de la configuración. En caso de que esta copia de seguridad no se guarde firmada y/o cifrada, cabría la posibilidad de modificar la configuración completa del dispositivo IoT alterando el fichero o ficheros de la copia de seguridad.

1.2.3 EJEMPLOS DE VULNERABILIDADES Y/O INCIDENTES IOT EMPLEANDO ESTE VECTOR DE ATAQUE

Una de las vulnerabilidades más importantes conocidas mediante el estudio del firmware es la denominada "Misfortune Cookie" (CVE-2014-9222). Esta vulnerabilidad se encontró en la gestión de la cookie HTTP del servidor web RomPager por debajo de la versión 4.34, que se encuentra embebido en varios routers. Se descubrió que era posible corromper la memoria del servidor web, enviando paquetes con cookies HTTP especialmente manipuladas, pudiendo escribir hasta 40 bytes en memoria. Fue publicada por Shahar Tal y Lior Oppenheiml (Checkpoint) en la presentación "Too Many Cooks: Exploiting the Internet of TR-069 Things" dn la conferencia CCC (31C3) de Hamburgo. Con la explotación exitosa de esta vulnerabilidad, fue posible evadir el control de acceso al interfaz web y posteriormente tomar el control del dispositivo afectado.

Referencias:

http://mis.fortunecook.ie/too-many-cooks-exploiting-tr069_tal-oppenheim_31c3.pdf

https://www.nccgroup.trust/globalassets/our-research/uk/whitepapers/2015/10/porting-the-misfortune-cookie-exploit-whitepaperpdf/

http://cawanblog.blogspot.com.es/2015/02/misfortune-cookie-cve-2014-9222.html

Otro ejemplo de vulnerabilidades encontradas y explotadas por medio del análisis del firmware (DWR-932_fw_revB_2_02_eu_en_20150709.zip) son las asociadas al router Dlink DWR-932B, en el que se han encontrado:

- Cuentas de usuarios para el acceso mediante puertas traseras.
- Puertas traseras.
- PIN WPS Wi-Fi por defecto.
- Generación del PIN WPS Wi-Fi débil.
- Múltiples vulnerabilidades en el servidor HTTP (qmiweb).
- Posibilidad de actualizaciones FOTA (Firmware Over The Air) remotas inseguras.
- Seguridad eliminada en el protocolo UPnP.
- Y en general, malas prácticas de seguridad.

Cabe destacar especialmente las vulnerabilidades de cuentas de usuario para el acceso a puertas traseras en telnet y SSH con credenciales por defecto admin:admin y root:1234. También es reseñable una puerta trasera que habilita el puerto telnet con permisos de root al enviar el string "HELODBG" al puerto UDP/39889. Y aunque la descarga del firmware FOTA (Firmware Over The Air) se realiza por medio de HTTPS, las credenciales por defecto se encuentran guardadas en el propio firmware (credenciales: qdpc:qdpc, qdpe:qdpe, qdp:qdp) y además el certificado digital empleado caducó en mayo de 2014.

Referencias:

https://pierrekim.github.io/blog/2016-09-28-dlink-dwr-932b-lte-routers-vulnerabilities.htm

Un ejemplo concreto reciente de extracción del firmware mediante la conexión a un puerto o interfaz UART interno del dispositivo Wi-Fi Virgin Super Hub 2ac, que permite el acceso a su memoria NAND flash, para su posterior análisis:

Referencias:

https://www.mdsec.co.uk/2017/09/extracting-firmware-from-the-virgin-super-hub-2ac/

1.3 COMUNICACIONES ENTRE EL DISPOSITIVO IOT Y "LA NUBE" (CLOUD)

1.3.1 DESCRIPCIÓN Y OBJETIVOS DEL VECTOR DE ATAQUE

Tradicionalmente, los dispositivos embebidos o IoT podían ser accedidos remotamente para su administración, gestión y control, o para la obtención o modificación de los datos asociados a su funcionalidad, facilitando su manejo a través de Internet (u otras redes de datos, típicamente TCP/IP) sin necesidad de que el propietario estuviese presente en la misma red local.

Para ello, se disponía fundamentalmente de dos opciones. Por un lado, podían abrirse los puertos TCP y/o UDP correspondientes a sus interfaces de gestión, como por ejemplo hacia su servidor y aplicación web en los puertos TCP/80 (HTTPS) y/o TCP/443 (HTTPS), en los dispositivos perimetrales de la red en la que se encontraban ubicados (ver apartado 2.7). El riesgo principal de seguridad de esta alternativa era que dichos puertos estaban abiertos permanentemente, y normalmente accesibles desde cualquier dirección IP origen, ya que el propietario del dispositivo requería disponer de acceso a los mismos desde diferentes ubicaciones y, por tanto, direcciones IP (como por ejemplo desde la oficina, desde su hogar, o desde un navegador web asociado a su dispositivo móvil, estando conectado a una red Wi-Fi o a la red de datos móviles 2/3/4G). Por otro lado, podía configurarse una gestión dinámica de puertos a través de protocolos como UPnP (Universal Plug and Play), opción que tampoco está exenta de vulnerabilidades y debilidades de seguridad.

Cuando se popularizaron los servicios en "la nube" (cloud), se generalizó la integración directa de los dispositivos IoT con los servicios remotos proporcionados a través de "la nube", existiendo numerosas soluciones, estándar o propietarias, según el fabricante del dispositivo. El uso de los servicios en "la nube" para la administración, gestión y control remoto del dispositivo IoT, o para la obtención de datos asociados a su funcionalidad (manual o automáticamente), no requiere abrir puertos previamente en el perímetro de la red dónde está ubicado el dispositivo ni hacer uso de UPnP, por lo que a priori se considera una solución más segura. En su lugar, es el propio dispositivo el que, de forma autónoma, y habitualmente de manera muy frecuente, actúa como cliente y contacta periódicamente con los servidores asociados al servicio en "la nube" para proporcionar datos e información recolectada durante su funcionamiento, o para permitir su gestión remota desde, por ejemplo, un navegador web estándar o una aplicación móvil específica asociada (ver apartado 2.4).

Este cambio en la filosofía de acceso remoto al dispositivo IoT hace que este juegue más un papel (o role) de cliente, iniciando y estableciendo las conexiones hacia el servicio en "la nube" (aunque dicha conexión permita también acceder remotamente al dispositivo como servidor), en lugar de un papel (o role) de servidor o servicio, escuchando y esperando a recibir conexiones por parte de otros clientes (asociado al modelo más tradicional de acceso).

La seguridad de esta integración entre el dispositivo IoT y los servicios en "la nube" depende de los requisitos de diseño identificados por el fabricante, y de su implementación, especialmente a la hora de llevar a cabo el proceso de registro (y de cancelación del registro) del dispositivo, que típicamente está asociado a un identificador de usuario en la plataforma residente en "la nube", el proceso de autentificación para la gestión o para la obtención de datos de los diferentes dispositivos IoT asociados a ese servicio, los mecanismos de comunicación entre el dispositivo IoT y el servicio, etc. Las capacidades de comunicación empleadas deberían hacer uso de canales autentificados y cifrados de manera robusta, donde también se verifica la integridad de los datos inter-

cambiados, y protegidos frente a ataques, por ejemplo, de suplantación o de repetición (replay). Se recomienda que el dispositivo IoT y/o el servicio en "la nube" proporcionen ajustes de configuración que permitan al propietario restringir las capacidades de interacción entre ambos, y que no permitan relajar el nivel de seguridad existente por defecto de los mismos.

Adicionalmente a las consideraciones de seguridad mencionadas, deben tenerse en cuenta las implicaciones asociadas desde el punto de vista de la privacidad del usuario, siendo relativamente habitual que los dispositivos desvelen y envíen más información de la necesaria sobre el propio usuario, los patrones de uso del dispositivo, y la información que éste recopila y envía hacia los servicios en "la nube". Se recomienda que el dispositivo IoT y/o el servicio en "la nube" proporcionen ajustes de configuración que permitan al propietario restringir y definir los datos intercambiados que afectan a su privacidad.

Como resultado, en la actualidad han surgido numerosas plataformas y servicios en "la nube" dirigidos específicamente al ecosistema IoT como, por ejemplo, Amazon AWS IoT, Microsoft Azure IoT Suite, Google Cloud IoT, Thing+, ThingWorx, IBM Watson IoT, etc.

1.3.2 TÉCNICAS Y HERRAMIENTAS DE ATAQUE

Para analizar, en primer lugar, y poder llevar a cabo ataques sobre las capacidades de integración entre el dispositivo IoT y el servicio en "la nube", al estar este último disponible remotamente y accesible a través de las redes de comunicaciones e intercambio de datos, basadas principalmente en TCP/IP, es necesario estudiar sus comunicaciones.

Para ello, por un lado, es posible capturar sus comunicaciones mediante un sniffer de red (por ejemplo, Wireshark) y estudiar todos los detalles asociados, intentando responder a algunas de las 5 W (en inglés):

- **What?:** ¿Qué protocolos son empleados, tanto estándar - HTTP(S), WebSockets o HTTP2 - como propietarios? y ¿qué información es intercambiada? y…
- **How?: …** ¿cómo es intercambiada esta información: en claro, codificada, cifrada, etc.?
- **Who?:** ¿Con quién se comunica el dispositivo IoT, incluyendo todos los servicios remotos en "la nube" y sus servidores asociados, aplicaciones moviles u otros destinos?
- **When?:** ¿Con qué frecuencia y cuándo se comunicaciones utiliza, ya que puede haber ciertos datos o funcionalidades que sólo están disponibles a través de ciertas capacidades de comunicación: Bluetooth, Wi-Fi, redes de telefonía móvil, interfaz LAN cableado, etc.?
- **Why?:** ¿Con qué propósito se comunica el dispositivo IoT con el servicio en "la nube" y otros destinos: envío de datos recolectados, estadísticas de uso, funcionalidad de gestión, etc.?

Por otro lado, se recomienda realizar un análisis más avanzado mediante la interceptación del tráfico intercambiado entre el dispositivo IoT y el servicio en "la nube", mediante un proxy de interceptación (por ejemplo, OWASP ZAP, Burp o mitmproxy, en el caso de protocolos de texto como HTTP, o Mallory, en el caso de protocolos binarios). Este tipo de herramientas permiten no sólo interceptar las comunicaciones, sino también inspeccionarlas en detalle, descartarlas, modificarlas o reenviarlas, disponiendo de plenas capacidades para su manipulación (incluyendo tanto las peticiones originadas en el dispositivo IoT como las respuestas remitidas por el servicio en "la nube", y viceversa). Por tanto, permiten el descubrimiento y explotación de vulnerabilidades tanto en el dispositivo IoT como en el servicio en "la nube".

Dentro del análisis de las comunicaciones existentes entre el dispositivo IoT y los servicios en "la nube" es necesario evaluar los detalles técnicos asociados al establecimiento de túneles de comunicación cifrados y autentificados, por ejemplo, mediante TLS. Se deben estudiar los protocolos y algoritmos de cifrado e integridad soportados, el proceso de verificación de los certificados digitales (X.509) de confianza, y detalles más concretos, como por ejemplo la posibilidad de hacer uso de capacidades como PFS (Perfect Forward Secrecy) o certificate pinning, entre otras.

A la hora de identificar las vulnerabilidades de seguridad asociadas al tráfico y las comunicaciones de datos, no sólo es necesario analizar la interacción entre el dispositivo IoT y el servicio en "la nube", sino también la integración de ambos con las aplicaciones móviles que habitualmente constituyen el mecanismo de acceso y gestión principal por parte de su propietario (apartado 2.4).

Por último, los mecanismos de integración con servicios en "la nube" hacen habitualmente uso del protocolo OAuth2 para llevar a cabo los procesos de autentificación y/o autorización sin desvelar las credenciales del usuario a terceros, sino mediante tokens.

Se han identificado diferentes vulnerabilidades en el diseño e implementación de OAuth en múltiples implementaciones, por lo que su análisis forma también parte fundamental de la seguridad de la solución de integración en "la nube".

1.3.3 EJEMPLOS DE VULNERABILIDADES Y/O INCIDENTES IOT EMPLEANDO ESTE VECTOR DE ATAQUE

En los últimos años han sido publicados diferentes estudios de investigaciones de seguridad con ejemplos de vulnerabilidades asociadas a las comunicaciones existentes entre los dispositivos IoT y sus servicios en "la nube".

Por ejemplo, en febrero de 2015 se publicaron las implicaciones de privacidad asociadas a la comunicación entre las TV inteligentes (o Smart TVs) de Samsung y los servicios asociados en "la nube", en este caso de una empresa tercera denominada Nuance Communications, Inc. Se descubrió que la TV capturaba el sonido ambiente existente a su alrededor, incluyendo cualquier conversación personal u otra información sensible, y lo reenviaba al servicio en "la nube", con el objetivo teóricamente de hacer uso de sus capacidades de reconocimiento de voz, para poder recibir y procesar comandos enviados por su propietario. Debe tenerse en cuenta que estas TV disponen de dos micrófonos, uno en la propia TV y otro en el mando a distancia. Adicionalmente, debe tenerse en cuenta que las TV disponen también de una cámara, y de capacidades para el reconocimiento de gestos del propietario y reconocimiento facial, con implicaciones aún mucho más graves desde el punto de vista tanto de la privacidad como de la seguridad de su propietario.

Referencia:
https://news.samsung.com/global/samsung-smart-tvs-do-not-monitor-living-room-conversations

Por otro lado, en abril de 2015 se publicaron los riesgos de seguridad asociados al Internet of Toys (IoT), y más específicamente, a la funcionalidad Hello Barbie del popular juguete de Mattel. La muñeca, con capacidades Wi-Fi y de conexión a "la nube" puede mantener conversaciones en tiempo real con su propietario mediante la grabación y procesamiento del audio en tiempo real, tras su envío a los servicios asociados en "la nube" (que hacen uso de técnicas de inteligencia artificial para generar las respuestas). Estas capacidades han sido desarrolladas por ToyTalk, empresa colaboradora (o partner) de Mattel.

Referencia:
http://offers.bluebox.com/rs/080-XOX-229/images/wp-hello-barbie.pdf

Más recientemente, en mayo de 2016, se han publicado las implicaciones de seguridad en el diseño de ecosistemas IoT complejos, como el asociado a Samsung SmartThings, dónde algunas aplicaciones móviles disponían de más privilegios de los necesarios sobre los dispositivos IoT, la ausencia de protecciones en el subsistema empleado para la notificación de eventos, utilizado para las comunicaciones asíncronas entre los dispositivos IoT y las aplicaciones móviles, especialmente, para los eventos que incluyen información sensible, como códigos de acceso, o la posibilidad para un potencial atacante de obtener el token OAuth empleado por la plataforma para autentificar a los usuarios.

Referencia:
https://iotsecurity.eecs.umich.edu/

Por último, las implicaciones de seguridad de la integración de los dispositivos IoT y los servicios en "la nube" se ve reflejada en un incidente de junio de 2016, donde un usuario, tras adquirir un conjunto de cámaras de seguridad IP de Netgear, crear su cuenta online en el servicio asociado en "la nube", y probarlas, al no cumplir sus expectativas, las devolvió. Sin embargo, semanas después, recibió una notificación de movimiento por parte de una de las cámaras, descubriendo, que disponía de la capacidad de acceder y gestionar las cámaras a través de su cuenta en el servicio en "la nube", pero en su nueva ubicación asociada a su nuevo propietario. Es decir, el proceso de registro (o cancelación de registro) de los dispositivos IoT permitía que estuviesen asociadas a múltiples cuentas de usuario, y no elimina las vinculaciones previas, teniendo en cuenta que para el registro sólo es necesario conocer (o adivinar) el número de serie del dispositivo IoT.

Referencia:
https://www.reddit.com/r/privacy/comments/4ortwb/i_bought_and_returned_a_set_of_wifi_connected/

Fuente: Google

1.4 COMUNICACIONES ENTRE EL DISPOSITIVO IOT Y DISPOSITIVOS Y/O APLICACIONES MÓVILES

1.4.1 DESCRIPCIÓN Y OBJETIVOS DEL VECTOR DE ATAQUE

Los dispositivos móviles se están posicionando como los gestores centrales o "cerebros" del Internet de las cosas, por lo que reciben gran parte de la información generada por los distintos dispositivos IoT o incluso los controlan, mediante el envío de comandos e instrucciones. Esta comunicación se puede realizar directamente, siendo un elemento más de la red local de dispositivos IoT, o remotamente mediante servidores en "la nube" con los que se establezca la comunicación entre el dispositivo IoT y el dispositivo móvil (ver apartado 2.3).
Las vulnerabilidades o amenazas a las que se enfrentan los dispositivos y las aplicaciones móviles (apps) que controlan los dispositivos IoT son:

•Almacenamiento de datos y contraseñas de manera insegura: Si las apps que controlan dispositivos IoT almacenan usuarios y contraseñas de manera insegura pueden revelar las mismas a personas que tengan acceso al dispositivo móvil.

• Contraseñas por defecto conocidas: Tanto si la app se comunica directamente con los dispositivos IoT, como a través de servidores en "la nube", necesitará utilizar algún tipo de credenciales (usuario y contraseña) para poder acceder a los mismos. Si estas contraseñas están pre-configuradas por defecto, de forma que siempre son las mismas, o siguiendo patrones predecibles, supondrán un problema de seguridad si no son cambiadas a la hora de hacer el despliegue.

• Contraseñas débiles o ausencia de las mismas: Si las contraseñas empleadas son débiles, pueden resultar vulnerables frente a ataques de diccionario o fuerza bruta. Si las contraseñas no son necesarias, es aún peor, ya que cualquier dispositivo se podría conectar al dispositivo IoT sin ningún tipo de restricción.

• Mecanismos de recuperación de contraseñas inseguros: La gestión de la recuperación de las contraseñas en caso de olvido pueden dar lugar a suplantación de usuarios de no hacerse apropiadamente. Es conveniente que se utilicen sistemas basados en cuentas de correo o números de teléfono configurados con anterioridad y bajo el estricto control del usuario.

• Comunicación entre el móvil y los dispositivos IoT: La comunicación que se establece entre los dispositivos IoT y el móvil debe estar correctamente protegida. De no ser así, un atacante podría tener acceso a los mensajes que se intercambien entre estos (incluyendo las contraseñas empleadas en el proceso de autentificación), o incluso suplantar a alguno de los actores en la comunicación. Las claves o certificados que se utilicen en esta comunicación deben estar adecuadamente custodiadas, ya que de lo contrario se inutilizaría esta medida de seguridad.

• Copias de seguridad: Los backups (o copias de seguridad) del dispositivo móvil deben estar correctamente protegidos, de forma que impidan el acceso a información sobre la infraestructura, comunicaciones y dispositivos IoT, especialmente la relacionada con su seguridad (como, por ejemplo, contraseñas). También deben contener medidas de integridad que prevengan su modificación, ya que, si se permite la restauración de un backup modificado, podrían desactivarse las medidas de seguridad que se hubieran definido previamente.

• Comandos enviados desde el dispositivo móvil: Al convertirse el dispositivo móvil, y sus aplicaciones móviles asociadas, en el "cerebro" del entorno o red de dispositivos IoT, éste es el encargado de enviar comandos, gestionar y controlar a todos los dispositivos IoT. Esto le convierte en uno de los objetivos principales de los ataques, ya que, si se obtiene acceso al dispositivo móvil, se podrían emitir comandos hacia los dispositivos IoT incluso sin que el usuario fuera consciente.

• Malware: Los dispositivos móviles son objetivo de ataques de malware. Si un malware toma control del dispositivo móvil podría llegar a suplantar al usuario o la aplicación que recibe información de los dispositivos IoT o envía instrucciones a los mismos.

• Suplantación de apps: Las aplicaciones móviles legítimas para el control de los dispositivos IoT pueden ser suplantadas en las correspondientes tiendas o mercados de aplicaciones públicos, llevando a los usuarios de los dispositivos móviles a instalarse apps de control maliciosas que pueden, por ejemplo, llegar a capturar credenciales de acceso o la configuración de los dispositivos IoT.

Intencionadamente, el conjunto de amenazas descrito previamente pone un foco especial en las contraseñas, empleando a modo de ejemplo esta información o dato como elemento crítico que no se desea sea accedido por un tercero no autorizado. Sin embargo, se debe generalizar o extrapolar este conjunto de amenazas a cualquier otra información sensible gestionada tanto por los dispositivos IoT como por los dispositivos y aplicaciones móviles.

1.4.2 TÉCNICAS Y HERRAMIENTAS DE ATAQUE

Debido a que el enfoque principal del presente estudio se centra en los dispositivos IoT, y a que no existen diferencias significativas entre la integración de los dispositivos y aplicaciones móviles en el ecosistema IoT y en cualquier otro entorno, no se ha querido duplicar, ni profundizar en detalle en, las diferentes técnicas y herramientas de ataque específicas para el análisis de dispositivos y aplicaciones en la primera edición del presente documento.

Los entornos móviles, incluyendo tanto dispositivos como aplicaciones móviles (apps), engloban numerosas tecnologías y aspectos asociados a otros apartados del presente documento, donde cabe destacar el uso de comunicaciones mediante TCP/IP, tecnologías de comunicación inalámbricas, un extenso uso de tecnologías web, integración con las capacidades de seguridad ofrecidas por el sistema operativo móvil, etc.

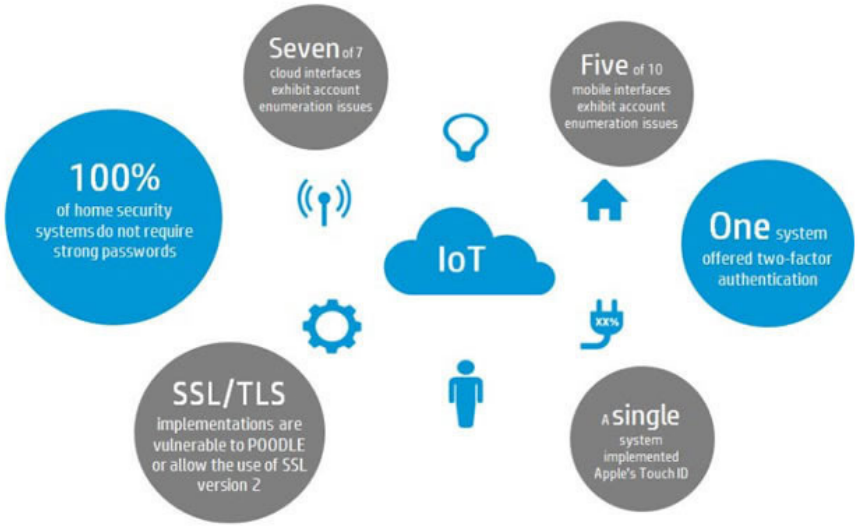
Por tanto, las herramientas que permiten atacar los entornos móviles son las mismas que permiten el análisis y la realización de actividades ofensivas en todas esas tecnologías (algunas de ellas ya descritas en otros apartados), tales como analizadores de red y protocolos, proxies de interceptación web y de otros protocolos binarios, herramientas de ingeniería inversa, herramientas de análisis forense o de los backups etc.

1.4.3 EJEMPLOS DE VULNERABILIDADES Y/O INCIDENTES IoT EMPLEANDO ESTE VECTOR DE ATAQUE

El siguiente estudio refleja como los dispositivos IoT y soluciones de seguridad doméstica, pese a tener un claro enfoque centrado en la seguridad física del hogar, descuidan la seguridad de las tecnologías empleadas, presentando diferentes vulnerabilidades que podrías ser explotadas por un potencial atacante. Muchas de estas soluciones de videovigilancia están integradas con "la nube" y con aplicaciones móviles que permiten su monitorización remota.

"Of 10 IoT-connected home security systems tested, 100% are full of security FAIL". Computerworld. Febrero 2015.

https://www.computerworld.com/article/2881942/cybercrime-hacking/of-10-iot-connected-home-security-systems-tested-100-are-full-of-security-fail.html



Fuente: https://www.computerworld.com/article/2881942/cybercrime-hacking/of-10-iot-connected-home-security-systems-tested-100-are-full-of-security-fail.html

1.5 COMUNICACIONES INALÁMBRICAS DEL DISPOSITIVO IOT

1.5.1 DESCRIPCIÓN Y OBJETIVOS DEL VECTOR DE ATAQUE

Lo más característico de las comunicaciones inalámbricas es que son un arma de doble filo; por un lado, permiten el acceso remoto al dispositivo con total libertad y alcanzando rangos de miles de metros, pero, por otro lado, la comunicación se propaga por el medio (aire) con la misma libertad, permitiendo a cualquier potencial atacante acceso inmediato a la misma. El objetivo de acceder a esta comunicación puede ser:

- Interceptación: Acceso y captura del contenido de la comunicación.
- Inyección, modificación y/o suplantación: Envío de datos no legítimos en una comunicación o alteración de la comunicación original (los conocidos ataques de replay se pueden entender como una combinación de interceptación/inyección).
- Denegación de servicio: Interrumpir la comunicación original entre el emisor y el receptor.

En las comunicaciones inalámbricas se debe tener en cuenta que, en condiciones normales, siempre se dispone de acceso físico al medio (aire) aunque este hecho no garantiza el acceso a la red (acceso lógico), según las medidas de seguridad existentes. Se ha resaltado esta peculiaridad ya que pone de manifiesto que ciertos vectores de ataque pueden estar diseñados para afectar a una o ambas etapas del acceso; una simple jaula de Faraday o un inhibidor de ruido blando gausiano impedirán toda comunicación por parte del dispositivo IoT víctima, atacando así el acceso físico. Sin embargo, un ataque inteligente a los protocolos de comunicación del dispositivo IoT puede conseguir los mismos resultados atacando el acceso lógico a la red o al dispositivo.

En todo caso, la disponibilidad de un vector de ataque que no requiere necesariamente de proximidad o acceso físico a los equipos analizados facilita el estudio de los protocolos de aplicación, habitualmente propietarios, que controlan la funcionalidad de los dispositivos IoT y que normalmente confían parte de la protección de sus comunicaciones a la tecnología inalámbrica o de radio que se esté usando en cada caso particular.

1.5.2 TÉCNICAS Y HERRAMIENTAS DE ATAQUE

La herramienta por excelencia para el estudio de comunicaciones inalámbricas o de radio frecuencia genéricas son los dispositivos SDR (Software Defined Radio). La característica principal de estos dispositivos es que implementan la mayoría de sus componentes en módulos software que se ejecutan en un ordenador, en lugar de en módulos hardware. Los módulos hardware necesarios para estudiar las señales no son más que un interfaz de radio frecuencia, cuyo sintonizador definirá el rango de frecuencias alcanzable con cada dispositivo y conversores analógicos/digitales y viceversa. Opcionalmente, los modelos de "gama alta" incorporan una FPGA para realizar un primer tratamiento más avanzado de la señal en el dispositivo, o tareas que requieren de más capacidad de cálculo en tiempo real, como el cifrado y descifrado de las comunicaciones. Los dispositivos SDR más extendidos y populares son el RTL-SDR, HackRF, BladeRF y USRP, pero desde luego no son los únicos. De hecho, cada día aparecen en el mercado más y más novedosos dispositivos SDR nuevos.

Para el procesamiento software en el ordenador, existen distintas opciones según el uso que se quiera hacer del dispositivo SDR:

- Estudio de la señal (reconocimiento, modulación, número de símbolos): baudline, audacity, etc.
- Estudio del espectro de frecuencias: GQRX, gr-fosphor, etc.
- Tratamiento de la señal: GNURadio, LuaRadio, etc.

Junto con los dispositivos SDR, es imprescindible elegir una antena diseñada y fabricada para trabajar con la frecuencia de la señal objetivo bajo estudio. Es también muy común el uso de filtros o amplificadores para mejorar la calidad de la señal. Existen otras múltiples herramientas disponibles para el estudio de señales al margen de SDR como, por ejemplo, placas como Arduino y Raspberry Pi que también disponen de accesorios para prácticamente todas las tecnologías: Wi-Fi, Bluetooth, 433MHz, 2G, 3G, etc.

La gran ventaja del uso de hardware SDR es su gran versatilidad, si bien la gran desventaja es que el conjunto

del dispositivo SDR y el software deben ser capaces de procesar la información en tiempo real con la precisión y velocidad requerida por la tecnología bajo estudio.

La gran ventaja del uso de hardware SDR es su gran versatilidad, si bien la gran desventaja es que el conjunto del dispositivo SDR y el software deben ser capaces de procesar la información en tiempo real con la precisión y velocidad requerida por la tecnología bajo estudio.

En ocasiones se pueden modificar ciertos dispositivos para emplearlos como herramientas de hacking, tal y como demostró el conocido investigador Samy Kamkar al utilizar un juguete de una conocida marca para realizar un ataque de fuerza bruta a puertas de garajes enviando distintas combinaciones de códigos de apertura. La atención que los investigadores han fijado en ciertas frecuencias propietarias (como 433MHz, 868MHz entre otras), ha provocado que se desarrollen dispositivos específicos como el Yard Stick One de Michael Ossmann para un conjunto de frecuencias y modulaciones específicas, Ubertooth One para el estudio únicamente comunicaciones Bluetooth– BLE y el dispositivo RZUSBstick para ataques a redes ZigBee.

Por último, los ataques Wi-Fi (más generalizados) comenzaron con la inyección de paquetes ARP en redes con cifrado WEP utilizando tarjetas específicas que permitían un correcto uso de la suite de herramientas aircrack-ng; las conocidas tarjetas Alfa. Para incrementar la distancia del ataque e incrementar la lista de redes objetivo, surgieron amplificadores específicos para esta tecnología, así como antenas direccionales con una gran ganancia (18-20 dBms).

Posteriormente, con los ataques de suplantación o Man-in-the-Middle a clientes Wi-Fi como Karma, surgió el conocido dispositivo comercial que implementa una variedad de diferentes ataques Wi-Fi: Wi-Fi Pineaple de Hak5.

1.5.3 EJEMPLOS DE VULNERABILIDADES Y/O INCIDENTES IOT EMPLEANDO ESTE VECTOR DE ATAQUE

Son innumerables los recientes ejemplos de interceptación, inyección y/o modificación de comunicaciones inalámbricas, por ello se citan algunos ejemplos que se han considerado más relevantes, agrupados por protocolos:

-Protocolos propietarios – 433 y 868MHz:
VerisureAlarm: ingeniería inversa de alarma doméstica, basada en la interceptación de las comunicaciones:
https://funoverip.net/2014/11/reverse-engineer-a-verisure-wireless-alarm-part-1-radio-communications/

-Protocolos propietarios – 315MHz:
Jeep: ataque de replay a la señal del mando que permite bloquear y desbloquear el coche:
http://calebmadrigal.com/hackrf-replay-attack-jeep/

-Múltiples ratones y teclados no-Bluetooth, empleando protocolos propietarios y no propietarios en la banda de 2,4 GHz:
Keysniffer: estudio que recoge diversas vulnerabilidades, así como análisis de ingeniería inversa, que han permitido capturar el tráfico de 8 fabricantes entre los que se incluyen Anker, EagleTec, General Electric, Hewlett-Packard, Insignia, Kensington, Radio Shack y Toshiba:
http://www.keysniffer.net

- Protocolo propietario - Z-Wave (900Mhz):
"Hacking the Z-Wave Protocol with a HackRF" es el nombre de la presentación donde se demostró que sólo 9 de 33 dispositivos analizados utilizaban cifrado en las comunicaciones, lo que permitió a los investigadores no sólo interceptar la comunicación sino controlar los dispositivos vulnerables:
http://www.rtl-sdr.com/hacking-the-z-wave-protocol-with-a-hackrf/

- Protocolo propietario - LoRa (LoRaWAN, Long Range Wide Area Network):
"Decoding the LoRa IoT Protocol with an RTL-SDR", recoge los avances publicados en RevSpace sobre el estudio de ingeniería inversa para demodular y analizar este protocolo del mundo IoT:
https://revspace.nl/DecodingLora

- Protocolo propietario - ZigBee y IEEE 802.15.4:
En la conferencia "ToorCon 11" se presentó una de las herramientas más conocidas y casos de uso para realizar ataques de interceptación y replay, entre otros; "KillerBee – Practical Zigbee Exploitation Framework":
http://www.willhackforsushi.com/presentations/toorcon11-wright.pdf

• **Ataques de suplantación: Celdas Falsas:**
- El investigador alemán Dieter Spaar, utilizando una celda falsa 2G, pudo estudiar las vulnerabilidades del sistema de BMW "Connected Drive", qué tras explotarlas, le permitieron bloquear y desbloquear los coches BMW afectados remotamente:
http://m.heise.de/ct/artikel/Beemer-Open-Thyself-Security-vulnerabilities-in-BMW-s-ConnectedDrive-2540957.html

- En el caso de las redes 3G y 4G donde la autenticación es mutua, el vector de ataque es una denegación de servicio de estas redes para forzar al dispositivo a utilizar únicamente la red 2G, donde estará esperando una celda falsa. El ataque se extiende un paso más, puesto que, o bien se utiliza previamente un equipo inhibidor que inutilice las frecuencias de estas tecnologías 3G y 4G, o bien se implementa un ataque de downgrade a una celda falsa 2G, utilizando para ello otra celda falsa 3G o 4G. Estas celdas no pueden dar servicio (no son funcionales), únicamente se presentan para engañar al dispositivo víctima con un error determinado y así mismo ofrecer como alternativa el uso de la celda falsa 2G, aprovechando que este tipo de transacciones ocurren en estas redes antes del proceso de autenticación.

• **Denegación de servicio:**
- "Attacking IoT with SDR" es el nombre de la presentación en la que se muestra como diseñar ataques de denegación de servicio (jamming) a tres tecnologías típicas en IoT, ZigBee, Z-Wave y Wi-Fi, utilizando únicamente para ello un dispositivo SDR:
http://es.slideshare.net/PacSecJP/jonathan-andersson-attacking-io-t-with-sdr-pacsec-2015-english-54952326

1.6 INTERFAZ WEB (Y OTROS INTERFACES DE GESTIÓN) DEL DISPOSITIVO IOT

1.6.1 DESCRIPCIÓN Y OBJETIVOS DEL VECTOR DE ATAQUE

Generalmente los dispositivos IoT disponen un interfaz web que permite su administración y configuración para facilitar al usuario la gestión de los mismos de una manera amigable. Parece lógico pensar que este tipo de dispositivos tienen embebidos servidores web conocidos, aunque puedan disponer de una configuración o versión específica para el dispositivo IoT en cuestión. A modo de ejemplo, en algunos de los dispositivos analizados se han encontrado servidores web como Boa y Apache. Por tanto, las vulnerabilidades que poseen estos servidores web en sus respectivas versiones son extensibles al dispositivo IoT.

El proyecto OWASP (Open Web Application Security Project), referencia de buenas prácticas en entornos web a nivel mundial, está desarrollando un área de análisis específica para IoT (OWASP Internet of Things Project). Este proyecto, aunque todavía se encuentra en versión inicial, proporciona información relevante en este ámbito.

Referencia:
"OWASP Internet of Things Project". OWASP. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

En lo que respecta al interfaz Web del dispositivo IoT, las vulnerabilidades más comúnmente conocidas que suelen ser explotadas se pueden resumir en el OWASP Top 10, dónde destacan:

•**Inyección SQL (SQLi)**
Este tipo de ataque se realiza construyendo sentencias SQL a partir de los campos de entrada enviados por el usuario, para realizar acciones en las bases de datos. En el ámbito del IoT, aunque no es muy habitual, algunos de los dispositivos tienen pequeñas bases de datos para almacenar información relativa a la configuración de los mismos, usuarios, roles, información recolectada, etc. Si no se efectúa un filtrado adecuado de los parámetros de entrada, se puede llevar a cabo la realización de acciones no autorizadas en la base de dato. En algunos casos se pueden crear, alterar o incluso eliminar valores contenidos en la base de datos.

• **Cross-Site Scripting (XSS)**
Consiste en la inyección de contenido web o código malicioso, generalmente JavaScript o HTML, en la respuesta de la página web legítima mediante la manipulación de los campos de entrada, con el objetivo de ejecutar pequeños programas o scripts en el navegador web del usuario víctima.

Normalmente esta vulnerabilidad permite, entre otros ataques, el secuestro de sesiones y robo de cookies por medio de las cuales es posible cambiar la configuración del dispositivo IoT. Por ejemplo, mediante Cross-Site Scripting persistente se podría realizar una suplantación en el portal web, concretamente en el formulario de autenticación, pudiéndose capturar las credenciales cuando el usuario las introduzca.

• **Cross-Site Request Forgery (CSRF)**
Esta vulnerabilidad se presenta cuando el usuario está autenticado en una página web que requiere disponer de una sesión establecida. Mientras que la sesión permanece abierta desde otra página web, mediante código HTML embebido, un atacante puede realizar acciones en la página web original suplantando al usuario legítimo, y de manera transparente para éste.

• **Enumeración de usuarios**
En múltiples ocasiones existen formularios para cambiar la contraseña o formularios de autentificación, entre otros, por medio de los cuales es posible averiguar si un usuario existe o no en el dispositivo IoT basándose, por ejemplo, en las respuestas o mensajes de error que devuelve la aplicación web.

• **Contraseñas débiles**
En muchos de los dispositivos IoT, no existen mecanismos de comprobación de la robustez de las contraseñas, por lo que se permiten usar aquellas que son fácilmente predecibles como '1234', '123456', 'admin', 'superuser', etc. En este caso se pueden averiguar las contraseñas que permitirán acceder al dispositivo IoT mediante un ataque de diccionario, o incluso por fuerza bruta (ver siguiente punto).

• **Bloqueo de cuentas**
Generalmente en los dispositivos IoT no se bloquean las cuentas de acceso tras un número de intentos fallidos, por lo que es fácil realizar un ataque por fuerza bruta que permita adivinar el usuario y la contraseña de alguna de las cuentas de gestión y administración del dispositivo.

• **Credenciales por defecto conocidas**
La mayoría de los dispositivos IoT vienen configurados con una cuenta de administración, no siendo obligatorio cambiar la contraseña la primera vez que se instala, configura o accede al dispositivo. Esto ocasiona que los dispositivos estén configurados con las contraseñas por defecto. Dichas cuentas de administración suelen ser fácilmente predecibles o incluso se pueden encontrar fácilmente por Internet, por ejemplo, en la documentación del fabricante o en numerosos listados existentes de contraseñas por defecto como, por ejemplo, Default Password List (http://www.defaultpassword.com). Este hecho permite que un usuario externo que tenga acceso al dispositivo IoT pueda cambiar cualquier parámetro de su configuración.

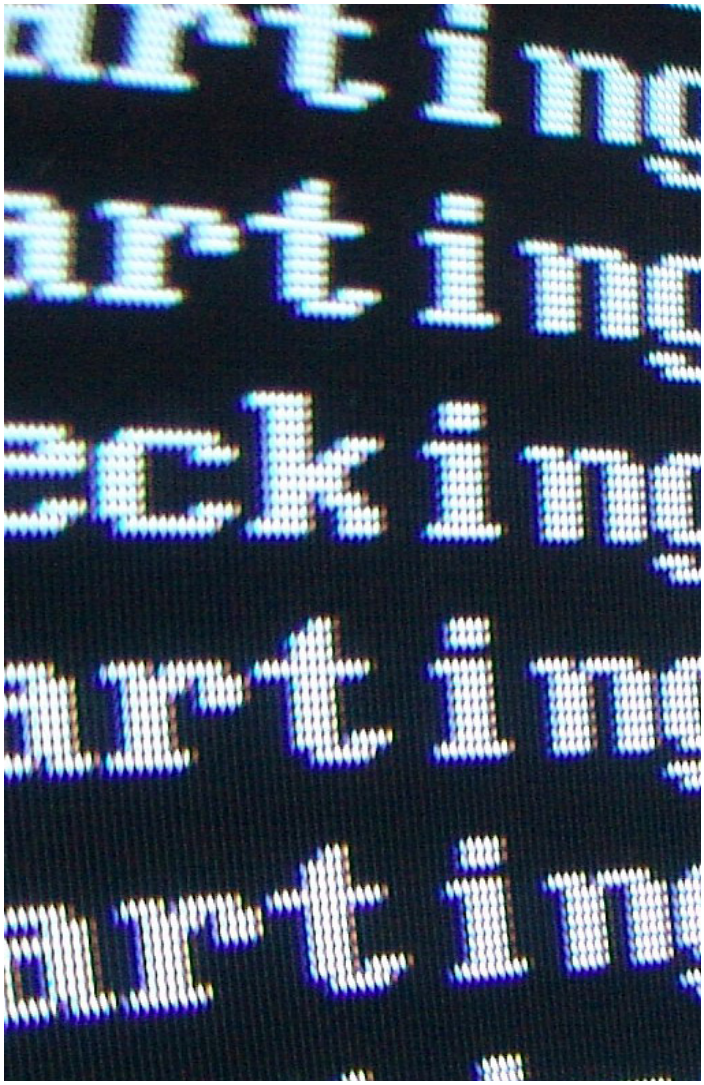
1.6.2 TÉCNICAS Y HERRAMIENTAS DE ATAQUE

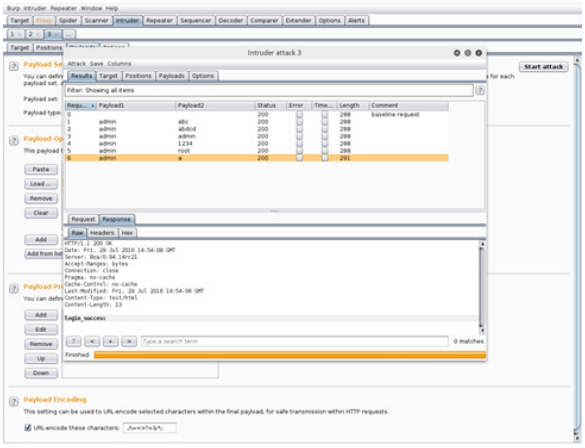
Para llevar a cabo los ataques sobre el servidor web del dispositivo IoT existen multitud de herramientas, la mayoría de ellas recogidas en el conjunto habitual de herramientas de auditoria de tecnologías web: https://www.owasp.org/index.php/Appendix_A:_Testing_Tools.

A continuación, se enumeran algunas de las más importantes:

• **OWASP ZAP**
El OWASP Zed Attack Proxy (ZAP) es una herramienta para identificar vulnerabilidades en aplicaciones web, mediante una interfaz amigable, aunque requiere saber configurarlo adecuadamente para poder sacar al máximo provecho de la herramienta y de sus numerosas capacidades. ZAP proporciona escaneos activos y pasivos, así como un conjunto de herramientas complementarias que permiten encontrar las vulnerabilidades de seguridad manualmente, como el proxy de interceptación web.

• **Burp Suite Proxy**
Burp es un proxy de interceptación web usado en auditorías de seguridad web que permite interceptar y modificar todo el tráfico HTTP(S), pudiendo trabajar con certificados digitales personalizados y clientes en modo proxy trasparente.
Igualmente, Burp también ZAP proporciona escaneos activos y pasivos, así como un conjunto de herramientas complementarias. Adicionalmente, permite realizar ataques por diccionario y fuerza bruta en los formularios web, así como numerosos tipos de ataques mediante sus diferentes funcionalidades como, por ejemplo, ataques de fuzzing mediante Burp Intruder.





Ejemplo de ataque de fuerza bruta con Burp.

• SQLmap

SQLmap es una herramienta avanzada de ataque que automatiza el proceso de verificación y explotación de vulnerabilidades de inyección SQL.

1.6.3 EJEMPLOS DE VULNERABILIDADES Y/O INCIDENTES IOT EMPLEANDO ESTE VECTOR DE ATAQUE

A continuación, se enumeran algunos ejemplos de vulnerabilidades asociadas a los interfaces web de los dispositivos IoT:

• Cross-Site Scripting (XSS)

La vulnerabilidad cuyo identificador es CVE-2016-5055 (Fuente: https://community.rapid7.com/community/infosec/blog/2016/07/26/r7-2016-10-multiple-osram-sylvania-osram-lightify-vulnerabilities-cve-2016-5051-through-5059) afecta a las bombillas OSRAM SYLVANIA Lightify , vulnerables a un Cross-Site Scripting (XSS) en la consola de administración.

Estas bombillas disponen de un control inalámbrico que tiene diversas funcionalidades, dependiendo de la bombilla, como pueden ser encender, apagar, cambiar el color y regular su intensidad.

Cabe destacar que para este producto también se publicaron diversas vulnerabilidades que permiten a un potencial atacante acceso a la red donde están conectadas.

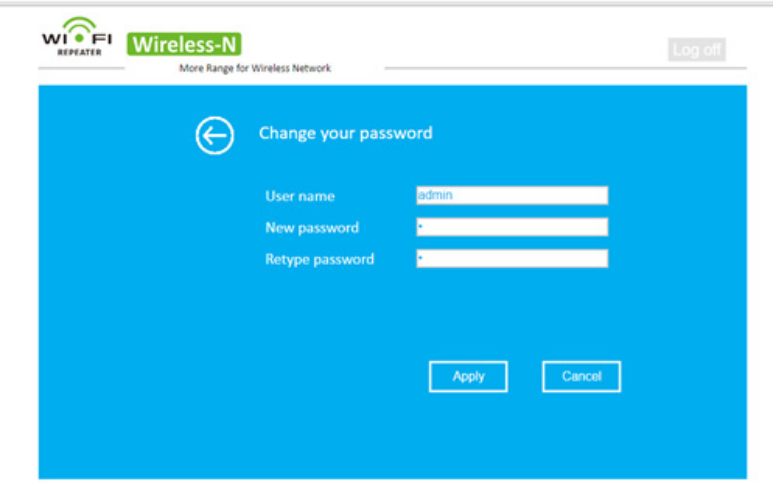
•Inyección SQL (SQLi)

Se ha encontrado una vulnerabilidad cuyo identificador es CVE-2016-2866 (Fuente: http://www.kb.cert.org/vuls/id/253708) que afecta a la cámara IP de video-vigilancia Grandsteam GXV3611_HD . Dicho dispositivo es vulnerable a un ataque de inyección SQL, si tiene la versión de firmware 1.0.3.6, lo que permite modificar la configuración del mismo.

• Cross-Site Request Forgery (CSRF)

La vulnerabilidad cuyo identificador es CVE- -2016-4494 (Fuente: https://ics-cert.us-cert.gov/advisories/ICSA-16-126-01) afecta al router multipuerto BACnet modelo BAC-5051E de KMC Controls. BACNET es un protocolo de comunicaciones para la gestión centralizada, empleado ampliamente en el ámbito industrial (o SCADA). Un usuario no autorizado podría leer la configuración del router.

Fuente imagen cámara: http://www.grandstream.com/sites/default/files/styles/product_100x100/public/GXV3611front.png?itok=9daVpfI
Fuente imagen bombilla: http://www.cnet.com/pictures/lightify-your-smart-home-with-osrams-new-leds-pictures/2/



Pantalla de cambio de contraseña del repetidor Wi-Fi.

- **Contraseñas débiles**

A modo ilustrativo, en un repetidor Wi-Fi (marca blanca) se permite cambiar la contraseña cuya longitud puede llegar a ser un único carácter. De este modo podríamos poner la contraseña 'a', la cual evidentemente es fácilmente adivinable mediante un ataque de diccionario o por fuerza bruta.

- **Bloqueo de cuentas**

En el repetidor Wi-Fi mencionado en la vulnerabilidad previa se pueden realizar múltiples intentos de autentificación o acceso sin que el usuario sea bloqueado, facilitando los ataques de fuerza bruta sobre la contraseña mencionados anteriormente.

- **Credenciales por defecto conocidas**

Existen páginas en Internet donde se puede obtener las cuentas por defecto de infinidad de dispositivos embebidos e IoT. A modo de ejemplo:

- http://www.defaultpassword.com
- https://www.cirt.net/passwords
- http://defaultpasswords.in

Incluso, en ocasiones, realizando una simple búsqueda en Google o Shodan se pueden encontrar dispositivos que en el propio banner (o pantalla de bienvenida) especifican las credenciales por defecto. A continuación, se muestra un ejemplo donde se indica que el usuario es admin y la contraseña 1234:

Ejemplo de búsqueda en Shodan con información de credenciales por defecto.

1.7 OTROS SERVICIOS DE RED DEL DISPOSITIVO IOT

1.7.1 DESCRIPCIÓN Y OBJETIVOS DEL VECTOR DE ATAQUE

Los dispositivos IoT presentan habitualmente numerosos puertos y servicios TCP/IP disponibles a través de la red, al igual que ocurre con otros equipos, ordenadores y/o dispositivos embebidos asociados a las nuevas tecnologías. Estos servicios se presentan cuando el dispositivo IoT juega el papel (o role) de servidor, frente al papel (o role) de cliente, por ejemplo, al conectarse a servicios en "la nube" (ver apartado 2.3).

Como resultado, si dichos servicios no están convenientemente protegidos o son vulnerables, estarán expuestos y permitirán comprometer el dispositivo IoT remotamente. Para un potencial atacante de un dispositivo IoT, puede resultar interesante realizar un estudio de estos servicios en su dispositivo víctima para:

1. Identificar qué servicios son los que están disponibles.

2. Enumerar toda la información posible acerca de los servicios: nombre, versión, plataforma, puerto, mecanismo de transporte (TCP/UDP), etc.

3. En último lugar, generar una huella digital (token) obtenido a partir de toda la información anterior y que debe identificar unívocamente a otras potenciales víctimas de ese mismo dispositivo a través de Internet. Para encontrar a otras potenciales víctimas que hacen uso de este modelo concreto de dispositivo, se utilizan palabras clave y operadores de búsqueda avanzados en buscadores como Shodan o Google.

Son muy conocidos los ejemplos de búsquedas avanzadas que permiten encontrar cámaras IP, impresoras, teléfonos VoIP y numerosos otros dispositivos en Internet a través de buscadores, por lo que es evidente que del mismo modo se pueden encontrar términos para buscar otros dispositivos (este tipo de búsquedas están disponibles en la Google Hacking DataBase (GHDB): https://www.exploit-db.com/google-hacking-database/). En el momento en que un dispositivo IoT víctima ha sido caracterizado, es posible escribir programas maliciosos que analicen si las máquinas que se están escaneando o comprometiendo son su víctima objetivo, para descargar y ejecutar el código malicioso, o si deben seguir buscando.

Los ataques sobre los servicios de red asociados a los dispositivos IoT pueden ser llevados a cabo manualmente y de manera dirigida, o mediante técnicas automáticas intentando infectar y comprometer el mayor número de víctimas. Uno de los métodos más habituales consiste en dirigir los ataques a los servicios que permiten establecer una conexión remota con el dispositivo IoT para su administración y gestión, como telnet, SSH o FTP, y hacer uso de vulnerabilidades o credenciales débiles, o credenciales configuradas por defecto, para acceder a los mismos. Una vez que se dispone de control completo del dispositivo IoT, éste puede ser utilizado para realizar otros ataques aprovechándose de su capacidad de cómputo y de su conectividad como, por ejemplo, ataques de denegación de servicio distribuidos (DDoS), sin que su propietario sea consciente de que el dispositivo ha sido infectado. Recientemente se ha publicado la existencia de varias botnets, o redes de dispositivos IoT comprometidos, como por ejemplo Mirai, asociadas a cámaras de seguridad (CCTVs) o routers caseros, empleados con este propósito.

1.7.2 TÉCNICAS Y HERRAMIENTAS DE ATAQUE

La herramienta por excelencia para realizar un barrido de servicios es el escáner de puertos Nmap, de la cual existen libros completamente dedicados a cómo realizar los distintos tipos de escaneos. En esta herramienta, existe la posibilidad de automatizar tareas a través del "Nmap Scripting Engine (NSE)", lo que ha facilitado enormemente la interacción con determinados servicios como SNMP ("Simple Network Management Protocol") para extraer información de la víctima (sistema operativo, nombre de red, procesos en ejecución, uptime, etc.).

Otro tipo de escáneres son las herramientas de análisis de vulnerabilidades, las cuales para realizar el diagnóstico también deben llevar a cabo la enumeración y reconocimiento de los servicios. Ejemplos de este tipo de herramientas son Nessus, OpenVAS y Retina.

Para la búsqueda de dispositivos IoT en internet las herramientas más efectivas son los buscadores web, en particular Shodan, Google y Bing.

Una vez se identifica la existencia de un dispositivo IoT vulnerable, es posible identificar y explotar las vulnerabilidades que éste pueda presentar a través de herramientas y kits de explotación como, por ejemplo, Metasploit.

1.7.3 EJEMPLOS DE VULNERABILIDADES Y/O INCIDENTES IOT EMPLEANDO ESTE VECTOR DE ATAQUE

Debido a que no existen diferencias significativas entre los servicios de red de los dispositivos IoT y del resto de dispositivos o equipos de la industria, ni tampoco en sus vulnerabilidades de seguridad, no se ha llevado a cabo un análisis detallado de estos en la primera edición del presente documento.

En el año 2015 se incrementó notablemente el número de especímenes de software malicioso (malware) cuyo objetivo era atacar específicamente a los dispositivos IoT, habiéndose llegado a identificar múltiples familias de malware distintas.

"IoT devices being increasingly used for DDoS attacks". Symantec. 22 Sep 2016.
http://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks

Posteriormente, en octubre de 2016, la botnet Mirai llevó a cabo uno de los mayores ataques de DDoS globales registrados hasta la fecha, afectando al proveedor DynDNS y en consecuencia a muchos de los grandes servicios disponibles en Internet actualmente:
https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/
https://krebsonsecurity.com/tag/mirai-botnet/

El siguiente artículo sobre el futuro de la piratería de la televisión de pago describe cómo se han conseguido identificar a los routers con un determinado servicio vulnerable y posteriormente se amplía la búsqueda en el portal Shodan para encontrar nuevas potenciales víctimas:
http://www.securitybydefault.com/2015/06/el-futuro-del-pirateo-de-la-tele-de.html

Ejemplo para obtener la búsqueda para encontrar paneles de control de plantas depuradoras de agua:
http://www.elladodelmal.com/2010/05/shodan-y-sistemas-scada.html

Los conversores de serie a Ethernet utilizados en algunas gasolineras también fueron localizados en Shodan, una vez se estudió el servicio que estaba conectado a Internet:
http://www.securitybydefault.com/2015/03/hasta-la-cocina-de-las-gasolineras.html

Por último, los fabricantes siguen descuidando la seguridad de los dispositvos IoT, tal como refleja la existencia del servicio telnet en cámaras IP de Samsung (modelo Samsung SmartCam) que, además, permiten el acceso privilegiado como root sin requerir una contraseña:
https://www.peerlyst.com/posts/samsung-smartcam-root-telnet-no-password-needed-peter-gamache-cissp

servicio telnet en cámaras IP de Samsung (modelo Samsung SmartCam) que, además, permiten el acceso privilegiado como root sin requerir una contraseña:
https://www.peerlyst.com/posts/samsung-smartcam-root-telnet-no-password-needed-peter-gamache-cissp

1.8 ALMACENAMIENTO LOCAL DE DATOS E INFORMACIÓN EN EL DISPOSITIVO IOT

1.8.1 DESCRIPCIÓN Y OBJETIVOS DEL VECTOR DE ATAQUE

Todo dispositivo IoT necesitará de algún tipo de memoria no volátil en la que almacenar tanto el firmware como los datos recopilados o generados por éste. El principal objetivo de los diferentes ataques dirigidos a los medios y unidades de almacenamiento, será la obtención de un volcado (dump) completo o parcial de los datos almacenados en esta memoria, con el fin de analizar el firmware mediante técnicas de ingeniería inversa (ver apartado 2.2), obtener contraseñas

Fuente: https://www.peerlyst.com/posts/samsung-smartcam-root-telnet-no-password-needed-peter-gamache-cissp

de acceso o claves de cifrado del contenido o acceder a los datos recopilados por el dispositivo IoT durante su uso en ficheros de configuración y bases de datos.

Para la obtención de un volcado del contenido de la memoria se pueden emplear diferentes técnicas de ataque, algunas de las cuales ya han sido descritas en apartados anteriores (apartado 2.2), que pueden requerir o no acceso físico al dispositivo. A lo largo de este apartado, se estudiarán las técnicas de ataque que requieren acceso físico al hardware y en concreto a la unidad de almacenamiento del dispositivo.

Salvo en casos puntuales, la mayoría de dispositivos IoT utilizan para el almacenamiento memorias tipo Flash, pudiendo ser NAND (usualmente en los controladores o hubs) o NOR (en sensores y actuadores principalmente) dependiendo del dispositivo. Dentro de la categoría de las memorias NAND existen dos formas de interconexión con el dispositivo IoT:

•Medios extraíbles: Como podrían ser todo tipo de tarjetas SD o flash, pendrives o discos SSD, que permiten una fácil obtención de un volcado binario completo mediante un simple adaptador USB.

• Integrados de memoria: Incluyen gran variedad de encapsulados diferentes (factor, forma y tipo de chip) que pueden integrar o no un controlador de memoria junto a la propia memoria NAND en el mismo microchip.

En definitiva, para poder obtener un volcado correcto, se deben utilizar diferentes técnicas y herramientas de extracción, que variarán según el tipo de memoria NAND o NOR que utilice el dispositivo IoT.

Una vez obtenido el volcado de la memoria se puede proceder al análisis de la misma mediante diferentes herramientas de software con el fin de identificar el sistema de archivos o ficheros empleado y extraer los ficheros de configuración y bases de datos para su análisis.

La ventaja de este vector de ataque es que permite acceder a los datos del dispositivo IoT al más bajo nivel (hardware), sin importar las medidas de protección que se hayan implementado a nivel lógico (software).

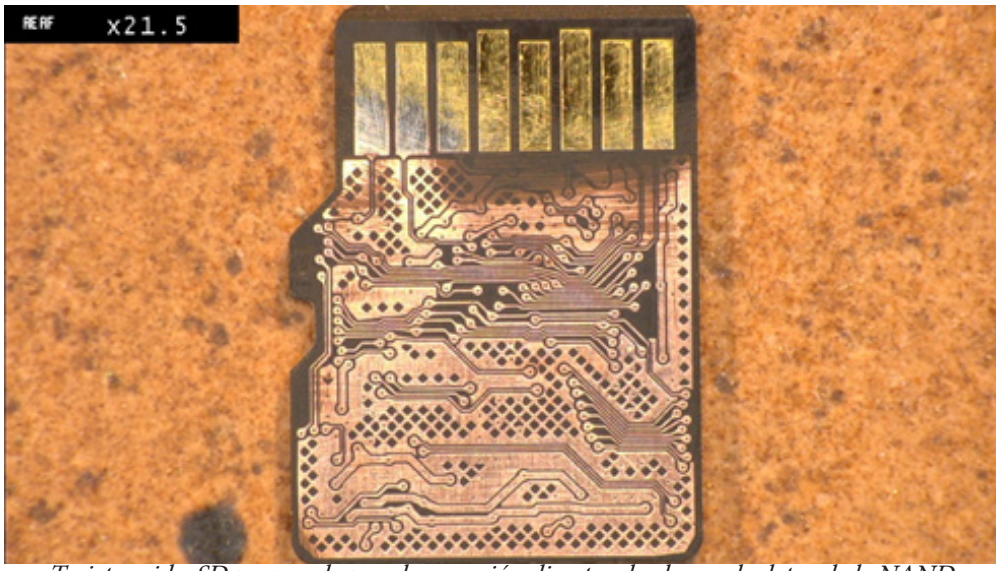
1.8.2 TÉCNICAS Y HERRAMIENTAS DE ATAQUE

Vulnerabilidades en el firmware, el interfaz web y otros interfaces de gestión (ya tratadas en el apartado 2.6), permiten la obtención de un volcado del contenido de la unidad de almacenamiento. A continuación, se enumerarán los vectores de ataque mediante el acceso físico a la placa base dispositivo IoT, comenzando por los interfaces o puertos de test o conexión:

JTAG: Acrónimo de "Join Test Action Group", es un standard que permite el testeo y programación de los circuitos integrados y conexiones en la PCB (placa base). Puede ser útil en dispositivos donde la NAND es un circuito integrado soldado en placa para evitar llevar a cabo un procedimiento de chip-off (o extracción del chip de memoria). Para identificar los diferentes pines JTAG en una PCB, se pueden utilizar controladoras JTAG como la XJTAG Expert, con el fin de analizar las señales y conectar los pines correctamente. Una vez establecida la conexión, se debe trabajar con los comandos adecuados para obtener acceso a la NAND y volcar su contenido completo o sólo de volúmenes concretos.

Una forma de proteger el dispositivo frente a este vector de ataque es deshabilitar físicamente el puerto JTAG tras su uso en fábrica, lo que impedirá futuras conexiones.

Buses de memoria en placa: Con este método se puede evitar también la extracción de la memoria NAND (chip-off), identificando los pin-out del chip de memoria sobre la propia PCB. También se hace necesario el empleo de estos buses en dispositivos monolíticos, en los cuales la memoria NAND se encuentra encapsulada junto al resto de controladores, como es el caso de las tarjetas microSD y algunas memorias SD y pendrives.



Tarjeta midroSD preparada para la conexión directa a los buses de datos de la NAND

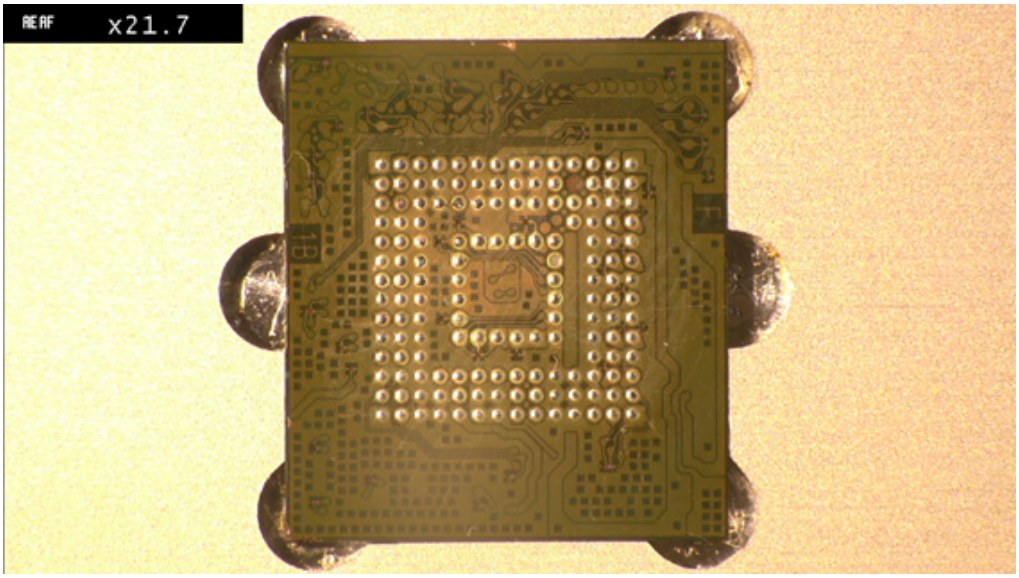
Las herramientas y técnicas utilizadas para el volcado de memoria mediante el acceso físico a la misma dependerán, en este caso, del tipo de memoria NAND implementada por el fabricante del dispositivo IoT.

Medios extraíbles: Tarjetas SD, micro SD e incluso pendrives o discos SSD pueden ser utilizados como medios de almacenamiento en estos dispositivos IoT. Este es el mejor de los supuestos para un potencial atacante, porque obtener un volcado binario del 100% de la NAND será tan sencillo como utilizar un adaptador USB y hacer una imagen utilizando, por ejemplo, el comando "dd" en Linux.

Memorias NAND con controladora integrada: En este tipo de memorias podríamos destacar las eMMC y eMCP. Incluyen en el mismo encapsulado la memoria NAND, la controladora de memoria y en algunos casos también LPDDR RAM para el dispositivo. Requieren en primer lugar la extracción cuidadosa del chip (chip-off) utilizando una estación BGA con el fin de no dañar el dispositivo. A continuación, dependiendo del encapsulado BGA utilizado por el fabricante de la memoria, habrá que tener identificados los diferentes buses de ese modelo de memoria o disponer de un socket de conexión para obtener un volcado con herramientas especializadas como Salvation Data Flash Doctor. La ventaja de este tipo de memorias es que, al integrar la controladora, el volcado obtenido no requerirá un post-proceso muy complejo, y se podrán extraer directamente ficheros del sistema de archivos.

Memorias NAND con controladora integrada: En este tipo de memorias podríamos destacar las eMMC y eMCP. Incluyen en el mismo encapsulado la memoria NAND, la controladora de memoria y en algunos casos también LPDDR RAM para el dispositivo. Requieren en primer lugar la extracción cuidadosa del chip (chip-off) utilizando una estación BGA con el fin de no dañar el dispositivo. A continuación, dependiendo del encapsulado BGA utilizado por el fabricante de la memoria, habrá que tener identificados los diferentes buses de ese modelo de memoria o disponer de un socket de conexión para obtener un volcado con herramientas especializadas como Salvation Data Flash Doctor. La ventaja de este tipo de memorias es que, al integrar la controladora, el volcado obtenido no requerirá un post-proceso muy complejo, y se podrán extraer directamente ficheros del sistema de archivos.

Algunos fabricantes pueden llegar a utilizar medios de protección físicos como escudos y resinas epoxy que dificultan mucho la extracción del circuito integrado, pero nunca llegan a imposibilitarlo completamente.



Memoria eMMC extraida de un smartphone

Memorias NAND sin controladora integrada: Son las de uso más extendido y se pueden encontrar en cualquier tarjeta o pendrive o, como en el caso de los dispositivos IoT, soldada directamente a la PCB. En este caso se requerirá también de un procedimiento de chip-off para la extracción de la NAND y de una herramienta como Flash Doctor para llevar a cabo la lectura de la misma. Al no tener la controladora de memoria integrada, el volcado binario obtenido contendrá no solo los datos almacenados por el dispositivo IoT, sino también los datos de service area, que incluye corrección de errores ECC y posicionamientos de bloque y página.

En este caso habrá que post-procesar ese binario con el fin de separar la información del service area de la información realmente almacenada y, posteriormente, ordenar los bloques de memoria. Una vez realizadas estas acciones podremos acceder al sistema de archivos para montarlo y extraer la información.

Memoria NAND TSOP-48 extraída de un router para su volcado

Memorias FLASH ROM: Las memorias tipo FLASH ROM, como por ejemplo las EEPROM, se caracterizan por ser mucho menos densas y más costosas de fabricar. Será más habitual encontrarlas en sensores y actuadores y su contenido puede incluir ciertos datos recabados e instrucciones de control del dispositivo IoT. Para su lectura será necesario el método chip-off y un lector de EEPROM para realizar el volcado. Este tipo de memorias no utilizan sistema de archivos y contienen datos de control codificados en posiciones (offset) concretas de la memoria. Su análisis es bastante complejo y requiere de técnicas de ingeniería inversa avanzadas.

Una vez obtenido el volcado por cualquiera de los métodos anteriores, podremos proceder al análisis del mismo con diferentes herramientas de software, con el fin de extraer los ficheros y bases de datos donde el dispositivo IoT almacena la información.

En primer lugar, se debe examinar el binario en busca de un MBR (Master Boot Record) o sector de arranque con el fin de identificar los volúmenes lógicos y el sistema de archivos utilizado. También en este primer análisis se detectará si existe algún tipo de cifrado total o parcial y si existe algún offset o desplazamiento de las particiones. Para esta tarea se puede utilizar un visor hexadecimal como HexViewer, que permite analizar el binario por sectores o bloques y facilita la identificación de los diferentes sistemas de archivos, sectores de cifrado y volúmenes lógicos.

Una vez identificado el sistema de archivos y las particiones, se procederá a la extracción completa de los ficheros y directorios para finalmente poder pasar al análisis de las diferentes bases de datos y ficheros de configuración del dispositivo, o cualquier otra información sensible, o a aplicar técnicas de ingeniería inversa (reversing) sobre el firmware con el fin de desgranar su funcionamiento y buscar todo tipo de vulnerabilidades. Para la extracción de la estructura de archivos, se puede utilizar software de recuperación de datos o de análisis forense informático que trabaje con ese sistema de archivos concreto. Encase Forensic trabaja con gran cantidad de sistemas de archivos y puede ser útil tanto para la extracción del contenido como para el análisis a nivel hexadecimal.

En el caso de analizar un dispositivo IoT con el contenido de la memoria cifrado y protegido por contraseña, se puede utilizar Encase para buscar patrones de clave hash (SHA256, SHA1, MD5, etc.) con el fin de intentar obtener su valor original mediante un ataque de fuerza bruta o de diccionario. Una vez obtenido el valor del hash y, por tanto, la clave de acceso, se realiza un proceso de reballing para volver a instalar la memoria NAND en el dispositivo y acceder a la gestión mediante la contraseña obtenida.

1.8.3 EJEMPLOS DE VULNERABILIDADES Y/O INCIDENTES IOT EMPLEANDO ESTE VECTOR DE ATAQUE

Un claro ejemplo de la utilización de técnicas de chip-off y acceso físico a la memoria NAND para vulnerar un sistema es el método desarrollado en 2016 por Sergei Skorobogatov para llevar acabo un bypass del código de acceso en un iPhone 5C. El método utilizado fue el "NAND mirroring" mediante el cual se reescriben los cambios que realiza el terminal en la NAND cada vez que hay un intento de acceso fallido al introducir el código de acceso. De esta manera el contador de intentos vuelve a cero y se pueden probar códigos de acceso de forma ilimitada, permitiendo un ataque por fuerza bruta que de otra manera no sería posible. El método se describe detalladamente en el artículo publicado por Sergei disponible en el siguiente enlace:
https://arxiv.org/abs/1609.04327

BLOQUE III:
IMPACTO DE LAS TECNOLOGÍAS IoT Y DISPOSITIVOS MÓVILES EN LA PRIVACIDAD DE LAS PERSONAS

1. ¿QUÉ ES LA PRIVACIDAD?

El concepto de privacidad no es unánime en todas las culturas legales si bien todos coinciden en señalar que se trataría de reclamar la protección frente a terceros de la vida privada, de aquellos aspectos personales que se preferiría no dar a conocer.

Según la RAE Privacidad es la cualidad de lo privado, es el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.

Visto así, la privacidad excluiría todo aquel conocimiento que fuera público o visible, o que hubiéramos expuesto voluntariamente en redes sociales o al aceptar unas condiciones generales al instalar una aplicación, empezar a usar un servicio o usar un objeto conectado. De ahí que sea necesario establecer un concepto más concreto que proteja a los ciudadanos del impacto del uso de objetos conectados y del tratamiento masivo de los datos con impacto a su intimidad. Ese concepto sería el de protección de datos, entendido como el derecho a la propiedad de los mismos, a retirar el consentimiento dado, a controlar su uso, en definitiva, allí donde los datos se encuentren. Así, los datos son siempre del titular de los mismos y puedo gestionarlos con total libertad y control. Son datos protegibles aquellos que identifican o son aptos para identificar a una persona física, lo que supone incluir en el ámbito de dato personal cualquiera, desde los generados automáticamente por los dispositivos y aplicaciones, hasta los facilitados voluntaria o inconscientemente por parte del usuario: metadatos, una dirección postal, fotos, huellas digitales, vídeos, cualquier dato al que, aplicada la adecuada minería de datos, permita identificar a la persona que está tras ellos.

1.1 | EL DERECHO A LA PROTECCIÓN DE DATOS

La primera actuación protectora de los datos personales tiene lugar en el marco del Consejo de Europa a través del Convenio Nº 108 del Consejo de Europa de 28 de Enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal , confiriéndole la consideración de derecho fundamental como viene siendo práctica común en la Unión Europea, frente a la protección de derecho del consumidor que otorga Estados Unidos.

En este sentido su artículo primero establece que: *“el fin del presente Convenio es garantizar en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (“protección de datos”)”.*

En 1995 se aprueba la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos , otorgando al derecho a la protección de datos el rango de derecho fundamental, tal y como se observa en su artículo primero al definir el objeto de la misma que no es otro que garantizar la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales. Amplía así el ámbito de protección con respecto al Convenio 108 puesto que este se aplica a tratamientos automatizados y la Directiva se aplica a tratamientos automatizados y no automatizados.

El compromiso de la Unión Europea en la protección de este derecho se consolida con la Carta de los Derechos Fundamentales de la Unión Europea del año 2000 , al incluir en el artículo 8 la protección de datos de carácter personal:

> 1.Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
>
> 2.Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
>
> 3.El respeto de estas normas quedar· sujeto al control de una autoridad independiente”.

Por último en fechas recientes y tras más de cuatro años de tramitación legislativa, se ha aprobado el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos): El Reglamento nace ante la necesidad de adaptar la normativa a los avances tecnológicos salvando las lagunas existentes en la Directiva 95/46/CE. Su entrada en vigor se produce el 25 de mayo de 2016 pero su aplicación se pospone hasta el 25 de mayo de 2018, fecha en la que queda derogada la Directiva 95/46/CE, lo que provoca una situación de transitoriedad en el momento de redactar estas líneas.

El derecho a la protección de datos en España, como no podía ser de otra manera, ha corrido en paralelo al de la Unión Europea, considerando como derecho fundamental la protección de datos personales. La primera manifestación se produce tras la ratificación del Convenio 108 con la promulgación de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal .

Posteriormente, fue derogada por la actual Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal , constituyendo el marco jurídico general en materia de protección de datos personales junto con su reglamento de desarrollo, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Posteriormente, fue derogada por la actual Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal , constituyendo el marco jurídico general en materia de protección de datos personales junto con su reglamento de desarrollo, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal .

Por su parte el Tribunal Constitucional en sus Sentencias 290/2000 y 292/2000 vino a reconocer el carácter de derecho fundamental de la protección de datos personales definiéndolo como un derecho de la autonomía de la voluntad del individuo sobre el control de sus propios datos manejados por terceros:

"un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática'", lo que se ha dado en llamar "libertad informática" (FJ 6, reiterado luego en las SSTC 143/1994, FJ 7, 11/1998, FJ 4, 94/1998, FJ 6, 202/1999, FJ 2). La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5, 94/1998, FJ 4).

Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran".

En el ámbito de la IoT y la movilidad también cabe destacar la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico , la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones y la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica .

1.2 | EL PROBLEMA DEL CONSENTIMIENTO EN EL IOT

Todo el esquema protector de la legislación de datos de carácter personal se basa en la adecuada obtención del consentimiento del titular de los datos, lo que requiere una previa información de a qué tipo de tratamiento se facili-

1. https://www.boe.es/boe/dias/1985/11/15/pdfs/A36000-36004.pdf

ta el consentimiento. Ello supone que esa información ha de ser clara, transparente, sin ambigüedades, en un lenguaje comprensible para el titular de los datos, de tal modo que el acto volitivo de consentir sea consciente.

En el mundo de las redes sociales, del uso de aplicaciones móviles o de objetos conectados, el consentimiento es simplemente ilusorio, bien porque no hay información previa ni vía de prestarlo, bien porque el tipo de información facilitada es tal larga e incomprensible, que el usuario no la lee. De hecho, los formularios de consentimiento están diseñados como un paso previo, necesario y sin cuya aceptación no se pueda alcanzar la pantalla siguiente y obtener el servicio o descargar la aplicación a la que pretendemos acceder.

En este sentido resulta revelador el trabajo realizado por la Universidad de Berkeley en que plantean un ejercicio para determinar si la presencia de un link a una política legal de privacidad (protección de datos) en una web o en la descarga de una app tiene alguna influencia significativa en la voluntad de los usuarios para facilitar información personal. Hay múltiples estudios que exploran el contenido y eficacia de estas políticas de privacidad. Como hemos indicado, se presume que la elección sobre si facilitar o no datos personales, viene regido por el consentimiento informado que parte de la premisa de que los usuarios son seres racionales capaces de leer en profundidad documentos legales para evaluar las prácticas de privacidad y protección de datos de una web o una aplicación móvil.

Múltiples estudios ya han confirmado que la mayoría de nosotros sabemos que estas condiciones legales se leen muy raramente, que leer las políticas de privacidad de cada web que se visita nos llevaría una cantidad de tiempo poco razonable ; que están a menudo escritas en un lenguaje tan complejo que están lejos de la compresión lectora de la mayor parte de los usuarios. En definitiva, las políticas de privacidad y protección de datos son documentos legales escritos por abogados para abogados y no para usuarios finales. Una encuesta de 2009 determinó que la mayoría de los participantes creían que las políticas de privacidad y protección de datos protegían sus derechos, cuando en realidad están orientadas a asegurarse la recogida de datos y cesión sin problemas. De hecho, muchas condiciones, aun cumpliendo la ley escrupulosamente, suponen de facto una invasión de la intimidad de sus usuarios.

En el piloto previo a este estudio comprobaron que ninguno de los participantes hizo clic en el link que llevaba a las condiciones de privacidad. El estudio parte de la base de que los usuarios no son conscientes de la elección que realizan y de las consecuencias e implicaciones que para su vida privada puede tener. Una decisión sin pensar como facilitar información de salud a través una app conectada con una pulsera de entrenamiento o un reloj inteligente, puede tener consecuencias negativas en el medio plazo si el desarrollador de la app cede (y sin duda lo hará) esos datos a una compañía de seguros que los puede utilizar para denegar un seguro de vida, de salud o para aumentar considerablemente la prima.

Parece, por tanto, que tal vez un sistema basado en la recogida de consentimiento pueda no estar protegiendo los derechos fundamentales a la intimidad y a la protección de datos de los individuos.

1.2.1 | EL CONSENTIMIENTO EN LA LEY

Tanto el artículo 5 de la LOPD como los artículos 12 a 14 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos de ahora en adelante "RGPD") obligan con carácter previo a la recogida de datos personales, a facilitar información clara y permanente al interesado sobre una serie de aspectos como son los fines y usos previstos. Dicho deber de transparencia en la información plantea problemas de diversa índole ya mencionadas, a saber:

• Uso de largas y farragosas políticas de protección de datos o privacidad que casi nadie entiende ni lee.

• En dispositivos de pantalla reducida el tamaño es un hándicap a la hora de facilitar esa información.

• Una vez que se ha informado sobre unos fines y/o comunicaciones previstas se plantean problemas de cómo informar y ser transparentes ante finalidades o comunicaciones no previstas en el momento inicial.

• Intervención de diversos responsables de tratamiento como el fabricante del producto, el diseñador del sistema operativo, tiendas de aplicaciones, diseñadores de aplicaciones, terceros (publicidad, operadores de servicios de comunicaciones, mercantil que regala un dispositivo wearable sobre el que obtiene posterior información a cambio de descuentos, puntos o premios, etc) e incluso esas mismas partes, pero de diferentes dispositivos cuando se conectan e interactúan entre ellos. Todos ellos deben de capaces de informar al interesado en los términos establecidos en la normativa de protección de datos.

En este sentido el artículo 12.7 del RGPD permite facilitar la información en combinación con iconos normalizados También se podrían establecer links permanentes a políticas de privacidad o facilitar la información en capas como ocurre con los avisos de cookies. En lo que respecta a los usos futuros, teniendo en cuenta que los dispositivos móviles y de IoT son inteligentes, podrían incluir de fábrica la posibilidad de informar al interesado a través de una advertencia en la pantalla con link a la nueva política de privacidad o a la versión modificada.

2. http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A31995L0046 3. http://www.europarl.europa.eu/charter/pdf/text_es.pdf

4 http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC

Salvo que el tratamiento pueda encuadrarse dentro de una de las excepciones al deber de obtener el consentimiento (ejecución de un contrato o precontrato en interés del afectado, interés legítimo del responsable de tratamiento o un tercero salvo que prevalezcan los derechos y libertades del interesado, etc) el consentimiento debe ser libre, específico, informado e inequívoco, lo que equivale a que sea expreso requiriendo en el RGPD una "declaración o una clara acción afirmativa". De tratarse de categorías especiales de datos incluidos en el artículo 7 de la LOPD o del artículo 9 y 10 del RGPD, el consentimiento deberá prestarse de manera explícita. Debe tenerse en cuenta que gran cantidad de APPs y dispositivos wearables son utilizados para realizar mediciones y monitorizaciones relacionadas con la salud del interesado. Al igual que ocurre con el derecho de información se plantean, entre otros, los siguientes problemas:

1. Que el consentimiento sea explícito o inequívoco requiere poder probar por parte del responsable de tratamiento que se otorgó. En esa línea el artículo 7.1 del RGPD dispone que cuando el tratamiento se base en el consentimiento, el responsable debe estar en disposición de demostrar que se otorgó. Por ello no basta con incluir por ejemplo una casilla para marcar y un botón con la palabra "acepto", sino que debe quedar registrado de algún modo que esa acción se realizó.

2. En relación con futuros tratamientos no previstos inicialmente, se deben diseñar procedimientos y métodos técnicos que hagan posible la obtención de nuevos consentimientos para nuevos tratamientos.

3. Al ser revocable, se deben establecer procedimientos y métodos técnicos de fácil localización y acceso permanente por parte del afectado.

4. En relación con la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), el artículo 5.3 establece la necesidad de obtención del consentimiento del abonado para captar información almacenada en el equipo terminal.

No es necesario obtenerlo si esa captación se realiza con el único fin de "efectuar o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de proporcionar a una empresa de información un servicio expresamente solicitado por el usuario o el abonado".

5. En relación con el tratamiento basado en un interés legítimo de responsable, cabe traer a colación para las tecnologías IoT el Considerando 49 del RGPD que entiende que las medidas destinadas a garantizar la seguridad de una red constituyen un interés legítimo.

6. Cuando se trata de servicios de la sociedad de la información destinados a menores de 16 años o 13, en el supuesto que el Estado miembro rebaje la edad como máximo hasta los 13 años, el RGPD establece que el consentimiento sólo será lícito si lo otorga el titular de la patria potestad o tutela legal del menor, debiendo realizar el responsable esfuerzos razonables atendiendo a la tecnología disponible para verificar esa autorización. Por su parte el artículo 13 del Real Decreto 1720/2007 establece con carácter general la edad de 14 años como edad a partir de la cual no es necesario contar con el consentimiento de padres o tutores.

7. Los diferentes responsables de tratamiento también deben obtener el consentimiento del interesado antes de iniciarse el tratamiento. En relación con las aplicaciones preinstaladas en el dispositivo debería ser posible su desinstalación si no son necesarias para el funcionamiento del mismo y, con carácter general, cuando se desinstale cualquier aplicación se debe entender que se ha revocado el consentimiento que legitima el tratamiento, entrando en juego la supresión de los datos o en su defecto los plazos de mantenimiento de los mismos, así como la comunicación de la supresión a los cesionarios.

En lo que respecta a las comunicaciones de datos (cesión a terceros) volvemos a tener idéntica problemática. El artículo 11 de la LOPD dispone con carácter general el consentimiento previo del interesado o que se ampare en alguna de las excepciones legalmente previstas (amparada por norma con rango de Ley, en interés vital del afectado, etc). Por su parte el RGPD tanto en su artículo 13.1.e) como en el 14.1.e) establece el deber de informar sobre "los destinatarios o las categorías de destinatarios de los datos personales, en su caso" y que sobre ese deber de información previo se solicitará el posterior consentimiento, por lo que nos remitimos a lo reflejado en líneas anteriores.

1.2.2 | LA MITIGACIÓN DE LA FALTA DE CONSENTIMIENTO DE FACTO: EL DERECHO A CANCELAR O CAMBIAR DE OPINIÓN

Transparencia e información, consentimiento y comunicaciones de datos no pueden ofrecer un óptimo nivel de protección sin un adecuado sistema de ejercicio de derechos de acceso, rectificación, cancelación y oposición (Título III de la LOPD) o de acuerdo con el RGPD acceso, rectificación, supresión "derecho al olvido", oposición, decisiones individuales automatizadas, portabilidad y limitación en el tratamiento. En relación con estos derechos se plantean las siguientes cuestiones:

- Se debe estar en disposición de informar sobre las comunicaciones de datos realizadas, tanto a otros responsables

y partes relacionadas con ese dispositivo, como de las realizadas al interactuar con otros dispositivos.

- Que se anonimicen lo datos no exime del deber de informar sobre la misma así como del riesgo de reidentificación existente y aceptable que se recoge en el análisis de riesgos realizado. Con un riesgo aceptable de reidentificación no aplica la normativa de protección de datos pero, como indicamos, ello no exime del deber de responder a la solicitud del ejercicio del derecho por parte del afectado.

- Se debe apostar por nuevos modelos que otorguen el control sobre sus datos a los interesados facilitándoles la portabilidad de los mismos y permitiéndoles en todo momento otorgar o revocar el consentimiento para el tratamiento, así como tener información permanente sobre los fines y usos, comunicaciones previstas o realizadas, etc, como pueden ser los denominados data personal spaces (espacios de datos personales) o data stores (almacenes de datos), y por los que han apostado tanto la Comisión Europea, como el Supervisor Europeo de Protección de Datos y ENISA .

Por todo ello, estos son alguno de los puntos principales a tener en cuenta por todos los intervinientes en un tratamiento de datos personales en IoT y movilidad:

- Cada responsable de tratamiento debe obtener los datos necesarios para la finalidad del tratamiento.

- Se deben establecer políticas de plazos de mantenimiento de la información.

- El usuario debe ser capaz de desconectar el dispositivo o alguna de sus aplicaciones y funcionalidades cuando no las esté utilizando.

El RGPD refuerza el principio de responsabilidad de los responsables de tratamiento. Anteriormente al analizar los principios relativos del tratamiento, constatábamos como el apartado 2 del artículo 5 del RGPD introduce el principio de "responsabilidad proactiva" al establecer que el responsable del tratamiento tiene que cumplir las estipulaciones recogidas en el apartado 1 de ese mismo artículo y se capaz de demostrarlo.

Por su parte el artículo 24 del RGPD introduce un nuevo concepto denominado "accountability", de difícil traducción al castellano (responsabilidad, compromiso,…). Queda reflejado en el artículo 24 del RGPD, en concreto en su apartado 1 al disponer:

"Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario".

Se abre por tanto un escenario de responsabilidad que en algunos supuestos será objetiva y en otros supuestos será subjetiva. En lo que respecta a la responsabilidad objetiva se producirá en la medida en la que el responsable de tratamiento no sea capaz de demostrar aspectos tales como:

• Que se informó previamente al interesado y que se obtuvo su consentimiento inequívoco o explicito según el caso, y si se facilita esa información de manera permanente y es de fácil localización.

• Que se ha atendido al ejercicio de un derecho formulado por un interesado respondiendo en plazo.

• Que la trasferencia internacional está amparada en alguno de los supuestos o excepciones que la legitiman.

• Que se ha notificado la violación de seguridad de datos a la autoridad de control y, en su caso, a los afectados.

• Que se ha realizado la preceptiva Evaluación de impacto en protección de datos.

Por otro lado tal y como comentábamos existe también un ámbito de responsabilidad subjetiva debido al enfoque basado en el riesgo dispuesto a lo largo del articulado del RGPD como se puede comprobar en los artículos 24 (responsabilidad), 25 (privacidad por diseño) y 32 (seguridad). Nos podemos encontrar ante estos supuestos cuando:

• Se produce un ciberataque con éxito a los sistemas de información del responsable o encargado de tratamiento. Será

responsable si se demuestra que no adoptó las medidas adecuadas atendiendo a la tecnología disponible, a los costes de implementación, a la naturaleza y fines de los tratamientos y a los riesgos de probabilidad y gravedad para los derechos y libertades de las personas físicas.

• Un empleado facilita información sobre horarios, itinerarios, aficiones, etc de clientes de la compañía a terceros. En base a los mismos criterios el punto anterior se deberá valorar si las medidas eran las adecuadas, máxime cuando el apartado 4 del artículo 32 del RGPD dispone que "el responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

2. EL TRATAMIENTO MASIVO DE DATOS Y MEDIDAS DE MITIGACIÓN

El artículo 35.1 RGPD establece la necesidad de realizar una evaluación de impacto "Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación de impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares".

Los dispositivos IoT permiten recoger datos que el artículo 9.1 del RGPD inserta en las categorías especiales de datos, entre ellos los relativos a la salud. Estos en el marco de la telemedicina se procesan por el responsable del tratamiento para monitorizar la salud de la persona física titular del Derecho a la Protección de Datos. Del mismo modo los dispositivos IoT también facilitan la confección de perfiles que pueden sustentar la toma de decisiones con efectos jurídicos.

El artículo 35.7 del RGPD describe el contenido mínimo que comprenderán las evaluaciones de impacto especificando que será:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas de seguridad previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Adquieren por ello especial relevancia todas las medidas tendentes a garantizar la minimización de los tratamientos, al igual que las medidas de seguridad aplicadas a los diferentes procesos.

El propio RGPD entiende como una medida apropiada aplicar la seudonimización y por supuesto que la anonimización de datos excluiría a ese tratamiento del ámbito de aplicación de la normativa de protección de datos (LOPD y RGPD). No obstante, se ha comprobado que uniendo información disociada de diversas fuentes puede reidentificar a titulares de esos datos personales, por lo que el mero hecho de anonimizar per se, no sería suficiente sino que se deben utilizar técnicas o incluso combinaciones de técnicas de anonimización que permitan tras un análisis de riesgos, que el riesgo residual de reidentificación sea aceptable. Debe tenerse en cuenta que la información anonimizada exime de realizar una Evaluación de impacto en protección de datos, pero no exime de realizar un análisis de riesgos de reidentificación y que anonimizar supone realizar un tratamiento de datos, con las consecuencias que ello conlleva.

El uso de herramientas de cifrado en la transmisión de datos o en el alojamiento de los mismos tanto en servidores físicos como virtuales se revela como muy recomendable para estos tratamientos. Lamentablemente como pone de manifiesto el Grupo de Trabajo del Artículo 29 en su Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos, estas herramientas no se están utilizando con carácter generalizado puesto que actualmente está primando la eficiencia ante la seguridad. No obstante, y atendiendo a lo dispuesto en los apartados 1 y 2 del artículo 32 del RGPD , el cifrado, seudonimización y anonimización van a tener que generalizarse para determinados tratamientos, sobre todo aquellos que supongan un riesgo para los derechos y libertades de los individuos, manejen a gran escala de categorías especiales de datos y tratamientos habituales y sistemáticos de aspectos personales de individuos.

Es más, los artículos 33 y 34 del RGPD extienden una obligación vigente a día de hoy para los operadores de servicios de comunicaciones electrónicas disponibles al público, recogida en el apartado 3 del artículo 41 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (LGT) que no es otra que notificar las violaciones de seguridad de los datos a la autoridad de control y, en algunos casos, a los propios afectados. En lo que respecta a la comunicación al interesado, se trata de una disposición muy beneficiosa puesto que el responsable o encargado de tratamiento no pueden ocultarla por miedo al daño reputacional, reclamación de daños y perjuicios o pérdida de clientes. Deberá realizarse cuando "sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas" y ante los daños de imagen pública y pérdida de volumen de negocio cabe destacar que hay requisitos de exoneración de ese deber que se encuentran recogidos en el apartado 3 del artículo 34 del RGPD que fomentan el uso de estas técnicas:

"3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados".

3. EL REGLAMENTO DE E-PRIVACY

El pasado mes de enero de 2017 se publicó la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas o reglamento e-Privacy como se le conoce).

Dicho reglamento, pertenece al paquete "telecom" y es el documento que regula las medidas que en materia de privacidad van a tener que adoptar las ITTs, pero no únicamente ellos. La legislación en materia de telecomunicaciones ha ido evolucionando desde las normas sobre telefonía fija, transporte de datos y acceso a internet, a la más amplia definición de comunicaciones electrónicas, que se ha visto superada por la aparición de la panconectividad de la que es el más claro exponente la IoT. Así, mientras el RGPD sería aplicable a los OTTs, esta norma está pensada para ser aplicada, entre otras, al mundo de las cosas interconectadas y, curiosamente, al de la publicidad en tanto traquean a los usuarios con la finalidad de tratar la información que de su comportamiento obtienen.

En este sentido, el Reglamento de ePrivacy define los datos y metadatos del siguiente modo:

• «datos de comunicaciones electrónicas»: el contenido de las comunicaciones electrónicas y los metadatos de las comunicaciones electrónicas;

• «contenido de comunicaciones electrónicas»: el contenido intercambiado por medio de servicios de comunicaciones electrónicas, como texto, voz, vídeos, imágenes y sonidos;

• «metadatos de comunicaciones electrónicas»: datos tratados en una red de comunicaciones electrónicas con el fin de transmitir, distribuir o intercambiar contenido de comunicaciones electrónicas; se incluyen los datos utilizados para rastrear e identificar el origen y el destino de una comunicación, los datos sobre la ubicación del dispositivo generados en el contexto de la prestación de servicios de comunicaciones electrónicas, así como la fecha, la hora, la duración y el tipo de comunicación.

Así pues, el Reglamento se aplica al tratamiento de datos de comunicaciones electrónicas llevado a cabo en relación con la prestación y utilización de servicios de comunicaciones electrónicas, así como a la información relacionada con los equipos terminales de los usuarios finales. En concreto resulta de aplicación tanto a la prestación de servicios de comunicaciones electrónicas a los usuarios finales en la UE así como a la protección de la información relativa a los equipos terminales de los usuarios finales situados en la UE.

El Reglamento ePrivacy como ya lo hiciera el RGPD se aplica también a los prestadores extracomunitarios, a los que se les obliga a designar por escrito a un representante que habrá de establecerse en uno de los Estados miembros en que estén situados los usuarios finales.

Los proveedores no habrá de obtener el consentimiento para el tratamiento cuando los datos de comunicaciones electrónicas sean necesarios para transmitir la comunicación, y ello durante el período necesario para ese fin, o cuando sean necesario para mantener o restablecer la seguridad de las redes y servicios de comunicaciones electrónicas, o detectar fallos o errores técnicos en la transmisión de las comunicaciones electrónicas, y ello durante el período necesario para ese fin.

Podrán igualmente tratar los metadatos de comunicaciones electrónicas sin consentimiento del usuario cuando sea necesario para cumplir las obligaciones en materia de calidad del servicio, cuando sea necesario para proceder a la facturación, calcular las tarifas de interconexión, detectar o impedir la utilización abusiva o fraudulenta de los servicios de comunicaciones electrónica o abonarse a ellos, o cuando el usuario final haya dado su consentimiento para el tratamiento de sus metadatos de comunicaciones para uno o más fines concretos, entre ellos la prestación de servicios específicos a ese usuario final, siempre que el fin o los fines de que se trate no puedan alcanzarse mediante el tratamiento de información anonimizada.

En el resto de los casos, el tratamiento del contenido de las comunicaciones electrónicas estarán sujetas a

• Con el fin exclusivo de prestar un servicio específico a un usuario final, siempre que el usuario final o los usuarios finales interesados hayan dado su consentimiento para el tratamiento del contenido de sus comunicaciones electrónicas y la prestación de dicho servicio no pueda llevarse a cabo sin el tratamiento de ese contenido, o

• Cuando todos los usuarios finales interesados hayan dado su consentimiento para el tratamiento del contenido de sus comunicaciones electrónicas con uno o más fines específicos que no puedan alcanzarse mediante el tratamiento de información anonimizada, y el proveedor haya consultado a la autoridad de control.

El proveedor del servicio de comunicaciones electrónicas, excepto en los casos en que cuente con consentimiento o los datos sean necesarios para mantener o restablecer la seguridad de las redes y servicios de comunicaciones electrónicas, o detectar fallos o errores técnicos, tendrá que:

• Suprimir el contenido de las comunicaciones electrónicas o anonimizará esos datos una vez los hayan recibido el destinatario o destinatarios previstos. Tales datos podrán ser registrados o almacenados por los usuarios finales o por un tercero encargado por ellos de registrar, almacenar o tratar de cualquier otra forma los datos, de conformidad con el Reglamento (UE) 2016/679.

• Suprimir los metadatos de comunicaciones electrónicas o los anonimizará cuando ya no sean necesarios para transmitir una comunicación, excepto cuando sean necesarios para la facturación y únicamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse su pago con arreglo a la legislación nacional.

El Reglamento ePrivacy dedica una artículo específico, el 8, a la protección de la información almacenada en los equipos terminales de los usuarios finales y relativa a dichos equipos, que resulta de plena aplicación a la IoT. Así, el uso de las capacidades de tratamiento y almacenamiento de los equipos terminales y la recopilación de información del equipo terminal de los usuarios finales, incluida la relativa a su soporte físico y lógico, excepto por parte del usuario final, estarán prohibidos, salvo:

• Cuando sean necesarios con el fin exclusivo de efectuar la transmisión de una comunicación electrónica a través de una red de comunicaciones electrónicas, o

• Cuando el usuario final haya dado su consentimiento, o

• Cuando sean necesarios para la prestación de un servicio de la sociedad de la información solicitado por el usuario final, o

• Cuando sean necesarios para medir la audiencia en la web, siempre que esa medición corra a cargo del proveedor del servicio de la sociedad de la información solicitado por el usuario final.

Como se ve, este artículo es heredero de aquél en el que se basó toda la obligación de información en materia de cookies, pero ampliándolo y extendiéndolo a un mundo de dispositivos contactados y de máxima movilidad.
El Reglamento de ePrivacy, además, prohíbe la recopilación de la información emitida por un equipo terminal para poder conectarse a otro dispositivo o a un equipo de red, excepto en los siguientes casos:

• Cuando se lleve a cabo con el fin exclusivo de establecer una conexión y solamente durante el tiempo necesario para ello, o

• Cuando se muestre una advertencia clara y destacada que informe, como mínimo, de las modalidades de recopilación, su finalidad, las personas responsables de ella y la información restante requerida de conformidad con el artículo 13 del Reglamento (UE) 2016/679 en caso de que se recojan datos personales, así como de cualquier medida que pueda adoptar el usuario final del equipo terminal para interrumpir o reducir al mínimo la recopilación.

La recopilación de esta información en los casos exceptuado queda supeditada a la aplicación de medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado en relación con los riesgos, según lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

La advertencia antes referida podrá proporcionarse en combinación con el uso de iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto, quedando encargada la Comisión para determinar la información que se ha de presentar mediante iconos normalizados y los procedimientos para suministrar dichos iconos.

Uno de los problemas incontestables que ya hemos señalado es el de la recogida del consentimiento informado en el mundo IoT en el que las posibilidades de entregar la información al usuario con carácter previo se encuentran, a menudo, limitadas. Teniendo esto en mente, el artículo 9 del Reglamento de ePrivacy establece que cuando sea técnicamente posible y factible, el consentimiento podrá expresarse mediante la configuración técnica adecuada de una aplicación informática que permita acceder a Internet. Los usuarios finales que hayan dado su consentimiento para el tratamiento de datos de comunicaciones electrónicas dispondrán de la posibilidad de retirar su consentimiento en cualquier momento, según lo dispuesto en el artículo 7, apartado 3, del Reglamento (UE) 2016/679, y se les recordará esta posibilidad a intervalos regulares de seis meses mientras continúe el tratamiento.

Los programas informáticos comercializados que permiten comunicaciones electrónicas, incluyendo la recuperación y presentación de información de Internet, ofrecerán la posibilidad de impedir a terceros almacenar información sobre el equipo terminal de un usuario final o el tratamiento de información ya almacenada en ese equipo. Al iniciarse la instalación, los programas deberán informar a los usuarios finales acerca de las opciones de configuración de confidencialidad y, para que pueda proseguir la instalación, solicitar el consentimiento del usuario final respecto de una configuración determinada.

Pensando en una próxima aprobación, el Reglamento establece que los programas que ya se hayan instalado a fecha 25 de mayo de 2018 deberán cumplir los requisitos de consentimiento en el momento de la primera actualización de los programas, que habría de producirse, en todo caso, antes del 25 de agosto de 2018.

4. CONCLUSIONES

La falta de virtualidad de las políticas de protección de datos y de las cláusulas de información previas al consentimiento, unido a los problemas técnicos de recogida del consentimiento en los objetos conectados, parece recomendable la adopción de medidas tendentes a obligar a que los dispositivos IoT sean Privacy conformance desde su diseño y por defecto que se basen en Privacy-enhancing technologies (PET). Este es el camino que transita el Reglamento de ePrivacy, que establece limitaciones del uso de los datos y metadatos recabados a los meramente necesarios para la prestación del servicio, habiendo de optar por la anonimización siempre que el servicio lo permita. Los datos y metadatos que no entren en esta excepción han de ser suprimidos, a no ser que sean necesarios para la facturación, o se cuente con el consentimiento del usuario para su tratamiento, en cuyo caso habrá que aplicarles las medidas técnicas y organizativas apropiadas a su riesgo de conformidad con el RGPD.

En este sentido, resultan de enorme utilidad las propuestas efectuadas por EPIC en cuanto a las medidas de minimización y anonimización a considerar en el mundo IoT:

- Las entidades que recogen datos desde dispositivos inteligentes u objetos conectados han de limitarán el número y tipo de datos a recoger, proceder a su borrado completo y automático en un plazo de tiempo dado, limitando la sincronización automática o por defecto de los datos del dispositivo con una base de datos centralizada.

- Se debe mantener el control de los titulares de los datos sobre los mismos, incluido el derecho a limitar la recogida y uso de los datos a lo estrictamente imprescindible. Como ya hemos señalado, el sistema de recogida del consentimiento informado simplemente no funciona en IoT al carecer los dispositivos, con carácter general de pantallas o teclados y ser virtualmente inútiles para hacer consciente a los usuarios de los riesgos que facilitar sus datos tiene. En su lugar, parece más adecuado el uso de "Fair Information Practices" en las que, de manera afirmativa, se establezcan los derechos de los consumidores y las responsabilidades de las compañías que recaban los datos o, como establece el Reglamento de ePrivacy, el uso de aplicaciones que recojan el consentimiento y recuerden cada seis meses las opciones de cancelación.

- Las entidades que recogen datos usando IoT o smart devices deben facilitar acceso a la información que de ellos tienen de manera sencilla y transparente así como accede a la lógica básica detrás del algoritmo usado para tomar decisiones con respecto a él.

- Las compañías deben minimizar la recogida de datos generados por smart services mediante la adopción del principio de pertinencia del dato o data minimization, para que solo se recojan y almacenen los datos necesarios para asegurar la funcionalidad del producto o del servicio. Esta minimización se puede llevar a efecto de diversas formas:

  • Recogida de datos periódica o aleatoria en lugar de constante y permanentemente;

  • Recogida de datos de algunos productos en modo sampling representativos de un porcentaje de los objetos conectados en lugar de recoger datos de todos los productos;

  • Recogida de datos agregados en lugar de información granular en particular de cada usuario.

BLOQUE IV:
BUENAS PRÁCTICAS Y MEDIDAS DE CONFIANZA EN DISPOSITIVOS IOT ORIENTADOS AL USUARIO FINAL

1. INTRODUCCIÓN

1.1 EL "ESTADO DEL DESASTRE" EN MATERIA DE SEGURIDAD EN IOT

La realidad, vivida en los últimos tiempos, sobre la seguridad de productos IoT, refleja en cada uno de los sectores anteriormente mencionados, un panorama desolador. Sólo algunos ejemplos:

- En 2016, un grupo de hackers Sirio consiguió acceder a la red Scada de una planta de tratamiento de agua y cambiar la composición química del agua que bebían 2 millones y medio de personas. (Verizon Report, Marzo 2016)

- En 2015, unos investigadores demostraron que era posible secuestrar el control de un vehículo Chrysler Jeep desde Internet, lo que provocó que Chrysler tuviese que revisar un millón cuatrocientos mil vehículos. En 2016, después de los enormes costes incurridos, los mismos investigadores demostraron que la solución proporcionada por Chrysler no era efectiva y que los coches eran aún vulnerables. (https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/)

- La campaña de Navidad de 2015 fue particularmente intensa en lo que se refiere al ámbito de los juguete interconectados. Compañías como Mattel, y Fisher Price lanzaron juguetes (Hello Barbie, Smart Toy) con múltiples vulnerabilidades de seguridad, que entre otras cosas permitían que los juguetes pudiesen ser utilizados como dispositivos de espionaje. Este mismo año, Vtech sufrió una de las mayores brechas de seguridad, que supuso la pérdida de casi cinco millones de cuentas, con datos de aproximadamente siete millones de niños (http://www.businessinsider.com/vtech-data-breach-information-statistics-2015-12)

- En enero de 2017, se confirmó que los dispositivos cardiacos implantados por el hospital St. Jude Medical's en Nueva York, presentaban una vulnerabilidad mediante la cual alguien remotamente podría agotar la batería de los dispositivos, modificar el ritmo de funcionamiento, o incluso administrar descargas en el caso de los desfibriladores. (https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm)

- A finales de 2016, sufrimos uno de los mayores ataques de denegación de servicio, originado desde los propios dispositivos IoT que habían sido vulnerados, y que temporalmente inhabilitaron servicios como Netflix o Paypal.

En definitiva podríamos rellenar páginas y páginas con incidentes parecidos a estos, y aún no habríamos rascado si no la superficie de un problema que se antoja difícil de resolver.

Por un lado, los fabricantes de productos de IoT no tienen una cultura ni tradición en la fabricación de productos con una componente tecnológica, ni por supuesto conciencia de la importancia de la Ciberseguridad y por otro los consumidores no disponen de herramientas para poder valorar las medidas de seguridad que implementan los productos que adquieren.

Los gobiernos, mientras tanto, aplazan las decisiones de regular la seguridad en IoT, en palabras de una representante de Maureen Ohlhausen, representante de la Comisión de Comercio Federal de Estados Unidos (https://www.theguardian.com/technology/2017/mar/14/federal-trade-commission-internet-things-regulation):

> "We don't know if that risk will materialize. It may well materialize, but a solution may materialize at the same time."

1.2 BUENAS PRÁCTICAS Y MARCA DE GARANTÍA DE CIBERSEGURIDAD EN IOT

En la actualidad, no se dispone en el mercado de mecanismos que garanticen a los usuarios que se han tenido en cuenta los riesgos de seguridad en el desarrollo del sistema IoT y que éstos han sido minimizados. Por este motivo, desde el Centro de Estudios de la Movilidad y el IoT (CEM) del ISMS Forum Spain se ha desarrollado este manual de buenas prácticas orientado a la certificación de los dispositivos IoT. Adicionalmente a este manual se ha desarrollado el Reglamento de uso de Marca de Garantía que define la normativa que deben cumplir los fabricantes para la obtención del Sello de Confianza IoT en sus dispositivos.

Las buenas prácticas se han distribuido en seis dominios diferentes:

- Seguridad en el diseño.
- Gobierno y seguridad en el ciclo de vida comercial.
- Protección del Hardware/Firmware.
- Seguridad en las comunicaciones.
- Seguridad en sistemas.
- Seguridad jurídica.

Para cada dominio se establecen una serie de directrices y como anexo se incluye un checklist con todos los controles definidos en el manual.

2. SEGURIDAD EN EL DISEÑO

En relación al diseño de productos de IoT, es especialmente importante que la seguridad no sea considerada sólo en las fases finales de puesta en producción, si no como una parte esencial a considerar en una fase temprana de la concepción y diseño del producto.

Aunque existen muchas razones y ejemplos muy notorios de por qué es necesario considerar la seguridad en las fases tempranas del diseño, mencionaremos sólo dos de las más importantes:

1.- Coste. Está demostrado que implementar un cambio en las fases tempranas en el ciclo de vida de diseño del producto puede ser hasta 1,000 veces más costoso cuando el producto ha sido lanzado al mercado, sin incluir los posibles impactos relativos a la imagen, pérdida de información u otras responsabilidades que se pueden derivar de la aparición de una vulnerabilidad en un producto de IoT.

2.- Viabilidad. En algunos casos muy notorios, los errores de diseño no son solucionables mediante la aplicación de modificaciones sencillas o parches, si no que para poder solucionar el problema, es necesario realizar una reingeniería completa y cambios profundos que pueden afectar a componentes tanto hardware como software.

En relación a la seguridad en el diseño, nuestra recomendación es la adopción de un marco de seguridad en el ciclo de vida como SAMM (Modelo de Madurez de Aseguramiento del Software), que permite la implementación de una estrategia completa de seguridad en el ciclo de vida de desarrollo. Para más información, visitar el proyecto en https://www.owasp.org/index.php/OWASP_SAMM_Project

Desde un punto de vista práctico, estas son algunas de las prácticas de seguridad en el Diseño que se consideran imprescindibles, desde el punto de vista de seguridad en el diseño:

1. Haber designado a una persona que actúe con el rol de responsable de Seguridad para el proceso de diseño del producto de IoT en cuestión.

2. Contar una guía de desarrollo seguro, comunicada a todos los actores que participan en el proceso de desarrollo software (empleados Internos y Proveedores) basada en los estándares y buenas prácticas definidas por OWASP, y particularizadas al lenguaje o lenguajes de programación utilizados.

3. Haber realizado un análisis de riesgo (que considere las amenazas y los impactos desde el punto de vista de Ciberseguridad) en la fase del diseño inicial del producto, y en las modificaciones mayores del software.

4. Haber realizado al menos un análisis estático y dinámico del sistema por parte de un actor independiente, previamente a la puesta en producción o liberación para consumo.

Y por otro lado entre las que se considera recomendables, podemos mencionar por ejemplo la siguiente:

1. Realizar un análisis de los componentes de terceros, incluyendo librerías o componentes, para identificar riesgos de seguridad y operativos de los componentes utilizados a lo largo del desarrollo.

3.GOBIERNO Y SEGURIDAD EN EL CICLO DE VIDA COMERCIAL

El Gobierno de la Seguridad en el Ciclo de Vida Comercial en el ámbito de IoT es un elemento fundamental para una estrategia de seguridad robusta y a largo plazo ya que la seguridad se configura como una parte en constante evolución en el ecosistema IoT por lo que el establecimiento de buenas prácticas resulta indispensable. Las buenas prácticas en este bloque se centran en los mecanismos de respuesta y reacción ante incidentes de seguridad. Hay dos momentos a tener en cuenta a la hora de establecer el checklist de autoevaluación en el Gobierno de la Seguridad en el Ciclo de Vida Comercial en dispositivos IoT: el período de uso del dispositivo y el momento de desmantelamiento del dispositivo.

- Período de uso del dispositivo: Plazo en el que el usuario hace un uso efectivo del dispositivo.
- Desmantelamiento del dispositivo: Inutilización del dispositivo al final de su vida útil o integración de los datos en un nuevo ecosistema o dispositivo.

Los controles a revisar en este apartado a modo ejemplificativo:

- Tiempo de respuesta al consumidor, que debería establecerse en función del tipo de dispositivo y brecha.
- Medidas en el supuesto de servicio, pérdida, robo o fin de vida útil.
    - Destrucción de la información.
    - Inutilización del dispositivo (ON/OFF).
- Monitorización de los aspectos de seguridad del ecosistema IoT.
- Disponibilidad y Distribución de actualizaciones y parches de seguridad del software.
- Plazo de garantía.
- Canal de comunicación directo con el consumidor: Helpdesk, Web, etc.
- Comunicación y denuncia de brechas de seguridad.

Estos son algunos de los controles más representativos considerados imprescindibles en este apartado:

1. Las condiciones de garantía, soporte y canal de atención al consumidor deben tener en cuenta de forma específica aspectos de ciberseguridad.
2. La garantía y soporte del producto en materia de Ciberseguridad (incluidos parches y actualizaciones) debe extenderse al menos por un periodo equivalente al tiempo medio de vida del producto, y en cualquier caso al menos durante el plazo legal de garantía.
3. Debe existir y ser comunicado al usuario un proceso y un canal de comunicación (email, teléfono) para que puedan comunicarse incidencias y brechas de seguridad del producto
4. Mantener continuamente informado al usuario respecto a los riesgos y vulnerabilidades de seguridad del producto IoT.
5. Deben figurar en las instrucciones o manual del producto recomendaciones al usuario en materia de Ciberseguridad, que le permitan en su caso mejorar las características de seguridad a través de la configuración, y el usuario debe ser informado de las mismas en la configuración inicial.
6. Monitorización continua de servicios expuestos en el ecosistema para descubrir y en su caso alertar sobre vulnerabilidades de seguridad.
7. Método documentado para la eliminación segura de la información almacenada en el ecosistema IoT en caso de sustitución o fin de vida útil.

Y a continuación algunos de los que siendo recomendables no se han establecido aún como imprescindibles:

1. Debe poderse eliminar la información e inutilizar el dispositivo de manera remota por parte del usuario en caso de pérdida o robo.
2. Debe existir algún mecanismo (Interruptor físico u opción en la configuración) para deshabilitar las funciones de comunicación del dispositivo, cuando el usuario no quiera que estas se encuentren activas.
3. Deberían existir procesos y herramientas orientados a la detección de ataques sobre los dispositivos de IoT, una vez éstos están siendo utilizados por el consumidor.
4. Garantía de por vida en materia de Seguridad Informática.
5. El dispositivo debería actualizarse de manera periódica y automática para solventar los problemas de seguridad detectados.

4. PROTECCIÓN EN EL HARDWARE / FIRMWARE

Uno de los principales canalizadores del crecimiento de IoT ha sido la evolución del hardware. Los avances en este campo han generado hardware de mejor calidad, tamaño reducido y un precio muy asequible, que pone al alcance de todos los usuarios la tecnología, y por tanto, la posibilidad de realizar proyectos de mayor o menor calado de manera autónoma. Existen multitud de dispositivos con capacidad de proceso, almacenamiento, sensores y emisores desde 15 a 200 dólares.

Respecto al firmware o sistema embebido, el fundamento de los “smart devices” (dispositivos inteligentes) parte de tener un sistema operativo embebido que utilice las capacidades de cómputo, almacenamiento y comunicación, para aportar un valor añadido a la actividad habitual del objeto al que están asociados.

Esta sección da cobertura a dispositivos IoT específicos, como sensores, actuadores, wearables, etc, pero no a aquellos que diseñados con un carácter generalista dan cobertura a una aplicación de IoT, como por ejemplo un smartphone.
Cualquier dispositivo IoT específico debe disponer una serie de medidas de seguridad orientadas a proteger el dispositivo frente a ataques al mismo de manera física (los ataques que se producen teniendo acceso físico al dispositivo).

El firmware de un dispositivo es un vector de ataque especialmente atractivo por:

- Persistencia. Al contrario que otras vías de ataque, el firmware reside en memoria no volátil, es el primer componente que se carga y por tanto puede controlar el funcionamiento posterior del dispositivo.
- Invisibilidad. Los sistemas de antivirus/antimalware no comprueban el firmware, lo que en la práctica las modificaciones maliciosas en el firmware son prácticamente indetectables.
- Acceso Total. Los sistemas operativos que se cargan sobre el dispositivo relegan muchas de las funciones de seguridad en las funciones del firmware, por lo que en caso de modificación, es posible obviar todos los mecanismos de protección establecidos.

Y a continuación algunos de los que siendo recomendables no se han establecido aún como imprescindibles:

- Acceso directo al sistema
- Acceso a los datos almacenados en el dispositivo
- Alteración del código en el dispositivo para modificar su comportamiento, acceder a áreas restringidas o escalar privilegios.
- Inyección de Malware

Algunos de los procesos específicos de protección que se recomiendan imprescindibles para evitar este tipo de amenazas son:

1. Deshabilitar aquellos puertos o interfaces externos que no son utilizados por el usuario final (ejemplo: USB, puertos HDMI, interfaces de red, etc).
2. Deshabilitar cualquier interfaz de depuración, externa (por ejemplo interfaces serie) o interna (por ejemplo JTAG)
3. El dispositivo debe validar de manera segura el fichero de actualización de Firmware previamente a aceptarlo para realizar una actualización, con el objetivo de validar su autenticidad y evitar modificaciones al firmware.

4. En el caso de utilización de servicios de configuración centralizada, debe autenticarse tanto al dispos como el propio servicio mediante un mecanismo de reconocimiento mutuo.

5. Los periféricos o componentes que utilice el dispositivo deben estar soldados en placa base, y medida de lo posible no utilizar dispositivos extraíbles. Si se utilizan dispositivos extraíbles, debe e un mecanismo de autenticación y control de integridad entre las partes (comprobación de conexió dispositivos no verificados).

Así mismo existen una serie de medidas que resultan recomendables para aquellos fabricantes realmente com metidos con la seguridad, o cuyos dispositivos deban ser protegidos de manera especial en razón de los datos manejan o de la criticidad que las acciones del dispositivo tengan sobre los activos de información o person entre ellas:

1. Si resulta aplicable, habilitar el soporte UEFI y el mecanismo de SecureBoot, de manera que cualq componente cargado en el proceso de arranque deberá contar con una firma electrónica que garantiza sólo es ejecutado el software previamente validado por el fabricante.
2. Tanto claves de cifrado como los firmwares de inicialización deben residir en un área protegida, no d tamente accesible desde el sistema operativo.
3. Para datos especialmente sensibles, como las claves de cifrado y firmwares de restauración, se r mienda la utilización de criptografía para protegerlos, garantizando que la información en reposo e dispositivos de almacenamiento esté cifrada.

5. SEGURIDAD EN LAS COMUNICACIONES

En el ámbito de IoT existen múltiples y variados elementos de comunicación entre los componentes que pued formar parte de un ecosistema de IoT. En todos ellos, y cuando hablemos de la comunicación entre las part siempre tendremos en cuenta la triada clásica en seguridad de la información:

- Confidencialidad, que garantice que la información en tránsito entre los distintos componentes no puede ser interceptada y su contenido desvelado.
- Integridad, que garantice que la información que una parte transmite no se pueda ver alterada en el tránsito y que el receptor la reciba tal y como fue originariamente transmitida.
- Disponibilidad, que considerará si ante un fallo en un canal de comunicación, somos capaces de encontrar alguna vía de comunicación alternativa que nos permita recuperar un comportamiento normal o degradado del sistema.

Para definir las buenas prácticas de seguridad en las comunicaciones se tendrán en cuenta tres aspectos: La se sibilidad de la Información transmitida, los actores, el modelo de arquitectura y el protocolo.

SENSIBILIDAD DE LA INFORMACIÓN

La seguridad en las comunicaciones debe depender de la sensibilidad de la información que se transmite. A ef tos de este manual de buenas prácticas se considera que la información protegida especialmente por alguna L o normativa sectorial tendrá una sensibilidad alta y, por tanto, unos requerimientos de seguridad más elevado

- Datos personales y de salud.
- Datos relativos a tarjetas de crédito.

ACTORES:

• Sensores y Actuadores
Son los que tienen la capacidad de acción o el origen de la información que sustenta el sistema IoT
• Sistemas intermedios de comunicación
Consolidan la información de los sensores o proporcionan el mecanismo de comunicación entre ell (elementos de middleware, pasarelas, etc).

• Dispositivos móviles
En los que el dispositivo móvil puede comportarse como un elemento intermedio de comunicación, o como un elemento con capacidad de procesamiento, almacenamiento y lógica en cuanto al sistema IoT.
• Servidores
Son las estaciones principales de procesamiento y almacenamiento del sistema. Los servidores pueden enviar información al sensor (configuración, órdenes, etc.), recibir información y aportar las capacidades de procesamiento y lógica más potentes, requeridas por el sistema.

MODELO DE ARQUITECTURA DE COMUNICACIÓN:

• Sensor/actuador a Sensor/actuador: dispositivos que se conectan entre ellos sin intermediario que tramite la comunicación.
• Sensor/actuador a Concentrador.
• Sensor/actuador a Dispositivo móvil: Comunicación con dispositivos móviles como punto de interacción con el usuario final y/o como elemento.
• Dispositivo Internet : dispositivos que conectan directamente con algún servicio en Internet
• Dispositivo Gateway : dispositivos que conectan con algún servicio en Internet a través de un elemento intermedio.

PROTOCOLOS DE COMUNICACIÓN:

Los aspectos a revisar en este apartado son la confidencialidad de la información transmitida (únicamente emisor y receptor pueden conocer la información que se transmite), la integridad de la misma (se debe evitar que la información se modifique durante su transmisión) y la disponibilidad del canal de comunicación (evitar/detectar interferencias, saturaciones e inhibiciones de la señal).

- Los mecanismos implicados en garantizar la confidencialidad son
  - el cifrado de los datos o del canal.
  - Identificación de origen y destino
  - la autenticación de emisor y receptor.
- Para garantizar la integridad de los datos se pueden
  - firmar y/o implementar algoritmos de checksum.
- Para garantizar la trazabilidad
  - Registros de la operativa y pistas de auditoria
- Por último, la disponibilidad del canal de comunicación se puede
  - comprobar realizando comunicaciones de control que alerten en caso de pérdida del canal y/o activen un canal de comunicaciones alternativo.

Algunas de las medidas imprescindibles en los elementos de comunicaciones son las siguientes:

1. La no utilización de protocolos intrínsicamente inseguros, como: WEP o WPA, o la utilización de mecanismos de transmisión no cifrados ni autenticados en medios compartidos (como el aire, por ejemplo con redes WIFI abiertas).
2. Para aquellos datos que así haya sido establecido en el análisis de riesgo, el establecimiento de medidas de cifrado y de integridad de la información.
3. Identificación unívoca de los dispositivos que participan en la comunicación, utilizando medios no replicables (por ejemplo criptografía de clave pública, o mecanismos de sincronización de tiempos).
4. Metódos de autenticación seguros con uso de contraseñas modificables por el usuario final, uso de certificados digitales únicos y mecanismos de revocacion de credenciales.
5. Mantener registros de las conexiones, en función de lo establecido en el análisis de riesgo.

Y por otro lado una muestra de las que se consideran recomendables:

1. Mecanismos de cifrado, protección y cambio de claves cuando la información no tenga sensibilidad alta.
2. Comprobaciones de cadena de certificación, validez del certificado y revocación del mismo.
3. Integridad del registro de las conexiones.
4. Medidas para prevenir la saturación del canal.
5. Existencia de un canal de comunicaciones alternativo.
6. Realizar un analisis de vulnerabilidades sobre las comunicaciones.

6. SEGURIDAD EN SISTEMAS

La seguridad de los sistemas tiene en consideración la dimensión del sistema operativo y del software de base de los actores expuestos en el apartado anterior.

Cuando se comparte información entre dispositivos IoT, se hace a través de aplicaciones destinadas a generar beneficio a los usuarios. Un ejemplo práctico podría ser una aplicación en un móvil recibiendo notificaciones desde dispositivos BLE (Bluetooth Low Energy) como los beacons. Esta aplicación a su vez, utilizaría esa información para comunicarse con un servidor que aportaría valor al usuario a través de servicios.

También se utilizan sistemas de Big Data y software analítico. Son uno de los grandes beneficios económicos de Internet of Things debido a las posibilidades que ofrece la cantidad de información que se genera a diario y el valor que tiene explotarla.

A continuación se enumeran los posibles riesgos potenciales asociados a la Seguridad en Sistemas, según los elementos identificados:

- Autorización/autenticación insuficiente: Posibilidad de acceso indebido al sistema, tanto de usuarios internos como externos, debido a fallos en el sistema de autenticación o autorización.
- Elevación de Privilegio, en el que puedan ejecutarse funciones con mayor nivel de seguridad del originariamente definido.
- Acceso a información confidencial almacenada en los diferentes sistemas.

Y algunas de las posibles vulnerabilidades que desde el punto de vista de sistemas pueden ayudar a la transformación de una amenaza en un impacto:

- Utilización de contraseñas de acceso al sistema estándar, o excesivamente simples.
- Sistemas de gestión y administración remota no seguros.
- Utilización de versiones de software con vulnerabilidades conocidas.
- Existencia de relaciones de confianza entre sistemas.
- Almacenamiento no cifrado de información confidencial en reposo.
- Utilización de programas o servicios con vulnerabilidades conocidas.
- Acceso a las versiones de firmware.
- Exposición de programas y/o servicios no necesarios en la fase de producción.

A continuación se enumeran algunas de las medidas que para la Seguridad en Sistemas establecen como obligatorias:

1. Obligar al usuario a cambiar las contraseñas por defecto la primera vez que accede al sistema.
2. Haber realizado un proceso de identificación de servicios y programas presentes en los sistemas y bastionado de todos los sistemas presentes en el ecosistema.
3. El control de acceso se debe basar en una gestión de usuarios y contraseñas, y debe garantizar que se permiten crear usuarios no administradores.
4. Disponer de una política de caducidad y complejidad de contraseñas para los usuarios finales que acceden al servicio.
5. Almacenar las contraseñas cifradas y disponer de un sistema de recuperación de contraseñas seguro.
6. Disponer de granularidad en los accesos, por ejemplo con sistemas basados en roles.
7. Mantener un registro de los eventos de seguridad.
8. Disponer de protecciones contra ataques de desbordamiento (anti-DoS), si en el análisis de riesgo se ha determinado que la disponibilidad es algo prioritario.
9. Disponer de protecciones anti-malware.

Y por otro lado algunas de las que se consideran recomendables :

1. Utilización de guías de bastionado de fuentes autoritativas, como CIS.
2. Utilización de mecanismos de autenticación de doble factor.
3. Utilización de un sistema de eventos de seguridad que se pueda consultar y que permita detectar y alertar incidentes de seguridad.
4. Permitir la implementación de arquitectura de alta disponibilidad.

7. SEGURIDAD JURÍDICA

Además de los aspectos técnicos, de gobierno y de ciclo de vida comercial, las buenas prácticas no estarían completas sin hacer referencia a las buenas prácticas que, desde el punto de vista jurídico, deben ser parte del diseño y la consideración de los fabricantes a la hora de desarrollar y producir un producto IoT.

Vivimos en una sociedad en la que la presión normativa es creciente, e inevitablemente aspectos como la Ciberseguridad y la Privacidad se hacen un hueco cada vez mayor en los ámbitos legislativos, obligando a fabricantes e instituciones al cumplimiento de un marco normativo complejo.

Entre otras normas y regulaciones que son de aplicación específica al ámbito de productos IoT orientados al consumidor final, se encuentran de manera principal:

- Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (conocido como Reglamento General de Protección de Datos o RGPD).
- Directiva 2016/1148 Del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (conocida como Directiva NIS).
- Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información.- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.
- Ley 17/2001, de 7 de diciembre, de Marcas.
- Ley 11/1986, de 20 de marzo, de Patentes.
- Ley 50/1980, de 8 de octubre, de Contrato de Seguro.
- Reglamento (CE) 593/2008 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013 sobre resolución de litigios en línea en materia de consumo.
- Reglamento (CE) 593/2008 del Parlamento Europeo y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las obligaciones contractuales (Roma I).

Es recomendable que, además de tener en cuenta la legislación general, cada fabricante analice su propio sector, actividad, producto concreto, etc., para identificar regulaciones específicas que apliquen al ámbito del producto IoT en cuestión, y que pueden en su caso, contener requisitos de aplicación.

Este dominio establece las características esenciales que, desde un punto estrictamente jurídico, debe reunir un producto IoT dirigido a consumidores (considerando que, en determinadas circunstancias, tal consumidor final puede ser una empresa). A partir de un catálogo de las normativas que se han considerado más relevantes, se establecen los requisitos de cumplimiento a considerar, tanto antes de la puesta en el mercado del producto IoT, como después de tal puesta en el mercado.

Los controles se agruparán en las siguientes materias:

1. Propiedad intelectual e industrial
2. Responsabilidad por los productos
3. Privacidad
4. Consumidores y usuarios
5. Medio ambiente y calidad
6. Resolución de disputas
7. Cambios en las condiciones de uso

Algunos de los controles obligatorios en el dominio de Seguridad Jurídica son, de forma resumida y no exhaustiva:

1. Haber realizado una evaluación de Impacto de la Privacidad del producto y de los datos que maneja
2. Disponer de un Seguro de Responsabilidad Civil que cubra indemnizaciones a terceros por los daños que se puedan causar relacionados con el producto IoT.
3. Cumplimiento de la normativa de Protección de Datos Personales: política de tratamiento de datos personales, procedimientos de atención a los derechos de los usuarios, determinación de las medidas técnicas de seguridad del dispositivo IoT teniendo en cuenta la técnica, los riesgos y la finalidad del tratamiento, realización de una evaluación de impacto en la privacidad, …
4. Información en el embalaje del producto (por ejemplo mediante un enlace a una página web) respecto a la política de tratamiento de datos personales y las medidas técnicas aplicadas.
5. Notificación de todas las brechas de seguridad a los usuarios afectados en todos los casos en los que sus datos se hayan visto comprometidos.
6. En la fabricación del producto y la implementación de las medidas de seguridad, tener en cuenta los riesgos que puedan afectar a la salud, seguridad y privacidad del usuario.

Y por otro lado se recomiendan establecer los siguientes, de forma resumida y no exhaustiva:

1. Proteger adecuadamente las marcas propias utilizadas en el producto IoT.
2. Inscribir correctamente las patentes propias aplicadas al producto IoT.
3. Previsión de indemnizar a los usuarios en caso de daños ocasionados por debilidades en ciberseguridad del producto IoT.
4. Que el usuario disponga de una aplicación u opción de configuración para conocer y controlar los datos personales que el ecosistema IoT (dispositivo, elementos intermedios, app móvil, cloud) está manejando, en la cual pueda ejercer de una forma inmediata sus derechos como sujeto de acuerdo a la regulación vigente.