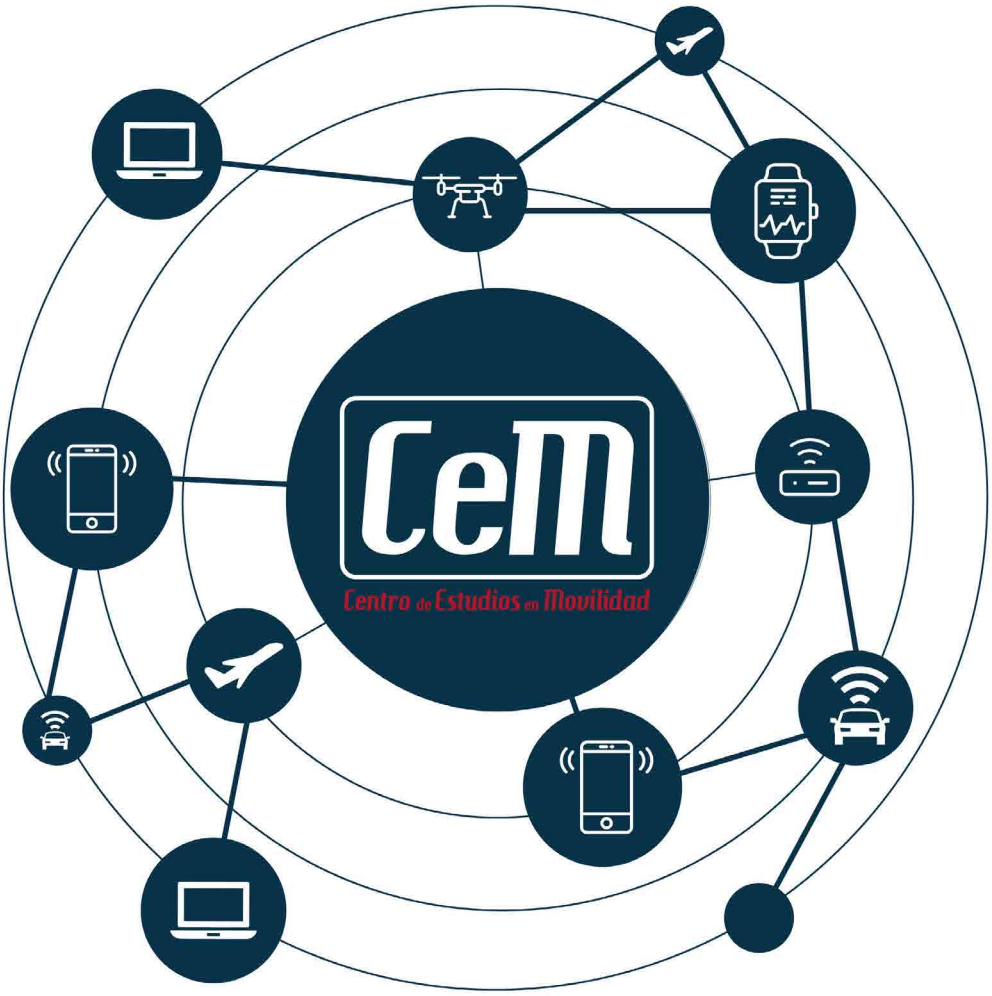
isms forum spain

AVANCE INFORMATIVO



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

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 COLABORACIÓN

García, Daniel
Campo, Laura do

ÍNDICE

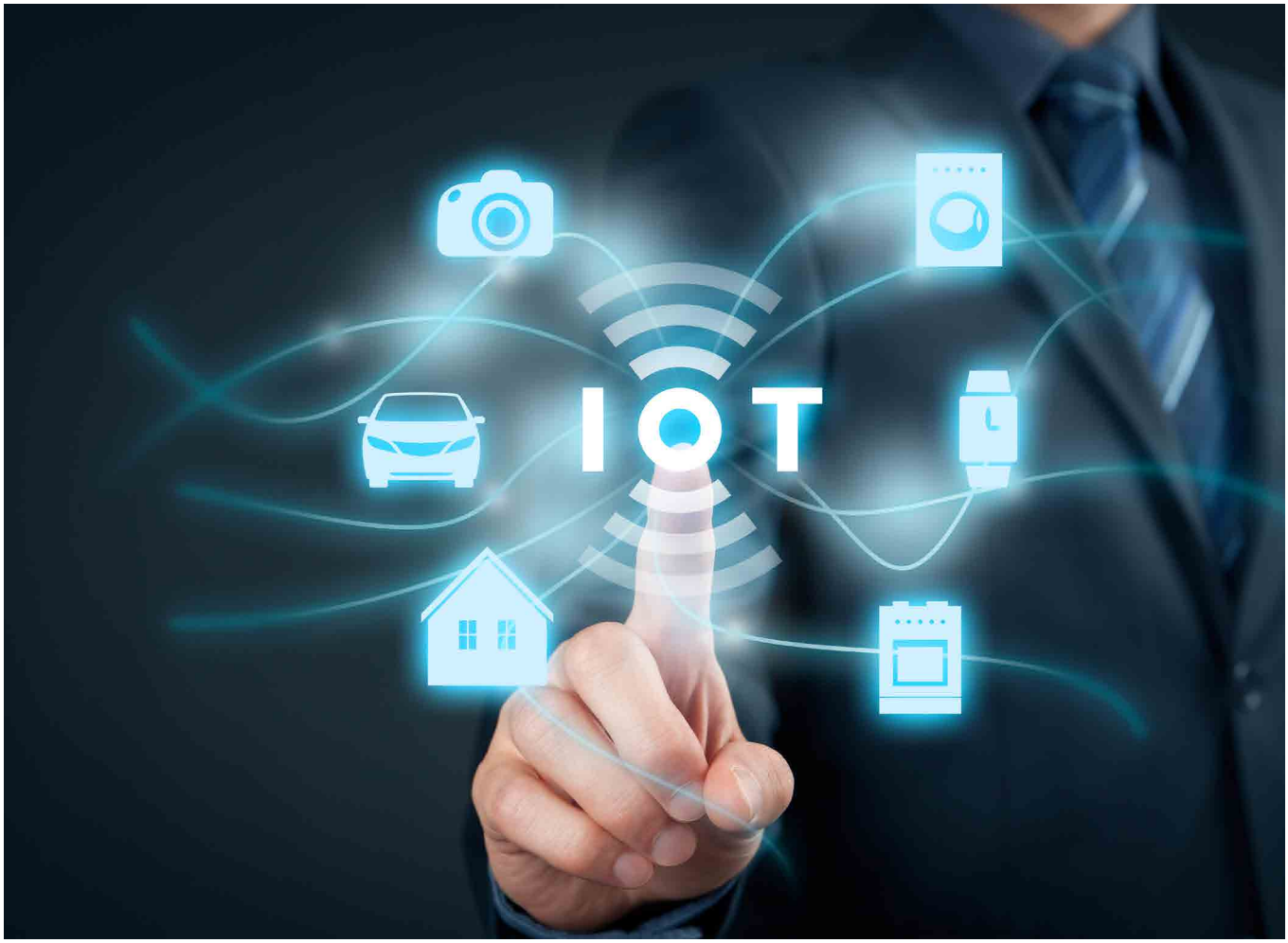
BLOQUE I:
ESTADO DEL ARTE DEL INTERNET DE LAS COSAS (IOT)

1. INTRODUCCIÓN

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.



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.

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:

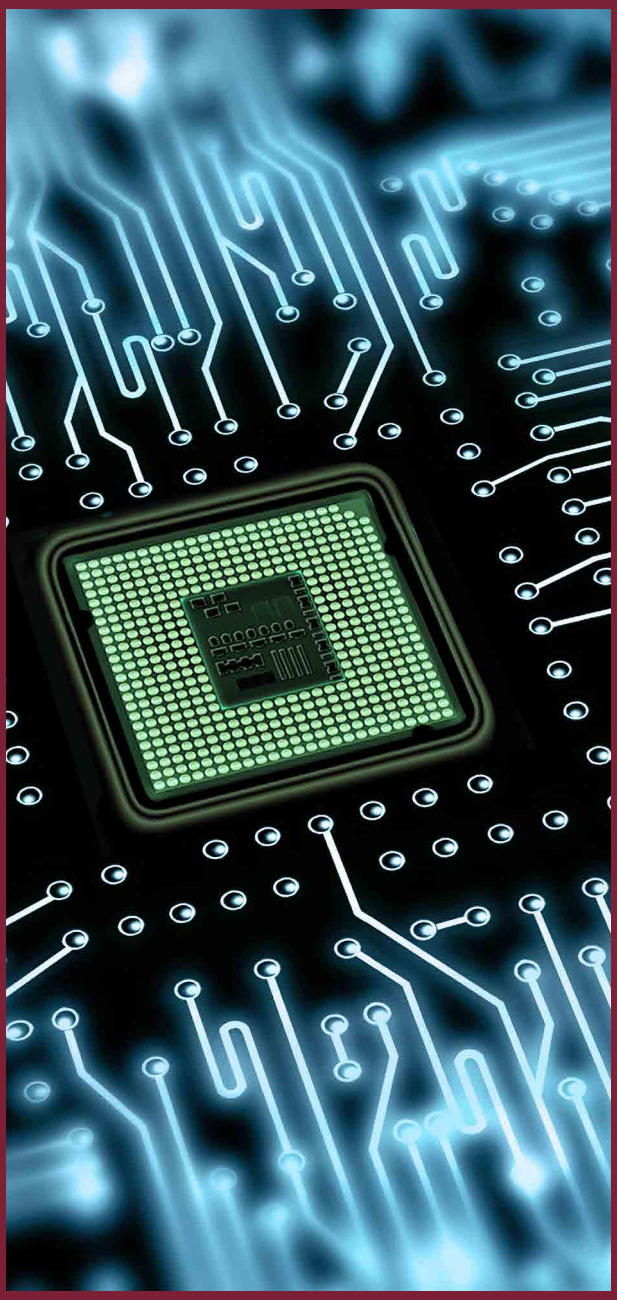
- Firmware o sistemas embebidos: El fundamento de los "smart devices" parte de tener un sistema operativo embebido que utilice las capacidades de cómputo, almacenamiento y comunicación necesarias para aportar un valor añadido.

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

- 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.



3. ÁMBITOS DE APLICACIÓN

La reciente eclosión del Internet de las cosas (IoT) 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.

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.

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.

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

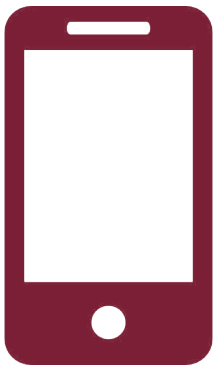
Las ciudades contarán con sensores de luz que no sólo responderán a las mediciones de luz ambiental, sino que en virtud del nivel de seguridad de la zona iluminarán con mayor o menor grado. Se instalarán sensores de limpieza en contendores y camiones, de luz, de ruido, de tráfico inteligente, entre otros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

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.

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.

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.

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 disponien 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. Dicha confianza de segurida es esa confianza de seguridad en la circulación donde surge la desconfianza de los expertos de seguridad de la información.

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.

Pero 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).

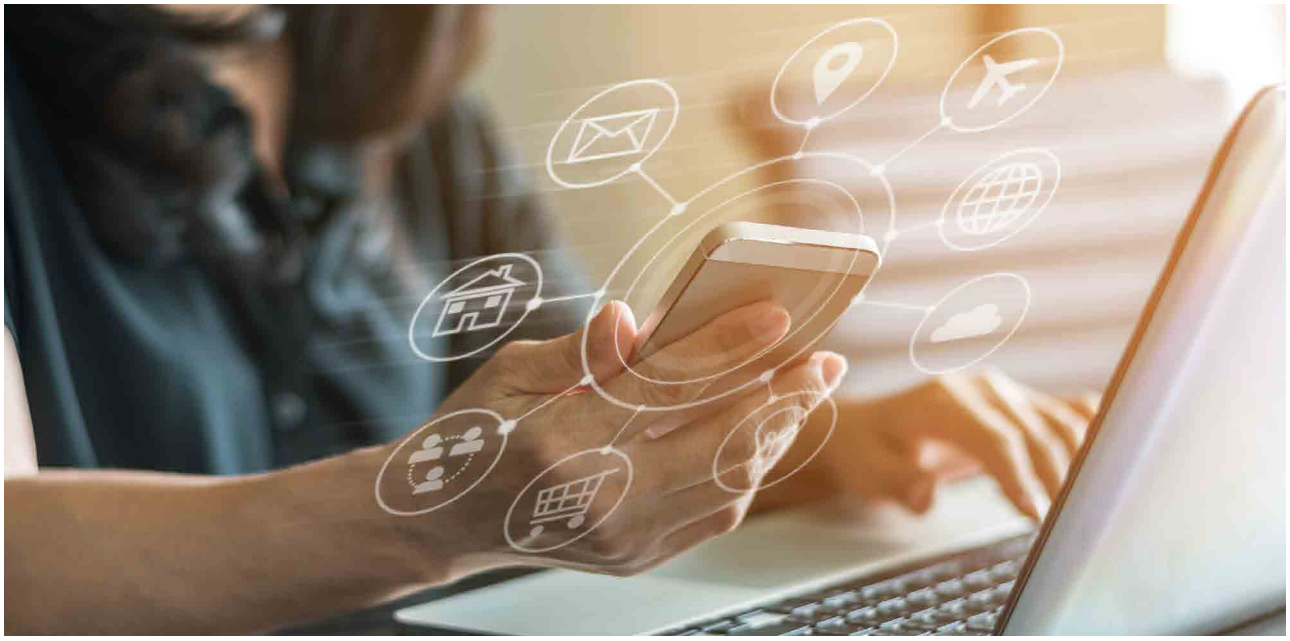
En la seguridad del IoT (lo que algunos llaman SoT) nos encontramos con una serie de desafíos tales como la seguridad en todo el ciclo de vida (desde los trabajos de diseño, hasta el difícil mantenimiento de actualizaciones / parches de seguridad) sumando a la forma a la que podremos proteger la red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



4.2 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 domestica, 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.

4.3 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 Riesgos (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. INTRODUCCIÓN

El estudio de los vectores de ataque asociados a los dispositivos y entornos del Internet de las cosas (IoT, Internet of Things) 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 permite evaluar de manera global la seguridad de cualquier dispositivo o solución IoT. Debe tenerse en cuenta que existen vulnerabilidades de seguridad comunes entre diferentes áreas, como por ejemplo debilidades en los mecanismos de autentificación, autorización, cifrado (tanto en reposo como en tránsito), etc.

Los distintos vectores de ataque asociados a un dispositivo IoT se pueden agrupar en múltiples categorías, según la naturaleza y la posible aproximación que tomaría un potencial atacante a la hora de intentar vulnerar su seguridad y la privacidad de su propietario o usuarios, o a la hora de encontrar debilidades en sus mecanismos de seguridad, en caso de disponer de alguno.

2. VECTORES DE ATAQUE

2.1. VECTOR DE ATAQUE FÍSICO

Representa aquellos ataques que requieren de acceso físico al dispositivo, por ejemplo, a través de sus puertos o interfaces USB, Ethernet, HDMI, serie, consola, depuración, JTAG, etc.

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.

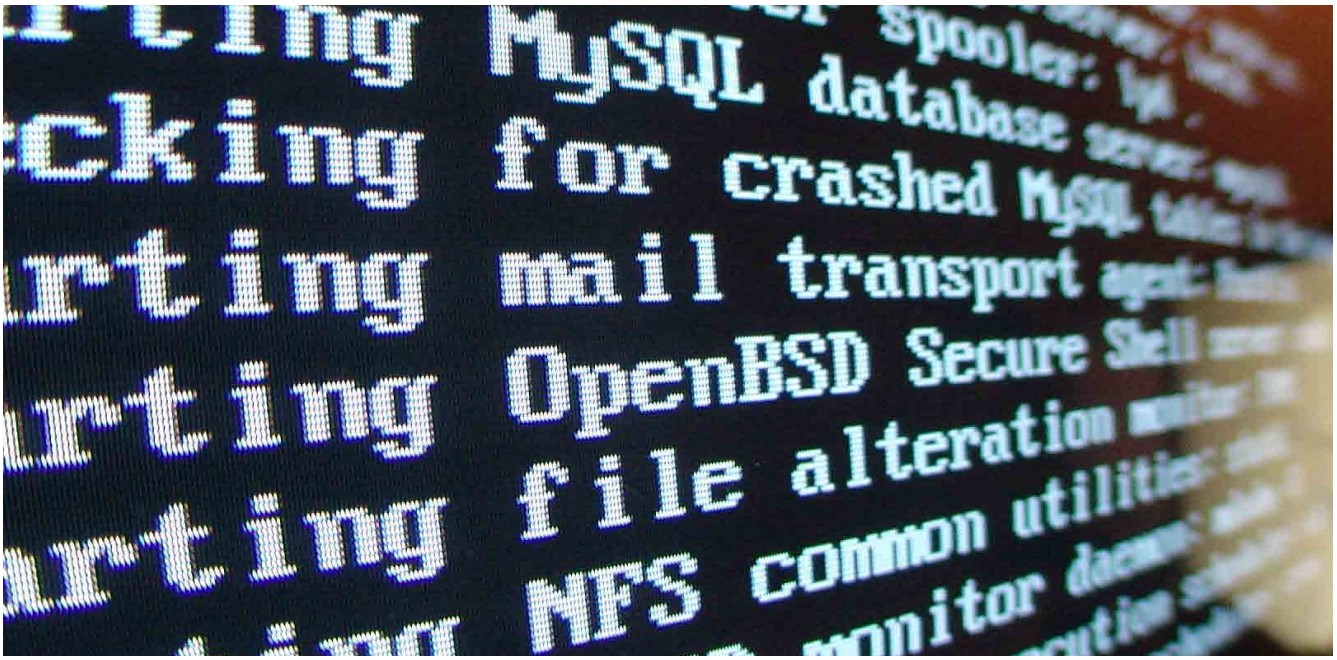
2.2. VECTOR DE ATAQUE SOBRE LAS COMUNICACIONES

Representa aquellos ataques cuyo objetivo es uno o varios protocolos o tecnologías de comunicación del dispositivo con un tercero (otro dispositivo, un servidor central, un dispositivo o aplicación móvil, servicios remotos, etc.).

Los ataques a las comunicaciones suelen tener como fin la interceptación para analizar los datos intercambiados (eavesdropping), así como la interceptación y/o 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 pueden clasificar las comunicaciones según el medio de transmisión: el aire libre (radio frecuencia o RF) o mediante una conexión física empleando un cable.

Dentro de las comunicaciones cableadas, es habitual encontrar estándares comunes en la industria como USB, Ethernet, HDMI, etc.

Dentro de las comunicaciones de radio, se puede 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, de aquellas comunicaciones comerciales (o reguladas) que sí requieren disponer de una licencia para poder transmitir.



Las comunicaciones inalámbricas no licenciadas hacen uso tanto de tecnologías muy comunes y ampliamente utilizadas, como por ejemplo Bluetooth y Wi-Fi, como de tecnologías de más reciente aparición, muy vinculadas a soluciones y entornos propios del IoT, como por ejemplo Bluetooth Low Energy (BLE), Z-Wave, LoRa, LoRaWan, SigFox, etc., y otros mecanismos de comunicación propietarios (ej. habitualmente empleando las frecuencias de 433 y 868 MHz en Europa).

Las comunicaciones inalámbricas licenciadas hacen uso de diferentes tecnologías como transmisiones de datos móviles (2/3/4G), LPWA, WiMax, etc.

2.3. VECTOR DE ATAQUE SOBRE LAS CAPACIDADES DE GESTIÓN

Representa aquellos ataques cuyo objetivo son los mecanismos de gestión de los propios dispositivos IoT. En determinadas circunstancias los ataques pueden ser lanzados contra la plataforma y/o capacidades de gestión remota de los dispositivos, lo cual podría dejar a todos ellos desconectados de su servicio central e incomunicados entre sí, y sin posibilidad de ser reconfigurados y monitorizados.

2.4. VECTOR DE ATAQUE SOBRE LOS SERVICIOS Y/O DATOS

Representa 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. En determinadas circunstancias, como las pulseras inteligentes (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.

La clasificación planteada pretende ofrecer una visión general de las áreas de exposición de los dispositivos IoT. A continuación de enumeran los vectores de ataque para cada una de las categorías definidas anteriormente:

- Puertos de conexión del dispositivo IoT.
- Firmware del dispositivo IoT.
- Comunicaciones entre el dispositivo IoT y “la nube” (Cloud).
- Comunicaciones entre el dispositivo IoT y dispositivos y/o aplicaciones móviles.
- Comunicaciones inalámbricas del dispositivo IoT.
- Interfaz web (y otros interfaces de gestión) del dispositivo IoT.
- Otros servicios de red del dispositivo IoT.
- Almacenamiento local de datos e información en el dispositivo IoT.

El estudio completo, y la metodología de análisis de la seguridad de los dispositivos IoT, que será publicado en el último trimestre del año 2017 por el CEM del ISMS Forum, profundizará en la descripción y los objetivos de cada uno de estos vectores de ataque, proporcionando detalles de las técnicas y herramientas de ataque que permiten aprovechar cada uno de estos vectores, complementados con ejemplos de vulnerabilidades y/o incidentes IoT empleando cada uno de estos vectores de ataque.

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

1. INTRODUCCIÓN

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, hacen 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 (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), 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 aplicarle las medidas técnicas y organizativas apropiadas a su riesgo de conformidad con el RGPD (Reglamento General de Protección de Datos).

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 el 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 (Reglamento General de Protección de Datos), 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 habrán 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, los tratamientos del contenido de las comunicaciones electrónicas estarán sujetas a previo consentimiento, en concreto:

• 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.
• 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 exceptuados 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.

2. RECOMENDACIONES

Por estos motivos, resultan de enorme utilidad las propuestas efectuadas por EPIC en cuanto a las medidas de minimización y anonimización a considerar en el mundo IoT, que recogemos como recomendaciones a modo de conclusión:

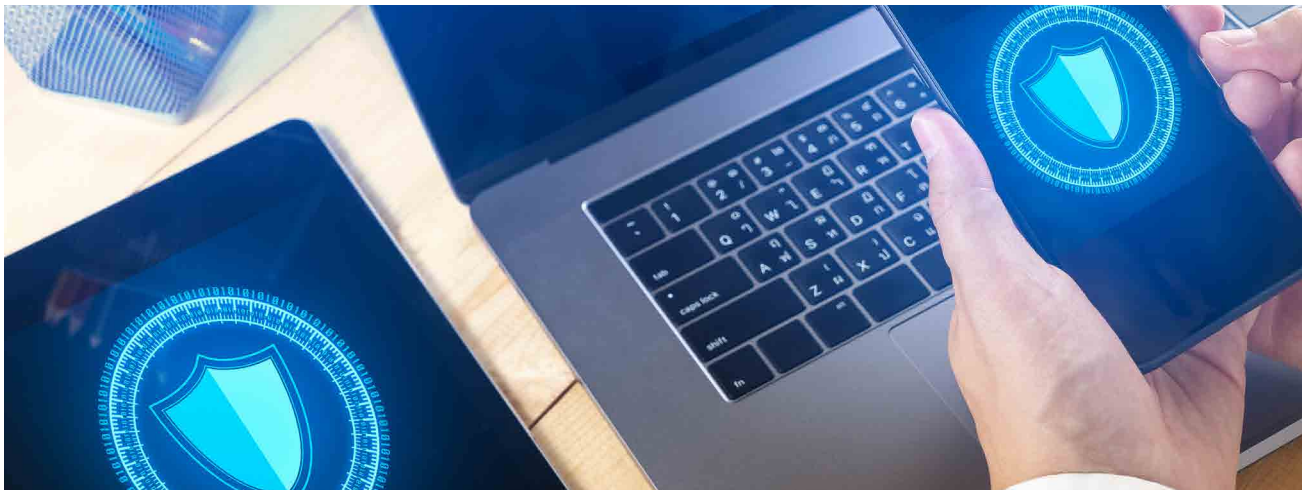
- Las entidades que recogen datos desde dispositivos inteligentes u objetos conectados han de limitar el número y tipo de datos a recoger, proceder a su borrado completo y automático en un plazo de tiempo dado, limitando la sincronización automática o por defecto de los datos del dispositivo con una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

  - o Recogida de datos periódica o aleatoria en lugar de constante y permanentemente.
  - o 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.
  - o Recogida de datos agregados en lugar de información granular en particular de cada usuario.



1.Comments Of The Electronic Privacy Information Center To National Telecommunications And Information Administration, U.S. Department Of Commerce On the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things [Docket No. 160331306-6306-01] June 2, 2016

BLOQUE IV:
BUENAS PRÁCTICAS EN DISPOSITIVOS IOT ORIENTADOS AL USUARIO FINAL

1. INTRODUCCIÓN

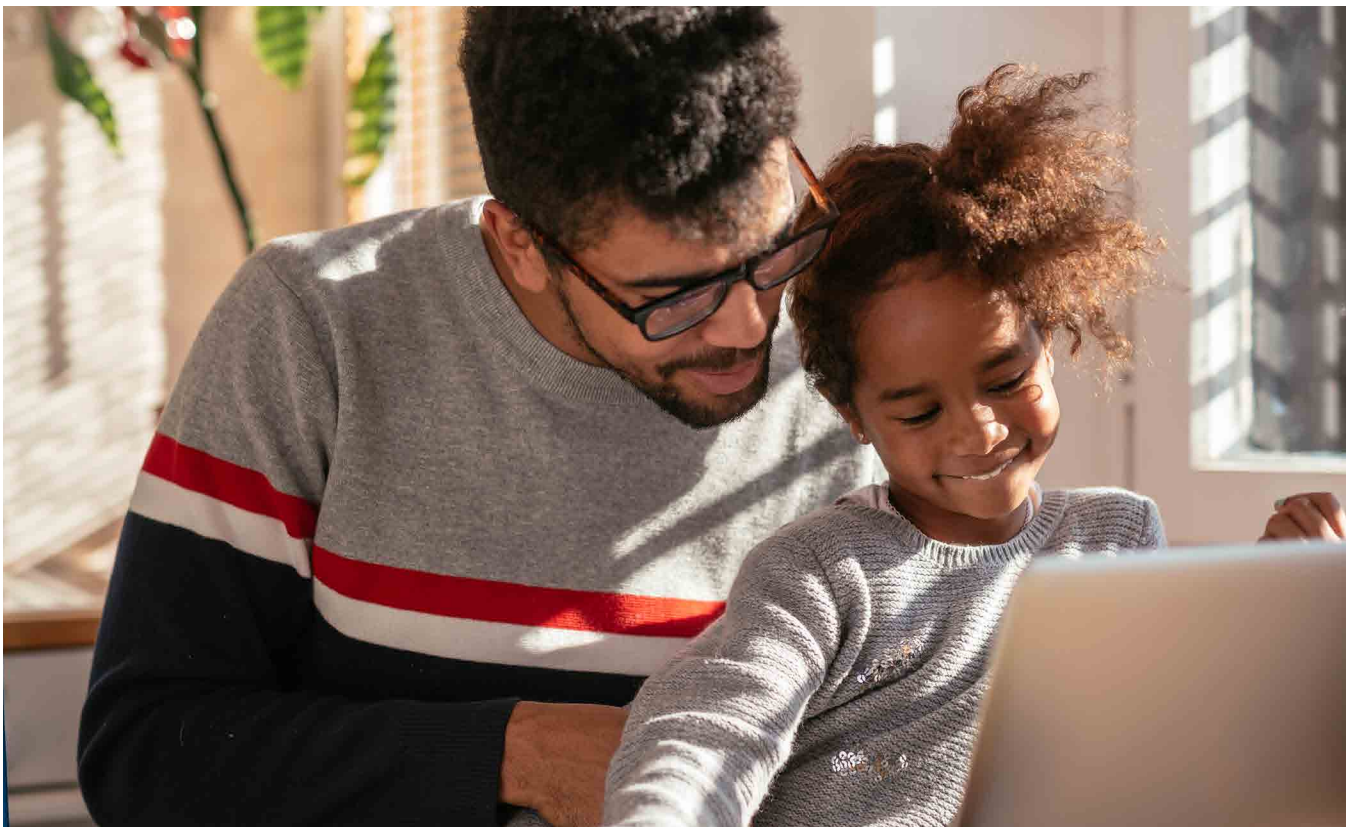
En la actualidad, no se dispone en el mercado de mecanismos que garanticen a los usuarios que se han tenido en cuenta los riesgos de seguridad en el desarrollo del sistema IoT y que éstos han sido minimizados.

Por este motivo, desde el Centro de Estudios de la Movilidad y el IoT (CEM) de ISMS Forum Spain se ha trabajado en dos líneas de manera coordinada: por un lado en la definición de un catálogo de buenas prácticas en el diseño e implementación segura de productos IoT, y por otro lado en dotar a la Industria de un mecanismo de reconocimiento de las medidas de seguridad implementadas (La Marca de garantía de Ciberseguridad en IoT).

1.1 CATÁLOGO DE BUENAS PRÁCTICAS EN EL DISEÑO E IMPLEMENTACIÓN SEGURA DE PRODUCTOS IOT

En cuanto a las buenas prácticas para los fabricantes de productos de IoT, éstas se han distribuido en seis dominios diferentes:

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



2. MARCA DE GARANTÍA DE CIBERSEGURIDAD IOT

Adicionalmente, y como una parte fundamental del trabajo de este grupo, se ha decidido crear un mecanismo tangible para que los fabricantes puedan poner en valor su compromiso con la seguridad y que los usuarios finales puedan verificar la seguridad de los productos que adquieren. Se trata de la Marca de Garantía de Ciberseguridad en IoT de ISMS Forum, la cual contará con un distintivo específico, que podrá ser incorporado en todas las referencias al producto, incluyendo el embalaje o la etiqueta del producto.

Para poder hacer uso de esta marca, que funciona esencialmente de una forma parecida a como lo hacen las denominaciones de origen, las empresas que lo desean deberán acogerse al reglamento de uso de la marca y realizar un proceso de autoevaluación de las medidas de seguri-

Ilustración 1.- Distintivo de la Marca de Garantía

Sólo tras la evaluación exitosa del producto, y previa validación por parte de ISMS del procedimiento y la plantilla de respuesta, será posible que exhiban este distintivo.

ISMS por su parte se reservará el derecho de realizar auditorías para comprobar que la información proporcionada por los fabricantes es fidedigna, y en caso de que se detecte alguna no conformidad grave, podrá solicitar al mismo la retirada del distintivo.

Como parte del reglamento, se establece una lista de controles a verificar, distribuidos en dos categorías: los obligatorios (necesarios para poder exhibir el distintivo) y los recomendables (cuyo cumplimiento es opcional).

A continuación, se describen algunos de los controles que los fabricantes deberán implementar para ser acreedores de la marca de garantía de ISMS Forum:

2.1. 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, sino como una parte esencial a considerar en una fase temprana de la concepción y diseño del producto.

En este dominio se exige que se haya realizado un diseño de seguridad del producto, así como que se haya seguido las mejores prácticas en materia de seguridad de la información, incluyendo por ejemplo la obligatoriedad de que las personas que diseñen un producto hayan recibido formación específica en seguridad, o que el producto haya sido testado por un agente independiente antes de ser libertado para el consumidor.

2.2. PROTECCIÓN DEL 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 precio 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.

En este dominio se exige a los fabricantes que deshabiliten cualquier característica física del equipo que pueda facilitar a un atacante tomar control del dispositivo, como por ejemplo puertos innecesarios. También se pone especial cuidado en las vías de actualización del firmware, ya que este elemento que hace de interlocutor con la parte física de los dispositivos es uno de los vectores de ataque más atractivos para los atacantes debido a su características de no volatilidad y acceso total a las funciones hardware del dispositivo.

2.3. SEGURIDAD EN LAS COMUNICACIONES

Los dispositivos IoT no actúan solos. Normalmente se comunican con elementos intermedios como nuestros dispositivos móviles, servicios basados en cloud, o incluso otros dispositivos IoT. Es lo que denominamos "ecosistema IoT".

En este "ecosistema", los fabricantes deberán demostrar unas medidas de seguridad acordes con la sensibilidad de los datos que manejan (a través del preceptivo análisis de riesgo), y aplicar medidas orientadas a proteger la confidencialidad, integridad y disponibilidad. También deberán lidiar con la "Identidad de las cosas", siendo obligatorio la implementación de mecanismos de autenticación en la comunicación de los distintos elementos.

2.4. SEGURIDAD EN LOS 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.

Entre otras cosas, los fabricantes deberán demostrar que las funciones de administración de los sistemas están protegidas, así como prevenir las temidas "contraseñas por defecto" que obligatoriamente deberán solicitar el cambio al usuario cuando éste utilice el producto por primera vez. Por otro lado, también se exigirá que los sistemas cuenten con protección antimalware.

2.5. 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 que el consumidor tenga garantías de que la seguridad del producto se mantiene durante su utilización, así como para que disponga de mecanismos de comunicación con el fabricante en materia de seguridad.

Para poder optar a la utilización de la marca, los fabricantes designación a una figura cualificada para que actúe como responsable de la seguridad de la información del producto IoT. También deberán proporcionar información clara y concisa sobre las medidas de seguridad que implementa el producto, así como del análisis de riesgo realizado. La seguridad deberá tener un tratamiento específico en los canales de comunicación y de soporte, recibiendo por parte del usuario información sobre

2.6. SEGURIDAD JURÍDICA

Este dominio pretende establecer 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).

En este dominio, se repasan algunas de las obligaciones que, desde el punto de vista jurídico y normativo los fabricantes deberán tener en cuenta, prestando especial atención a los aspectos de privacidad, responsabilidad civil y propiedad intelectual, como por ejemplo la notificación obligatoria al consumidor en caso de que el fabricante haya sufrido una brecha, o la obligatoriedad de cubrir cualquier daño causado por un dispositivo IoT, cuando el origen del problema esté en un problema de seguridad.

isms forum spain