Recomendaciones sobre la seguridad y la privacidad de la Internet de las cosas (IoT) INFORME DEL GRUPO DE ASESORAMIENTO TÉCNICO DE LA INTERNET DE BANDA ANCHA

Un informe de acuerdo uniforme

Emitido:

Noviembre de 2016

Derechos de autor / Aviso legal

Sobre el CAPI

El Grupo de Asesoramiento Técnico sobre Internet de Banda Ancha (BITAG) es una organización sin ánimo de lucro y con múltiples partes interesadas que se dedica a reunir a ingenieros y tecnólogos en un Grupo de Trabajo Técnico (TWG) para desarrollar un consenso sobre las prácticas de gestión de redes de banda ancha y otras cuestiones técnicas relacionadas que pueden afectar a la experiencia de los usuarios en Internet, incluido el impacto hacia y desde las aplicaciones, los contenidos y los dispositivos que utilizan Internet.

La misión del CAPI incluye: (a) educar a los responsables políticos en estas cuestiones técnicas; (b) abordar cuestiones técnicas específicas en un esfuerzo por minimizar las disputas políticas relacionadas; y (c) servir de caja de resonancia de nuevas ideas y prácticas de gestión de la red. Las funciones específicas del GTT también pueden incluir: (i) identificar las "mejores prácticas" por parte de los proveedores de banda ancha y otras entidades; (ii) interpretar y aplicar las prácticas de "puerto seguro"; (iii) proporcionar de otro modo orientación técnica a la industria y al público; y/o (iv) emitir dictámenes consultivos sobre las cuestiones técnicas relacionadas con la misión del TWG que puedan subyacer a los conflictos relativos a las prácticas de gestión de la red de banda ancha.

El Grupo de Trabajo Técnico del BITAG y sus Comités individuales toman decisiones mediante un proceso de consenso, con los correspondientes niveles de acuerdo representados en la portada de cada informe. Cada representante del GTT trabaja para lograr el consenso en torno a las recomendaciones que sus respectivas organizaciones apoyan, aunque incluso en el nivel más alto de acuerdo, el consenso del BITAG no requiere que todas las organizaciones miembros del GTT estén de acuerdo con todas y cada una de las frases de un documento. El Presidente de cada Comité del GTT determina si se ha alcanzado el consenso. En el caso de que haya un desacuerdo dentro de un Comité sobre si hay consenso, el CAPI tiene un proceso de votación con el que se pueden alcanzar e indicar más formalmente varios niveles de acuerdo. Para más información, consulte el Manual del Grupo de Trabajo Técnico del CAPI, disponible en la página web del CAPI: www.bitag.org.

Los informes del GTT del BITAG se centran principalmente en cuestiones técnicas, especialmente en aquellas que pueden interpretarse como anticompetitivas, discriminatorias o motivadas por factores no técnicos. Aunque los informes pueden referirse a una amplia gama de cuestiones relacionadas con una determinada práctica de gestión de redes, no pretenden abordar o analizar de forma exhaustiva las cuestiones económicas, jurídicas, reglamentarias o de política pública que pueda plantear la práctica. El BITAG agradece los comentarios del público. No dude en enviar sus comentarios por escrito a través del correo electrónico comments@bitag.org.

Resumen ejecutivo

En los últimos años, muchos de los nuevos dispositivos conectados a Internet no han sido ordenadores personales, sino más bien una variedad de dispositivos integrados con conectividad y funciones de Internet. Esta clase de dispositivos se ha descrito generalmente como la *Internet de los objetos* (IoT) y ha traído consigo nuevos riesgos de seguridad y privacidad.

El término "IoT" tiene un alcance potencialmente amplio. Puede referirse a implantaciones en hogares, empresas, instalaciones de fabricación, industrias de transporte y otros lugares. Por lo tanto, IoT puede referirse a mucho más que a dispositivos orientados al consumidor. A efectos de este informe, utilizamos el término IoT para referirnos únicamente a los dispositivos orientados al consumidor y a sus sistemas de software locales y remotos asociados, aunque algunas o todas nuestras recomendaciones pueden ser de aplicación más amplia. Este informe se refiere a los escenarios en los que los consumidores instalan, configuran y administran los dispositivos que alquilan o poseen.

El número y la diversidad de dispositivos IoT de consumo están creciendo rápidamente; estos dispositivos ofrecen muchas aplicaciones nuevas para los usuarios finales, y en el futuro probablemente ofrecerán aún más. Muchos dispositivos IoT ya están disponibles o se están desarrollando para su despliegue en un futuro próximo, entre ellos:

- sensores para comprender mejor los patrones de la vida cotidiana y controlar la salud
- monitores y controles para las funciones del hogar, desde cerraduras hasta sistemas de calefacción y agua
- Dispositivos y aparatos que se anticipan a las necesidades del consumidor y pueden tomar medidas para satisfacerlas (por ejemplo, dispositivos que controlan el inventario y reordenan automáticamente los productos para un consumidor).

Estos dispositivos suelen interactuar con el software que se ejecuta en otros lugares de la red y a menudo funcionan de forma autónoma, sin requerir la intervención humana. Además, cuando se combinan con el análisis de datos y el aprendizaje automático, los dispositivos de la IO pueden ser capaces de realizar acciones más proactivas, revelar patrones de datos interesantes y útiles o hacer sugerencias a los usuarios finales que pueden mejorar su salud, su entorno, sus finanzas y otros aspectos de su vida.

Aunque los consumidores se enfrentan a amenazas generales de seguridad y privacidad como resultado de *cualquier* dispositivo conectado a Internet, la naturaleza de la IO de los consumidores es única en el sentido de que puede implicar a consumidores no técnicos o no interesados, lo que supone un reto para el descubrimiento de dispositivos y el inventario en las redes domésticas de los consumidores a medida que prolifera el número y la variedad de dispositivos, impactos en el servicio de acceso a Internet tanto del consumidor como de otros que se ejecutan en enlaces de red compartidos, y efectos en otros servicios en el sentido de que cuando los dispositivos de la IO se ven comprometidos por el malware pueden convertirse en una plataforma para el tráfico de datos no deseados -como el spam y los ataques de denegación de servicio- que pueden interferir con la prestación de estos otros servicios.

Varios informes recientes han demostrado que algunos dispositivos no cumplen con las mejores prácticas rudimentarias de seguridad y privacidad. En algunos casos, los dispositivos se han visto comprometidos y han permitido que usuarios no autorizados realicen tareas de vigilancia y seguimiento, obtengan acceso o control, induzcan fallos del dispositivo o del sistema y molesten o acosen a los usuarios autorizados o a los propietarios de los dispositivos.

Entre los posibles problemas que contribuyen a la falta de mejores prácticas de seguridad y privacidad se encuentran: la falta de experiencia de la cadena de suministro de la IO con la seguridad y la privacidad, la falta de incentivos para desarrollar y desplegar actualizaciones después de la venta inicial, la dificultad de las actualizaciones de software seguras a través de la red, los dispositivos con recursos de hardware restringidos o limitados (que impiden ciertas medidas de seguridad básicas o de "sentido común"), los dispositivos con interfaces de usuario restringidas o limitadas (que si están presentes, pueden tener sólo una funcionalidad mínima), y los dispositivos con malware insertado durante el proceso de fabricación.

La aparición de la IO presenta oportunidades para una importante innovación, desde los hogares hasta las ciudades inteligentes. En muchos casos, unos cambios sencillos en los procesos de desarrollo, distribución y mantenimiento de los dispositivos pueden evitar la distribución de dispositivos IoT que sufren importantes problemas de seguridad y privacidad. El BITAG cree que seguir las directrices descritas en este informe puede mejorar drásticamente la seguridad y la privacidad de los dispositivos IoT y minimizar los costes asociados a los daños colaterales que, de otro modo, afectarían tanto a los usuarios finales como a los ISP. Además, a menos que el sector de los dispositivos IoT -el sector de la industria que fabrica y distribuye estos dispositivos- mejore la seguridad y la privacidad de los dispositivos, la reacción de los consumidores puede impedir el crecimiento del mercado de IoT y, en última instancia, limitar la promesa de IoT.

Observaciones. A partir del análisis realizado en este informe y de la experiencia combinada de sus miembros en lo que respecta a los dispositivos de la Internet de los objetos, el Grupo de Trabajo Técnico del BITAG hace las siguientes *observaciones*:

- **Vulnerabilidades de seguridad:** Algunos dispositivos IoT salen "de fábrica" con un software obsoleto o que se queda obsoleto con el tiempo. Otros dispositivos IoT pueden salir de fábrica con un software más actual, pero pueden descubrirse vulnerabilidades en el futuro. Las vulnerabilidades que se descubren a lo largo de la vida útil de un dispositivo pueden hacer que éste sea menos seguro con el paso del tiempo, a menos que cuente con un mecanismo para actualizar posteriormente su software.

- **Comunicaciones inseguras:** Muchas de las funciones de seguridad diseñadas para dispositivos informáticos de uso más general son difíciles de implementar en los dispositivos de la IO y se han detectado varios fallos de seguridad sobre el terreno, como comunicaciones no cifradas y fugas de datos de los dispositivos de la IO.
    - **Comunicaciones no autenticadas:** Algunos dispositivos IoT proporcionan actualizaciones automáticas de software. Sin embargo, sin autenticación y cifrado, este enfoque es insuficiente porque el mecanismo de actualización podría verse comprometido o desactivado. Además, muchos dispositivos IoT no utilizan la autenticación en el curso de la comunicación.
    - **Comunicaciones no cifradas:** Muchos dispositivos IoT envían algunos o todos los datos en texto claro, en lugar de hacerlo de forma cifrada. Las comunicaciones en texto claro pueden ser observadas por otros dispositivos o por un atacante.

- **Falta de autenticación y autorización mutua:** Un dispositivo que permite que una parte desconocida o no autorizada cambie su código o configuración, o que acceda a sus datos, es una amenaza. El dispositivo puede revelar que su propietario está presente o ausente, facilitar la instalación o el funcionamiento de malware, o hacer que su función principal de IoT se vea fundamentalmente comprometida.

- **Falta de aislamiento de la red:** Estos dispositivos también crean nuevos riesgos y son susceptibles de sufrir ataques *dentro* del hogar. Dado que muchas redes domésticas no aíslan por defecto las diferentes partes de la red entre sí, un dispositivo conectado a la red puede ser capaz de observar o intercambiar tráfico con otros dispositivos de la misma red doméstica, lo que hace posible que un dispositivo observe o afecte al comportamiento de otros dispositivos no relacionados.

- **Fugas de datos: Los** dispositivos IoT pueden filtrar datos privados de los usuarios, tanto desde la nube (donde se almacenan los datos) como entre los propios dispositivos IoT.

  - **Filtraciones desde la nube:** Los servicios en la nube podrían sufrir una filtración de datos debido a un ataque externo o a una amenaza interna. Además, si los usuarios confían en métodos débiles de autenticación o cifrado para estos servicios alojados en la nube, los datos de los usuarios también pueden verse comprometidos.

  - **Filtraciones desde y entre dispositivos:** En algunos casos, los dispositivos de la misma red o de redes vecinas pueden observar los datos de otros dispositivos, como los nombres de las personas de un hogar, la ubicación geográfica precisa de un hogar o incluso los productos que compra un consumidor.

- **Susceptibilidad a la infección por malware y otros abusos: El malware** y otras formas de abuso pueden interrumpir las operaciones de los dispositivos IoT, obtener acceso no autorizado o lanzar ataques.

- **Posible interrupción del servicio:** La posible pérdida de disponibilidad o conectividad no solo disminuye la funcionalidad de los dispositivos IoT, sino que también puede degradar la seguridad de los dispositivos en algunos casos, como cuando un dispositivo IoT ya no puede funcionar sin dicha conectividad (por ejemplo, un sistema de alarma doméstico que se desactiva si se pierde la conectividad).

- **Posibilidad de que persistan los problemas de seguridad y privacidad de los dispositivos: Es probable que los problemas de seguridad de los dispositivos** IoT persistan porque muchos dispositivos pueden no recibir nunca una actualización de software, ya sea porque el fabricante (u otra parte de la cadena de suministro de IoT, o el proveedor de servicios de IoT) no proporcione actualizaciones o porque los consumidores no apliquen las actualizaciones que ya están disponibles.

  - **Muchos dispositivos IoT nunca serán corregidos:** El despliegue de actualizaciones de software que parchean vulnerabilidades de seguridad críticas es difícil en general. Muchos proveedores y fabricantes de dispositivos no tienen sistemas o procesos para desplegar actualizaciones de software a miles de dispositivos, y el despliegue a través de la red

Las actualizaciones de los dispositivos que funcionan en los hogares de los consumidores es difícil, ya que a veces las actualizaciones pueden interrumpir el servicio y a veces tienen el potencial de "brickear" el dispositivo, si se hace incorrectamente. Además, es posible que algunos dispositivos ni siquiera sean capaces de actualizar el software.

  - **Las actualizaciones de software van más allá de los errores:** Las actualizaciones de software no están destinadas simplemente a corregir errores de seguridad o privacidad. También pueden estar destinadas a introducir nuevas funciones importantes, o a mejorar el rendimiento y la seguridad.

  - **Es poco probable que los consumidores actualicen el software de los dispositivos IoT:** Pocos usuarios finales actualizan sistemáticamente el software de los dispositivos por iniciativa propia; es mejor asumir que la mayoría de los usuarios finales nunca tomarán medidas por su cuenta para actualizar el software.

- **La sustitución del dispositivo puede ser una alternativa a las actualizaciones de software, en el caso de los dispositivos baratos o "desechables":** En algunos casos, la sustitución de un dispositivo por completo puede ser una alternativa a las actualizaciones de software. Algunos dispositivos IoT pueden ser tan baratos que la actualización del software puede ser poco práctica o no rentable.

Recomendaciones. El Grupo de Trabajo Técnico del CAPI también tiene lo siguiente *recomendaciones*:

- **Los dispositivos IoT deben utilizar las mejores prácticas de software actuales:**
  - Los dispositivos IoT **deben enviarse con un software razonablemente actual:** El BITAG recomienda que los dispositivos IoT se envíen a los clientes o a los puntos de venta con un software razonablemente actual que no contenga vulnerabilidades graves y conocidas.

  - **Los dispositivos IoT deben contar con un mecanismo de actualizaciones de software automatizadas y seguras:** Los errores de software deben minimizarse, pero son inevitables. Por lo tanto, es fundamental que un dispositivo IoT cuente con un mecanismo de actualizaciones de software automáticas y seguras. El BITAG recomienda que los fabricantes de dispositivos IoT o los proveedores de servicios IoT diseñen sus dispositivos y sistemas basándose en la suposición de que con el tiempo se descubrirán nuevos errores y vulnerabilidades. Deberían diseñar sistemas y procesos que garanticen la actualización automática del software de los dispositivos IoT, sin requerir ni esperar ningún tipo de acción por parte del usuario, ni siquiera su aceptación.

  - **Los dispositivos IoT deben utilizar una autenticación fuerte por defecto:** El BITAG recomienda que los dispositivos IoT estén protegidos por defecto (por ejemplo, protegidos con contraseña) y no utilicen nombres de usuario y contraseñas comunes o fáciles de adivinar (por ejemplo, "admin", "password").

  - **Las configuraciones de los dispositivos IoT deben ser probadas y reforzadas:** Algunos dispositivos IoT permiten al usuario personalizar el comportamiento del dispositivo. El BITAG recomienda que los fabricantes prueben la seguridad de cada dispositivo con una serie de configuraciones posibles, en lugar de limitarse a la configuración por defecto.

- **Los dispositivos IoT deben seguir las mejores prácticas de seguridad y criptografía:** El BITAG recomienda que los fabricantes de dispositivos IoT aseguren las comunicaciones utilizando Seguridad de la Capa de Transporte (TLS) o Criptografía Ligera (LWC). Si los dispositivos se basan en una infraestructura de clave pública (PKI), entonces una entidad autorizada debe ser capaz de revocar los certificados cuando se vean comprometidos, y los fabricantes deben tener cuidado de evitar los métodos de cifrado, protocolos y tamaños de clave con debilidades conocidas. Otras buenas prácticas de cifrado son las siguientes:
    - Cifrar las comunicaciones de configuración (mando y control) por defecto
    - Comunicaciones seguras desde y hacia los controladores del IoT
    - Cifrar el almacenamiento local de datos sensibles
    - Autenticar las comunicaciones, los cambios de software y las solicitudes de datos
    - Utilice credenciales únicas para cada dispositivo
    - Utilice credenciales que puedan actualizarse
    - Cierre los puertos y desactive los servicios innecesarios
    - Utilice las bibliotecas que se mantienen y apoyan activamente

- **Los dispositivos IoT deben ser más restrictivos que permisivos en la comunicación:** Siempre que sea posible, los dispositivos no deberían ser accesibles a través de conexiones entrantes por defecto. Los dispositivos IoT no deben confiar únicamente en el cortafuegos de la red para restringir la comunicación, ya que algunas comunicaciones entre dispositivos dentro del hogar pueden no atravesar el cortafuegos.

- **Los dispositivos IoT deben seguir funcionando si se interrumpe la conectividad a Internet:** El BITAG recomienda que un dispositivo IoT sea capaz de realizar su función o funciones principales (por ejemplo, un interruptor de la luz o un termostato deben seguir funcionando con controles manuales), incluso si no está conectado a Internet, ya que la conectividad a Internet puede interrumpirse debido a causas que van desde una mala configuración accidental hasta un ataque intencionado. Los dispositivos de la IO que tienen implicaciones para la seguridad de los usuarios deben seguir funcionando en régimen de desconexión para proteger la seguridad de los consumidores.

- **Los dispositivos IoT deben seguir funcionando si falla el back-end de la nube:** Muchos servicios que dependen o utilizan un back-end en la nube pueden seguir funcionando, aunque sea en un estado degradado o parcialmente funcional, cuando la conectividad con el back-end en la nube se interrumpe o el propio servicio falla.

- **Los dispositivos IoT deben ser compatibles con las mejores prácticas de direccionamiento y nomenclatura:** Muchos dispositivos IoT pueden permanecer desplegados durante varios años después de su instalación. La compatibilidad con los últimos protocolos de direccionamiento y nomenclatura garantizará que estos dispositivos sigan funcionando durante años.
    - **IPv6:** El BITAG recomienda que los dispositivos IoT sean compatibles con la versión más reciente del Protocolo de Internet, IPv6.

- **DNSSEC:** El BITAG recomienda que los dispositivos IoT admitan el uso o la validación de las extensiones de seguridad del DNS (DNSSEC) cuando se utilicen nombres de dominio.

- **Los dispositivos IoT deben ser enviados con una política de privacidad que sea fácil de encontrar y entender:** El BITAG recomienda que los dispositivos IoT se envíen con una política de privacidad, pero esa política debe ser fácil de encontrar y entender para un usuario típico.

- **Revele los derechos de disminución remota de la funcionalidad del dispositivo IoT:** El BITAG recomienda que si la funcionalidad de un dispositivo IoT puede ser disminuida de forma remota por un tercero, como el fabricante o el proveedor de servicios IoT, esta posibilidad debe quedar clara para el usuario en el momento de la compra.

- **La industria de los dispositivos IoT debería considerar un programa de ciberseguridad de la industria:** El BITAG recomienda que la industria de los dispositivos IoT o un grupo relacionado con la electrónica de consumo considere la creación de un programa respaldado por la industria bajo el cual se podría llevar algún tipo de logotipo o anotación de "Dispositivo IoT seguro" en los envases minoristas de IoT. Un conjunto de mejores prácticas respaldado por la industria parece ser el medio más pragmático para equilibrar la innovación en la IO con los desafíos de seguridad asociados con la naturaleza fluida de la ciberseguridad, y evitar la "mentalidad de lista de control" que puede ocurrir con los procesos de certificación.

- **La cadena de suministro del IoT debe desempeñar su papel en la resolución de los problemas de seguridad y privacidad del IoT: Los** usuarios finales de los dispositivos de IoT dependen de la cadena de suministro de IoT, desde el fabricante hasta el minorista, para proteger su seguridad y privacidad, y algunas o todas las partes de esa cadena de suministro de IoT desempeñan un papel crítico durante todo el ciclo de vida del producto. Además de otras recomendaciones en esta sección, el BITAG recomienda que la cadena de suministro de la IO tome las siguientes medidas:

    - **Política de privacidad:** Los dispositivos deben tener una política de privacidad que sea clara y comprensible, especialmente cuando un dispositivo se vende junto con un servicio continuo.

    - **Mecanismo de restablecimiento:** Los dispositivos deben tener un mecanismo de restablecimiento para los dispositivos IoT que borre toda la configuración para su uso cuando un consumidor devuelva o revenda el dispositivo. Los fabricantes de dispositivos también deben proporcionar un mecanismo para borrar o restablecer cualquier dato que el respectivo dispositivo almacene en la nube.

    - **Sistema de notificación de errores:** Los fabricantes deben proporcionar un sistema de notificación de fallos con mecanismos de presentación de fallos bien definidos y una política de respuesta documentada.

    - **Cadena de suministro de software segura:** Los fabricantes deben proteger la cadena de suministro de software seguro para evitar la introducción de programas maliciosos durante el proceso de fabricación; los vendedores y fabricantes deben tomar las medidas adecuadas para asegurar su cadena de suministro de software.

- **Apoyo al dispositivo IoT durante toda su vida útil:** Los fabricantes deben dar soporte a un dispositivo IoT a lo largo de su vida útil, desde el diseño hasta el momento en que se retira el dispositivo, incluyendo la transparencia sobre el período de tiempo durante el cual planean proporcionar soporte continuo para un dispositivo, y lo que el consumidor debe esperar de la función del dispositivo al final de su vida útil.
- **Métodos de contacto claros:** Los fabricantes deben proporcionar métodos claros para que los consumidores determinen con quién pueden ponerse en contacto para recibir asistencia y métodos para ponerse en contacto con los consumidores para difundir información sobre las vulnerabilidades del software u otros problemas.
- **Informar sobre el descubrimiento y la reparación de las vulnerabilidades:** Los fabricantes deben informar sobre el descubrimiento y la corrección de las vulnerabilidades del software que suponen una amenaza para la seguridad o la privacidad de los consumidores.
- **Proceso claro de notificación de vulnerabilidades:** Los fabricantes deben proporcionar un proceso de notificación de vulnerabilidades con un formulario de notificación de vulnerabilidades bien definido, fácil de localizar y seguro, así como una política de respuesta documentada.

Índice de contenidos

1 Introducción

En los últimos años, muchos de los nuevos dispositivos conectados a Internet no han sido ordenadores personales, sino más bien una variedad de dispositivos integrados con conectividad y funciones de Internet. Algunos ejemplos de estos dispositivos son los termostatos, los enchufes inteligentes y las cámaras en red. Esta clase de dispositivos se ha descrito generalmente como la *Internet de los objetos* (IoT), y está claro que esta nueva clase de dispositivos experimentará un fuerte crecimiento en los próximos años, con estimaciones variables de diferentes fuentes, pero todas prevén muchos miles de millones de estos dispositivos para 2020 [1].

El número y la diversidad de los dispositivos IoT están creciendo rápidamente; estos dispositivos ofrecen muchas aplicaciones nuevas para los usuarios finales, y en el futuro ofrecerán aún más. Muchas soluciones de IoT ya están disponibles o se están desarrollando para su despliegue en un futuro próximo, entre ellas:

- sensores para comprender mejor los patrones de la vida cotidiana y controlar la salud
- monitores y controles para las funciones del hogar, desde cerraduras hasta sistemas de calefacción y agua
- Dispositivos y aparatos que se anticipan a las necesidades del consumidor y pueden tomar medidas para satisfacerlas (por ejemplo, dispositivos que controlan el inventario y reordenan automáticamente los productos para un consumidor).

Además, cuando se combinan con el análisis de datos y el aprendizaje automático, los dispositivos de la IO pueden ser capaces de tomar acciones más proactivas, exponer patrones de datos interesantes o hacer sugerencias a los usuarios finales que pueden mejorar su salud, su entorno, sus finanzas y otros aspectos de sus vidas.

La aparición de la IO ofrece oportunidades para una innovación significativa, desde los hogares hasta las ciudades inteligentes. Desgraciadamente, muchos dispositivos de la IO han salido al mercado con graves fallos de seguridad y privacidad [2]; en la sección 3 se analizan en detalle muchos ejemplos recientes. Estos fallos ponen en peligro a los usuarios finales que adquieren los dispositivos de diversas maneras y pueden afectar al servicio de acceso a Internet tanto del usuario de los dispositivos como de otros usuarios cuyo tráfico discurre por los mismos enlaces de Internet compartidos. Los fallos también crean problemas de seguridad y mitigación más amplios para los objetivos de los ataques, los proveedores de servicios de Internet (ISP), así como otros proveedores de servicios -por ejemplo, servicios de motores de búsqueda, correo electrónico basado en la web y sitios de juegos- y, lo que es más importante, introducen nuevos costes de soporte y mitigación (que normalmente se trasladan a los usuarios finales) [3]. También pueden imponerse costes adicionales a los propios fabricantes de dispositivos, que pueden tener que tomar medidas para mitigar estos problemas.

En muchos casos, unos cambios sencillos en los procesos de desarrollo, distribución y mantenimiento de los dispositivos pueden evitar la distribución de dispositivos IoT que sufren importantes problemas de seguridad y privacidad. El BITAG cree que seguir las directrices descritas en este informe puede mejorar drásticamente la seguridad y la privacidad de los dispositivos IoT y minimizar los costes asociados a los daños colaterales que, de otro modo, afectarían tanto a los usuarios finales como a los ISP. Además, a menos que el sector de los dispositivos IoT -el sector de la industria que fabrica y distribuye estos dispositivos- mejore la seguridad y la privacidad de los dispositivos, la reacción de los consumidores puede impedir el crecimiento del mercado de IoT y, en última instancia, limitar la promesa de IoT para los usuarios finales.

2 ¿Qué es el Internet de los objetos?

El Internet de las cosas (IoT) comprende dispositivos que funcionan como sensores, actuadores, controladores y registradores de actividad. Estos dispositivos suelen interactuar con el software que se ejecuta en otro lugar de la red, como en un teléfono móvil, un dispositivo informático de propósito general (por ejemplo, un ordenador portátil), una máquina en la Internet pública (por ejemplo, en "la nube"), o una combinación de ellos. Los dispositivos IoT suelen funcionar de forma autónoma, sin requerir la intervención humana.

El término "IoT" tiene un alcance potencialmente amplio. Puede referirse a implantaciones en hogares, empresas, instalaciones de fabricación, industrias de transporte y otros lugares. Por lo tanto, la IO puede referirse a mucho más que a los dispositivos orientados al consumidor.

A efectos de este informe, el término IoT se utiliza para referirse únicamente a los dispositivos orientados al consumidor y a sus sistemas de software1 asociados, aunque algunas o todas nuestras recomendaciones pueden ser de aplicación más amplia. Este informe se refiere a los escenarios en los que los consumidores instalan, configuran y administran los dispositivos que alquilan o poseen.

2.1 Limitaciones del alcance

El informe no tiene en cuenta directamente los dispositivos destinados a entornos industriales o de empresa a empresa, como los sensores de las redes de hoteles o aeropuertos, las ciudades inteligentes, la automatización industrial, el control de edificios comerciales o el control de inventarios en la fabricación. En estos entornos, los clientes suelen tener los recursos e incentivos para especificar y gestionar las características de seguridad y privacidad de los productos que compran. Además, muchos de estos dispositivos utilizan conexiones inalámbricas comerciales que no proporcionan un acceso completo a y desde Internet. Dicho esto, algunas de las mismas cuestiones abordadas en este informe pueden estar presentes también en esos entornos.

El alcance de este informe también se limita a los dispositivos IoT que originan o terminan un flujo de datos. Más concretamente, el informe no se centra en los dispositivos que pasan por el tráfico que puede contener datos que van o vienen de los dispositivos IoT, entre otro tráfico, como una puerta de enlace doméstica, un punto de acceso inalámbrico o un router.

Además, el informe se centra únicamente en los dispositivos y sistemas que utilizan el Protocolo de Internet (IP), ya sea IPv4, IPv6 o ambos. Una variedad de dispositivos IoT utilizan otros mecanismos de transporte, como Zigbee 1.0 [4], X10 [5], etc. Estos dispositivos no pueden conectarse a Internet si no es a través de un dispositivo que realice la conversión del protocolo. Funcionan en una red aislada. Sin embargo, las recomendaciones aquí expuestas siguen siendo válidas para el dispositivo que realiza la conversión del protocolo (por ejemplo, el concentrador o la pasarela de automatización del hogar).

Este informe se centra en los problemas específicos de los dispositivos de una red IP local que pueden comunicarse a través de Internet. Los problemas de privacidad y seguridad que se producen en redes aisladas que no tienen conectividad con la Internet pública están fuera del alcance de este informe.

2.2 Dispositivos IoT que los usuarios han modificado

El software de algunos dispositivos puede actualizarse o sustituirse por otro distinto al previsto por el fabricante, creando en muchos sentidos un nuevo producto. Por ejemplo, un usuario puede instalar software de código abierto en un dispositivo, en lugar de utilizar el software suministrado por el proveedor. El producto resultante puede estar sujeto a las consideraciones y recomendaciones de este informe, pero en este caso el dispositivo debe considerarse como un producto distinto del que el usuario es responsable.

[1] Cuando el BITAG utiliza el término "software", pretende incluir el firmware del dispositivo, que es una forma de software, y todos los demás tipos de software.

3 Por qué la seguridad y la privacidad del IoT son de especial interés

Los dispositivos IoT se enfrentan a los mismos tipos de problemas de seguridad y privacidad que muchos dispositivos convencionales de usuario final. Por otra parte, los dispositivos IoT no suelen ofrecer ni controles claros ni documentación para informar al usuario sobre los riesgos que se introducen cuando se despliegan estos dispositivos. Además, los estudios han demostrado que confiar en el usuario final para las decisiones de seguridad y privacidad es propenso al fracaso [6,7,8].

3.1 Consumidores no técnicos o desinteresados.

Los usuarios finales no tienen los conocimientos técnicos necesarios para evaluar las implicaciones en materia de privacidad y seguridad de un dispositivo IoT concreto, o pueden carecer de interés en hacerlo [9]. Además, la mayoría de las veces, los dispositivos desplegados carecen de mecanismos automatizados para realizar actualizaciones seguras o aplicar la política de seguridad [9,10].

3.2 Desafío de descubrimiento e inventario de dispositivos.

Los consumidores ya tienen dificultades para identificar y solucionar los problemas de los dispositivos que actualmente están conectados a sus redes domésticas [11]. Los dispositivos IoT agravarán esta situación, ya que los consumidores conectan una variedad cada vez más amplia de dispositivos a sus redes domésticas.
Es probable que los usuarios pierdan la pista de los dispositivos conectados a Internet con el paso del tiempo, lo que dificultará aún más su protección. Además, los ISP tendrán dificultades para ayudar a los consumidores a identificar las fuentes de los problemas de seguridad. Aunque los ISP puedan determinar que algún dispositivo de la red doméstica de un cliente está comprometido, es posible que no puedan identificar el dispositivo específico comprometido, debido a tecnologías como la traducción de direcciones de red (NAT) y otras tecnologías que pueden ocultar la identidad de los dispositivos individuales.

3.3 Efectos sobre el servicio de acceso a Internet.

Los dispositivos IoT comprometidos por el malware (véanse las secciones 4.5 y 5.3) pueden afectar al servicio de acceso a Internet tanto del usuario de dichos dispositivos IoT como de otros usuarios cuyo tráfico discurra por los mismos enlaces de Internet compartidos. Estos dispositivos también pueden representar una amenaza para el usuario y otros objetivos del malware [12]. Este malware puede utilizarse para lanzar ataques DDoS [13],

enviar spam, atacar a otros dispositivos en la red del usuario, o interferir maliciosamente en el servicio de acceso a Internet del usuario.

Estos problemas aumentan los costes del proveedor de servicios de Internet, que debe dedicar esfuerzos a mitigar estos ataques, a prestar asistencia a los usuarios que no pueden determinar por qué su servicio de acceso a Internet se comporta de forma deficiente o anormal, e incluso a desactivar el servicio de acceso a Internet de los usuarios cuyos dispositivos están realizando actividades maliciosas en la red. Los problemas también aumentan los costes para el consumidor al degradar el rendimiento y crear la posibilidad de pérdida de credenciales. Por último, imponen costes al objetivo de estos ataques y a los propios fabricantes de dispositivos IoT (u otras partes de la cadena de suministro IoT), que pueden tener que tomar medidas para mitigar estos problemas.

3.4 Efectos en otros servicios.

Los dispositivos IoT comprometidos por el malware pueden convertirse en una plataforma para el tráfico no deseado, como el spam y los ataques de denegación de servicio -incluidos los ataques de reflexión y amplificación, por los que un atacante envía tráfico a un dispositivo con la dirección de origen falsa de una víctima, haciendo que el dispositivo envíe grandes cantidades de tráfico hacia la víctima- [14], lo que puede interferir con la capacidad de un proveedor de servicios para prestar un servicio [15]. Los dispositivos comprometidos también pueden ser utilizados para espiar el tráfico de la red local o como "trampolín" para atacar otros dispositivos y servicios en la red local del cliente, creando la posibilidad de que se produzcan fugas de datos. Los proveedores que ofrecen servicios como motores de búsqueda, correo electrónico basado en la web y sitios de juegos deben invertir recursos para mitigar estos ataques. Las víctimas de estos ataques también soportarán costes financieros y de privacidad. Los dispositivos IoT comprometidos también pueden afectar ocasionalmente al modelo de negocio de un proveedor de servicios. Un ejemplo es el malware DNSChanger, que permitía a los atacantes insertar sus propios anuncios en las páginas web de las víctimas [16].

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

Los dispositivos IoT ya se han convertido en una plataforma de abusos y ataques. Muchos tecnólogos han descubierto diversos riesgos para la seguridad y la privacidad asociados a los dispositivos IoT que ya están disponibles [17,18,19,20,21,22,23,24]. Es probable que en los próximos años se desplieguen decenas de millones de dispositivos IoT más, lo que crea el potencial de convertirse en una gran plataforma para lanzar ataques -tanto a otros dispositivos en el hogar del usuario como a Internet en general- y para recopilar subrepticiamente información privada sobre usuarios finales específicos o grupos de usuarios. Además de las pérdidas que puedan experimentar los consumidores, los ISP pueden sufrir un aumento de las llamadas de asistencia técnica y de las incidencias de los ataques, lo que eleva el coste de las operaciones que se trasladan a los consumidores.

En varios informes recientes se han estudiado las características de seguridad y privacidad de los dispositivos de la IO y se ha descubierto que algunos de ellos no respetan las mejores prácticas rudimentarias de privacidad y seguridad [25,26,27,28,29,30,31]. En algunos casos, los dispositivos se han visto comprometidos [32].

Entre los posibles problemas que contribuyen a esta falta de buenas prácticas de privacidad y seguridad se encuentran:

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

En el caso de los dispositivos IoT de consumo que se venden a través de canales minoristas, los proveedores de dispositivos pueden tener pocos incentivos para ofrecer actualizaciones de software después de la venta inicial. Si los ingresos de un dispositivo provienen únicamente de la venta inicial, cualquier mantenimiento del dispositivo erosiona esos ingresos iniciales, disminuyendo los beneficios. Esta estructura puede fomentar la obsolescencia planificada, en la que los vendedores dan prioridad a la venta de nuevos dispositivos frente al mantenimiento de los existentes.

4.2 Dificultad de las actualizaciones de software seguras a través de la red

Los dispositivos IoT pueden no estar diseñados y configurados para recibir actualizaciones de software seguras a través de la red, lo que lleva a procesos de actualización engorrosos.

4.3 Dispositivos con recursos limitados

Los dispositivos IoT vendidos en un entorno de consumo de bajo margen pueden estar diseñados con recursos de hardware limitados. Como resultado, algunas medidas de seguridad básicas, como el cifrado, la verificación de firmas de software y el control de acceso seguro, no son viables. Así, los diseños que limitan la capacidad de procesamiento y de memoria de un dispositivo pueden impedir la ejecución de software de seguridad basado en el host o impedir que se actualice de forma segura. En el apartado 5.1 se analiza esta cuestión con más detalle.

4.4 Dispositivos con interfaces limitadas

Muchos tipos de dispositivos IoT tienen interfaces de usuario limitadas o inexistentes. Incluso cuando un dispositivo expone una interfaz de usuario a través de un dispositivo secundario (por ejemplo, una aplicación para smartphone), su funcionalidad puede ser mínima. Como resultado, tareas como la configuración de un cortafuegos local o la desactivación de servicios remotos pueden ser imposibles. Los dispositivos también pueden carecer de la capacidad de mostrar condiciones de error y alertas significativas a aquellos usuarios que pueden utilizar la información de error

para proteger mejor un dispositivo.

4.5 Dispositivos con malware insertado durante la fabricación.

El malware puede ser introducido en los dispositivos en el momento de su fabricación o embalaje por empleados del fabricante u otras personas con acceso al entorno de fabricación o embalaje. A menudo, un dispositivo comprometido puede parecer que funciona con normalidad, en cuyo caso la brecha de seguridad o privacidad puede persistir hasta que se detecte el compromiso. Los cortafuegos y el aislamiento de la red no pueden defenderse de los ataques lanzados por estos dispositivos comprometidos a otros dispositivos internos de la red aislada. Para ver ejemplos conocidos de estos dispositivos comprometidos y una discusión adicional sobre los efectos del malware, véase la sección 5.3.

4.6 Falta de experiencia del fabricante en materia de seguridad y privacidad

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

4.7 Riesgos debidos a los dispositivos vulnerables

Los siguientes ejemplos ilustran el alcance y la magnitud de los problemas que son posibles cuando los dispositivos de la IO se vuelven vulnerables a los ataques a la seguridad y la privacidad. Un usuario no autorizado puede ser capaz de:

- **Realizar una vigilancia y un seguimiento no autorizados.**
    - saber si una persona concreta está en casa, qué habitación ocupa y cuándo entra en el hogar
    - saber qué otros dispositivos están conectados a la red doméstica y cómo interactúan los usuarios con ellos
    - activar a distancia un micrófono o una cámara en un dispositivo para espiar a alguien [33]
    - descubrir si una puerta o un garaje se ha abierto y cerrado recientemente para determinar si hay alguien en casa, para ayudar en un robo físico
    - instalar un malware en una cámara IoT para acceder a la alimentación de vídeo de la cámara [34]
- **Obtener acceso o control no autorizado.**
    - apagar un termostato durante los meses de invierno para provocar la rotura de las tuberías de agua, dañando la vivienda
    - encender o apagar las luces, como por ejemplo apagar la iluminación del perímetro para ayudar en un robo físico
    - desbloquear puertas para ayudar en una intrusión física
    - supresión de la alarma de un sensor de puerta o ventana
    - reutilizar un dispositivo para un uso ilícito (por ejemplo, como minero de Bitcoin [35])
- **Provocar fallos en el dispositivo o en el sistema.**
    - activar los sistemas de aire acondicionado residenciales para crear una sobrecarga inesperada en una red eléctrica en un intento de

crear condiciones de caídas de tensión o apagones

- subvertir los sensores de recogida de datos sanitarios para modificar los datos de salud, como la presión arterial, el azúcar en sangre o la información sobre el peso, que pueden transmitirse a un servicio de vigilancia de la salud o a un dispositivo médico (como una bomba de insulina)
- emular el software de gestión del dispositivo para que parezca que funciona con normalidad, pero en cambio deshabilitar funcionalidades importantes o realizar otros cambios operativos, lo que hace que los equipos o sistemas de hardware fallen de forma importante [36].
- impedir que un termostato controle la calefacción o la refrigeración del edificio, lo que provoca calor o frío extremos

- **Molestar o acosar a los usuarios.**
  - activar de forma remota un altavoz y participar en amenazas verbales o acoso
  - activar las alarmas de humo u otras alarmas de seguridad

Todos estos escenarios crean graves riesgos de privacidad y seguridad para los usuarios finales y para Internet en su conjunto. Algunos riesgos para la seguridad y la privacidad de los usuarios finales también podrían permitir una nueva forma de acoso digital. En casos extremos, la subversión de la recogida de datos sanitarios podría provocar lesiones o la muerte. En el caso de los dispositivos ampliamente desplegados, los riesgos de seguridad pueden agravarse a través de cientos o miles de dispositivos para crear ataques distribuidos a la infraestructura crítica.

Los problemas de seguridad y privacidad de los dispositivos de la IO podrían, en última instancia, limitar el crecimiento futuro del sector de la IO. Un pequeño número de incidentes de gran repercusión podría reducir la demanda de dispositivos de IoT o limitar de otro modo el crecimiento y el potencial de IoT. Por lo tanto, es fundamental abordar estas cuestiones para apoyar la salud, la vitalidad y el crecimiento a largo plazo del mercado de la IO.

5 Observaciones sobre los problemas de seguridad y privacidad del IoT

No es realista esperar que los fabricantes creen productos de software libres de fallos; todo el software tiene fallos, y la producción de software libre de tales defectos sigue siendo un problema sin resolver. Como resultado, algunos dispositivos del IoT salen "de fábrica" con un software que o bien está obsoleto o bien se queda obsoleto con el tiempo. No se trata de enviar software con errores, lo cual es inevitable; lo que preocupa es que los fabricantes puedan enviar dispositivos con software obsoleto que contenga muchas vulnerabilidades de seguridad significativas y documentadas, algunas de las cuales pueden explotarse inmediatamente cuando el dispositivo se conecta a Internet por primera vez [37].

Otros dispositivos IoT pueden salir de fábrica con un software más actual que no contiene vulnerabilidades de seguridad importantes conocidas en el momento de su envío. Incluso en estos casos, es posible que se descubran vulnerabilidades en el futuro, lo que puede hacer que un dispositivo sea menos seguro con el paso del tiempo, a menos que cuente con un mecanismo para actualizar posteriormente su software. Desgraciadamente, muchos dispositivos IoT carecen de mecanismos de actualización de software seguros y automatizados que puedan parchear las vulnerabilidades una vez que los dispositivos han sido enviados y desplegados. [2] Sin la adopción generalizada de métodos de actualización de software seguros y automatizados, es probable que el número de dispositivos IoT inseguros y comprometidos aumente drásticamente en los próximos años.

Los dispositivos IoT que salen de fábrica con problemas de seguridad y privacidad o que los desarrollan con el tiempo pueden crear una nueva población de dispositivos que pueden ser utilizados por hackers malintencionados, por ejemplo, para realizar ataques de reflexión y amplificación [41]. Estos dispositivos no sólo suponen riesgos para los propios propietarios de los mismos, sino que también pueden ser explotados para abusar de otras partes. Por lo tanto, la seguridad de los dispositivos de la IO no solo interesa a los fabricantes (y otras partes de la cadena de suministro de la IO) y a los clientes de los dispositivos de la IO, sino también a Internet en general.

Por último, aunque este informe proporciona muchos ejemplos de dispositivos de la IO que tienen o han tenido previamente problemas de seguridad o privacidad, en muchos casos los ejemplos destacados aquí pueden haber sido abordados por las partes pertinentes antes de la publicación de este informe.

5.1 Comunicaciones de red inseguras

Los dispositivos del IoT en general pueden ser bastante limitados en cuanto a recursos, ya que carecen de la potencia de cálculo y el ancho de banda de los dispositivos informáticos más convencionales, como los teléfonos móviles, los ordenadores portátiles y los ordenadores de sobremesa, como se explica en la sección 4. Como resultado, muchas de las funciones de seguridad diseñadas para dispositivos informáticos de uso más general son más difíciles de implementar en los dispositivos del IoT. Por ejemplo, el cifrado de clave pública -que subyace en las comunicaciones seguras modernas basadas en la Seguridad de la Capa de Transporte (TLS) [42] y la Seguridad de la Capa de Transporte de Datagramas (DTLS)[43]- puede ser difícil de implementar en ciertos dispositivos IoT con recursos limitados. Por ejemplo, los dispositivos Arduino y Raspberry Pi pueden tardar muchos segundos en realizar una operación de cifrado o descifrado asimétrico [44,45].

Más allá de las limitaciones inherentes a los dispositivos IoT y a las plataformas IoT en las que se ejecutan, se han identificado una serie de fallos de seguridad en el campo, incluyendo comunicaciones no encriptadas, fugas de datos de los dispositivos IoT y efectos negativos para la red en la que está conectado el dispositivo IoT [25,26,27,46,47].

Por ejemplo, algunas implementaciones de servidores TLS son vulnerables a los llamados ataques de "downgrade", por los que un atacante puede forzar a un servidor a utilizar una versión más antigua del protocolo TLS, que puede tener problemas de seguridad conocidos, como vulnerabilidades a los ataques man-in-the-middle. En estos casos, la comunicación entre un dispositivo IoT y el servicio alojado en la nube que lo soporta podría verse comprometida.

▪ Comunicaciones no autentificadas

Algunos dispositivos IoT proporcionan actualizaciones automáticas de software. Sin embargo, sin autenticación y cifrado, este enfoque es insuficiente, ya que el mecanismo de actualización podría verse comprometido o desactivado [48]. El propio mecanismo de actualización y cualquier tráfico de comando y control asociado deben estar autenticados y cifrados, y la integridad de las comunicaciones entre el dispositivo y otros puntos finales debe estar protegida. [3] Desgraciadamente, muchos dispositivos IoT no utilizan la autenticación en el curso de la comunicación. Por ejemplo, el concentrador Lightwave RF Smart enviaba tráfico a un servidor remoto de la red cada vez que se reiniciaba y, posteriormente, cada quince minutos cuando buscaba actualizaciones de software [29]. Si la conexión no está asegurada, no es difícil para un atacante con acceso a la red llevar a cabo un ataque man-in-the-middle.

▪ Comunicaciones no codificadas

Muchos dispositivos IoT envían algunos o todos los datos en texto claro, en lugar de hacerlo de forma cifrada. Esto significa que los datos pueden "filtrarse" y ser observados por otros dispositivos o por un atacante.

Como resultado, algunos dispositivos IoT filtran información del usuario (por ejemplo, a un observador del tráfico de la red), y esto puede identificar el o los dispositivos IoT que se están utilizando, así como revelar la actividad y el comportamiento actual del usuario [17]. [4] Por ejemplo:

- Un marco de fotos digital lleva la dirección de correo electrónico del usuario en texto claro durante la sincronización de fotos, y la actividad actual del usuario también se muestra en claro [10].
- Una cámara web envía archivos de vídeo en texto claro [29].
- Un asistente personal de audio transporta los comandos de audio del usuario, las lecturas de los sensores y las direcciones de correo electrónico del usuario en texto claro [29].
- Un termostato transporta datos meteorológicos locales con información precisa sobre la ubicación del usuario en texto claro, y es claramente identificable como un termostato de una marca específica en función de los puertos utilizados. [5]
- Un concentrador de dispositivos IoT tiene un perfil de tráfico de texto claro tan regular y específico que el concentrador de dispositivos puede identificarse simplemente tomando una huella digital del patrón de tráfico de texto claro [29].
- Algunos marcapasos habilitados para el IoT utilizan canales de comunicación no cifrados [52].

- **Falta de autenticación y autorización mutua**

Muchos ataques se originan detrás de un cortafuegos en la frontera de una red, en el hogar o en otro lugar. Por ello, las comunicaciones detrás de un cortafuegos no deben considerarse necesariamente fiables. Por lo tanto, un dispositivo debe establecer la confianza entre dispositivos, independientemente de si está en una red de área local o en Internet; debe asumir que otros dispositivos no son de confianza por defecto y deben ser autenticados y autorizados explícitamente. Un dispositivo que permite que una parte desconocida o no autorizada cambie su código o configuración, o que acceda a sus datos, es una amenaza; el dispositivo puede revelar que su propietario está presente o ausente, facilitar la instalación o el funcionamiento de malware, o hacer que su función principal de IoT se vea fundamentalmente comprometida.

Afortunadamente, a diferencia de los dispositivos informáticos de uso general, como los ordenadores portátiles, que pueden comunicarse con muchos destinos de Internet, los dispositivos IoT suelen comunicarse con un número reducido de destinos bien definidos. Por ejemplo, un dispositivo puede comunicarse regularmente solo con un servidor de control o de actualización que tenga un nombre DNS o una dirección IP conocidos; una comunicación importante con otros destinos puede ser motivo de preocupación.

- ***Falta de aislamiento de la red***

Además de los riesgos para la seguridad y la privacidad que introducen los dispositivos IoT fuera de la red doméstica donde está instalado el propio dispositivo IoT (véase la sección 4), estos dispositivos también crean nuevos riesgos y son susceptibles de sufrir ataques *dentro* del hogar. Dado que muchas redes domésticas no aíslan, por defecto, las diferentes partes de la red entre sí, un dispositivo conectado a la red puede ser capaz de observar o intercambiar tráfico con otros dispositivos en la misma red doméstica, lo que hace posible que un dispositivo observe o afecte al comportamiento de dispositivos no relacionados.

Aunque es una práctica común utilizar cortafuegos para aislar los dispositivos de una red entre sí, los cortafuegos por sí solos no siempre pueden defender contra los compromisos de los dispositivos o las fugas de datos, y no pueden defender contra el malware en los dispositivos que ya están dentro de la red doméstica. Hoy en día, una red doméstica típica ofrece poco o ningún aislamiento entre dispositivos. En la sección 6 se analizan con más detalle los cortafuegos y otros mecanismos de aislamiento de la red.

Esta falta de aislamiento supone una amenaza para la seguridad y la privacidad de todos los dispositivos de la red, tanto como resultado de acciones específicas del fabricante (o de otras partes de la cadena de suministro del IoT) como a consecuencia del compromiso de los dispositivos [27,54,55]. En concreto, un atacante puede ser capaz de recopilar inteligencia o información personal de otros dispositivos de la misma red. Normalmente, cada dispositivo de una red doméstica puede ver el tráfico de otros dispositivos que están en la misma red. Si los dispositivos transmiten el tráfico en texto claro, un dispositivo puede ser capaz de descubrir los detalles de la actividad de otro dispositivo. Trabajos recientes han demostrado que incluso la capacidad de observar detalles más "gruesos", como las búsquedas de DNS y los cambios en los volúmenes de tráfico, pueden revelar información sobre la actividad de los dispositivos y el comportamiento de los usuarios [56]. Así, un atacante que comprometa un dispositivo puede ser capaz de inferir información significativa sobre un usuario final, como las horas de entrada y salida de la casa a través de sensores de puerta comprometidos o grabaciones de audio y vídeo de micrófonos y cámaras de vídeo incrustadas en dispositivos IoT. El diseño de seguridad de muchas redes inalámbricas domésticas permite realizar ataques de "paso a paso" [57], mediante los cuales un atacante puede comprometer un dispositivo IoT vulnerable y utilizar ese compromiso como mecanismo para obtener acceso a otros dispositivos conectados desde el interior de la red. Algunos ejemplos son:

- Un producto de reloj inteligente incluía un servidor DNS que funcionaba y que los atacantes externos podían utilizar para atacar otros dispositivos de la red a la que estaba conectado el reloj inteligente. El mismo producto tenía una vulnerabilidad que permitía que el tráfico de la red local fuera visto por atacantes de la red externa [27].

- Una bombilla inteligente podría ser engañada para que enviara credenciales de red inalámbrica que atacantes externos podrían utilizar para controlar las luces y ver el tráfico de la red local [54].

- Algunos fabricantes de dispositivos e ISP han expuesto interfaces de gestión remota inseguras de millones de dispositivos y equipos de instalaciones de clientes (por ejemplo, módems, routers domésticos) que compartían la misma clave privada conocida, exponiendo estos dispositivos a ataques man-in-the-middle tanto pasivos como activos [55].

- Las vulnerabilidades en un determinado modelo de teléfono VoIP permitirían a un atacante de la red local proporcionar actualizaciones de firmware maliciosas al teléfono [58].

5.2 Fugas de datos

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

▪ Filtraciones de la nube

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

Además, si los usuarios confían en métodos débiles de autenticación o cifrado para estos servicios alojados en la nube, los datos del usuario también pueden verse comprometidos.

Algunos ejemplos son:

- Una aplicación web asociada a un oso de peluche (que contiene una pequeña cámara en su nariz) contenía una vulnerabilidad de seguridad que dejaba expuestas las identidades de los niños [59].
- El muñeco enviaba chats encriptados entre el muñeco y los servidores alojados en la nube utilizando una versión de TLS que era vulnerable a un ataque de downgrade, lo que permitía espiar las grabaciones de los niños [60].
- Una filtración de datos en un fabricante de juguetes para niños expuso los datos personales de más de seis millones de niños [61].
- Los puntos débiles en la configuración del punto de acceso Wi-Fi en los vehículos de motor dieron lugar a que muchas localizaciones de vehículos fueran rastreadas en sitios web que recogen los nombres de los puntos de acceso Wi-Fi y sus ubicaciones [62].
- El sistema de un fabricante de automóviles enviaba estadísticas de ahorro de combustible, coordenadas geográficas precisas, velocidad, dirección y destino en texto claro a un servidor central [63].

Existen muchos otros ejemplos de filtraciones de datos desde estos dispositivos [25,28,30,32,64,65,66,67]. Las fugas de datos desde la nube no son nuevas ni específicas de los dispositivos IoT, pero la prevalencia de las vulnerabilidades de las fugas de datos en los servicios alojados en la nube es especialmente problemática para los dispositivos IoT de consumo, que no solo son cada vez más omnipresentes, sino que también recogen cada vez más datos personales y privados.

▪ Fugas desde y entre dispositivos

En la misma red de área local pueden residir dispositivos IoT de distintos fabricantes, que ejecutan muchas aplicaciones de software diferentes. Aunque las técnicas estándar de cifrado de Wi-Fi pueden proteger la confidencialidad de las transmisiones de datos en la red de área local, el cifrado por sí solo no garantiza la privacidad del usuario.

En algunos casos, los dispositivos de la misma red o de redes vecinas pueden observar los datos de otros dispositivos. Por ejemplo, un dispositivo puede "filtrar" datos a dispositivos o usuarios cercanos (ya sea en la misma red de área local, en la red Wi-Fi o simplemente en las cercanías). Incluso con el cifrado Wi-Fi, un dispositivo puede observar la presencia de otros dispositivos en la misma red de área local, y las direcciones de hardware de los otros dispositivos -que a menudo pueden revelar el tipo de dispositivo- también suelen ser visibles en texto claro. Este nivel de visibilidad podría, por ejemplo, hacer posible que el software de un marco de fotos digital supervise las interacciones de un usuario con otros dispositivos en la misma red.

Los datos que se filtran de un dispositivo a otro pueden incluir información como los nombres de las personas en un hogar, la ubicación geográfica precisa de una casa o incluso los productos que compra un consumidor. Por ejemplo, un estudio reciente descubrió que un termostato filtraba información geográfica precisa del hogar [17]. En otro estudio reciente, los investigadores fueron capaces de determinar el PIN de un cajero automático de un usuario basándose en los datos del acelerómetro filtrados a través de Bluetooth desde un dispositivo de seguimiento de la actividad física [68].

5.3 Susceptibilidad a la infección por malware y otros abusos

El malware, que es un software malicioso instalado en un dispositivo de usuario que suele interrumpir las operaciones, obtener acceso no autorizado o lanzar ataques, puede infectar los dispositivos IoT a través de diversos mecanismos. Además, pueden producirse otras formas de abuso. Algunos ejemplos son:

- El fabricante puede no asegurar adecuadamente la cadena de suministro de software [69] y, por tanto, permitir que se coloque malware en el software inicialmente enviado del dispositivo IoT [34], como se indica en la sección 4.5.
- Los dispositivos pueden salir de fábrica con software no actualizado que contiene vulnerabilidades conocidas. Cuando un usuario conecta el dispositivo a la red, éste se convierte inmediatamente en un objetivo para los atacantes. Estudios anteriores demuestran que el "tiempo de supervivencia" (es decir, el tiempo que un dispositivo está conectado a la red antes de ser infectado) puede ser en algunos casos inferior a diez minutos [70]. [6] Si un dispositivo se envía con un software desactualizado y no busca inmediatamente las actualizaciones de software, corre el riesgo de infectarse inmediatamente.
- Los mecanismos de actualización de software pueden no incluir la autenticación de las cargas de software para garantizar que el software procede de una fuente de confianza. A través de la ingeniería social, el usuario puede ser influenciado o inducido a cargar software comprometido en un dispositivo IoT.
- El software puede incluir capacidades de línea de comandos o interfaces de programación de aplicaciones (API) que pueden ser explotadas (con o sin la participación del usuario) para cargar malware en un dispositivo IoT.
- El dispositivo tiene puertos innecesarios abiertos y no protegidos, como el de telnet. Estos puertos innecesarios se han utilizado para comprometer un dispositivo, por ejemplo, instruyendo al dispositivo para que acceda a un destino con el fin de descargar malware [71,72,73]. Los puertos innecesarios también pueden utilizarse en ataques de amplificación.
- El dispositivo utiliza una autenticación débil por defecto, como nombres de usuario y contraseñas comunes o fáciles de adivinar (por ejemplo, "admin", "password") [74]. Además, es posible que la autenticación para el acceso remoto no esté asegurada, lo que permite a otras personas que no están físicamente presentes en el hogar iniciar sesión en el dispositivo e instalar malware en él [13,75,76,77,78].

5.4 Posible interrupción del servicio

Un aspecto importante de la seguridad de los dispositivos IoT es la disponibilidad del servicio frente a los fallos y ataques de los dispositivos. La posible pérdida de disponibilidad o conectividad no solo disminuye la funcionalidad de los dispositivos IoT, sino que también puede degradar la seguridad de los dispositivos en algunos casos, como cuando un dispositivo IoT ya no puede funcionar sin dicha conectividad (por ejemplo, un sistema de alarma doméstico que se desactiva si se pierde la conectividad). Un dispositivo IoT puede experimentar la interrupción del servicio de varias maneras.

- **Pérdida de soporte de una aplicación alojada en la nube.** Si el dispositivo depende de la comunicación con un servicio en la nube, el dispositivo puede dejar de funcionar cuando pierda la conectividad con el servicio en la nube. Dicha desconexión puede producirse por diversas razones, como la interrupción de la conectividad a Internet, errores en el servicio de software en la nube, la quiebra de un proveedor o fabricante, o la decisión del consumidor de interrumpir la suscripción al servicio.
- **Pérdida de conectividad a la red. La conectividad** dentro de una red doméstica puede interrumpirse, quizás debido a un cable de alimentación desenchufado, a interferencias de radio con la Wi-Fi o a que un cortafuegos decida restringir el acceso, por ejemplo.

- **Daños en el dispositivo.** Un dispositivo puede dañarse físicamente, o su software puede corromperse o quedar inoperativo (lo que a veces se denomina "brickear" un dispositivo).

Un dispositivo "brickeado", es decir, dañado física o lógicamente, puede ser irrecuperable, mientras que un dispositivo que depende de la comunicación con un servicio alojado en la nube puede volver a ser operativo cuando se restablece la comunicación.
Las interrupciones de ciertos servicios pueden dañar la propiedad y poner en peligro a los usuarios. Por ejemplo, un error de software en un termostato IoT hizo que los sistemas de calefacción de las casas no funcionaran y, como consecuencia, se congelaran las tuberías de los hogares [51]. El mal funcionamiento de los sistemas de calefacción y refrigeración puede provocar muertes. Cuando los dispositivos IoT son responsables de todo, desde la salud personal hasta la seguridad del hogar, lo que está en juego es la seguridad del usuario.

5.5 Posibilidad de que persistan los problemas de seguridad y privacidad de los dispositivos

Esta sección analiza brevemente por qué es probable que persistan los problemas de seguridad señalados en la sección anterior. Cabe esperar que muchos de estos dispositivos IoT no reciban nunca una actualización de software, ya sea porque el fabricante (u otra parte de la cadena de suministro de IoT, o el proveedor de servicios de IoT) no proporcione actualizaciones o porque los consumidores no apliquen las actualizaciones que ya están disponibles. Hay muchos ejemplos de esto con tipos de dispositivos similares [79,80,81,82].

▪ Muchos dispositivos del IoT nunca se arreglarán

El despliegue de actualizaciones de software que parchean vulnerabilidades de seguridad críticas es difícil en general, pero los dispositivos IoT plantean desafíos únicos. En primer lugar, muchos proveedores y fabricantes de dispositivos no tienen sistemas o procesos para desplegar actualizaciones de software a miles de dispositivos (o más). En segundo lugar, el despliegue de actualizaciones a través de la red a los dispositivos que funcionan en los hogares de los consumidores es difícil, ya que las actualizaciones a veces pueden interrumpir el servicio y a veces tienen el potencial de "bloquear" el dispositivo, si se hace incorrectamente. Además, es posible que algunos dispositivos ni siquiera sean capaces de actualizar el software [83].

En la industria de la electrónica de consumo han surgido tres enfoques de actualización de software, dos de los cuales dependen de la acción de los usuarios (un defecto fundamental), mientras que el tercero es automático sin necesidad de que el usuario actúe. La eficacia de cada uno de ellos varía en la práctica. Estos enfoques son los siguientes:

- **Actualizaciones de software iniciadas por el usuario.** Este enfoque requiere que el administrador local del dispositivo inicie manualmente la comprobación e instalación de cualquier actualización de software en un dispositivo. Un ejemplo de este modelo se encuentra en el típico mercado de dispositivos de puerta de enlace doméstica o routers. Algunos de estos dispositivos requieren que el usuario descargue una nueva imagen de software del sitio web del fabricante, luego acceda a una página web de administración local del dispositivo, encuentre la interfaz para las actualizaciones de software y cargue un archivo. Este proceso no sólo lleva mucho tiempo, sino que puede ser desalentador para los usuarios no técnicos o casuales para los que un dispositivo puede seguir funcionando "suficientemente bien".

- **Comprobación automática de las actualizaciones de software, con la aprobación del usuario.** Estos dispositivos comprueban periódicamente si hay nuevas actualizaciones de software. Cuando hay una actualización disponible, el dispositivo presenta al usuario un aviso que le pide permiso para proceder a la actualización. Los dispositivos de televisión inteligente y las consolas de juegos suelen utilizar este método. En estos casos, la aplicación de una determinada actualización de software puede tardar varios minutos -o más-, por lo que se ofrece al usuario la opción de aplazar la instalación.

- **Actualizaciones de software totalmente automatizadas.** Algunos dispositivos comprueban periódicamente si hay un nuevo software disponible; si lo hay, lo descargan y lo instalan sin intervención del usuario [84,85]. En algunos casos, el dispositivo puede aplicar la actualización en un momento determinado del día, como por ejemplo a última hora de la noche o cuando no ha habido actividad relacionada con el dispositivo durante algún periodo de tiempo, para minimizar la interrupción del usuario. Desgraciadamente, las actualizaciones automáticas de software también pueden plantear problemas para algunos usuarios que tienen límites de datos (en su caso), y

cuando las propias actualizaciones introducen nuevos errores [51].

Los enfoques habituales para las actualizaciones de software son los iniciados por el usuario o los aprobados por el usuario, y ambos tienden a conducir a tasas de actualización relativamente bajas [86]. Como resultado, es probable que millones de pasarelas domésticas propiedad de los clientes (COAM) nunca reciban una actualización de software. Por ejemplo, algunos modelos de pasarela doméstica NetGear se enviaron con un fallo de software que hacía que estos dispositivos inundaran aleatoriamente los servidores DNS de los ISP con miles de peticiones DNS por segundo, sumando millones al día, o una avalancha de consultas NTP a los servidores NTP [87,88,89,90]. Aunque este fallo de software específico ha sido reportado durante muchos años, los operadores de red todavía observan que estos dispositivos ejecutan software antiguo y se comportan mal en la red, realizando inadvertidamente ataques DDoS debido a fallos de software.

- **Las actualizaciones de software van más allá de los errores**

También hay que tener en cuenta que las actualizaciones de software no están destinadas simplemente a corregir errores de seguridad o privacidad. También pueden estar destinadas a introducir nuevas funciones importantes. Además, pueden estar relacionadas de forma más general con el rendimiento y la seguridad, como la compatibilidad o la corrección de errores relacionados con el direccionamiento IPv6, la validación de las extensiones de seguridad del DNS (DNSSEC) y el control del búfer TCP (por ejemplo, "buffer bloat") o la gestión activa de colas (AQM).

- **Es poco probable que los consumidores actualicen el software de los dispositivos IoT**

Pocos usuarios finales actualizan sistemáticamente el software de sus dispositivos por iniciativa propia, a no ser que la interfaz gráfica de usuario (GUI) del dispositivo se lo recuerde de forma constante y obvia (es decir, una ventana emergente normal en un PC, un contador en una tienda de aplicaciones para móviles, un icono de aplicación que rebota, etc.), una lección que se entiende bien en la disciplina de la interacción persona-ordenador [86]. Otros trabajos recientes sugieren que los usuarios renuncian a aplicar actualizaciones de software tanto en dispositivos fijos como móviles por diversas razones, que van desde la interrupción de su ciclo de trabajo hasta los costes de datos asociados a las actualizaciones de software [86].

Aunque no se han realizado estudios en profundidad sobre el comportamiento de actualización de software de los usuarios en los dispositivos IoT, es probable que la situación sea peor que la de los dispositivos convencionales, o no IoT. Además del comportamiento ya arriesgado de los usuarios con respecto a las actualizaciones de software, muchos dispositivos IoT carecen de una interfaz gráfica de usuario u otro indicador de que el nuevo software está disponible o es necesario. Además, la proliferación de dispositivos -tanto en número como en diversidad- hace que el seguimiento de las actualizaciones de software sea una tarea difícil para el consumidor típico de Internet.

Así, en el caso de los dispositivos IoT, lo mejor es asumir que la mayoría de los usuarios finales nunca tomarán medidas por su cuenta para actualizar el software del dispositivo.

5.6 La sustitución de dispositivos puede ser una alternativa a las actualizaciones de software

En algunos casos, sustituir un dispositivo por completo puede ser una alternativa a las actualizaciones de software. Algunos dispositivos IoT pueden ser tan baratos que la actualización del software puede ser poco práctica o no rentable. Por ejemplo, puede que un adaptador de carga que cuesta 0,99 dólares tenga alguna función IoT limitada. Con ese coste unitario, la actualización de un dispositivo puede no ser económica; en su lugar, puede tener más sentido reciclar el dispositivo y comprar un reemplazo. Sin embargo, este enfoque requiere los siguientes elementos para proporcionar una alternativa segura a las actualizaciones de software:

- Una forma de identificar cuándo una o varias vulnerabilidades acumuladas en un dispositivo lo han puesto en peligro hasta el punto de que debe ser sustituido.
- Una forma de desactivar la comunicación con el dispositivo una vez que se determine que es vulnerable. Algunos ejemplos de métodos potenciales incluyen la desactivación remota del dispositivo desde la red, o el bloqueo del acceso al dispositivo desde una puerta de enlace doméstica.
- Una forma de notificar a los usuarios que la comunicación con el dispositivo se ha desactivado.

Incluso en estos casos, por supuesto, los usuarios pueden ser reacios a dejar de usar un dispositivo mientras siga funcionando en parte. Sin embargo, mientras se haya desactivado la capacidad de comunicación del dispositivo, su uso

continuado no debería presentar una vulnerabilidad de seguridad.

6 Un posible papel para la tecnología de redes domésticas

El hecho de que los fabricantes de dispositivos los aseguren por defecto constituye un paso importante para mejorar la seguridad y la privacidad del IoT, pero no es en absoluto suficiente. Incluso los dispositivos IoT que no están infectados con malware pueden espiar el tráfico de otras redes domésticas (por ejemplo, a través de software instalado por el fabricante o de terceros), comprometiendo la privacidad del usuario. Un hogar suele considerarse un entorno aislado o con un cortafuegos, y varios dispositivos IoT no relacionados suelen tener acceso sin restricciones detrás de este cortafuegos. Además, como se menciona en las secciones 3.4 y 5.1, un solo dispositivo inseguro o comprometido en la red doméstica puede dar lugar a ataques escalonados, por lo que la "defensa en profundidad" [91] es fundamental.

Estudios e informes recientes han sugerido que, en el futuro, un dispositivo de red doméstico puede desempeñar algún papel en el control y la gestión del tráfico que los dispositivos IoT intercambian entre sí y con el resto de Internet [92]. Entre las posibles capacidades de un dispositivo de red de este tipo se incluyen:

- Descubrimiento e inventario automático de los dispositivos conectados a Internet en el hogar [93].
- Mecanismos para presentar al usuario información clara sobre (1) qué datos está enviando el dispositivo al resto de Internet y (2) con qué otros dispositivos del hogar está hablando el dispositivo, como se ha hecho en el pasado para los smartphones y los navegadores [94,95].
- Mecanismos que proporcionen al usuario formas sencillas de impedir o desactivar la comunicación de un único dispositivo con otros dispositivos IoT en la red doméstica, o con servidores de almacenamiento en la nube, *sin perjudicar la funcionalidad principal del dispositivo.* Un estudio reciente pudo lograr esto con dos dispositivos IoT de ejemplo, una bombilla Philips Hue y un termostato Nest [92].

La tecnología de red para mejorar la seguridad y la privacidad puede adoptar en última instancia una de varias formas. Una pasarela de red doméstica, ya sea independiente (por ejemplo, un concentrador de IoT o un router doméstico independiente) o integrada en el equipo proporcionado por el ISP, podría realizar mediciones dentro de la red que ayuden a los usuarios a comprender los complejos flujos de datos tanto entre los dispositivos de IoT en el hogar como entre estos dispositivos y los sitios y servicios de terceros fuera del hogar. En este sentido, la tecnología de red en el hogar que supervisa el tráfico de los dispositivos puede, en última instancia, ayudar a mejorar la *transparencia* del comportamiento de estos dispositivos IoT.

Existe un cierto conflicto entre la supervisión y la gestión del tráfico IoT por parte de un concentrador y la seguridad de extremo a extremo del propio tráfico. Cabe señalar que, incluso si el tráfico de red hacia y desde estos dispositivos está cifrado de extremo a extremo, ciertas características, como los otros dispositivos y las ubicaciones con las que se comunica cualquier dispositivo en particular, seguirán siendo evidentes a partir de este tráfico. La estandarización para permitir la clasificación y protección cooperativa del tráfico con un centro de IoT de este tipo permitiría que el dispositivo fuera una parte reconocida y autentificada del ecosistema, proporcionando esa gestión con un control de grano fino disponible para el originador del tráfico sobre una base opt-in.

Además de ayudar a visualizar estos flujos de tráfico, una pasarela de este tipo podría aplicar una configuración *predeterminada razonable* para mejorar la seguridad y la privacidad de los dispositivos IoT conectados. Por ejemplo, investigaciones recientes sugieren que un cortafuegos de la red doméstica puede impedir que ciertos dispositivos filtren registros y otra información a proveedores de la nube de terceros, sin que se vea afectada la funcionalidad del propio dispositivo [92]. Una cuestión abierta es la de identificar la configuración razonable del cortafuegos por defecto que podría instalarse en dicha puerta de enlace para mejorar la seguridad y la privacidad. Dado que un cortafuegos de red doméstica de este tipo podría instigar una "carrera armamentística por la privacidad" (por ejemplo, cabría imaginar que un fabricante de dispositivos no proporcionara actualizaciones de seguridad a un usuario que bloqueara las capacidades de rastreo del dispositivo), uno de los aspectos de la certificación de dispositivos para fabricantes y vendedores podría consistir, en última instancia, en garantizar que los consumidores mantengan la *posibilidad de elegir* con conocimiento de causa la forma en que estos dispositivos se comunican entre sí y con sitios y servicios de terceros.

Por último, la interacción entre dispositivos IoT puede requerir una mediación más compleja. Por ejemplo, aunque un usuario no desee generalmente que ciertos dispositivos se comuniquen o interactúen entre sí, puede haber casos de uso específicos

que permitan la comunicación o la interacción entre dispositivos para tareas concretas. Como ejemplo posible, consideremos un escenario en el que un usuario quiera atenuar automáticamente las luces cuando vea una película en casa. En este caso, la aplicación podría implicar una comunicación mediada entre un dispositivo de streaming (por ejemplo, un Roku o Apple TV) y los enchufes e interruptores inteligentes (por ejemplo, un interruptor Belkin WeMo). Por otro lado, en general, un usuario puede no querer que estos dispositivos interactúen, o incluso que observen el tráfico de los demás. Por ello, la pasarela de red, junto con la interfaz de usuario adecuada, puede ofrecer en última instancia mejores oportunidades para este tipo de interacción mediada compleja.

Informes recientes sugieren que muchos de estos objetivos están probablemente al alcance de la mano. Por ejemplo, los investigadores utilizaron un cortafuegos de red doméstica para impedir que un termostato Nest enviara sus registros de estado a la nube, sin perjudicar al propio dispositivo [92]. Sin embargo, dado que es poco probable que el usuario típico configure reglas de cortafuegos, estas funciones de cortafuegos deben ser más utilizables -y, si es posible, automatizadas- antes de que puedan considerarse prácticas.

7 Recomendaciones

Esta sección del informe presenta las recomendaciones del Grupo de Trabajo Técnico (GTT) del BITAG. Aunque en las secciones anteriores de este informe se ha discutido el potencial de las soluciones a largo plazo y con visión de futuro (por ejemplo, el papel de la tecnología de la red doméstica para mitigar la inseguridad de los dispositivos), esta sección se centra en las recomendaciones que el BITAG cree que son factibles a corto plazo utilizando la tecnología existente.

7.1 Los dispositivos IoT deben utilizar las mejores prácticas de software actuales

- **Los dispositivos IoT deben venir con un software razonablemente actual**

  El BITAG recomienda que los dispositivos IoT se envíen a los clientes o a los puntos de venta con un software razonablemente actual que no contenga vulnerabilidades graves y conocidas. Sin embargo, los errores de software son una especie de "hecho de la vida" y no es raro que se descubran nuevas vulnerabilidades mientras los dispositivos están en el estante. Por ello, es fundamental que un dispositivo IoT cuente con un mecanismo por el que los dispositivos reciban actualizaciones de software automáticas y seguras (véase el siguiente punto).

- **Los dispositivos IoT deben contar con un mecanismo de actualizaciones de software automatizadas y seguras**

  Los errores de software deben reducirse al mínimo, pero -como ya se ha dicho- son inevitables. Por ello, es fundamental que un dispositivo IoT cuente con un mecanismo de actualización automática y segura del software, como se explica en la sección 5.5.

  El BITAG recomienda que los fabricantes de dispositivos IoT o los proveedores de servicios IoT diseñen sus dispositivos y sistemas basándose en la suposición de que con el tiempo se descubrirán nuevos fallos y vulnerabilidades. Deben diseñar sistemas y procesos que garanticen la actualización automática del software de los dispositivos IoT, sin requerir ni esperar ningún tipo de acción por parte del usuario, ni siquiera su aceptación.

  Aunque estas actualizaciones deberían ser automáticas y obligatorias para los usuarios finales, si por alguna razón el sistema de actualización debe permitir una opción de exclusión o inclusión, entonces, basándose en los estudios de interacción persona-ordenador, cualquier sistema de este tipo debería ser de exclusión, de modo que las actualizaciones se produzcan automáticamente por defecto y sin ninguna intervención del usuario, aprobación del usuario u otra acción del usuario final. La posibilidad de que el usuario configure la naturaleza de las actualizaciones del software puede ser importante para algunos usuarios finales, como los que utilizan dispositivos en entornos con recursos limitados (por ejemplo, conexiones por satélite u otros lugares donde los costes de los datos son elevados).

  En algunos casos, los dispositivos de la red doméstica podrían interactuar con los consumidores para lanzar alertas periódicas que faciliten la toma de decisiones con conocimiento de causa (por ejemplo, encuestando al usuario con preguntas que pueda entender sobre cómo quiere que interactúen los dispositivos). La incorporación de este tipo de funciones requiere un cuidado extremo en el diseño, para garantizar que estas alertas al usuario sean significativas y que el volumen de actualizaciones no sea abrumador. Este tipo de funcionalidad puede ser complicada de implementar de forma fiable.

- **Los dispositivos IoT deberían utilizar una autenticación fuerte por defecto**

  El BITAG recomienda que los dispositivos IoT estén protegidos por defecto (por ejemplo, protegidos con contraseña) y que no utilicen nombres de usuario y contraseñas comunes o fáciles de adivinar (por ejemplo, "admin", "password"). Por último, la autenticación para el acceso remoto debe ser segura, ya que potencialmente permite que otras personas que no están físicamente presentes en el hogar supervisen y controlen aspectos dentro de la casa (por ejemplo, cambiar los controles de climatización, supervisar la actividad del usuario).
  Las credenciales de autenticación deben ser únicas para cada dispositivo.

  Los posibles métodos de autenticación por defecto que satisfacen estos criterios son:
  (1) enviando cada dispositivo con una contraseña fija por defecto pero exigiendo al usuario que la cambie como parte del proceso de instalación (es decir, antes de que el dispositivo funcione); y (2) enviando cada dispositivo con una contraseña única para cada unidad e imprimiendo la contraseña en una etiqueta que se coloca en el dispositivo.

- **Las configuraciones de los dispositivos IoT deben ser probadas y reforzadas**

  Algunos dispositivos IoT permiten al usuario personalizar el comportamiento del dispositivo. El BITAG recomienda que los fabricantes prueben la seguridad de cada dispositivo con una serie de configuraciones posibles, en lugar de limitarse a la configuración por defecto. La interfaz de un dispositivo debe evitar -o al menos desalentar activamente- que los usuarios configuren el dispositivo de una manera que lo haga menos seguro.

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

El BITAG recomienda que los fabricantes de dispositivos IoT aseguren las comunicaciones utilizando Seguridad de la Capa de Transporte (TLS) o Criptografía Ligera (LWC) [96,97,98]. Algunos dispositivos pueden realizar un cifrado de clave simétrica en tiempo casi real. Además, la criptografía ligera (LWC) ofrece opciones adicionales para asegurar el tráfico hacia y desde dispositivos con recursos limitados. Si los dispositivos se basan en una infraestructura de clave pública (PKI), una entidad autorizada debe poder revocar los certificados cuando se vean comprometidos, como hacen los navegadores web y los sistemas operativos de los PC [99,100,101,102,103,104,105]. Los servicios en la nube pueden reforzar la integridad de los certificados emitidos por las autoridades de certificación mediante, por ejemplo, la participación en Certificate Transparency [106]. Por último, los fabricantes deben procurar evitar los métodos de cifrado, los protocolos y los tamaños de clave con debilidades conocidas.

Los proveedores que dependen del soporte alojado en la nube para los dispositivos IoT deben configurar sus servidores para seguir las mejores prácticas, como configurar la implementación de TLS para que solo acepte las últimas versiones del protocolo TLS.

- **Cifrar las comunicaciones de configuración (mando y control) por defecto**

  Como se explica en la Sección 5.1, el uso de comunicación no autenticada o en texto claro para la gestión de un dispositivo plantea un riesgo de seguridad significativo. El BITAG recomienda que toda la comunicación para la gestión de dispositivos se realice a través de un canal autenticado y seguro.

- **Comunicaciones seguras desde y hacia los controladores del IoT**

  Si los dispositivos IoT utilizan un controlador centralizado para facilitar la comunicación a través de Internet con un servicio en la nube, el BITAG recomienda que este canal de comunicación esté protegido en ambas direcciones.

- **Cifrar el almacenamiento local de datos sensibles**

  El BITAG recomienda que todos los datos sensibles o confidenciales (por ejemplo, la clave privada, la clave precompartida, la información del usuario o de la instalación) residan en un almacenamiento cifrado.

- **Autenticar las comunicaciones, los cambios de software y las solicitudes de datos**

  El BITAG recomienda que los dispositivos IoT autentifiquen los puntos finales con los que se comunican. La autenticación de la comunicación implica la verificación de la identidad del punto final, lo que a su vez

implica también la verificación de que el certificado que utiliza el punto final está firmado por una autoridad de certificación en la que el dispositivo confía y que no ha sido revocada.

- **Utilice credenciales únicas para cada dispositivo**

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

- **Utilice credenciales que puedan actualizarse**

  El BITAG recomienda que los fabricantes de dispositivos admitan un mecanismo seguro mediante el cual se puedan actualizar las credenciales utilizadas por un dispositivo. Sin embargo, la aplicación de esta recomendación de forma segura requiere un cuidado especial, ya que una implementación incorrecta puede introducir por sí misma un nuevo vector de ataque.

- **Cierre los puertos y desactive los servicios innecesarios**

  El BITAG recomienda que los fabricantes de dispositivos cierren los puertos innecesarios, como el de telnet, ya que los puertos innecesarios pueden no ser seguros o pueden verse comprometidos de alguna manera [107]. Los dispositivos deberían cerrar o desactivar las interfaces y funciones administrativas que no se estén utilizando. Los dispositivos tampoco deberían incluir controladores que no se utilicen.

- **Utilice las bibliotecas que se mantienen y apoyan activamente**

  Muchas de las recomendaciones de este informe requieren la implementación de canales de comunicación seguros. Sin embargo, las implementaciones caseras de protocolos criptográficos y canales de comunicación seguros pueden introducir vulnerabilidades. El BITAG recomienda que, a la hora de implementar las recomendaciones de este informe, los fabricantes de dispositivos utilicen bibliotecas y marcos de trabajo que reciban soporte y mantenimiento activo siempre que sea posible.

7.3 Los dispositivos IoT deben ser más restrictivos que permisivos en la comunicación

BITAG recomienda que los dispositivos IoT se comuniquen sólo con puntos finales de confianza. Siempre que sea posible, los dispositivos no deberían ser accesibles a través de conexiones entrantes por defecto. Los dispositivos IoT no deben confiar únicamente en el cortafuegos de la red para restringir la comunicación, ya que algunas comunicaciones entre dispositivos dentro del hogar no necesariamente atraviesan el cortafuegos.

Tenga en cuenta que una recomendación del BITAG para restringir la *configuración de las* comunicaciones de los dispositivos IoT no debería ir en detrimento de un ecosistema abierto. Un usuario debe ser capaz de configurar las comunicaciones entre dispositivos IoT arbitrarios, y los dispositivos que confían entre sí deben poder comunicarse. Las comunicaciones seguras pueden arrancar listas de confianza restringidas que reflejen el conjunto de dispositivos con los que cualquier dispositivo espera comunicarse. Estas comunicaciones entre dispositivos sólo deberían permitirse a través de mecanismos de confianza y canales de comunicación seguros.

7.4 Los dispositivos IoT deben seguir funcionando si se interrumpe la conectividad a Internet

El BITAG recomienda que un dispositivo IoT sea capaz de realizar su función o funciones principales (por ejemplo, un interruptor de la luz o un termostato deben seguir funcionando con controles manuales), incluso si no está conectado a Internet. Esto se debe a que la conectividad a Internet puede verse interrumpida por causas que van desde una mala configuración accidental hasta un ataque intencionado (por ejemplo, un ataque de denegación de servicio); el funcionamiento del dispositivo debe ser robusto ante este tipo de interrupciones de la conectividad.

Los dispositivos IoT que tienen implicaciones para la seguridad de los usuarios deben seguir funcionando en régimen de desconexión para proteger la seguridad de los consumidores. En estos casos, el dispositivo o el sistema backend debe notificar al usuario sobre el fallo.

En la medida de lo posible, los fabricantes de dispositivos deben facilitar a los usuarios la desactivación o el bloqueo (por

ejemplo, con un cortafuegos) de diversos tráficos de red sin obstaculizar la función principal del dispositivo.

7.5 Los dispositivos IoT deben seguir funcionando si falla el back-end de la nube

Muchos servicios que dependen o utilizan un back-end en la nube pueden seguir funcionando, aunque sea en un estado degradado o parcialmente funcional, cuando la conectividad con el back-end en la nube se interrumpe o el propio servicio falla. Por ejemplo, un termostato cuya configuración puede modificarse a través de un servicio en la nube debería, en el peor de los casos, seguir funcionando con la última configuración conocida o con la predeterminada. Una cámara de seguridad doméstica alojada en la nube debe ser accesible desde el hogar, incluso cuando falle la conectividad a Internet.

7.6 Los dispositivos IoT deben admitir las mejores prácticas de direccionamiento y nomenclatura

Muchos dispositivos IoT pueden permanecer desplegados durante muchos años después de su instalación. Por ello, los dispositivos IoT deben ser compatibles con las mejores prácticas relativamente recientes, aunque actuales, para el direccionamiento IP y el uso del sistema de nombres Doman (DNS). Admitir los protocolos más recientes para el direccionamiento y la asignación de nombres garantizará que estos dispositivos sigan funcionando durante años, que tengan un buen rendimiento y que puedan admitir importantes funciones de seguridad basadas en el DNS.

- **IPv6**

  BITAG recomienda que los dispositivos IoT sean compatibles con la versión más reciente del Protocolo de Internet, IPv6.

- **DNSSEC**

  El BITAG recomienda que los dispositivos IoT admitan el uso o la validación de las extensiones de seguridad del DNS (DNSSEC) cuando se utilicen nombres de dominio. Por ejemplo, si un dispositivo IoT se comunica con un servicio en la nube utilizando el dominio example.com, el proveedor de la nube debe poder firmar el dominio, y el dispositivo IoT debe poder validar esa firma (o asegurarse de que su resolvedor de DNS ascendente lo ha hecho y lo ha indicado en una respuesta de DNS).

7.7 Los dispositivos IoT deben incluir una política de privacidad fácil de encontrar y entender

El BITAG recomienda que los dispositivos IoT se entreguen con una política de privacidad, pero esa política debe ser fácil de encontrar y entender para un usuario típico.

7.8 Divulgar los derechos para disminuir a distancia la funcionalidad de los dispositivos IoT

BITAG recomienda que si la funcionalidad de un dispositivo IoT puede ser disminuida de forma remota por un tercero, como por ejemplo por el fabricante o el proveedor de servicios IoT, esta posibilidad debe quedar clara para el usuario en el momento de la compra.

7.9 El sector de los dispositivos IoT debería considerar un programa de ciberseguridad industrial

El BITAG recomienda que la industria de los dispositivos IoT o un grupo relacionado con la electrónica de consumo considere la creación de un programa respaldado por la industria bajo el cual se podría llevar algún tipo de logotipo o anotación de "Dispositivo IoT seguro" en los envases minoristas de IoT. Dicho programa podría ser análogo a la forma en que la Wi-Fi Alliance u otros grupos validan que los dispositivos cumplen con diversos estándares y/o mejores prácticas.

Un conjunto de mejores prácticas respaldado por la industria parece ser el medio más pragmático para equilibrar la innovación en la IO con los desafíos de seguridad asociados a la naturaleza fluida de la ciberseguridad, y evitar la mentalidad de lista de control que puede ocurrir con los procesos de certificación.

7.10 La cadena de suministro del IoT debe desempeñar su papel en la resolución de los problemas de seguridad y privacidad del IoT

En la actual cadena de suministro de la fábrica al comercio minorista, a menudo es difícil definir las funciones que desempeña cada parte a lo largo del tiempo. Por ello, aquí se definen simplemente como la "cadena de suministro del IoT". Los usuarios finales de los dispositivos IoT y otros dependen de la cadena de suministro IoT para proteger su seguridad y privacidad, y algunas o todas las partes de esa cadena de suministro IoT desempeñan un papel fundamental durante todo el ciclo de vida del producto. Además de otras recomendaciones en esta sección, el BITAG recomienda que la cadena de suministro de la IO tome

las siguientes medidas:

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

- Los dispositivos deben tener un **mecanismo de restablecimiento** para los dispositivos IoT que borre toda la configuración para su uso cuando un consumidor devuelva o revenda el dispositivo. Los fabricantes de dispositivos también deben proporcionar un mecanismo para borrar o restablecer cualquier dato que el respectivo dispositivo almacene en la nube.

- Los fabricantes deben proporcionar un **sistema de notificación de fallos** con mecanismos de presentación de fallos bien definidos y una política de respuesta documentada.

- Los fabricantes deben proteger la **cadena de suministro de software seguro** para evitar la introducción de programas maliciosos durante el proceso de fabricación; los vendedores y fabricantes deben tomar las medidas adecuadas para asegurar su cadena de suministro de software.

- Los fabricantes deben **prestar apoyo a un dispositivo IoT a lo largo de su vida útil**, desde el diseño hasta el momento en que se retira el dispositivo, incluyendo la transparencia sobre el período de tiempo durante el cual planean proporcionar apoyo continuo a un dispositivo, y lo que el consumidor debe esperar de la función del dispositivo al final de su vida útil.

- Los fabricantes deben proporcionar **métodos claros para que los consumidores determinen con quién pueden ponerse en contacto para recibir asistencia** y **métodos para ponerse en contacto con los consumidores** para difundir información sobre las vulnerabilidades del software u otros problemas.

- Los fabricantes deben **informar sobre el descubrimiento y la corrección de las vulnerabilidades de los programas informáticos** que suponen una amenaza para la seguridad o la privacidad de los consumidores.

- Los fabricantes deben proporcionar un **proceso de notificación de vulnerabilidades** con un formulario de notificación de vulnerabilidades bien definido, fácil de localizar y seguro, así como una política de respuesta documentada. Los fabricantes deberían considerar el cumplimiento de la norma ISO 30111 [108], un estándar para la gestión de informes de vulnerabilidad.

8 Otros grupos centrados en este tema

Si bien el BITAG tiene un punto de vista único sobre esta cuestión, cabe señalar que otros grupos también se centran en diversos aspectos de esta cuestión. Entre estos grupos se encuentran:

- Protocolo de Internet para la Alianza de Objetos Inteligentes (IPSO) [109]
- Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) [110]
- Institutos Nacionales de Normas y Tecnología (NIST) [111]
- Internet Engineering Task Force [112]
    - LWIG (Light-Weight Implementation Guidance) [113]
    - 6Lo (IPv6 sobre redes de nodos con recursos limitados) [114]
    - 6TiSCH (IPv6 sobre el modo TSCH de IEEE 802.15.4e) [115]
    - ROLL (Routing Over Low power and Lossy networks) [116]
    - CoRE (Constrained RESTful Environments) [117]

    - DICE (DTLS en entornos restringidos) [118]
    - ACE (Autenticación y Autorización para Entornos Restringidos) [119]
    - COSE (CBOR Object Signing and Encryption) [120]
    - 6lowpan IPv6 sobre WPAN de baja potencia (cerrado) [121]
- GSMA: Vida conectada [122]
- IRTF: Grupo de Trabajo de Investigación de Internet [123]
    - T2TRG: Grupo de Investigación Thing-to-Thing [124]
- W3C: Consorcio Mundial de la Web [125]
    - WoT: Web of Things Interest Group [126]
- Comisión Federal de Comercio de Estados Unidos (FTC) [127,128,129]
- Departamento de Comercio de EE.UU., Administración Nacional de Telecomunicaciones e Información (NTIA) [130, 131]
- Foro de Gobernanza de Internet (IGF) [132]
- Alianza para la Confianza en Línea [133]
- Comité Técnico Conjunto 1 de la Organización Internacional de Normalización (ISO/IEC JTC1) [134]: Creó dos grupos de trabajo especiales sobre la gestión y el Internet de las cosas; uno de ellos está administrado por el ANSI.
    - Comisión Electrotécnica Internacional [135]: Aunque la CEI no se limita únicamente a los dispositivos de la IO (y trabaja en todas las tecnologías eléctricas/electrónicas), ha realizado varios trabajos de investigación sobre la IO que pueden contener normas.
- Comité Internacional de Normas de Tecnología de la Información (INCITS) [136]: Acreditado por ANSI, para "servir como grupo central de asesoramiento técnico de Estados Unidos para un esfuerzo global".

- Grupo de trabajo multisectorial sobre privacidad en la IO de TRUSTe [137]: Con el objetivo de elaborar normas técnicas para ayudar a las empresas a desarrollar las soluciones necesarias para proteger la privacidad de los consumidores en la IO.
- Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) P2413 [138]: Un proyecto del IEEE relativo a un estándar para un marco arquitectónico para el IoT.
- Foro de la IO inalámbrica [139]: "No es una organización de normalización, pero tiene como objetivo entregar los requisitos... a los organismos de normalización donde hay una falta de normas (por ejemplo, la conectividad inalámbrica de largo alcance), e impulsar el consenso donde hay normas que compiten (por ejemplo, el descubrimiento de dispositivos domésticos)."
    - Grupo de aplicaciones: grupo de trabajo que revisa las API estándar
    - Grupo de conectividad: grupo de trabajo que evalúa el acceso radioeléctrico.
    - Grupo de reglamentación: grupo de trabajo que armoniza la reglamentación mundial sobre la exención de licencias y la disponibilidad del espectro con licencia.
- Open Connectivity Foundation (antes llamada Open Interconnect Consortium) [140]: Organización creada por Intel, Cisco y Samsung para crear una especificación interoperable abierta para el IoT. También adquirió el Foro UPnP.
- Object Management Group (OMG) [141]: Un consorcio internacional de estándares tecnológicos sin ánimo de lucro, que está realizando un importante trabajo sobre el IoT industrial.
    - Consorcio de Internet Industrial [142]: "... es el consorcio internacional sin ánimo de lucro de composición abierta... que establece el marco arquitectónico y la dirección de la Internet Industrial". Trabaja para acelerar la adopción de tecnologías WAN inalámbricas dedicadas al mercado del IoT. Fundado por CISCO, incluye a Accenture, Arkessa, BT Telensa y WSN.
- oneM2M [143]: Desarrollar especificaciones técnicas que aborden la necesidad de una capa de servicio M2M común que pueda integrarse en diversos equipos y programas informáticos.
- Sociedad Internacional de Automatización (ISA) [144]: "Asociación profesional sin ánimo de lucro que establece normas para quienes aplican la ingeniería y la tecnología para mejorar la gestión, la seguridad y la ciberseguridad de los sistemas modernos de automatización y control." Ha realizado algunas investigaciones sobre la IO, aunque no hay indicios de un grupo de trabajo.
- OASIS [145]: "Consorcio sin ánimo de lucro que impulsa el desarrollo, la convergencia y la adopción de estándares abiertos para la sociedad global de la información".
    - OASIS Advanced Message Queuing Protocol (AMQP) TC: Definición de un protocolo de Internet omnipresente, seguro, fiable y abierto para gestionar la mensajería empresarial.
    - OASIS Message Queuing Telemetry Transport (MQTT) TC: Proporciona un protocolo ligero de transporte de mensajería fiable de publicación/suscripción adecuado para la comunicación en contextos M2M/IoT en los que se requiere una pequeña huella de código y/o el ancho de banda de la red es un problema.
    - OASIS Open Building Information Exchange (oBIX) TC: Permite que los sistemas de control mecánico y eléctrico de los edificios se comuniquen con las aplicaciones empresariales.
- Hypercat [146]: Un consorcio y un estándar que impulsa un IoT seguro e interoperable para la industria y las ciudades.
- Alianza AllSeen [147]: Creó AllJoyn, que es un "ecosistema colaborativo y abierto".

- Grupo Thread [148]: Creó el protocolo Thread, que es un protocolo de red libre de derechos para el Internet de las cosas. Ofrece certificación de productos.

9 Referencias

1] James Manika y otros, The Internet of Things: Mapping the Value Beyond the Hype, McKinsey Global Institute, junio de 2015, http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the- physical-world.

[2] Brian Krebs, "IoT Reality: Smart devices, Dumb defaults", Krebs on Security, Blog, 8 de febrero de 2016, http://krebsonsecurity.com/2016/02/iot-reality-smart-devices-dumb-defaults/.

[3] Kalev Leetaru, "How the Internet of Things will Turn your Living Room Into The Future Cyber Battleground", 6 de noviembre de 2015, Forbes.com, http://www.forbes.com/sites/kalevleetaru/2015/11/06/how-the-internet-of-things-will-turn-your-living-room-into-the- future-cyber-battleground/ (última visita el 18 de noviembre de 2016).

[4] IEEE Standards Association, IEEE 802.15: Wireless Personal Area Networks (PANs), https://standards.ieee.org/about/get/802/802.15.html (última visita el 18 de noviembre de 2016).

[5] X10, https://www.x10.com/ (visitado por última vez el 18 de noviembre de 2016).

[6] Hewlett Packard, Internet of Things Research Study: 2015 Report, HP Enterprise, 2015, *disponible en* https://www.hpe.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

[7] John Pescatore, Securing the Internet of Things Survey, Sans Institute Analyst Survey, enero de 2014, *disponible en* https://www.sans.org/reading-room/whitepapers/analyst/securing-internet-things-survey-34785.

[8] Charlie Osborne, "Internet of Things devices lack fundamental security, study finds", 8 de abril de 2015, ZDNet, http://www.zdnet.com/article/internet-of-things-devices-lack-fundamental-security-study-finds/ (visitado por última vez el 18 de noviembre de 2016).

[9] Ka-Ping Yee, "Aligning security and usability". IEEE Security & Privacy 2.5 (2004): 48-55, *disponible en* http://zesty.ca/pubs/yee-sid- ieeesp2004.pdf.

[10] Veracode, El Internet de las cosas: Security Research Study, Whitepaper, 2014, *disponible en* https://www.veracode.com/sites/default/files/Resources/Whitepapers/internet-of-things-whitepaper.pdf

[11] Rebecca E. Grinter, et al., "El trabajo para hacer funcionar una red doméstica". *ECSCW 2005*. Springer Netherlands, 2005, *disponible en* http://www.cc.gatech.edu/~beki/c27.pdf.

[12] Yin Min Pa Pa, et al. "IoTPOT: Analizando el aumento de los compromisos de IoT". (2015), *disponible en* https://www.usenix.org/system/files/conference/woot15/woot15-paper-pa.pdf

[13] Symantec, "IoT devices being increasingly used for DDoS attacks", Symantec Security Response, 22 de septiembre de 2016, *disponible en:* http://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks.

[14] Steve Rogerson, "IoT blamed for denial of service attacks", IoT MTM Council, 29 de abril de 2015, *disponible en* http://www.iotm2mcouncil.org/serviceattacks.

[15] Energin Janina, "Distributed denial-of-service (DDoS) attack knocked the file-sharing site Pirate Bay offline", 17 de mayo de 2012, ceoworld.biz, http://ceoworld.biz/ceo/2012/05/17/distributed-denial-of-service-ddos-attack-knocked-the-file-sharing-site-pirate-bay- offline.

[16] Angela Moscaritolo, "El FBI detiene a seis personas por una estafa cibernética de clics que supuso 14 millones de dólares", SC Magazine, 9 de noviembre de 2011, http://www.scmagazine.com/fbi-arrests-six-in-click-fraud-cyber-scam-that-netted-14m/article/216399/

[17] Sarthak Grover y Nick Feamster, The Internet of Unpatched Things, PrivacyCon 2016, https://www.ftc.gov/system/files/documents/public_comments/2015/10/00071-98118.pdf.

[18] Bruce Schneier, "The Internet of Things Is Wildly Insecure - And Often Unpatchable", Wired, 6 de enero de 2014, https://www.schneier.com/essays/archives/2014/01/the_internet_of_thin.html.

[19] Bruce Schneier, "Surveillance and the Internet of Things", Blog, 21 de mayo de 2013, https://www.schneier.com/blog/archives/2013/05/the_eyes_and_ea.html.

[20] Matt Loeb, "Internet of Things Security Issues Require a Rethink on Risk Management", Wall Street Journal, 14 de octubre de 2015, http://blogs.wsj.com/cio/2015/10/14/internet-of-things-security-issues-require-a-rethink-on-risk-management/.

[21] Arik Hesseldahl, "A Hacker's-Eye View of the Internet of Things", Recode.net, 7 de abril de 2015, http://recode.net/2015/04/07/a- hackers-eye-view-of-the-internet-of-things/.

[22] Arik Hesseldahl, "The Internet of Things Is the Hackers' New Playground", Recode.net, 29 de julio de 2014, http://recode.net/2014/07/29/the-internet-of-things-is-the-hackers-new-playground/.

[23] Julie Knudson, "Security Challenges of the Internet of Things: The IoT's lack of standardized protocols and new traffic flows complicate administrators' security efforts", Enterprise Networking Planet, 13 de mayo de 2015, http://www.enterprisenetworkingplanet.com/netsecur/security-challenges-of-the-internet-of-things.html.

[24] Reddit, Lista de discusión sobre privacidad, "Compré y devolví un conjunto de cámaras de seguridad domésticas conectadas por WiFi, olvidé borrar mi cuenta y ahora puedo ver al nuevo propietario", https://www.reddit.com/r/privacy/comments/4ortwb/i_bought_and_returned_a_set_of_wifi_connected/ (última visita el 18 de noviembre de 2016).

[25] Christina Cardoza, "Neumáticos de Princeton para saber si tus dispositivos IoT son seguros", SD Times, 22 de enero de 2016, *disponible en* http://sdtimes.com/princeton-tries-to-find-out-are-your-iot-devices-safe/.

[26] Christian Dancke Tuen, "Security in Internet of Things Systems", tesis de máster, Universidad Noruega de Ciencia y Tecnología, Departamento de Telemática, junio de 2015, *disponible en* https://brage.bibsys.no/xmlui/bitstream/handle/11250/2352738/12892_FULLTEXT.pdf?sequence=1&isAllowed=y.

[27] Hewlett Packard, Internet of Things Security Study: Smartwatches, IoT Research Series 2014, http://go.saas.hpe.com/l/28912/2015-07-20/325lbm/28912/69038/IoT_Research_Series_Smartwatches.pdf.

[28] Kim Zetter, "Hospital Networks are Leaking Data, Leaving Critical Devices Vulnerable", 25 de junio de 2014, https://www.wired.com/2014/06/hospital-networks-leaking-data/.

[29] Mario Ballano Barcena & Candid Wueest, Insecurity in the Internet of Things, 12 de marzo de 2015, Symantec, https://www.symantec.com/content/en/us/enterprise/fact_sheets/b-insecurity-in-the-internet-of-things-ds.pdf.

[30] Katie Natopoulos, "Somebody's watching: how a simple exploit lets strangers tap into private security cameras", 3 de febrero de 2012, The Verge, http://www.theverge.com/2012/2/3/2767453/trendnet-ip-camera-exploit-4chan.

[31] Brian Krebs, "This is Why People Fear the Internet of Things", 8 de febrero de 2016, Krebs on Security, https://krebsonsecurity.com/2016/02/this-is-why-people-fear-the-internet-of-things/

[32] Brady Dale, "Eight Internet of Things Security Fails: Cambia las contraseñas de tus routers cuando los configures por Dios", Observer, 16 de julio de 2015, http://observer.com/2015/07/eight-internet-of-things-security-fails/.

[33] Michael Winter, "Un joven californiano admite el complot de 'sextorsión' de Miss Teen USA", USA Today, 12 de noviembre de 2013, http://www.usatoday.com/story/news/nation/2013/11/12/miss-teen-usa-sextortion-guilty-plea/3510461/.

[34] Kevin Townsend, "Malware Found in IoT Cameras Sold by Amazon", Security Week, 11 de abril de 2016, http://www.securityweek.com/malware-found-iot-cameras-sold-amazon.

[35] Johannes Ullrich, "Coin Mining DVRs: A compromise from start to finish", Internet Storm Center, SANS ISC InfoSec Forums, https://isc.sans.edu/forums/diary/Coin+Mining+DVRs+A+compromise+fromart+to+finish/18071/.

[36] Kim Zetter, "Una mirada sin precedentes a STUXNET, la primera arma digital del mundo", WIRED, 3 de noviembre de 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[37] Swati Khandelwal, "IoT Botnet - 25.000 CCTV Cameras Hacked to launch DDoS Attack", The Hacker News, 28 de junio de 2016, http://thehackernews.com/2016/06/cctv-camera-hacking.html.

[38] Dahua, Cyber Security Statement, comunicado de prensa, 1 de octubre de 2016, *disponible en* http://www.dahuasecurity.com/en/us/single.php?nid=274.

[39] Dahua, Dahua Support Wiki Main Page, http://www.dahuawiki.com/Main_Page (visitado por última vez el 18 de noviembre de 2016).

[40] Dahua, Cómo crear un sistema de seguridad más seguro, http://www.dahuasecurity.com/en/us/best-practices.php (visitado por última vez el 18 de noviembre de 2016).

[41] Grupo Asesor Técnico de Internet de Banda Ancha (BITAG), SNMP Reflected Amplification DDoS Attack Mitigation, agosto de 2012, http://bitag.org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation.pdf.

[42] T. Dierks & E. Rescorla, "The Transport Layer Security (TLS) Protocol 1.2", RFC 5246, Aug. 2008, https://tools.ietf.org/html/rfc5246.

[43] E. Rescorla & N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, Jan. 2012, https://tools.ietf.org/html/rfc6347.

[44] Aaron Ardiri, "¿Es posible asegurar los microcontroladores utilizados dentro de IoT?", EVO Things, Blogs/Tutorials, 27 de agosto de 2014, https://evothings.com/is-it-possible-to-secure-micro-controllers-used-within-iot/;

[45] Reinhard Seiler, Blog, Truecrypt benchmark for Raspberry Pi, 20 de julio de 2012, http://blog.rseiler.at/2012/07/truecrypt-benchmark- for-raspberry-pi.html.

[46] Darlene Storm, "MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks", Computerworld, 8 de junio de 2015, http://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create- backdoors-in-hospital-networks.html.

[47] Kim Zetter, "How Thieves Can Hack and Disable Your Home Alarm System", WIRED, 23 de julio de 2014, https://www.wired.com/2014/07/hacking-home-alarms/.

[48] Marek Majkowski, "Say Cheese: a snapshot of the massive DDoS attacks coming from IoT cameras", 11 de octubre de 2018, Cloudflare Blog, https://blog.cloudflare.com/say-cheese-a-snapshot-of-the-massive-ddos-attacks-coming-from-iot-cameras/ (visitado por última vez el 18 de noviembre de 2016).

[49] Nest, "Nest Learning Thermostat software update history", Nest Support, https://nest.com/support/article/Nest-Learning- Thermostat-software-update-history (visitado por última vez el 18 de noviembre de 2016).

[50] Nest, "How do I update the software on my Nest Learning Thermostat," Nest Support, https://nest.com/support/article/How-do-I- update-the-software-on-my-Nest-Learning-Thermostat (visitado por última vez el 18 de noviembre de 2016).

[51] Nick Bilton, "Nest Thermostat Leaves Users in the Cold", 13 de enero de 2016, NYTimes, *disponible en* http://www.nytimes.com/2016/01/14/fashion/nest-thermostat-glitch-battery-dies-software-freeze.html.

[52] Catalin Cimpanu, "Security Researcher with Implanted Pacemaker Sounds the Alarm on IoT Medical Devices", Softpedia, 5 de enero de 2016, http://news.softpedia.com/news/security-researcher-with-implanted-pacemaker-sounds-the-alarm-on-iot-medical-devices- 498448.shtml.

[53] Russ Housley, Palabras del presidente del IAB: Declaración del IAB sobre la confidencialidad en Internet, IETF Journal marzo 2015, https://www.internetsociety.org/publications/ietf-journal-march-2015/words-iab-chair-12.

[54] Jane Wakefield, "Smart LED light bulbs leak wi-fi passwords", BBC News, 8 de julio de 2014, http://www.bbc.com/news/technology- 28208905.

[55] SEC Consult, "House of Keys: Industry-Wide HTTPS Certificate and SSH Key Reuse Endangers Millions of Devices Worldwide", Blog, 25 de noviembre de 2015, http://blog.sec-consult.com/2015/11/house-of-keys-industry-wide-https.html (visitado por última vez el 18 de noviembre de 2016).

[56] Erik C. Davis, "Clustering and Outlier Detection: Methods and Applications in Smart Home Networks", tesis de licenciatura, Investigación de Operaciones e Ingeniería Financiera. Universidad de Princeton. Junio de 2016.

[57] Yin Zhang & Vern Paxson, "Detecting Stepping Stones", USENIX *Security Symposium,* agosto de 2000, https://www.cs.utexas.edu/~yzhang/papers/stepping-sec00.pdf.

[58] Robert Vamosi, "Covert Hacking of IoT Trivial Say Researchers", Mocana, 28 de febrero de 2014, https://www.mocana.com/blog/2014/02/28/covert-hacking-iot-trivial-say-researchers.

[59] Lorenzo Franceschi-Bicchierai, "Internet-Connected Fisher Price Teddy Bear Left Kids' Identities Exposed", Motherboard, 2 de febrero de 2016, http://motherboard.vice.com/read/internet-connected-fisher-price-teddy-bear-left-kids-identities-exposed.

[60] Lorenzo Franceschi-Bicchierai, "Bugs in 'Hello Barbie' Could Have Let Hackers Spy on Children's Chats", Motherboard, 4 de diciembre de 2015, http://motherboard.vice.com/read/bugs-in-hello-barbie-could-have-let-hackers-spy-on-kids-chats.

[61] Lorenzo Franceschi-Bicchierai, "Hacked Toymaker VTech Admits Breach Actually Hit 6.3 Million Children", Motherboard, 1 de diciembre de 2015, http://motherboard.vice.com/read/hacked-toymaker-vtech-admits-breach-actually-hit-63-million-children.

[62] BBC, "Alarma del coche híbrido Mitsubishi Outlander 'hackeada'", BBC News: Tecnología, 6 de junio de 2016, http://www.bbc.com/news/technology-36444586.

[63] Darlene Storm, "Nissan Leaf leaks secretly driver location, speed to websites", ComputerWorld, 14 de junio de 2011, http://www.computerworld.com/article/2470123/endpoint-security/nissan-leaf-secretly-leaks-driver-location--speed-to- websites.html.

[64] Leo Kelion, "Nissan Leaf electric cars vulnerability disclosed", BBC News: Tecnología, 24 de febrero de 2016, http://www.bbc.com/news/technology-35642749.

[65] Colin Neagle, "Smart refrigerator hack exposes credentials", NetworkWorld, 26 de agosto de 2015, http://www.networkworld.com/article/2976270/internet-of-things/smart-refrigerator-hack-exposes-gmail-login-credentials.html.

[66] Newswise, "Georgia Tech advierte de las amenazas al almacenamiento de datos en la nube y a los dispositivos móviles en el último informe sobre "ciberamenazas emergentes"", comunicado de prensa, 6 de noviembre de 2013, http://www.newswise.com/articles/georgia-tech-warns-of-threats-to-cloud-data-storage-mobile-devices-in-latest-emerging-cyber-threats-report

[67] Institute for Information Security & Privacy, Georgia Institute of Technology, Emerging Cyber Threats Report 2016, 2016, *disponible en* http://www.iisp.gatech.edu/sites/default/files/documents/2016_georgiatech_cyberthreatsreport_onlinescroll.pdf.

[68] Phys.Org, "Your smartwatch is giving away your ATM PIN", 6 de julio de 2016, http://phys.org/news/2016-07-smartwatch-atm-pin.html (visitado por última vez el 7 de octubre de 2016).

[69] Robert J. Ellison et al., "Evaluating and Mitigating Software Supply Chain Security Risks", Software Engineering Institute, Technical Note, mayo de 2010, *disponible en* http://www.sei.cmu.edu/reports/10tn016.pdf.

[70] Internet Storm Center, Survival Time: Summary, https://isc.sans.edu//survivaltime.html (visitado por última vez el 18 de noviembre de 2016).

[71] Brian Krebs, "KrebsOnSecurity Hit with Record DDoS", KrebsOnSecurity, 21 de septiembre de 2016, https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/ (última visita el 3 de octubre de 2016).

[72] Flashpoint, "Attack of Things!", Blog Post, 17 de septiembre de 2016, https://www.flashpoint-intel.com/attack-of-things/ (visitado por última vez el 18 de noviembre de 2016).

[73] Drew Fitzgerald, "Hackers Infect Army of Cameras, DVRs for Massive Internet Attacks", Wall Street Journal, 30 de septiembre de 2016, http://www.wsj.com/articles/hackers-infect-army-of-cameras-dvrs-for-massive-internet-attacks-1475179428 (visitado por última vez el 3 de octubre de 2016).

[74] Comisión Federal de Comercio, "ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk", comunicado de prensa, 23 de febrero de 2016, *disponible en* https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges- insecure-home-routers-cloud-services-put.

[75] Network World, "KrebsOnSecurity moves to Project Shield for protection against DDoS attack censorship", Blog de la Sra. Smith, 25 de septiembre de 2016, http://www.networkworld.com/article/3123806/security/krebsonsecurity-moves-to-project-shield-for-protection-against-ddos- attack-censorship.html (última visita el 3 de octubre de 2016).

[76] Brian Krebs, "The Democratization of Censorship", KrebsOnSecurity, 16 de septiembre de 2016, https://krebsonsecurity.com/2016/09/the- democratization-of-censorship/ (última visita el 3 de octubre de 2016).

[77] Tim Greene, "Largest DDoS attack ever delivered by botnet of hijacked IoT devices", Network World, 23 de septiembre de 2016, http://www.networkworld.com/article/3123672/security/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html (visitado por última vez el 3 de octubre de 2016).

[78] Dan Goodin, "Record-breaking DDoS reportedly delivered by >145k hacked cameras", ArsTechnica, 28 de septiembre de 2016, http://arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/ (última visita el 3 de octubre de 2016).

[79] David Plonka y Elisa Boschi, The Internet of Old and Unmanaged, 2016, *disponible en* https://down.dsg.cs.tcd.ie/iotsu/subs/IoTSU_2016_paper_25.pdf.

[80] David Plonka, Measurement and Analysis for the Internet of Things, 18 de julio de 2016, *disponible en* https://www.ietf.org/proceedings/96/slides/slides-96-maprg-8.pdf.

[81] Lucian Constantin, "Attackers hijack CCTV cameras to launch DDoS attacks, Computerworld", 22 de octubre de 2015, http://www.computerworld.com/article/2996079/internet-of-things/attackers-hijack-cctv-cameras-to-launch-ddos-attacks.html.

[82] Kashmir Hill, "This guy's light bulb performed a DoS attack on his entire smart house", Fusion.net, 3 de marzo de 2015, http://fusion.net/story/55026/this-guys-light-bulb-ddosed-his-entire-smart-house/.

[83] Tom Spring, "Inseguridad: Pinpointing the Problems", ThreatPost, 21 de julio de 2016, https://threatpost.com/iot-insecurity-pinpointing- the-problems/119389/.

[84] DirectTV, Guía del usuario: Genie and earlier HD DVR Receivers, pg. 107, http://www.directv.com/learn/pdf/System_Manuals/DIRECTV/DIRECTV_HDDVR_HR20-44.pdf.

[85] Roku, "¿Cómo puedo actualizar el software de mi reproductor Roku?", https://support.roku.com/hc/en-us/articles/208755668-How-can-I- update-the-software-on-my-Roku-player- (visitado por última vez el 18 de noviembre de 2016).

[86] Arunesh Mathur, et al. "They Keep Coming Back Like Zombies': Improving Software Updating Interfaces", *USENIX Symposium on Usable Security and Privacy,* 2016, *disponible en* https://www.usenix.org/system/files/conference/soups2016/soups2016-paper- mathur.pdf.

[87] David Plonka, Flawed Routers Flood University of Wisconsin Internet Time Server, 19 de julio de 2006, http://pages.cs.wisc.edu/~plonka/netgear-sntp/.

[88] Comcast, "Some NetGear Routers Causing Flood of DNS Queries", Comcast DNS News, 20 de mayo de 2013, http://dns.xfinity.com/index.php/entry/some-netgear-routers-causing-flood-of-dns-queries.

[89] Lista de discusión de la comunidad NetGear, "¿Miles de solicitudes de DNS por segundo?", 2 de marzo de 2012, https://community.netgear.com/t5/General-WiFi-Routers/Thousands-of-DNS-Requests-Per-Second/td-p/414710.

[90] Benoit Panizzon, ¿Ataque DDOS por productos Netgear causado por CNAME en lugar de un registro A?, Lista de discusión [SWINOG], 27 de junio de 2013, http://lists.swinog.ch/public/swinog/2013-June/005863.html.

[91] National Security Agency, Defense in Depth, Whitepaper, 2010, *disponible en* https://citadel-information.com/wp-content/uploads/2010/12/nsa-defense-in-depth.pdf.

[92] Vijay Sivaraman et al. "Network-Level Security and Privacy Control for Smart-Home IoT Devices", *IEEE Wireless and Mobile Computing, Networking, and Communications.* 2015, https://www.researchgate.net/publication/281275810_Network- Level_Security_and_Privacy_Control_for_Smart-Home_IoT_Devices.

[93] Konstantinos Grivas y Stelios Zerefos, Augmented Home Inventories, European Conference on Ambient Intelligence, 2015.

[94] William Enck, et al. "TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones", en Proc. of the USENIX Symposium on Operating Systems Design and Implementation (OSDI), octubre de 2010, *disponible en* http://appanalysis.org/tdroid10.pdf.

[95] Disconnect, Disconnect Privacy Tool, https://disconnect.me/ (visitado por última vez el 18 de noviembre de 2016).

[96] Masanobu Katagi y Shiho Moriai, Lightweight Cryptography for the Internet of Things, 2011, https://www.iab.org/wp- content/IAB-uploads/2011/03/Kaftan.pdf.

[97] GitHub, "SSL and TLS Deployment Best Practices", SSL Labs Wiki, https://github.com/ssllabs/research/wiki/SSL-and-TLS- Deployment-Best-Practices (última visita el 3 de octubre de 2016).

[98] Mozilla, "Security/Server Side TLS", Mozilla Wiki, https://wiki.mozilla.org/Security/Server_Side_TLS (última visita el 18 de noviembre de 2016).

[99] Dan Auerbach, "2011 In Review: Ever-Clearer Vulabilities in Certificate Authority System", Electronic Frontier Foundation, 27 de diciembre de 2011, https://www.eff.org/deeplinks/2011/12/2011-review-ever-clearer-vulnerabilities-certificate-authority-system.

[100] Wikipedia, Lista de revocaciones, https://en.wikipedia.org/wiki/Revocation_list (visitada por última vez el 18 de noviembre de 2016).

[101] Dennis Fisher, "Final Report on Diginator Hack Shows Total Compromise of CA Servers", ThreatPost, 31 de octubre de 2012, https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/.

[102] Eric Mill, "Certificate Authorities are Actually a Tremendous Problem", Blog Post, 21 de junio de 2013, https://konklone.com/post/certificate-authorities-are-actually-a-tremendous-problem (visitado por última vez el 18 de noviembre de 2016).

[103] Chester Wisniewski, "Another certificate authority issues dangerous certificates, Naked Security", 3 de noviembre de 2011, https://nakedsecurity.sophos.com/2011/11/03/another-certificate-authority-issues-dangerous-certficates/ (visitado por última vez el 18 de noviembre de 2016).

[104] Glenn Fleishman, "The Huge Web Security Loophole That Most People Don't Know About, And How It's Being Fixed", FastCompany, *disponible en* http://www.fastcompany.com/3042030/tech-forecast/the-huge-web-security-loophole-that-most-people-dont-know- about-and-how-its-be.

[105] Steve Roosa, "The Flawed Legal Architecture of the Certificate Authority Trust Model", Freedom to Tinker, 15 de diciembre de 2010, https://freedom-to-tinker.com/blog/sroosa/flawed-legal-architecture-certificate-authority-trust-model/ (visitado por última vez el 18 de noviembre de 2016).

[106] Google, Certificate Transparency Project, ¿Qué es la transparencia de los certificados?, https://www.certificate-transparency.org/what-is-ct (visitado por última vez el 18 de noviembre de 2016).

[107] Level 3 Threat Research Labs, "Attack of Things!", Level 3 Blog, http://blog.level3.com/security/attack-of-things/ (visitado por última vez el 18 de noviembre de 2016).

[108] Organización Internacional de Normalización, ISO/IEC 30111:2013: Information Technology - Security techniques - Vulnerability handling processes, 2013, *disponible en* http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231.

[109] Alianza IPSO, http://www.ipso-alliance.org (visitado por última vez el 18 de noviembre de 2016).

[110] Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), https://www.ieee.org (última visita el 18 de noviembre de 2016).

[111] Departamento de Comercio de EE.UU., Instituto Nacional de Normas y Tecnología, http://nist.gov (visitado por última vez el 18 de noviembre de 2016).

[112] Internet Engineering Task Force (IETF), http://www.ietf.org (visitado por última vez el 18 de noviembre de 2016).

[113] Internet Engineering Task Force (IETF), Light-Weight Implementation Guideance (lwig) https://datatracker.ietf.org/wg/lwig/ (última visita el 18 de noviembre de 2016).

[114] Internet Engineering Task Force (IETF), IPv6 Over Networks of Resource-Constrained Nodes (6lo), https://datatracker.ietf.org/wg/6lo/ (última visita el 18 de noviembre de 2016).

[115] Grupo de Trabajo de Ingeniería de Internet (IETF), IPv6 sobre el modo TSCH de IEEE 802.15.4e (6tisch), https://datatracker.ietf.org/wg/6tisch/ (última visita el 18 de noviembre de 2016).

[116] Internet Engineering Task Force (IETF), Routing over Low power and Lossy networks (roll), https://datatracker.ietf.org/wg/roll/ (última visita el 18 de noviembre de 2016).

[117] Grupo de Trabajo de Ingeniería de Internet (IETF), Constrained RESTful environments (core), https://datatracker.ietf.org/wg/core/ (última visita el 18 de noviembre de 2016).

[118] Internet Engineering Task Force (IETF), DTLS in Constrained Environments (dados), https://datatracker.ietf.org/wg/dice (última visita el 18 de noviembre de 2016).

[119] Grupo de Trabajo de Ingeniería de Internet (IETF), Authentication and Authorization for Constrained Environments (ace), https://datatracker.ietf.org/wg/ace/(última visita el 18 de noviembre de 2016).

[120] Grupo de Trabajo de Ingeniería de Internet (IETF), CBOR Object Signing and Encryption (cose) https://datatracker.ietf.org/wg/cose/ (última visita el 18 de noviembre de 2016).

[121] Grupo de Trabajo de Ingeniería de Internet (IETF), IPv6 sobre WPAN de baja potencia (6lowpan), https://datatracker.ietf.org/wg/6lowpan (última visita el 18 de noviembre de 2016).

[122] Groupe Speciale Mobile Association (GSMA), GSMA IoT Security Guidelines, http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/ (última visita el 18 de noviembre de 2016).

[123] Internet Research Task Force, http://irtf.org (visitado por última vez el 18 de noviembre de 2016).

[124] Internet Research Task Force, Thing-to-Thing Research Group, https://irtf.org/t2trg (visitado por última vez el 18 de noviembre de 2016).

[125] World Wide Web Consortium (W3C), http://www.w3c.org (última visita el 18 de noviembre de 2016).

[126] World Wide Web Consortium (W3C), Web of Things Interest Group, https://www.w3.org/WoT/IG/ (última visita el 18 de noviembre de 2016).

[127] Comisión Federal de Comercio, Oficina de Protección del Consumidor y Oficina de Planificación de Políticas, In The Matter of The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancemenet of the Internet of Things, Docket No. 160331306-6306-01, Comments of Staff, https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection- office-policy-planning-national-telecommunications/160603ntiacomment.pdf.

[128] Comisión Federal de Comercio, Internet of Things: Privacy & Security in a Connected World, Staff Report, enero de 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled- internet-things-privacy/150127iotrpt.pdf.

[129] Dennis Fisher, FTC Warns of Security and Privacy Risks in IoT Devices, 3 de junio de 2016, https://www.onthewire.io/ftc-warns-of- security-and-privacy-risks-in-iot-devices/ (última visita el 18 de noviembre de 2016).

[130] Administración Nacional de Telecomunicaciones e Información, Internet de las Cosas, https://www.ntia.doc.gov/category/internet- things (visitado por última vez el 18 de noviembre de 2016).

[131] La Administración Nacional de Telecomunicaciones e Información del Departamento de Comercio de EE.UU. busca Comment on Potential Policy Issues Related to Internet of Things, comunicado de prensa, 5 de abril de 2016, https://www.ntia.doc.gov/press- release/2016/us-department-commerce-seeks-comment-potential-policy-issues-related-internet-thi

[132] Foro para la Gobernanza de Internet, Coalición Dinámica sobre la Internet de las Cosas, https://www.intgovforum.org/cms/documents/igf-meeting/igf-2016/827-dciot-2015-output-document- 1/file.

[133] Online Trust Alliance, Internet of Things, 19 de septiembre de 2016, https://otalliance.org/initiatives/internet-things (visitado por última vez el 18 de noviembre de 2016).

[134] Organización Internacional de Normalización (ISO), Comité Técnico Conjunto ISO/IEC sobre Tecnología de la Información, http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?c ommid=45020 (última visita el 18 de noviembre de 2016).

[135] Comisión Electrotécnica Internacional (CEI), http://www.iec.ch/ (última visita el 18 de noviembre de 2016).

[136] Comité Internacional de Normas de Tecnología de la Información, http://www.incits.org/ (última visita el 18 de noviembre de 2016).

[137] TRUSTe, Cumbre de Riesgos de Privacidad 2016, 8 de junio de 2016, http://www.truste.com/events/privacy-risk/

[138] Instituto de Ingenieros Electrónicos y Eléctricos (IEEE), P2413 - Standard for an Architectural Framework for the Internet of Things (IoT), https://standards.ieee.org/develop/project/2413.html (última visita el 18 de noviembre de 2016).

[139] Wireless IoT Forum, http://www.wireless-iot.org/ (visitado por última vez el 18 de noviembre de 2016).

[140] Open Connectivity Foundation, https://openconnectivity.org/ (visitado por última vez el 18 de noviembre de 2016).

[141] Object Management Group, http://www.omg.org/ (visitado por última vez el 18 de noviembre de 2016).

[142] Industrial Internet Consortium, http://www.iiconsortium.org/ (visitado por última vez el 18 de noviembre de 2016).

[143] oneM2M, http://www.onem2m.org/ (visitado por última vez el 18 de noviembre de 2016).

[144] Bill Lydon, "Internet de las cosas: Industrial automation industry exploring and implementing IoT", InTech Magazine, Mar-Apr 2014, *disponible en* https://www.isa.org/standards-and-publications/isa-publications/intech-magazine/2014/mar-apr/cover-story-internet-of-things/.

[145] OASIS, OASIS Committee Categories:IoT/M2M, https://www.oasis-open.org/committees/tc_cat.php?cat=iot (última visita el 18 de noviembre de 2016).

[146] HYPERCAT, http://www.hypercat.io/ (visitado por última vez el 18 de noviembre de 2016).

[147] AllSeen Alliance, https://allseenalliance.org/ (visitado por última vez el 18 de noviembre de 2016).

[148] Thread, http://threadgroup.org/ (visitado por última vez el 18 de noviembre de 2016).

10 Colaboradores y revisores de documentos

- Fred Baker, *CISCO*
- Steven Bauer, *MIT*
- Richard Bennett
- Don Bowman, *Sandvine*
- William Check, *NCTA*
- kc claffy, *UCSD/CAIDA*
- David Clark, *MIT*
- Shaun Cooley, *CISCO*
- Amogh Dhamdhere, *UCSD/CAIDA*
- Nick Feamster, *Universidad de Princeton*
- Francis Ferguson, *Nivel 3*
- Joseph Lorenzo Hall, *Centro para la Democracia y la Tecnología*
- Ken Ko, *ADTRAN*
- Jason Livingood, *Comcast*
- Patrick McManus, *Mozilla*
- Chris Morrow, *Google*
- Donald Smith, *CenturyLink*
- Barbara Stark, *AT&T*
- Darshak Thakore, *CableLabs*
- Matthew Tooley, *NCTA*
- Jason Weil, *Charter Communications*
- Greg White, *CableLabs*
- Todd Whitenack, *Cellcom*

David Winner, *Comunicación de la Carta*