EL INTERNET DE LAS COSAS Y SUS RIESGOS PARA LA PRIVACIDAD

González Larín Yeisson Germán
yeisson416@hotmail.com
Universidad Piloto de Colombia

***Resumen*—**El presente artículo tiene como finalidad exponer una tendencia que se está tomando el mundo de la tecnología, la cual se llama Internet de las cosas (o IoT por sus siglas en inglés "Internet of Things"), así como detallar los principales sectores en los cuales se está desarrollando este concepto. Se listan las principales tecnologías de comunicación existentes en el mundo, junto con las empresas que están incursionando en este nuevo ámbito. Adicionalmente se da una breve explicación de las principales vulnerabilidades y riesgos a los que las personas, sociedades y/o empresas se pueden ver expuestos al incursionar en el IoT, para finalmente terminar con unas sencillas recomendaciones del Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP por sus siglas en inglés, "Open Web Application Security Project") para mitigar los riesgos más significativos en el IoT.

Índice de Términos—Internet de las Cosas, OWASP, riesgos, seguridad informática, tecnología.

Abstract—This article aims at exposing a trend that is taking the world of technology, which is called Internet of Things (IoT), as well as to detail the main sectors in which this concept is being developed. It lists the main communication technologies existing in the world, along with the companies that are entering this new field. Additionally, a brief explanation of the main vulnerabilities and risks that individuals, the society and / or companies can be exposed to when entering the IoT is given, in order to finally finish with some simple recommendations of the Open Web Application Security Project (OWASP) to mitigate the most significant risks in IoT.

Keywords—Internet of Things, OWASP, risks, informatic security, technology.

I. INTRODUCCIÓN

El mundo ha cambiado considerablemente en los últimos años gracias a la llegada de la tecnología. En el pasado, actividades como el uso del Smartphone para conversar por medio de chats con otras personas o el uso de GPS para revisión del tráfico, eran cosas impensables, pero en la actualidad constituyen acciones cotidianas, las cuales avanzan y se complementan día a día.

Entre las tendencias más novedosas de la actualidad está el Internet de las cosas, el cual consiste principalmente en la búsqueda de la interconexión de objetos por medio del internet, ya sea con tecnologías inalámbricas como bluetooth, radiofrecuencia, Wi-Fi y, en algunos dispositivos inteligentes, los actuadores o sensores que están integrados [1].

Cada día es mayor la población que hace uso de estas tecnologías para suplir sus necesidades, por lo que ahora es común ver personas monitorear su ritmo cardiaco por medio de pulseras, bombillas que se apagan solas a ciertas horas o al no detectar ninguna presencia, personas que encienden su calefacción desde su Smartphone antes de llegar a casa, neveras que informan sí falta algún alimento y realizan el pedido a tiendas en línea, entre otras.

Es tal el crecimiento de la tecnología IoT, que en la actualidad se estima que existen cerca de 20.000 millones de dispositivos conectados a Internet que generan diariamente millones de Terabytes de información, de la cual lamentablemente cerca del 90% no es utilizada y, según proyecciones para el 2020, la cifra de dispositivos conectados podría superar los 50.000 millones [2], [3].

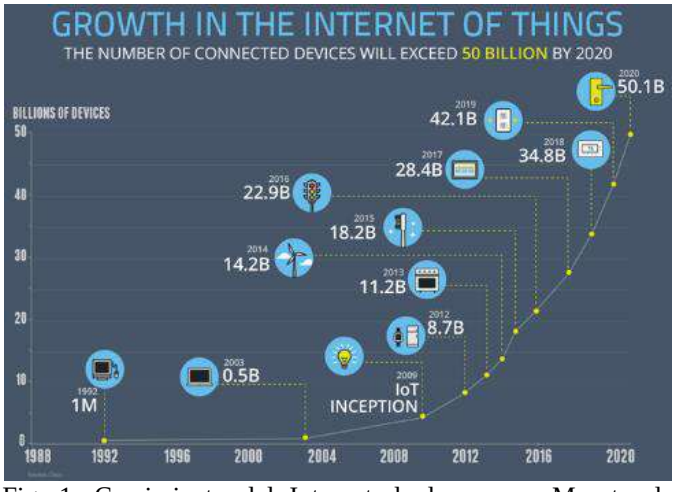

Fig. 1. Crecimiento del Internet de las cosas. Muestra la cantidad de dispositivos conectados a Internet por año [3]

Pero esta revolución tecnológica trajo consigo grandes desafíos en cuanto a la seguridad informática, como lo han señalado empresas especializadas en seguridad como Fortinet, Symantec, Eset y Cisco. Aunque todas estas nuevas herramientas sean funcionales y estén supliendo ciertas necesidades, no se puede dejar de lado la seguridad. La importancia de esta afirmación se vio reflejada el pasado viernes 21 de octubre del presente año, cuando por medio de tres oleadas de ataques de denegación de servicio distribuidos DDoS, que, utilizando una red de dispositivos IoT infectados con malware y funcionando como una botnet, provocaron la caída o lentitud en plataformas como Twitter, Spotify, Reddit, Paypal, Pinterest, New York Times, entre otras [4].

II. INTERNET DE LAS COSAS (IoT)

El Internet de las cosas es un concepto implementado por Kevin Ashton en el Auto-ID Center del MIT (Massachusetts Institute of Technologies o el Instituto de Tecnología de Massachusetts) en 1999, como un sistema basado en la interconexión de cualquier objeto de la cotidianidad a Internet, con el fin de generar soluciones y lograr la automatización de las tareas del ser humano en diferentes campos, para que sean manejadas eficientemente por las personas o por otros dispositivos electrónicos. Esto permite la captura e intercambio automático de información sobre uso y rendimiento, y, por lo tanto, un mayor control sobre las cosas. Este valor agregado de la tecnología en las tareas cotidianas de las personas ya se puede evidenciar en el propio hogar, en algunos electrodomésticos y pequeños aparatos llamados gadgets, que toman la información de su entorno como temperatura, humedad, actividad y otros, para luego enviarlos a un centro de procesamiento que permita determinar la acción a seguir en tiempo real. Un ejemplo de esto se ve en los sistemas de calefacción independientes, alarmas de seguridad que se activan ante movimientos sospechosos cerca de la vivienda y vehículos autónomos como los fabricados por la compañía Tesla Motors.

Esto en el sector de la industria puede significar mejoras o automatización de procesos, ahorros o disminución de tiempos muertos, mayores eficiencias operativas, mejoras en la seguridad, cámaras de vigilancia en las calles y/o lugares públicos, ventajas competitivas frente a la competencia, entre otros [5], [6], [7].

En campos como la agricultura, en el cual por medio del uso de sensores, dispositivos y aplicaciones informáticas se puede obtener la información detallada de los cultivos, el estado del suelo y la condiciones climáticas que pueden impactar la calidad de los productos, esta tecnología trae consigo mejoras significativas en el proceso y cuidados de los cultivos al automatizar el riego, protección de las heladas, y son un gran insumo para la toma de decisiones en pro de la reducción de los costos [2]. En otros sectores en los cuales se están desarrollando proyectos con este nuevo concepto es en la construcción, debido a que muchos arquitectos y diseñadores están implementándolo para generar valor agregado a sus productos, como casas inteligentes para clientes exclusivos. Éste es el caso de la empresa Bang & Olufsen, quienes, por medio del ideal de hacer la vida más agradable y sencilla al mismo tiempo, implementaron el concepto de IoT para que sus clientes desde un sencillo control remoto puedan dar órdenes a su casa, tales como abrir la puerta principal, encender la calefacción, la música, abrir las cortinas, etc.; ellos lo llaman “Lujo sencillo”. [8], [9].

Adicionalmente a lo anterior, esta empresa no solo enfoca sus esfuerzos en los dueños de la vivienda, sino que también identificaron como un interesado clave al personal encargado de instalar y configurar los sistemas de integración de viviendas. Para esto emplean tecnología de fácil acceso y uso, la cual se puede adaptar e integrar fácilmente como un sistema con la demás tecnología que tenga el usuario.

Es tal la fuerza que ha tomado el IoT, que ya se habla de ciudades inteligentes o Smart Cities, donde se mantiene el concepto de recolección de información, pero se lleva a gran escala, para lo cual, utilizando una gran red de sensores, se puede alterar el comportamiento en tiempo real de alarmas, semáforos. alcantarillas, alumbrado y en

teoría cualquier objeto conectado de la ciudad. Una Smart City es la ciudad New Songdo¸ ubicada en una isla frente a la ciudad de Inchon, a 60 kilómetros al oeste de Seúl (Corea del Sur). Esta ciudad fue creada con el fin de integrar e interconectar todos los sistemas por medio del internet, en la cual los computadores, celulares inteligentes y demás dispositivos de última tecnología de las personas que habitan el lugar están integrados a las viviendas, las calles y las oficinas, por lo tanto, las personas pueden acceder fácilmente a información sin necesidad de estar físicamente en el lugar, como por ejemplo sensores que controlan la temperatura, sistemas que succionan la basura directamente desde el hogar y la reciclen de inmediato, el uso de energía, el tráfico, entre otras.

Sin embargo, aunque la idea de vivir en una "ciudad inteligente" llama la atención de muchas personas en el mundo, menos del 20% de las oficinas y establecimientos comerciales están siendo utilizados, debido a los altos costos que conlleva el vivir en esta ciudad, lo que ha obstaculizado que muchas personas se muden a vivir allí [10].

Otros de los sectores en los cuales este concepto está cogiendo fuerza es en el de la salud, debido a que esta tendencia posibilita a que personas de todo el mundo puedan tener acceso a especialistas sin tener que estar ubicados físicamente en el mismo lugar, lo que conllevaría a un servicio médico con mayor cobertura a nivel mundial.

III. TECNOLOGÍAS DE COMUNICACIÓN

Los dispositivos del Internet de las cosas actualmente continúan utilizando muchos de los protocolos de comunicación tradicionales. Estos protocolos, aunque hoy en día garantizan la conectividad de los dispositivos, es necesario que continúen evolucionando, ya que los cambios y la adaptación a la tecnología son clave en este mercado tan cambiante. Dependiendo de la aplicación, rango de cobertura, seguridad, tamaño de los datos, exigencia de energía y duración de la batería, éstas son algunas de las principales tecnologías de comunicación utilizadas por el IoT:

A. Wi-Fi (Wireless Fidelity)

Son una serie de especificaciones para redes locales inalámbricas basadas en el estándar IEEE 802.11. Este tipo de redes realizan la transferencia de datos a través de radiofrecuencia y permiten conectar dispositivos compatibles que estén cercanos geográficamente [11].

B. Bluetooth

La tecnología inalámbrica Bluetooth es un estándar universal abierto para enlaces de radio de baja potencia, hace parte de las redes Wireless Personal Area Network (WPAN) que normalmente abarcan distancias máximo de 10 metros, con un bajo consumo de energía, lo que la hace muy popular para la comunicación de dispositivos peer-to-peer [12]. Desde el 2010, este protocolo evolucionó a Bluetooth 4.0, mejorando la velocidad y el bajo consumo, precisamente pensando en su implementación en sistemas donde el uso de baterías podía ser un problema. A mediados del 2016, la compañía fabricante (Bluetooth Special Interest Group, "SIG") anunció la liberación de su versión 5 para inicios del 2017 y afirman que ésta tendrá el doble de velocidad, mejor rango de cobertura y 800% mayor capacidad que la versión 4 [13].

C. Telefonía Móvil (1G, 2G, 3G y 4G)

Comunicación inalámbrica a través de ondas electromagnéticas. Esta tecnología está formada por una red de comunicaciones compuesta por antenas a lo largo de la superficie terrestre y de las células (teléfonos móviles también llamados celulares), que permiten la comunicación desde casi cualquier lugar [14].

D. RFID

Una tecnología que por medio de etiquetas de identificación Rifad se pueden seleccionar a los dispositivos remotamente por medio de señales de radiofrecuencia y así almacenar la información, para luego ser procesada por los sistemas de gestión [15].

E. ZigBee

Es un estándar desarrollado por la Alianza ZigBee que define una serie de protocolos para la implementación de redes inalámbricas de corta

distancia y baja velocidad de datos. La comunicación ZigBee es de muy bajo consumo, lo que la hace muy atractiva para dispositivos que dependen de una batería para su funcionamiento [16].

F. Z-Wave

Tecnología inalámbrica ampliamente utilizada en productos domésticos (domótica). Tiene una cobertura de 30.5 metros y cada red puede incluir hasta 232 nodos.

G. 6LowPAN (IPv6 Over Low Power Wireless Personal Area Networks)

Son una serie de recomendaciones sobre el uso de IPv6 en redes, basadas en el estándar IEEE 802.15.4. Está enfocado a dispositivos simples y al utilizar IPv6 es el ideal para redes con un gran número de sensores [17], [18].

Según la fuente [19], como lo señaló en su momento Jan Brockmann, Director de operaciones de Electrolux, sí se desea crear una plataforma universal, ésta solo funcionará si todos se unen. Y es que, con la amplia gama de protocolos y formas de comunicación, es necesario que todos los dispositivos hablen el mismo idioma. Ante este problema han surgido varias alianzas que intentan imponer un estándar común, las dos alianzas que sobresalen son:

- AllSeen Alliance: La asociación de empresas como Microsoft, Cisco, Qualcomm, Panasonic, LG, Harman, HTC, Sharp, Bosch, Haier y Sony, junto con el apoyo de Linux Foundation, han creado el estándar basado en software Open Source llamado AllJoyn, que garantiza una interoperabilidad entre los dispositivos de los fabricantes con distintos sistemas operativos. Lo definen como un estándar flexible, dinámico, avanzado y compatible, que quiere enfocarse en resolver problemas de alto nivel. El sistema en un principio fue creado por Qualcomm, pero fue adoptado y mejorado con la contribución de todos los aliados.
- Open Interconnect Consortium: La conforman empresas como Intel, Samsung, Dell, Broadcom Corporation, Atmel y Wind River. Esta alianza también es de código abierto y se enfoca en temas que no están abarcados en AllSeen, entre ellos la seguridad y acceso remoto. Adicionalmente ofrece normas de interconectividad para desarrolladores, fabricantes y usuarios finales.

IV. EMPRESAS QUE LE APUESTAN AL IoT

Es difícil imaginar tareas que desarrolle el ser humano que en algún momento de la historia no puedan llegar a ser desarrolladas por medio de la unión de la ciencia y la tecnología. Hoy en día, por medio de diversos protocolos y aplicaciones, se encuentran más dispositivos conectados a Internet que seres humanos sobre la tierra, y es que gracias a la gran masificación del IoT, cada vez son más las empresas que están adoptando estrategias de mercado de estas tecnologías para su negocio. Éstas son algunas de las empresas líderes en esta tecnología, con sus proyectos más ambiciosos:

- Intel: El mayor fabricante de circuitos integrados del mundo ha creado una placa computacional llamada Intel Joule, enfocada a utilizar funciones de visión computacional, robótica, drones, microservidores, realidad virtual, entre otros, dirigida a desarrolladores y empresas del ámbito del IoT. Por ejemplo, en una asociación con la empresa francesa PivotHead con el uso de Joule crearon unas gafas de realidad aumentada para mejorar la seguridad en entornos industriales [2].
- Amazon: Con la idea de que la cloud juegue un papel importante para el IoT, creó el servicio AWS IoT que ayuda a desarrollar aplicaciones para conectar dispositivos a través de la cloud. Al día de hoy, ya se han dado a conocer dispositivos de domótica, vehículos y sistemas de salud desarrollados a través de este servicio, junto con la unión de otras de sus herramientas como S3, Kinesis y DinamoDB [20].
- Google: La empresa que cuenta con más productos enfocados al IoT, entre ellos se destaca un sistema operativo específico

para estos dispositivos, basado en Android. También ha creado toda una división de desarrollo de esta tecnología llamada X. Entre sus proyectos más destacados se encuentran las Google Glass (gafas de realidad aumentada), un vehículo autónomo y una herramienta para ayudar a los diabéticos a verificar constantemente sus niveles de glucosa sin utilizar ningún método intrusivo [2], [21].

- IBM: Con una inversión de 200 millones de dólares para el campo de la computación cognitiva, con su proyecto Watson, quieren crear sistemas que comprendan el lenguaje natural de las personas, puedan recopilar y asimilar grandes cantidades de datos, responder a preguntas complejas y aprender de la experiencia [2].
- Microsoft: El gigante tecnológico que gracias a su plataforma de servicios en la nube Azure ha creado varias soluciones en el ámbito del IoT, entre ellas Azure IoT Suite, que permite a las empresas monitorear y manejar sus soluciones IoT, la Azure IoT Hub para gestionar dispositivos por medio de herramientas de software y nuevas herramientas de enrutamiento de una forma más potente y sencilla; Windows 10 IoT Core, un sistema operativo de bajo costo para dispositivos que hacen parte del Internet de las Cosas [22].
- Samsung: Con la promesa que para el año 2020 todos sus dispositivos hagan parte del IoT y así mejorar la calidad de vida de las personas en todo el mundo, en junio del presente año destinó una inversión de 1.200 millones de dólares en el desarrollo de esta tecnología junto con I + D [23].

La mayoría de las empresas están empezando a usar esta tecnología para la fabricación de sus productos a la vanguardia, sin embargo, algunas compañías se están dedicando a modificar los aparatos electrónicos ya existentes, adaptándolos con señales Wifi de internet, con el fin de que las personas no tengan que cambiar todos sus aparatos electrónicos, sino solamente adaptarles unos dispositivos para que puedan entrar en esta tendencia.

V. RIESGOS DEL INTERNET DE LAS COSAS

Con esta masificación de dispositivos conectándose a Internet y cada vez con más tecnologías para su comunicación, el controlar las vulnerabilidades de estos dispositivos es una tarea muy dispendiosa y, que muchas veces no se tiene en cuenta. Hasta hace unos días, para gran parte de la población era casi imposible que se produjera un ataque de denegación de servicio distribuido DDoS, como el que se presentó el viernes 21 de octubre del presente año, en el cual, por medio de millones de dispositivos IoT infectados con malware, se logró provocar la caída de varias de las plataformas más sofisticadas del mundo e intermitencia en el servicio de internet de más del 30% del mundo [1].

Aunque en los eventos IoT Solutions World Congress de los últimos años se ha hecho especial énfasis en los temas de la seguridad, quedó en evidencia que muchos de los grandes fabricantes de estas tecnologías aún no están tomando el tema con el cuidado que se merece o simplemente se les ha salido de las manos. Para agravar un poco más el panorama, se suma el aumento significativo de ciberataques y técnicas de hacking cada vez más sofisticadas.

Es innegable que el papel de la seguridad informática nunca había tenido tanta importancia, porque con el paso del tiempo cada vez hay más en juego; un solo ataque con éxito a la red de dispositivos que conforma el Internet de las Cosas podría llegar a afectar todos los objetos físicos que nos rodean y, en el peor de los casos, la integridad física de las personas.

En los últimos años, importantes empresas y asociaciones se han tomado el trabajo de evaluar qué tan seguras son las soluciones IoT, y los resultados obtenidos siempre llevan a la conclusión de que esta tendencia es muy riesgosa tanto para empresas como para las personas.

La Asociación de Auditoria y Control de Sistemas de Información (ISACA por sus siglas en inglés, “Information Systems Audit and Control Association”) revela que los grandes retos a los que se enfrenta el IoT son la protección de la privacidad

de los datos, la gestión de la identidad de acceso, los requisitos de cumplimiento, la propiedad de los datos fuera de IT y mayores amenazas de seguridad [24].

Según la fuente [25], un estudio realizado por HP (Hewlett-Packard) a 10 dispositivos IoT de seguridad para el hogar y a sus componentes de aplicación en la nube y móviles, reveló que la totalidad de estos dispositivos contenían vulnerabilidades significativas como problemas de seguridad, cifrado y autenticación. Los dispositivos seleccionados para las pruebas fueron de varios fabricantes líderes que operan con distintos sistemas operativos, lo que le da mayor valor al estudio.

Resumiendo, algunas de las vulnerabilidades más críticas detectadas en el estudio fueron:

- Autorización insuficiente: Los sistemas con aplicaciones web conectadas a la nube no exigían contraseñas seguras. Aunque era obligatoria, bastaba con ingresar una contraseña alfanumérica de seis caracteres de longitud, debido a que no existían políticas que exigieran cierto grado de complejidad.
- Interfaces inseguras: Por medio de técnicas de recolección de cuentas se logró tener acceso. Estas técnicas consisten en que al no existir el bloqueo de cuentas y política de contraseñas seguras se pueden realizar ataques de fuerza bruta.
- Problemas de privacidad: Todos los dispositivos recolectan información constantemente, y en algunos casos, esta información es sensible; como por ejemplo los números de tarjetas de crédito. Cabe añadir que algunos de los dispositivos cuentan con cámaras de video integradas que permiten la visualización del hogar de forma remota, lo cual también podría resultar en un problema de privacidad.
- Falta de cifrado: Aunque los dispositivos utilizados en las pruebas ya contaban con cifrados de transporte, aun había muchas conexiones a la nube que estaban vulnerables.

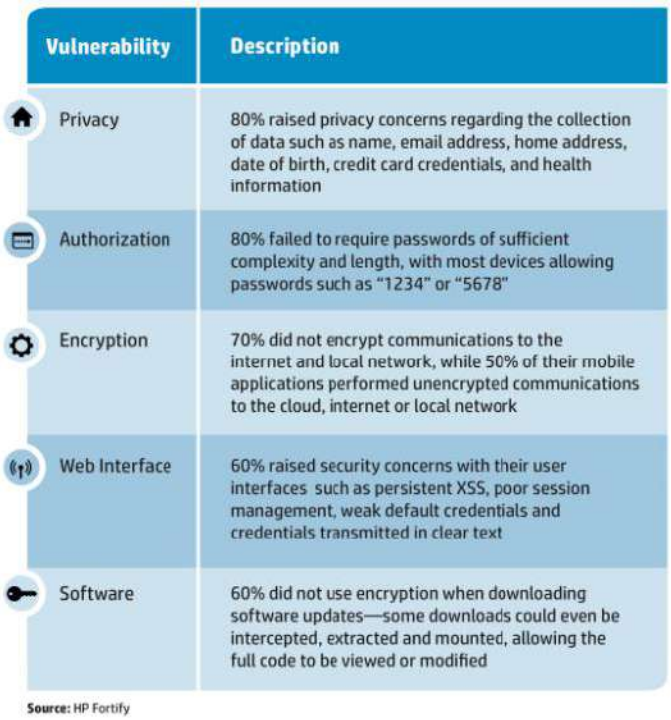

Fig. 2. Principales vulnerabilidades del IoT. La figura muestra las principales vulnerabilidades que afectan a los dispositivos IoT, según el estudio realizado por HP en el año 2014 [26]

Sin restarle importancia a cada una de las vulnerabilidades del IoT, es evidente que las que más afectan a las personas y empresas son las relacionadas con la privacidad de la información que están recolectando, y es que, con todas las tecnologías emergentes, la información ha pasado a ser un activo sumamente importante, por lo que gran parte de la población ha tomado acciones para protegerla. En Colombia se creó la Ley 1581 de 2012 con los mecanismos para garantizar la protección, almacenamiento y el buen uso de datos personales. Esta norma concede el derecho a todas las personas de conocer y solicitar la eliminación de sus datos personales registrados en cualquier base de datos susceptibles de tratamiento en entidades públicas y privadas [27]. Igual que esta ley para Colombia, en el resto del mundo existen otras legislaciones con el mismo fin como la Ley Federal Bundesdatenschutzgesetz para Alemania o la Privacy Act de 1974 en Estados Unidos (en algunos países latinoamericanos como Argentina, Chile, Panamá, Paraguay, Brasil y Uruguay se utiliza un modelo similar al europeo), pero todas estas leyes solo protegen los datos considerados sensibles. Según la ley 1581 de 2012 los datos sensibles son

todos aquellos que por el uso indebido puedan generar algún tipo de discriminación al titular [27].

Y aunque es importante que existan este tipo de normativas, se quedan cortas frente a la realidad por la que atraviesa el mundo moderno, la llamada "era digital" que gira en torno a la información.

El valor que se le da a la información es diferente para cada organización y/o individuo, y cada uno la califica frente a los beneficios o daños en los que podría verse involucrado, pero siempre tiene alguna cuantía. Por dar un ejemplo, en algo tan simple como los datos de geolocalización recolectados por algunos de los llamados gadgets para vestir o los Smartphone, que se están enviando constantemente a un servidor en algún lugar del mundo, ya sea para indicar la ruta en la que el sujeto hizo alguna actividad deportiva o sugerir la mejor ruta para llegar a un destino; sí esta información cayera en manos de un atacante, éste podría detectar las costumbres o rutinas de la víctima y así encontrar el momento justo para hacer daño, ya sea directamente a la persona o alguno de sus bienes cuando no esté presente, todo esto gracias a la localización exacta proporcionada por los dispositivos.

Si bien por medio del ejemplo se refleja la importancia de cualquier dato, por simple u obvio que sea, éstos no están incluidos en todas las legislaciones actuales como datos sensibles, y aunque los fabricantes o prestadores de los servicios al perder la información tienen un fuerte impacto en sus ganancias, credibilidad, entre otras, no le prestan atención a las consecuencias que podrían tener los verdaderos dueños de la información. Referente a este tema, aún existe un problema importante con los prestadores de servicios que establecen que la información recolectada por medio de sus soluciones es de su propiedad siempre y cuando no sean datos natos del usuario final como su nombre, correo, cuentas bancarias y otros del mismo estilo.

Pero, así como se han detectado vulnerabilidades en los dispositivos IoT, organizaciones especializadas en seguridad ajenas a los fabricantes están trabajando para reducir los riesgos. Una de estas organizaciones es el Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP por sus siglas en inglés, "Open Web Application Security Project"), reconocido por la documentación relacionada a la seguridad de aplicaciones web y las listas Top 10 de vulnerabilidades. En el año 2014 hizo pública su lista OWASP Internet of Things Top Ten Project, en la cual dan a conocer las debilidades más críticas del IoT, sus agentes de amenaza, vectores de ataque, impactos técnicos, impactos del negocio y algunas recomendaciones para mitigar el riesgo [28].

Según el portal web oficial de OWASP [29], [30], éstas son las vulnerabilidades más críticas de la IoT:

A. Interfaz Web Insegura

Esta vulnerabilidad es la más común en el mundo del IoT y se presenta cuando los sistemas permiten la enumeración de cuentas, falta de bloqueo de las cuentas o credenciales débiles. Su impacto es clasificado como grave porque puede provocar la pérdida o corrupción de datos, denegación de acceso y pérdida completa del control del dispositivo. Las recomendaciones para proteger la interfaz web son cambiar la contraseña predeterminada durante la configuración inicial, exigir contraseñas robustas, verificar que las contraseñas no sean expuestas en el tráfico de las redes internas o externas y configurar el bloqueo de las cuentas después de cierto número de intentos de acceso erróneos.

B. Autenticación / Autorización insuficiente

La debilidad se presenta cuando los mecanismos de autenticación o autorización no son lo suficientemente fuertes para evitar la intrusión de usuarios no autorizados a los sistemas, lo que podría comprometer totalmente el dispositivo atacado. Para mitigar el riesgo es necesario establecer contraseñas robustas, implementar la autenticación de dos factores y exigir autenticación de la aplicación, del dispositivo y el servidor.

C. Servicios de red inseguros

Los servicios de red podrían ser vulnerables a ataques de desbordamiento de búfer o denegación del servicio, dejando al usuario sin acceso a los dispositivos, alterando la integridad de los datos o facilitando ataques a otros dispositivos. Para asegurar los servicios de red es necesario verificar que solo los puertos necesarios están abiertos, garantizar que no son vulnerables a los ataques de denegación de servicio y bloquear todas las solicitudes de servicios anormales.

D. Falta de cifrado de transporte

Esta vulnerabilidad permite que los datos sean legibles a través de las redes, generalmente en las locales, porque se asume que éstas no son visibles por los atacantes; pero en el caso de las redes inalámbricas, por una mala configuración, la información quedaría accesible para cualquier persona conectada a esa red. Para garantizar que esta vulnerabilidad no sea explotada, se pueden implementar protocolos de cifrado de datos como SSL, y mientras se mueven por las redes el cifrado TLS, asegurando la integridad de los datos recibidos.

E. Preocupaciones de privacidad

Las preocupaciones de privacidad se consideran una vulnerabilidad por la forma desproporcionada en la que se recolecta información innecesaria o no se protegen de la mejor forma los datos. Su impacto está categorizado como grave al involucrar datos personales de los usuarios y, en sí, toda su información. Las recomendaciones para reducir el riesgo son: garantizar que los dispositivos solo recolectan los datos básicos para su funcionamiento, en lo posible evitando que sean datos sensibles y cifrar la información.

F. Interfaz cloud insegura

Cuando la interfaz cloud es insegura, ésta podría ser atacada por cualquier persona con acceso a Internet, ya sea por credenciales de acceso fáciles de adivinar o por la enumeración de cuentas; y de ser explotada la vulnerabilidad, se podrían comprometer los datos de los usuarios y el control total sobre los dispositivos. Para minimizar el riesgo de explotación se deben cambiar las contraseñas predefinidas por contraseñas robustas, definir el bloqueo de cuentas después de cierto número de intentos fallidos de inicio de sesión, proteger los campos de entrada para evitar inyección de SQL, implementar una doble autenticación y bloquear todas las solicitudes de intentos anormales.

G. Interfaz móvil insegura

Esta debilidad causada por falta de estrictas políticas de autenticación en las interfaces móviles podría ocasionar alteración en los datos de los usuarios y pérdida parcial o total de los sistemas IoT. Para prevenir su explotación es necesario implementar políticas para la creación de contraseñas robustas, el bloqueo de las cuentas móviles por el número erróneo de autenticación, implementar la tecnología de ofuscación de aplicaciones web, proteger la memoria y evitar la ejecución de la aplicación móvil en ambientes para los que no fue concebida.

H. Configuración de seguridad insuficiente

Está presente cuando los usuarios tienen pocos o ningún privilegio para modificar sus controles de seguridad; esto es evidente cuando no se pueden configurar los permisos de los usuarios o forzar el uso de contraseñas seguras. La configuración de seguridad insuficiente podría llevar a comprometer los dispositivos intencional o accidentalmente y, como consecuencia, la pérdida de datos. Como sugerencias OWASP se recomienda permitir la separación de usuarios normales de los administrativos, políticas de contraseñas seguras, así como guardar el registro y notificar de los eventos de seguridad.

I. Software / Firmware inseguro

Este problema común en todo tipo de dispositivos se presenta cuando los archivos de actualización y la red en la que se transportan no están protegidos, por lo que se puedan alterar antes de llegar a su destino y, como resultado, instalar en el dispositivo IoT software malicioso, perder el control del dispositivo y realizar ataques contra otros equipos. Para prevenir estos incidentes, es necesario asegurarse que el archivo esté encriptado, que está firmado por el fabricante y verificar que la red por la que se transmite el archivo tiene una conexión cifrada.

J. Mala seguridad física

Se presenta cuando un atacante puede acceder físicamente a un dispositivo, ya sea directamente o por medio de alguno de sus puertos externos, y modificar su configuración o robar información. De acuerdo a OWASP, es importante que la información en reposo esté cifrada, solamente estén disponibles los puertos externos necesarios para el funcionamiento y se garantice que no se tenga acceso al dispositivo fácilmente.

Por su parte el Instituto de Ingeniería Eléctrica y Electrónica (IEEE por sus siglas en inglés, "Institute of Electrical and Electronics Engineers") creó un grupo para trabajar en la estandarización del IoT, haciendo énfasis en aspectos de seguridad como el descubrimiento del dispositivo, la autenticación, alertas, rastreo de personas y la gestión de la privacidad. La Organización Internacional de Normalización (ISO) en el 2014 publicó un informe preliminar de estándares y, aunque no tenía ningún enfoque específico, trabajó sobre algunos aspectos de seguridad para tecnologías IoT como la gestión de los datos, privacidad / confidencialidad, infraestructura y comunicaciones [31], [32].

La idea no es que se implementen todos los controles y recomendaciones expuestos en las normas, sino que, a raíz de un excelente análisis de vulnerabilidades, se determinen cuáles son las que se van a tratar, pensando en conjunto con las afectaciones que tendrían tanto las empresas fabricantes, como los desarrolladores independientes, comercializadoras y usuarios finales.

VI. CONCLUSIONES

Está claro que la tecnología siempre está evolucionando, y el factor predominante hoy en día es la conectividad de los objetos cotidianos. Muchas formas de comunicación están emergiendo y otras se están perfeccionando, a esto se suma el interés de grandes compañías que, al ver la proyección de inversión del IoT, están cambiando sus estrategias y alineando esta tendencia para crear nuevas líneas de negocios o mejorar las ya existentes.

Contar con los objetos de uso cotidiano conectados a Internet, implica serios problemas para la privacidad de la información, a esto se suma la indiferencia hacia la seguridad de muchos fabricantes y, aunque algunos trabajan para asegurar sus dispositivos, no lo hacen al ritmo al que avanza la tecnología. A diario aparecen nuevas técnicas de hacking más sofisticadas y cada vez es mayor el número de ciberataques exitosos al IoT. Para ayudar a mitigar un poco este problema, organizaciones de regulación y de seguridad se han tomado el trabajo de crear normas de estandarización del IoT, abarcando aspectos de seguridad. Por su parte OWASP creó una lista de las vulnerabilidades más críticas junto a sus respectivas recomendaciones de mitigación.

Pero sin lugar a dudas los beneficios que trae el IoT para la era moderna son incalculables. Como se mencionó anteriormente, grandes fabricantes crearon alianzas para estandarizar la comunicación entre dispositivos y junto con el trabajo de los organismos de seguridad y estandarización, ya se están dando avances significativos en la prevención de ataques en el internet de las cosas.

Finalmente, entre los controles que se deben implementar para reducir los riesgos en la privacidad, es importante la creación de políticas de seguridad, no solo de los grandes fabricantes, sino de todos los participantes que de una u otra manera trabajan en pro de esta tecnología. Asimismo, se debe concientizar a los usuarios sobre los riesgos asociados al Internet de las Cosas, así como el almacenamiento y tratamiento que tendrán sus datos.

REFERENCIAS

[1] Mora González, S. (septiembre de 2015). Entendiendo el Internet de las cosas. Investiga TEC. Academic Journal [Online]. Disponible en: http://revistas.tec.ac.cr/index.php/investiga_tec/article/view/2381/2169

[2] Futurizable. (4 de noviembre de 2016). Tres letras que están cambiando el mundo. [Online]. Disponible en: http://futurizable.com/iot

[3] SmartTravelNews. (2016). Infografía: El imparable crecimiento del internet de las cosas. [Online]. Disponible en: http://www.smarttravel.news/2016/05/14/infografia-el-imparable-crecimiento-del-internet-de-las-cosas

[4] O'Brlen, S. A. (21 de octubre de 2016). *Un ciberataque tumba sitios populares de internet como Reddit, Twitter y Netflix. [Online]*. Disponible en: http://cnnespanol.cnn.com/2016/10/21/esta-seria-la-razon-por-la-que-twitter-reddit-y-netflix-estan-caidos/#0

[5] TEC. (8 de febrero de 2015). El Internet de las Cosas [Archivo de video]. [Online]. Disponible en: https://www.youtube.com/watch?v=G1NH3k8EFHA

[6] TEC. (22 de febrero de 2015). El Internet de las Cosas – Parte 2 [Archivo de video]. [Online]. Disponible en: https://www.youtube.com/watch?v=TbRTnfhxLds&t=182s

[7] Mirales, D. (28 de noviembre de 2014). ¿Qué es el Internet de las Cosas? [Archivo de video]. [Online]. Disponible en: https://www.youtube.com/watch?v=s641-eJAB1w

[8] Bang Olufsen. (2016). *THE LIVING HOME*. [Online]. Disponible en: http://www.bang-olufsen.com/fr/solutions/beolink-smarthome

[9] Gassée, J.-L. (2014). Internet of Things: The "Basket of Remotes" Problem. *Monday NOTE*. [Online]. Disponible en: https://mondaynote.com/internet-of-things-the-basket-of-remotes-problem-f80922a91a0f#.t0zylmhas

[10] LA NACION. (5 de Septiembre de 2013). *Songdo, la ciudad más inteligente del mundo*. [Online]. Disponible en: http://www.lanacion.com.ar/1616937-songdo-la-ciudad-mas-inteligente-del-mundo

[11] INFORMATICAHOY. (s.f.). *¿Qué es Wifi?*. [Online]. Disponible en: http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-Wifi.php

[12] Corredor Camargo, O. F., Pedraza Martinez, L. F., Hernández, C. A. F. (2009). TECNOLOGÍA BLUETOOTH: ALTERNATIVA PARA REDES. *Visión Electrónica*. [Online]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/4168662.**pdf**

[13] Bluetooth. (2015). Bluetooth® 5 Quadruples Range, Doubles Speed, Increases Data Broadcasting Capacity by 800%. [Online]. Disponible en: https://www.bluetooth.com/news/pressreleases/2016/06/16/-bluetooth5-quadruples-rangedoubles-speedincreases-data-broadcasting-capacity-by-800

[14] Área Tecnológica. (s.f.). *Telefonía Móvil*. [Online]. Disponible en: http://www.areatecnologia.com/telefonia-movil.htm

[15] Niño, D. L. (2015). *PANORAMA DE APLICACIÓN DE INTERNET*. Bogotá: Universidad Santo Tomás, Facultad de Ingeniería de Telecomunicaciones. [Online]. Disponible en: http://porticus.usantotomas.edu.co/bitstream/11634/672/1/Panorama%20de%20aplicacion%20de%20internet%20de%20las%20cosas.pdf

[16] Dignani, J. P. (2011). *ANÁLISIS DEL PROTOCOLO ZIGBEE* . La Plata: Universidad Nacional de La Plata. [Online]. Disponible en: http://postgrado.info.unlp.edu.ar/Carreras/Especializaciones/Redes_y_Seguridad/Trabajos_Finales/Dignanni_Jorge_Pablo.pdf

[17] Ravera, G. (2010). *ZigBee o 6lowPAN*. Networking and Internet Technologies. [Online]. Disponible en: http://blogs.salleurl.edu/networking-and-internet-technologies/zigbee-o-6lowpan

[18] García, D. G. (2015). *Estudio de 6loWPAN para su aplicación a Internet de las Cosas.* La Laguna: Escuela Superior de Ingeniería y Tecnología. [Online]. Disponible en: http://riull.ull.es/xmlui/bitstream/handle/915/945/Estudio%20de%206loWPAN%20para%20su%20aplicacion%20a%20Internet%20de%20las%20Cosas.pdf?sequence=1&isAllowed=y

[19] *Maria, G. (2014). La marea del Internet of Things.* smartcio.es. [Online]. Disponible en: *http://smartcio.es/internet-of-things/*

[20] Amazon, Inc. (2016). ¿Cómo funciona la plataforma AWS IoT?. [Online]. Disponible en: *https://aws.amazon.com/es/iot/how-it-works/*

[21] Google. (2016). INTERNET OF THINGS (IOT) SOLUTIONS. [Online] Disponible en: *https://cloud.google.com/solutions/iot/*

[22] Microsoft. (2016). *Cloud Platform*. Obtenido de Internet Of Things Azure. [Online]. Disponible en: https://www.microsoft.com/en-us/cloud-platform/internet-of-things-azure-iot-suite

[23] News Samsung. (21 de Junio de 2016). *Samsung Shows Dedication to IoT with $1.2 Billion Investment and R&D*. [Online]. Disponible en: https://news.samsung.com/global/samsung-electronics-announces-vision-for-a-human-centered-internet-of-things-planning-1-2-billion-for-u-s-research-and-development-of-iot

[24] ISACA. (2015). Internet of Things: Risk and Value Considerations . ISACA. Academic Journal. [Online]. Disponible en: http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/internet-of-things-risk-and-value-considerations.aspx

[25] Geek. (5 de Junio de 2015). Estudio de HP revela vulnerabilidades en los sistemas de seguridad para el hogar IoT. [Online]. Disponible en: http://geek.com.mx/2015/06/estudio-de-hp-revela-vulnerabilidades-en-los-sistemas-de-seguridad-para-el-hogar-iot/

[26] Miessler, D. (29 de Julio de 2014). *HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack*. [Online]. Disponible en: https://community.hpe.com/t5/Protect-Your-Assets/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.WEPH4uZ97IU

[27] EL CONGRESO DE COLOMBIA. (2012). *LEY ESTATUTARIA 1581 DE 2012. [Online]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981*

[28] OWASP. (2014). OWASP Internet of Things Project. [Online]. Disponible en: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

[29] OWASP. (2014). Top 10 IoT Vulnerabilities (2014). [Online]. Disponible en: https://www.owasp.org/index.php/Top_10_IoT_Vulnerabilities_(2014)

[30] OWASP. (2014). Internet of Things Top Ten. [Online]. Disponible en: https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf

[31] Ballarin, Usieto, P. (2016). *Gestionar la seguridad del Internet de las cosas.* Govertis Advisory Services. [Online]. Disponible en: http://www.govertis.com/gestionar-la-st-de-las-cosas

[32] ISO/IEC JTC 1 Information technology. (2014). *Internet of Things (IoT). Preliminary Report 2014*. ISO. [Online]. Disponible en: http://www.iso.org/iso/internet_of_things_report-jtc1.pdf

González Larin, Yeisson German. Ingeniero de Sistemas de la Escuela Colombiana de Carreras Industriales. Se desempeña como Ingeniero de desarrollo y Consultor de proyectos de software.